# EST over coaps

Peter van der Stok, Sandeep Kumar, Panos Kampanakis
Martin Furuhed, ShahidRaza

IETF 98 - ACE Working Group

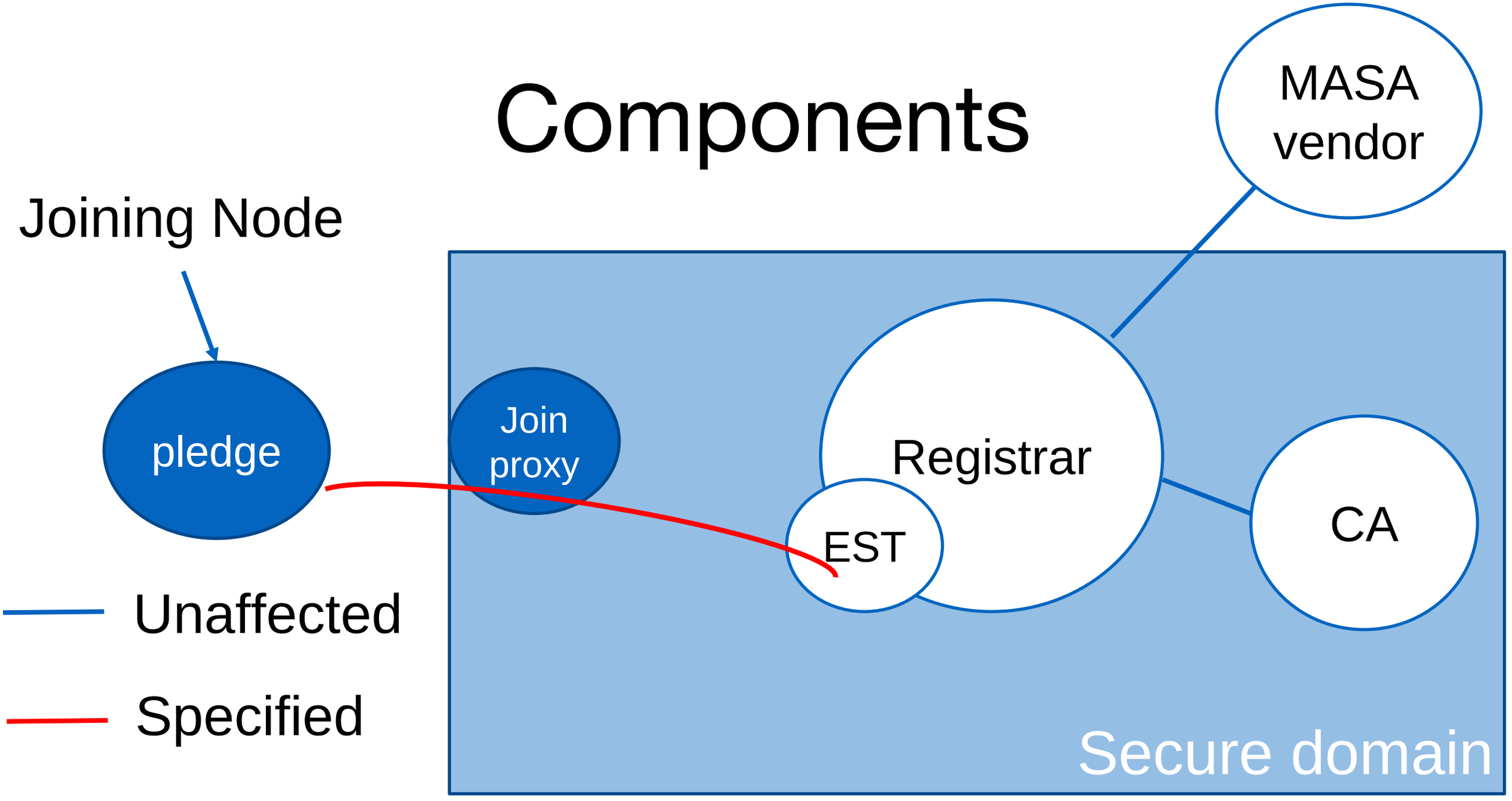
# EST over coaps

Bootstrapping of Remote Secure Key Infrastructures (BRSKI)
[ietf-anima-bootstrapping-keyinfra]
uses Enrollment over Secure Transport (EST) [RFC7030]

Where EST is currently based on HTTP and TLS
This draft proposes CoAP and DTLS

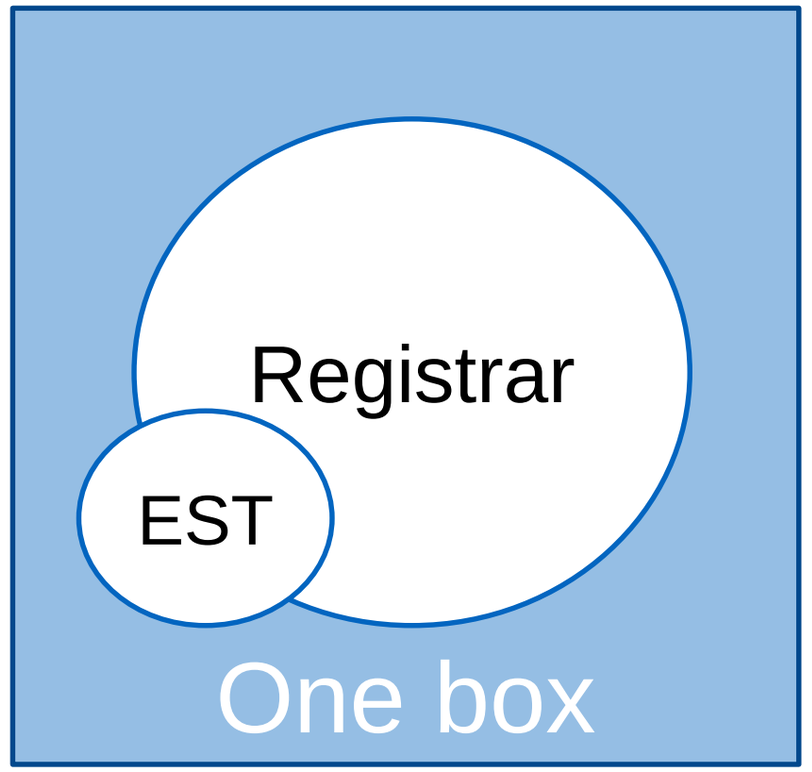
to support secure bootstrapping of low resource devices

# Components




DTLS at transport is applied between pledge and EST server. Pledge and EST server exchange Certificates and Vouchers [ietf-anima-voucher].

# Motivation




When *anima* takes off,
Boxes with EST server and Registrar will be available.

Adding the CoAP/UDP interface to box:

- enables secure bootstrapping in low resource networks,
- removes need for http/coap proxy,
- equalizes treatment of low-resource and regular devices.

# Contents

- Specify use of DTLS and CoAP Block with examples
- Conformance with ACE profiles

Differences with EST:

- No human (password) intervention
- No full PKI messages
- Extensions needed for BRSKI
- Discovery of path base: /est
- Payload formats “pkcsxx” use CBOR

Ongoing:

- Comparison with 6tisch approach: EDHOC, OSCOAP

# Details

| endpoints/resources: | | /application/….. | | |
|---|---|---|---|---|
| /cacerts | uses | pkcs7-mime | | |
| /simpleenroll | uses | pkcs7-mime | pkcs10 | |
| /simplereenroll | uses | pkcs7-mime | pkcs10 | |
| /csrattrs | uses | csrattrs | | |
| /serverkeygen | uses | pkcs7-mime | pkcs10 | pkcs8 |
| /requestvoucher | uses | voucherrequest | | |
| /voucher_status | uses | json | | |
| /enrollstatus | uses | json | | |

BRSKI endpoint

# TODO

- Operational parameter values
- Appendix examples for all endpoints
- Security considerations
- And others…..