# Constrained BRSKI (cBRSKI)

## draft-ietf-anima-constrained-voucher-25


*Image: various brands of constrained brewski*

IETF 121, Dublin, November 2024

**Esko Dijk – IoTconsultancy.nl (presenting)**

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

# Recap & Goal – Constrained BRSKI

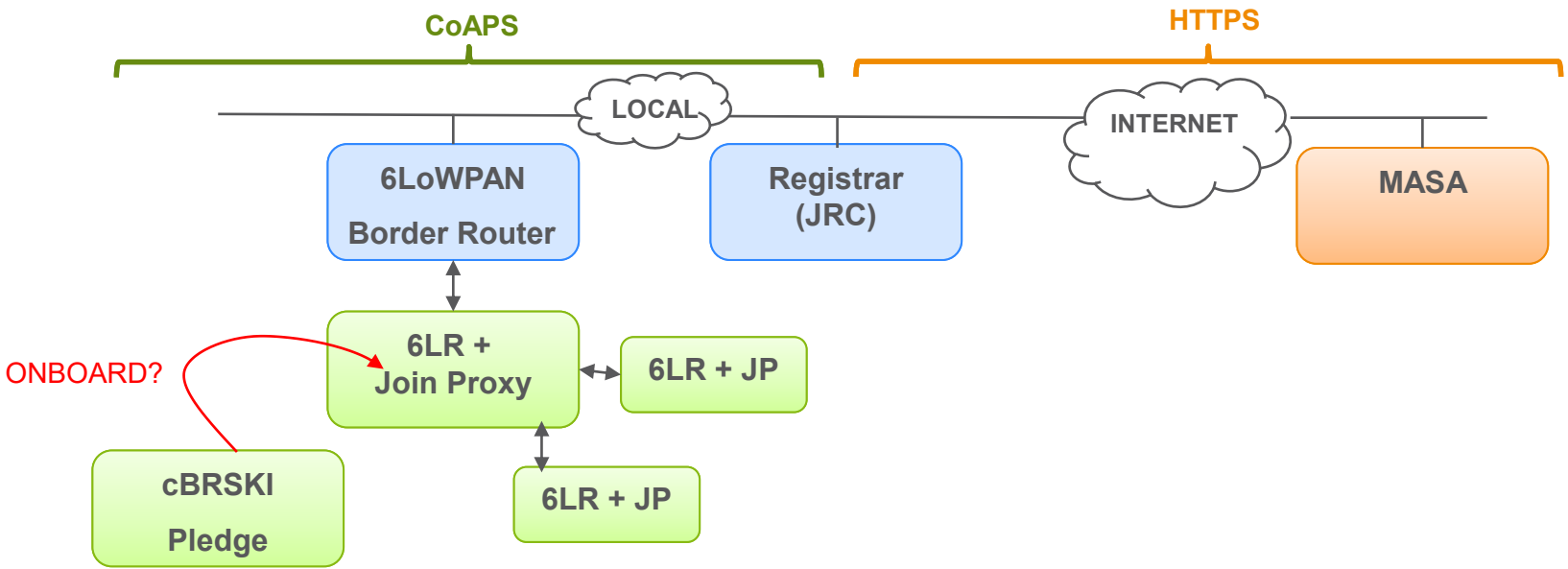
- **BRSKI onboarding, for constrained (IoT) devices & networks**

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

  - 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**

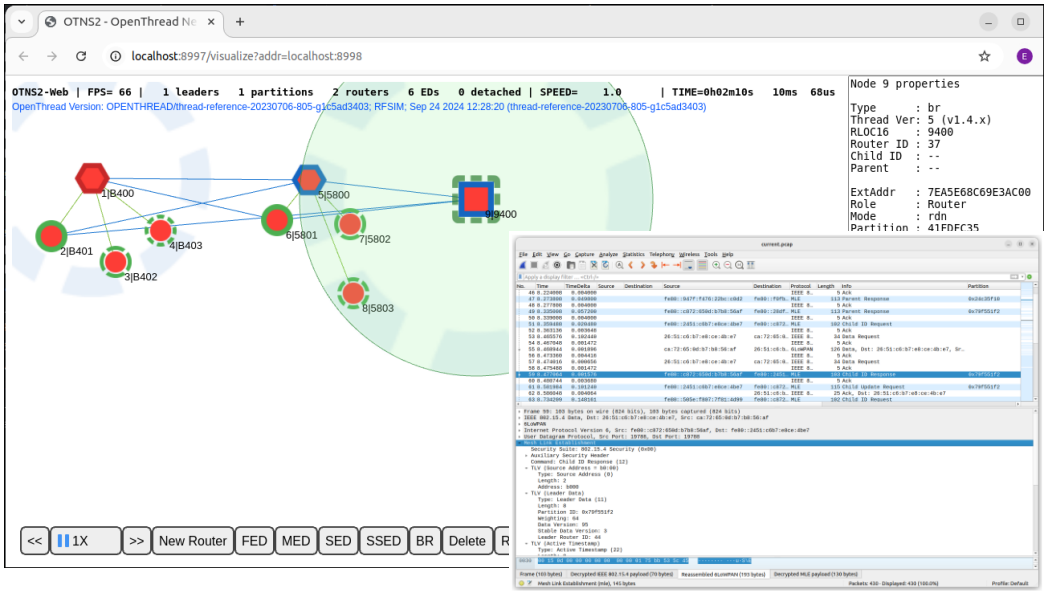


# cBRSKI Implementation & Interop

- Pledge: **cBRSKI for OpenThread**
  - open source Proof of Concept – C/C++ code
  - Thread 6LoWPAN low-power wireless mesh networking standard

- Registrar: **OpenThread Registrar**
  - open source Registrar, MASA, Pledge
  - Java code
  - using **Github issue tracker**

- Simulation environment: **OTNS2** →
  - open source, not related to NS2 ☺
  - fully simulated radio environment for OpenThread nodes
  - easier & faster development iterations
  - Tutorial available.



# Updates Since -21 (@IETF-118)

- Many editorial updates! Text simplified to focus on the default flows.
  - Appendices for additional options & alternatives.

- Pledge EST enrollment now requires support for **multiple** CA certificates in "/crts"
  - Reason: single CA cert too limited for future / owner-change scenarios
  - New, simpler CBOR multipart content format for CA certificates response
  - `application/multipart-core`
    `[ 287, h'3082' ... 'd713', 287, h'3082' ... 'a034' ]`

- Constrained Join Proxy details removed – now refer to draft-anima-constrained-join-proxy

# Updates Since -21 (@IETF-118)

- New media type name for COSE Voucher: `application/voucher+cose`

- Simplified discovery details to only one method: CoAP discovery
  - Alternative methods to be handled by draft-ietf-anima-brski-discovery
  - Brief mentions of DNS-SD service names to use for DNS-SD / mDNS case

- Support DTLS 1.3 extension `record_size_limit`

# Updates Since -21 (@IETF-118)

- Further rebased text onto draft-anima-rfc8366-bis
  - instead of RFC 8366 (Voucher)
- Appendix A (Software) extended with open source SW pointers
- New Appendix E: Pledge Discovery of Onboarding and Enrollment Options
  - Good to document this, but in practice not used much (?) – so not in main text.

# Thank you!

# Comments/questions?


*Image: various brands of constrained brewski*

https://github.com/anima-wg/constrained-voucher/