EST over coaps

Peter van der Stok, Sandeep Kumar, Panos Kampanakis
Martin Furuhed, Shahid Raza, Michael Richardson

IETF 100 - ACE Working Group

EST over coaps

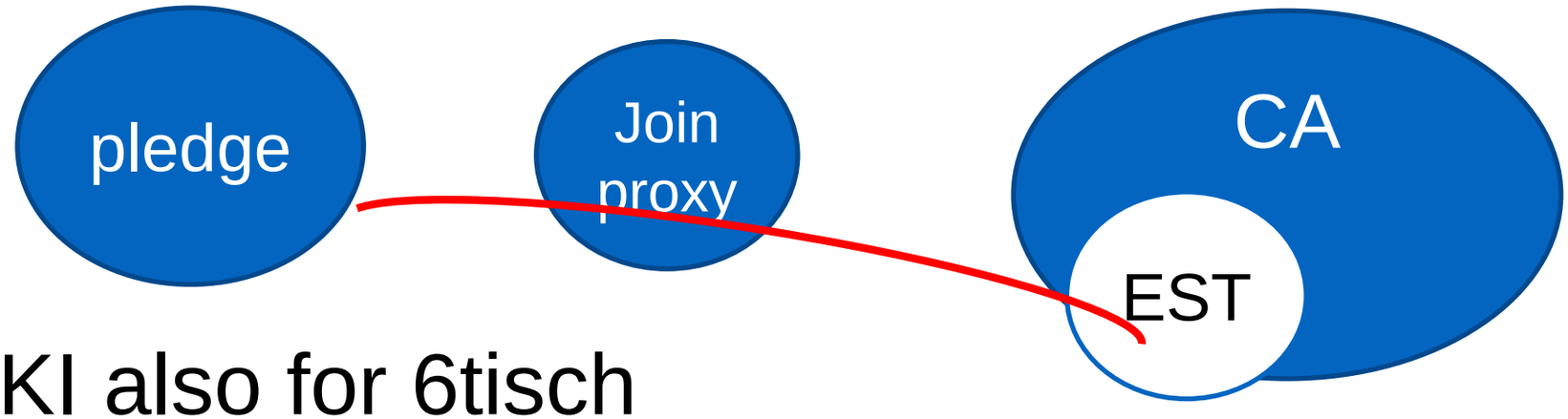
Enrollment over Secure Transport (EST) [RFC7030]
uses HTTP and TLS

This draft proposes CoAP and DTLS
to support low resource devices

Application areas:

- Secure bootstrapping devices
- Distribution of identity (certificates) and keying material

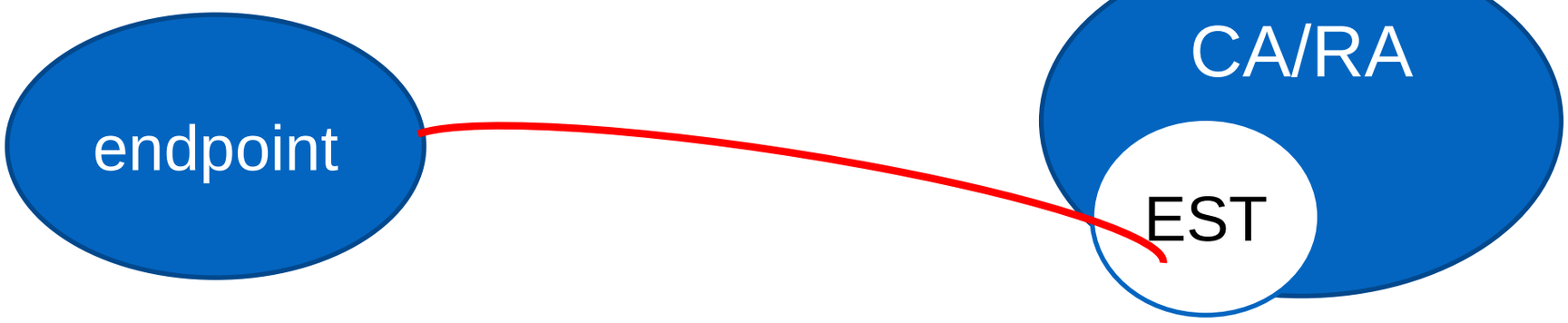
Application areas



BRSKI also for 6tisch

Pledge and EST server exchange Certificates and Vouchers

Authenticated/authorized endpoint cert enrollment (and optionally key provisioning) through a CA or Registration Authority.



Current issues

- Proxying section too terse?
- Motivation of draft beyond BRSKI
- Many BRSKI extensions to support voucher transport
- Use of response codes 2.05 and 2.01
- Server side key generation using simple multipart encoding
- Combination of existing RFCs
- Content formats use binary encoding, no others

TODO

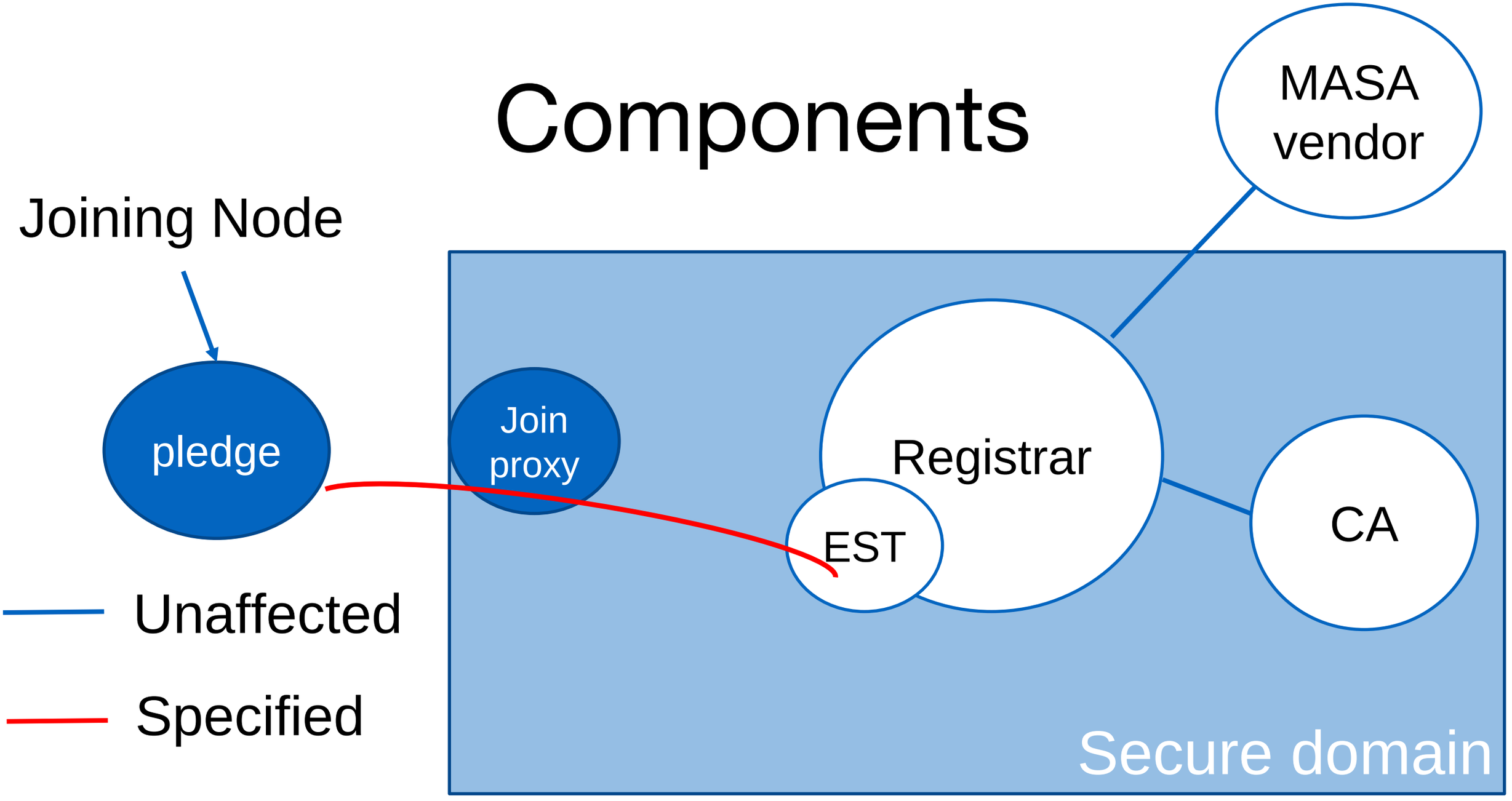
- Operational parameter values
- Change motivation section
- Add server-side key generation
- React to reviews
- And others…..

Next Steps

Ready for WG Draft?

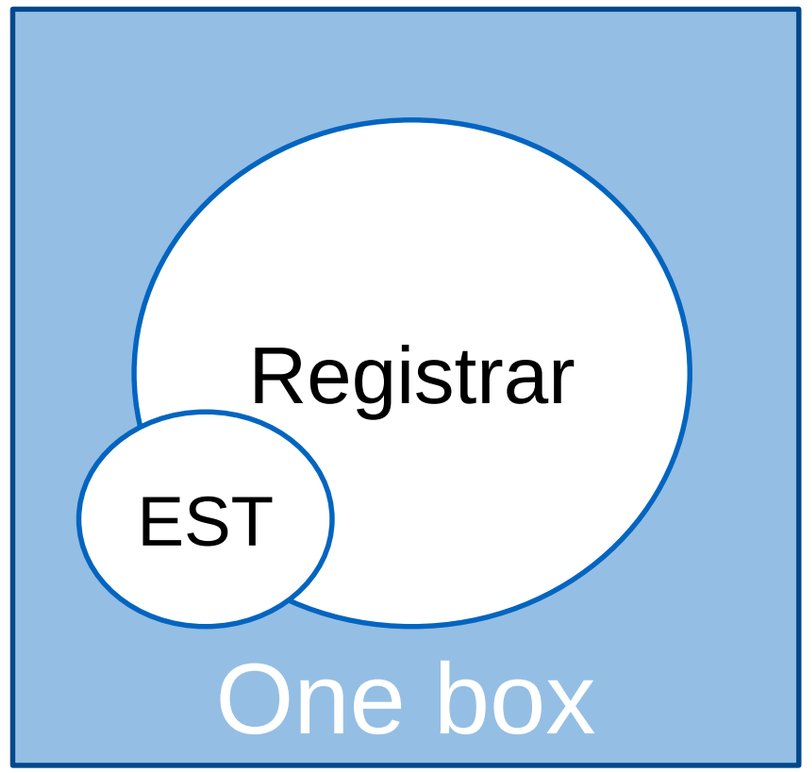
Reminder

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: e.g. /est
- Payload formats “pkcsxx” use binary

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