Constrained join proxy

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 103 - ANIMA Working Group

Constrained join proxy

BRSKI uses EST, HTTP and TLS

This draft proposes

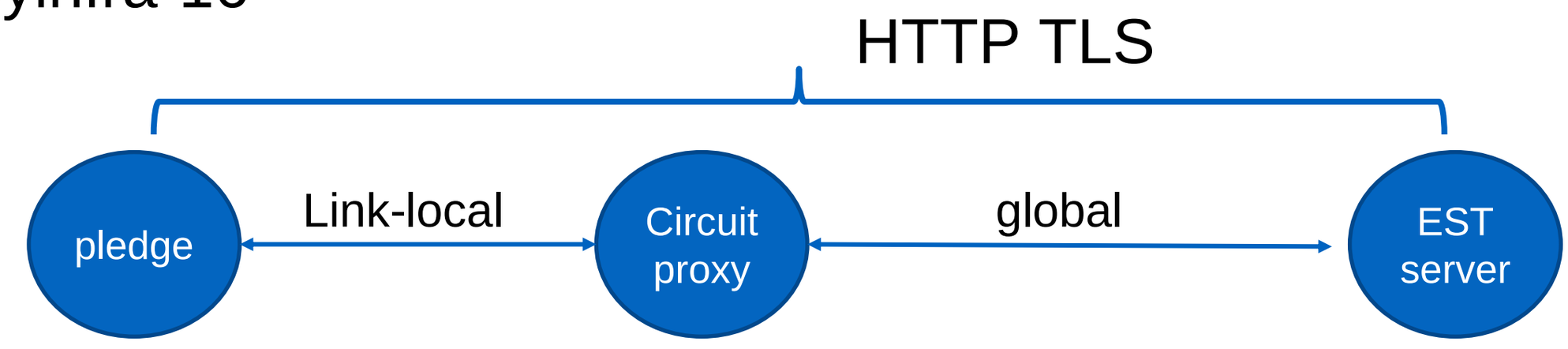
- Replacement of circuit proxy, using
- CoAP to support EST connection between pledge and EST server

Based on stateless part of kumar-dice-dtls-relay

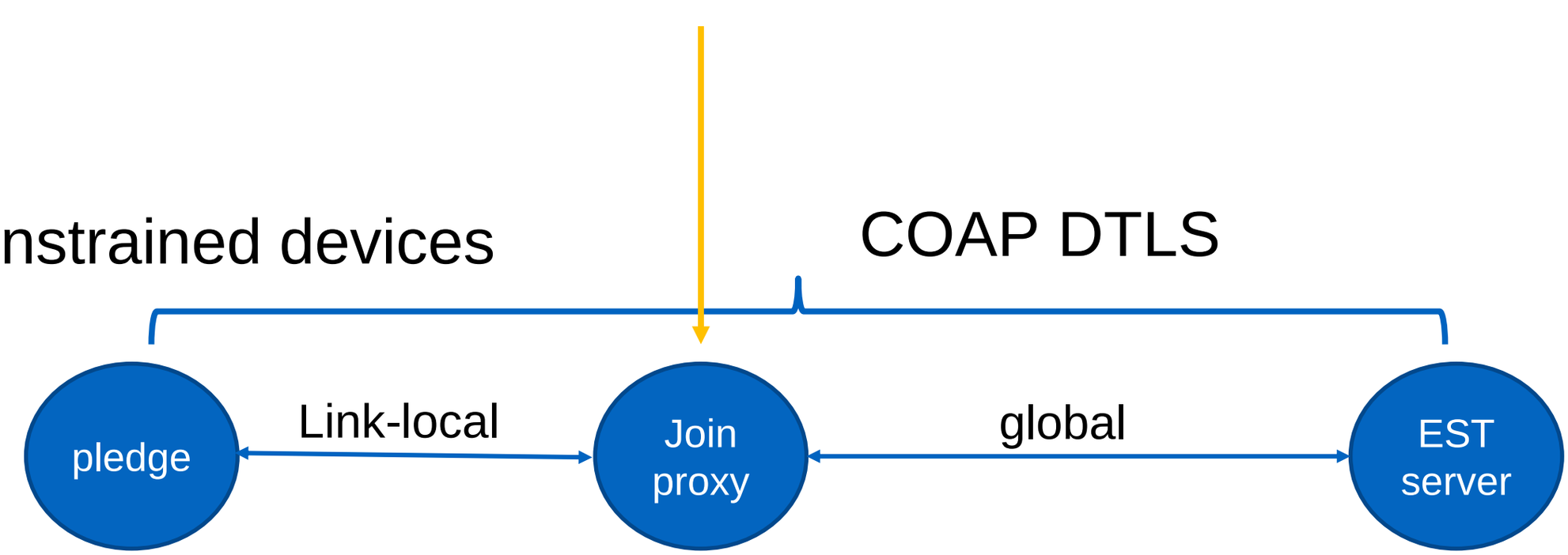
EST: Enrollment over Secure Transport (RFC7030)
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
CBOR: Concise Binary Object Representation (RFC 7049)

Graphic explanation

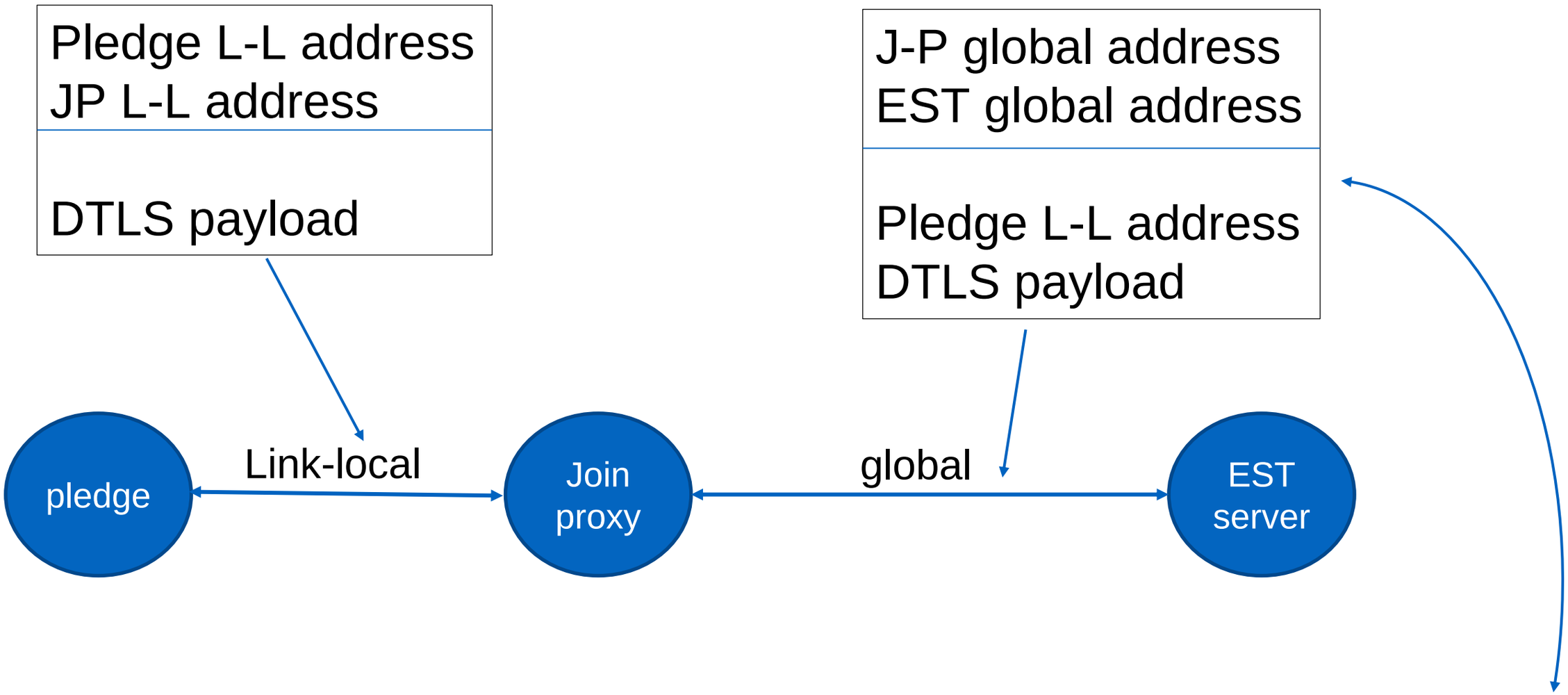
Keyinfra-16



Constrained devices



Transport format



Ct=287; CBOR array: [ct=60, [L-L IPv6, port, ident], ct=281, <DTLS encoded>]

ct=287: application/multipart-core; ct=60: application/cbor;
ct=281:application/pkcs7-mime; smime-type=certs-only

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

TODO

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

Question

Interesting to ANIMA?