Constrained join proxy

`draft-vanderstok-anima-constrained-join-proxy-02`

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 105 - 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
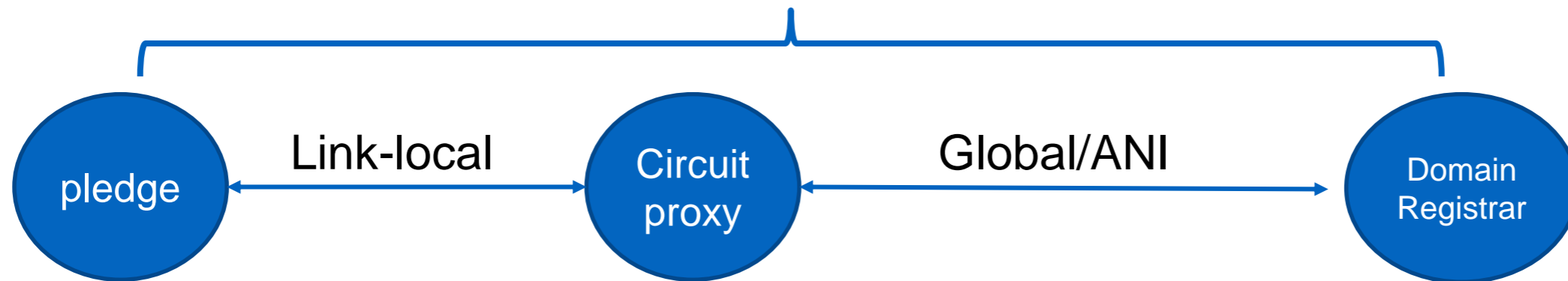
Based on kumar-dice-dtls-relay

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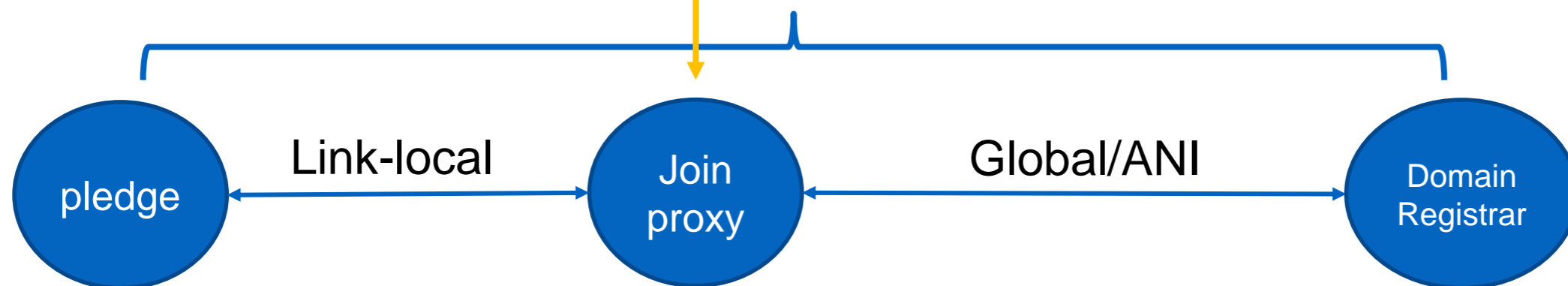BRSKI: Bootstrapping of Remote Secure Key Infrastructures

Graphic explanation

BRSKI-22

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

Assumption:

Join Proxy discovers (knows) address of Domain Registrar

Pledge discovers address of Join Proxy

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 encapsulated in the request

Discovery

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

Pledge discovers Join Proxy

- Mesh: coap discovery

- 6tisch: enhanced beacon

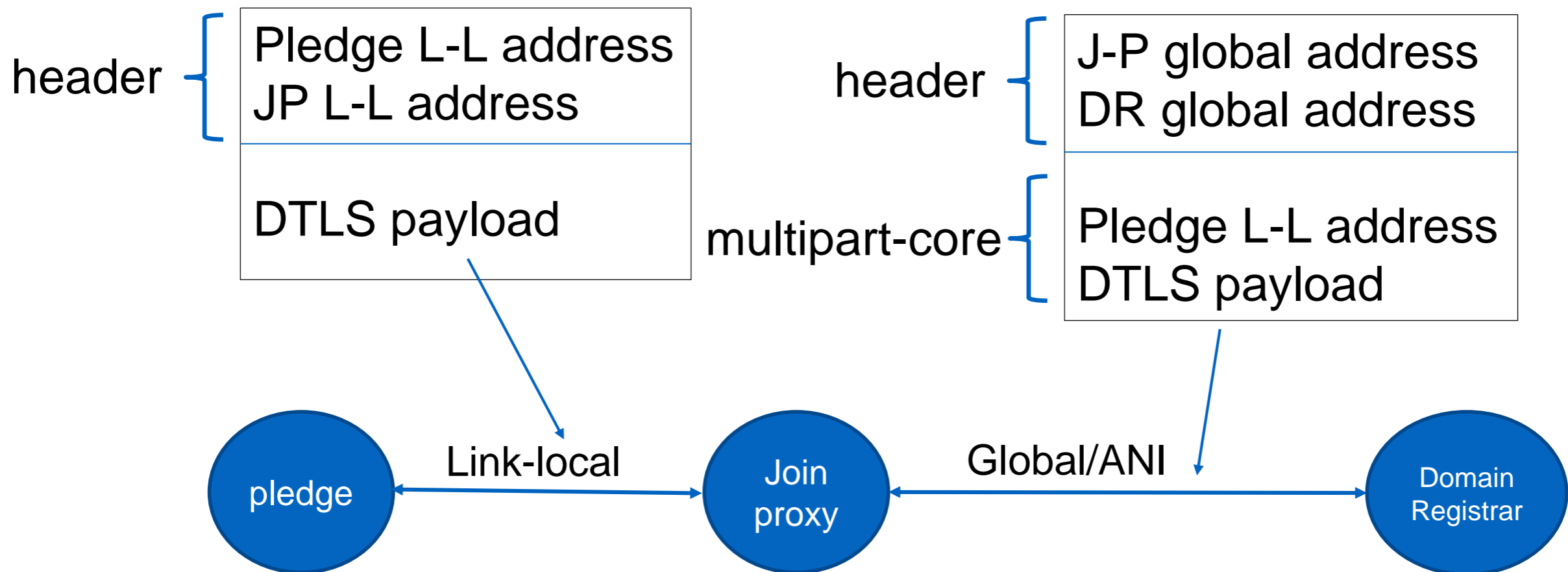**Join Proxy discovers Domain Registrar**

- ANI: GRASP

- NOT ANI: coap discovery

Packet Format

Stateless
State-less packet uses mediatype: application/multipart-core
between Join Proxy and Domain Registrar
draft-ietf-core-multipart-ct-03

header
| Pledge L-L address |
| JP L-L address |
| DTLS payload |

header
| J-P global address |
| DR global address |

multipart-core
| Pledge L-L address |
| DTLS payload |

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

Diagnostic CBOR of Multipart-core payload:
[60, [IP_p, p_P, ident], cf-EST, h'DTLS-content']

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 multipart-ct draft	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

- Hope for comments

Question

Interesting to ANIMA?