Constrained join proxy

`draft-vanderstok-anima-constrained-join-proxy-01`

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 104 - ANIMA Working Group

Constrained join proxy

BRSKI uses HTTP and TLS

This draft proposes
- Replacement of circuit proxy, using
- CoAP and DTLS to support connection between
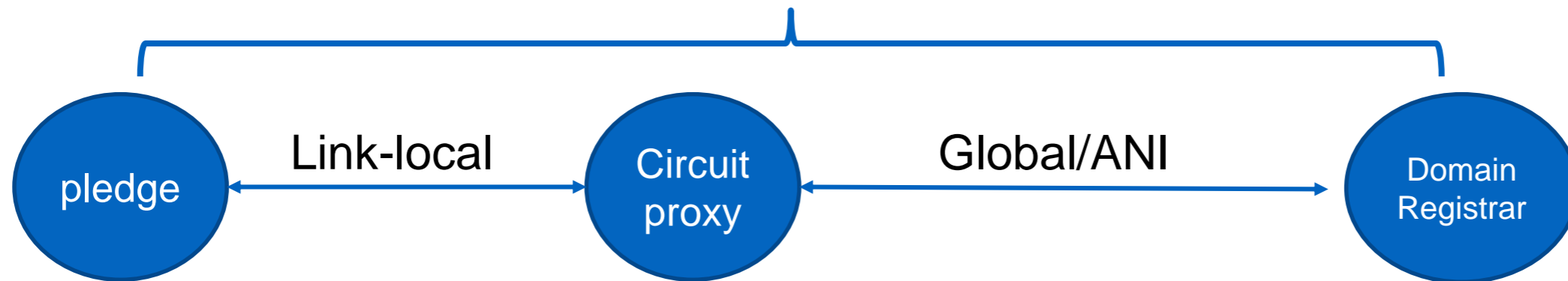 pledge and Domain Registrar

Based on kumar-dice-dtls-relay

EST: Enrollment over Secure Transport (RFC7030)
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
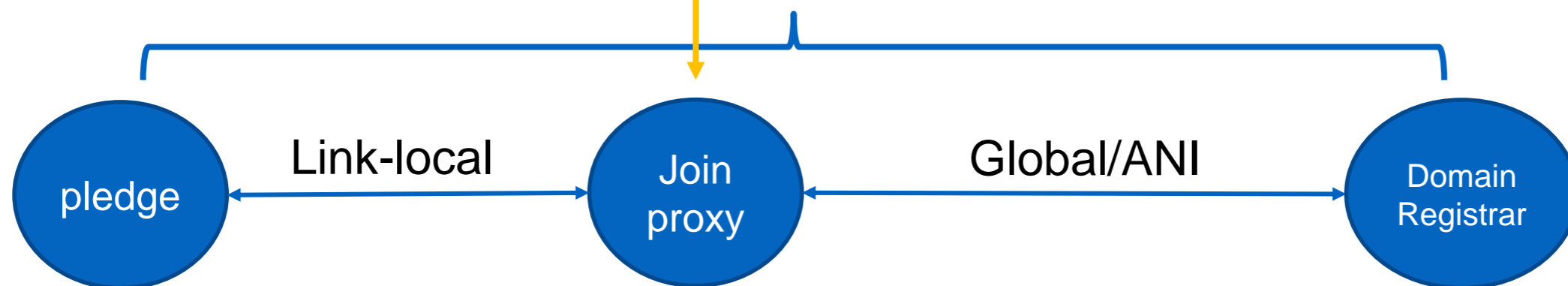
Graphic explanation

BRSKI-19

HTTP TLS

pledge — Link-local → Circuit proxy ← Global/ANI → Domain Registrar

Constrained devices

COAP DTLS

pledge — Link-local → Join proxy ← Global/ANI → Domain Registrar

State-full <-> State-less

pledge — Link-local — Join proxy — Global/ANI — Domain Registrar
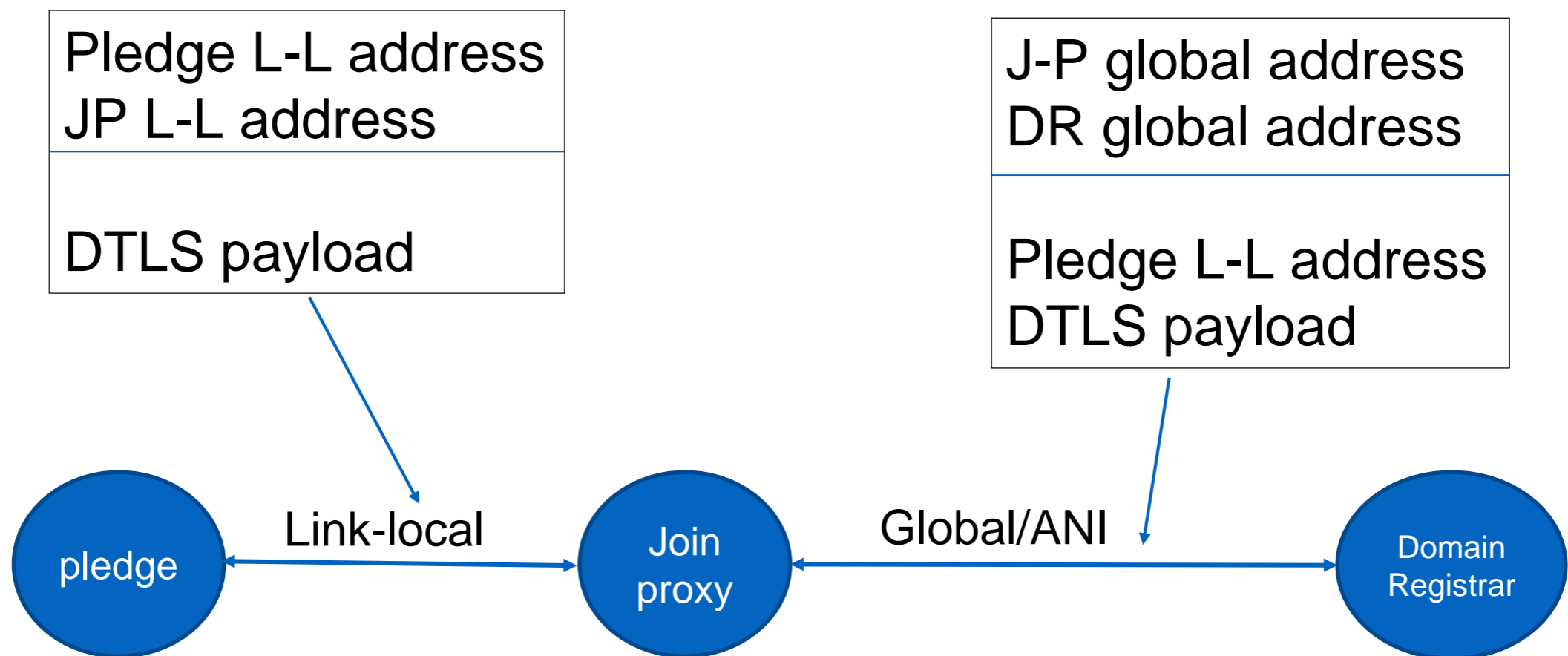
Latest draft version adds state-full mode

State-full:
Join-proxy stores link-local address and port of pledge
(a form of NAT66)

State-less:
Link-local address and port of pledge stored in network

Current discussion

What is the format of the state-less packet
between join-proxy and Domain Registrar

Pledge L-L address
JP L-L address

DTLS payload

J-P global address
DR global address

Pledge L-L address
DTLS payload

pledge ⟷ Link-local → Join proxy ⟷ Global/ANI → Domain Registrar

Draft relations

Draft	WG	uses	extends
BRSKI	ANIMA	HTTP/TLS EST CMS	EST with Voucher requests MASA Circuit proxy
EST-coaps	ACE	CoAP/DTLS EST	EST with coap/dtls
Voucher	ANIMA	YANG/JSON CMS	BRSKI with voucher spec
Constrained voucher	ANIMA	YANG/CBOR Voucher COSE/CMS/CBOR	Voucher with 2 fields BRSKI with COSE/CBOR and SID BRSKI with CMS/CBOR and SID
Constrained Join-proxy	ANIMA?	CBOR multipart-ct draft ?	BRSKI with constrained join proxy and EST-coaps

TODO

- Update example payloads
- Improve/extend discovery text
- Hope for comments

Question

Interesting to ANIMA?