Constrained BRSKI (cBRSKI)

draft-ietf-anima-constrained-voucher-27

Image: various brands of constrained brewski

IETF 122, Bangkok, March 2025

Esko Dijk – IoTconsultancy.nl (presenting)

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

GitHub

Recap & Goal – Constrained BRSKI

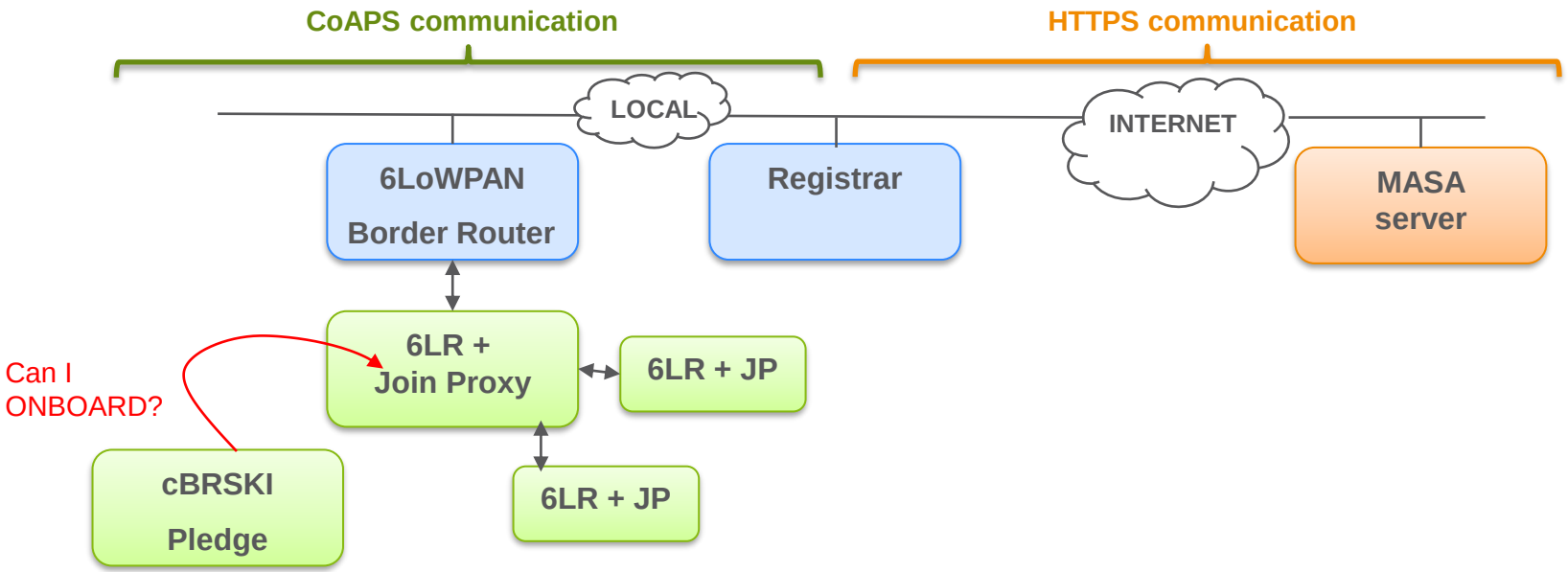
- **BRSKI onboarding, for constrained (IoT) devices & networks**

- 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 -25 (@IETF-121)

- Many editorial updates!

- Clarify use of COSE “x5bag” to store the signer’s X509 certificates
  - Allows Registrar to fully check Voucher signature
  - No overhead of these certificates on the constrained network segment

- Require CBOR format for BRSKI telemetry messages
  - avoid needless variation

- Added base Resource Type for “ace.est”
  - simplify & minimize EST-coaps discovery operation

Nearing completion – what's missing?

- Describe how a voucher can have "signing timestamp" #310
  - Re-use COSE method for this: *include CWT claim "iat" parameter (RFC 8392)*

- Update the BRSKI Parameters Registry PR #328
  - Changes field "URI" to more correct "Path Segment"

- Progress the dependencies
  - draft-ietf-anima-constrained-join-proxy *see 2 slides from now*
  - draft-ietf-anima-rfc8366bis

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-16

Image: various brands of constrained brewski

IETF 122, Bangkok, March 2025

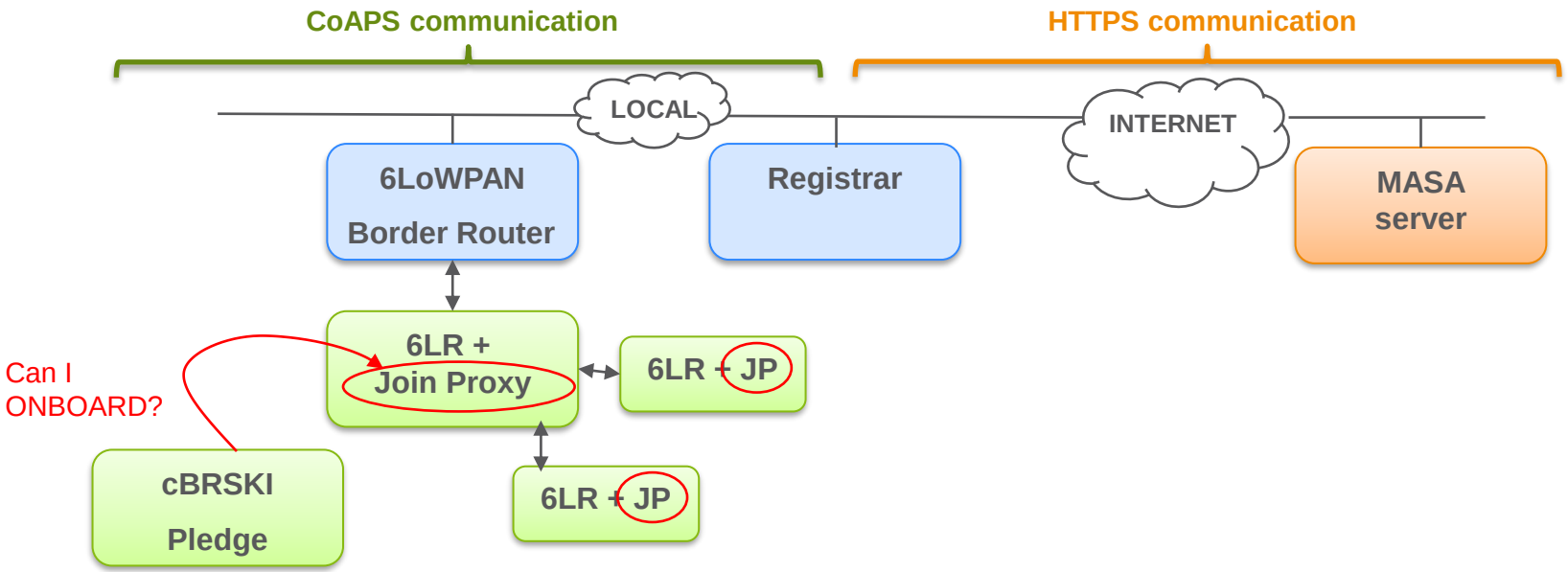
Esko Dijk – IoTconsultancy.nl (presenting)

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**



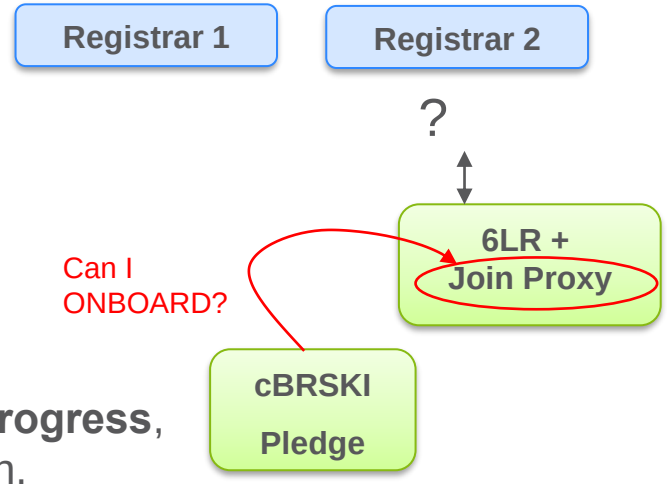
Updates Since -15 (since Nov 2023)

- Simplify stateless / stateful Join Proxy mode selection #69
  - Mode is either defined by a “profile” (single choice) or configured in network
  - Avoiding “autodetect” of mode reduces errors / testing-efforts / dead code

- Editorial overhaul & corrections
  - Applied all known pending reviews (TSVART, IOTDIR, WGLC, WG, …)
  - Security Considerations expanded

- Focus on default CoAP discovery of Registrars / Join Proxies, remove GRASP/6TiSCH/… discovery
  - Other discovery methods delegated to draft-ietf-anima-brski-discovery

Next Steps



- Registrar Selection Problem
  - Join Proxy may discover “malicious Registrar” #33
  - Registrar may be unresponsive – try another? #65
  - The problem is that the Pledge **knows if it’s making progress**, but the Join Proxy **determines** the Registrar destination.
  - In some cBRSKI implementations, no discovery but **configuration** of 1 Registrar.

- After above is solved:
  With so many text changes, have a 2nd WGLC?

Thank You!

Comments or Questions?

Image: various brands of constrained brewski

GitHub cBRSKI
GitHub Join Proxy