Constrained BRSKI (cBRSKI)

draft-ietf-anima-constrained-voucher-28

Image: real vs counterfeit constrained brewski

IETF 123, Madrid, July 2025

Esko Dijk – IoTconsultancy.nl
(presenting)

Co-authors:
M. Richardson
P. van der Stok
P. Kampanakis

GitHub

Recap & Goal – Constrained BRSKI

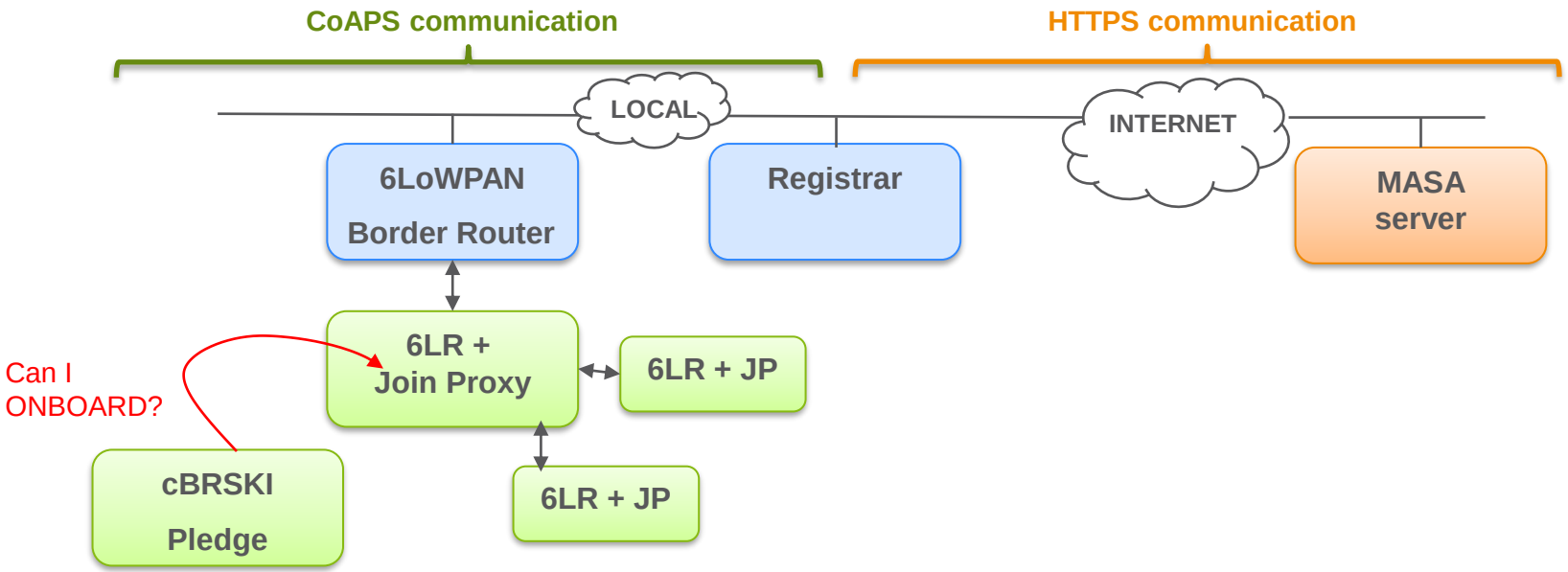
- **BRSKI onboarding, for constrained (IoT) devices & networks**

- Suitable for 6LoWPAN networks and other constrained IP networks.
  Minimize **onboarding time** & **code overhead**:
  - minimize data size
  - minimize round-trips
  - minimize different-formats parsing
  - minimize optional functions

- Modifications
  - CoAP + DTLS ⇨ instead of HTTP + TLS
  - COSE-signed CBOR ⇨ instead of CMS-signed JSON
  - EST-coaps (RFC 9148) ⇨ instead of ‘classic’ EST (RFC 7030)

Recap & Goal – Constrained BRSKI

› **BRSKI onboarding, for constrained (IoT) devices & networks**



Updates Since -27 (@IETF-122)

New functionality

- Explain how information can be stored in the COSE signature header (#310)
  - Example: a `uint` timestamp of signing, using the “iat” CWT claim parameter

Editorial & fixes

- Fix/Update IANA BRSKI well-known URIs registry – header names (#326)
- Fixes in EdDSA curve selection text
- Cleanup normative vs informative references
- Unify COSE header parameters terminology (#330)
- Formatting & editorial updates

Nearing completion – what's missing?

- Progress the dependencies
  - draft-ietf-anima-constrained-join-proxy → *see 2 slides from now*
  - draft-ietf-anima-rfc8366bis
- Second WGLC
  - This is advisable, given many text changes!
- Earlier review comments were addressed.
  - Any new actions/reviews needed?
  - E.g. Based on the new content

SECDIR Early review (of -23) by Kathleen Moriarty **Ready**
YANGDOCTORS IETF Last Call review (of -21) by Xufeng Liu **Ready**
GENART IETF Last Call review (of -21) by Russ Housley **Almost ready**
IOTDIR Early review (of -21) by Henk Birkholz **Ready w/nits**

Implementations

- Appendix A.1 lists open source projects
  - Client & simulation code work was at IETF 121 Hackathon!
- cBRSKI features are partly implemented
  - providing confidence that it works
- Currently, no plans for a full implementation

Join Proxy for Bootstrapping of Constrained Network Elements

draft-ietf-anima-constrained-join-proxy-17

IETF 123, Madrid, July 2025

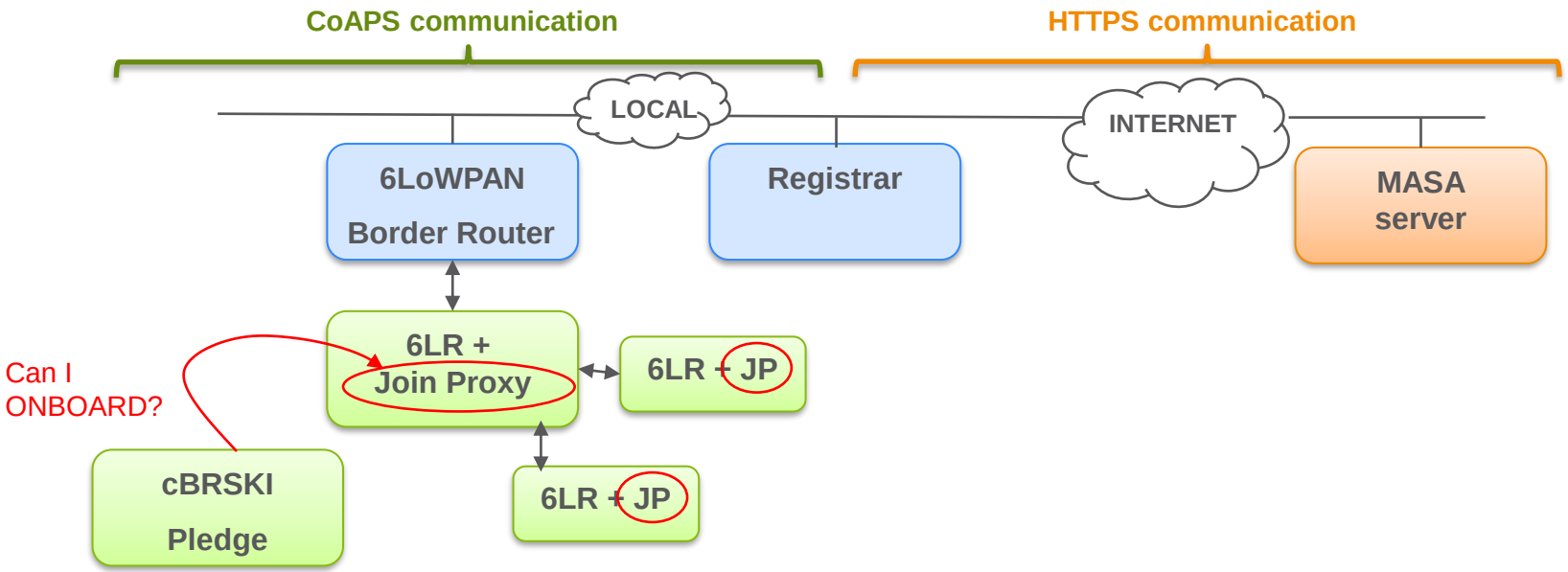
Esko Dijk – IoTconsultancy.nl
(presenting)

Co-authors:
M. Richardson
P. van der Stok
P. Kampanakis

GitHub

Recap & Goal – Join Proxy for cBRSKI

› **Join Proxy (JP) residing on constrained nodes for cBRSKI**



Updates Since -16 (since IETF 122)

New functions

- Security consideration: genuine Join Proxy may relay to malicious Registrar (#33)
- Solution for using multiple Registrars & onboarding protocols (#45, #65)
- Clarify that Registrar address(es) can be configured, or discovered (#76)
- Define conditions for implementing only a single Join Proxy mode – stateful or stateless (#69)
- Improved JPY Header security by adding integrity protection (#74)

Editorial

- Fixed format definition of example JPY Header (#74)
- Editorial updates.

Nearing completion – what's missing?

- Second WGLC
  - This is advisable, given many text changes!

- Previous reviews have been addressed.
  - Any need to redo / recheck w.r.t. latest changes?

OPSDIR IETF Last Call review (of -14) by Jürgen Schönwälder ! Has issues
GENART IETF Last Call review (of -14) by Ines Robles Almost ready
SECDIR IETF Last Call review (of -14) by Mališa Vučinić i Has nits
IOTDIR IETF Last Call review (of -14) by Russ Housley Almost ready
ARTART IETF Last Call review (of -10) by Rich Salz Ready w/nits
TSVART IETF Last Call review (of -10) by Spencer Dawkins Ready

Thank You!

Comments or Questions?

GitHub cBRSKI
GitHub Join Proxy