Certificate enrollment in ACE

Peter van der Stok, Sandeep Kumar, Panos Kampanakis
Michael Richardson

ACE Working Group
Interim meeting 19/10/2017

Why certificate enrollment

Enrollment of Secure Transport (EST) RFC7030 is integrating part of Bootstrapping Remote Secure Key Infrastructures (BRSKI) I-D.anima-bootstrapping-keyinfra.

EST is announced by multiple manufacturers

Its use in constrained environments (i.e. over coap) is required by Thread, Fairhair and other organizations c.q. manufacturers.

Why ACE

Reflected in the title and charter, ACE addresses

- Authentication and Authorization (use DTLS)
- Constrained Environments (use coap)

Current DTLS profiles of ACE do not specify how keying/ auth material is acquired by the protocol participants.

ACE is THE security WG that has security competence that is applied to constrained environments

EST over coaps

EST is currently based on HTTP and TLS.
The est-coaps draft proposes CoAP and DTLS

It adheres strictly to the existing protocols (EST and BRSKI)

It details the coap and DTLS aspects with extensive examples to guide the protocol implementers

It describes the relation with ACE profiles.

Its authors are new authoring resources for ACE

EST-coaps in ACE

There is a clear need for certificate provisioning in constrained environments. In particular, EST-coaps fulfills assumption of many ACE drafts (existence of keying material).

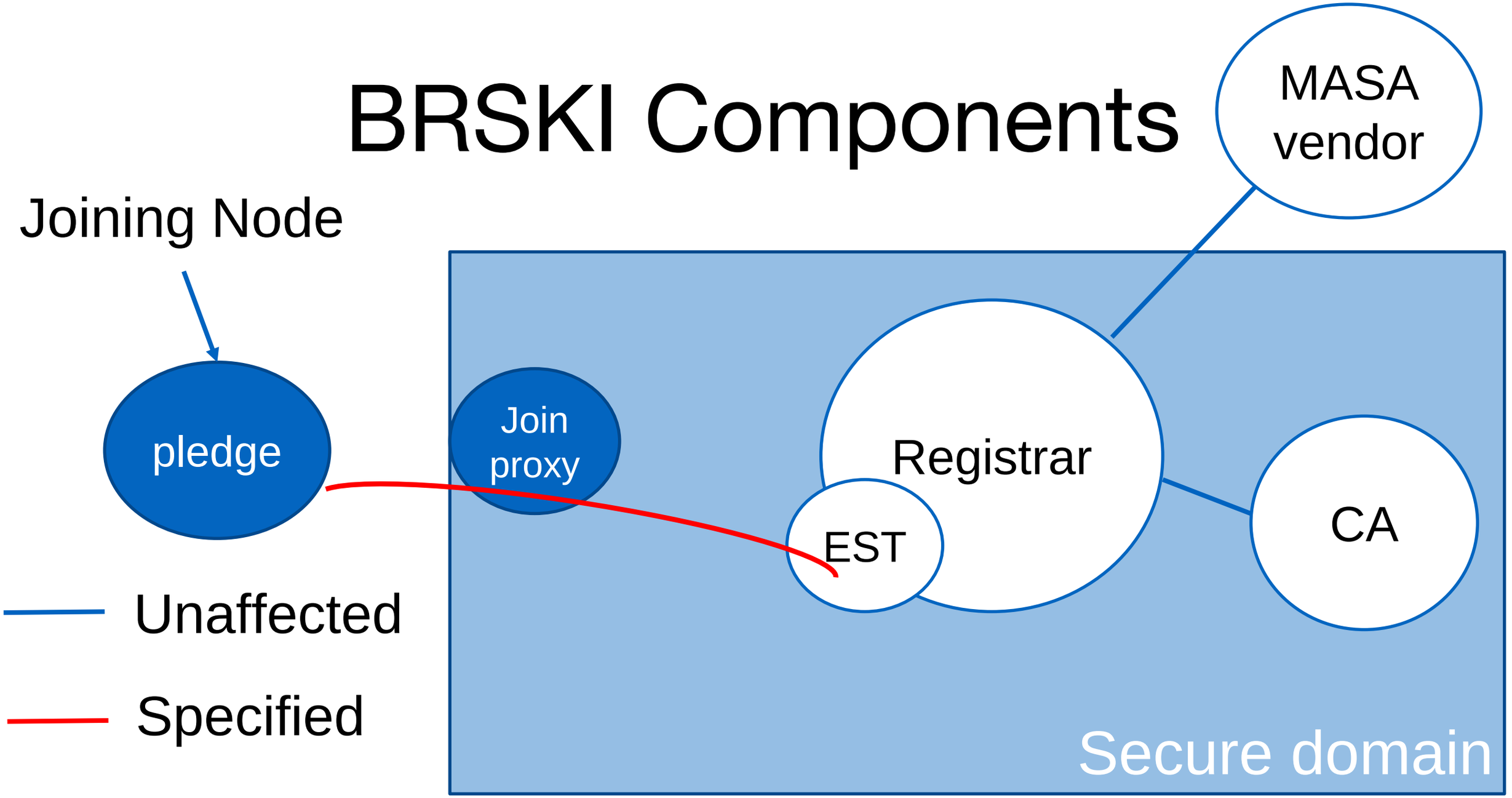
EST-coaps is based on existing, tested, implemented, and chosen technology (DTLS, CoAP).

Two proposals: EALS and EST-coaps

- ➢ EALS provides application security,
- ➢ EST-coaps provides transport security.
- ❖ EALS is more innovative with OSCORE and ECDHE,
- ❖ EST-coaps is more conservative with DTLS

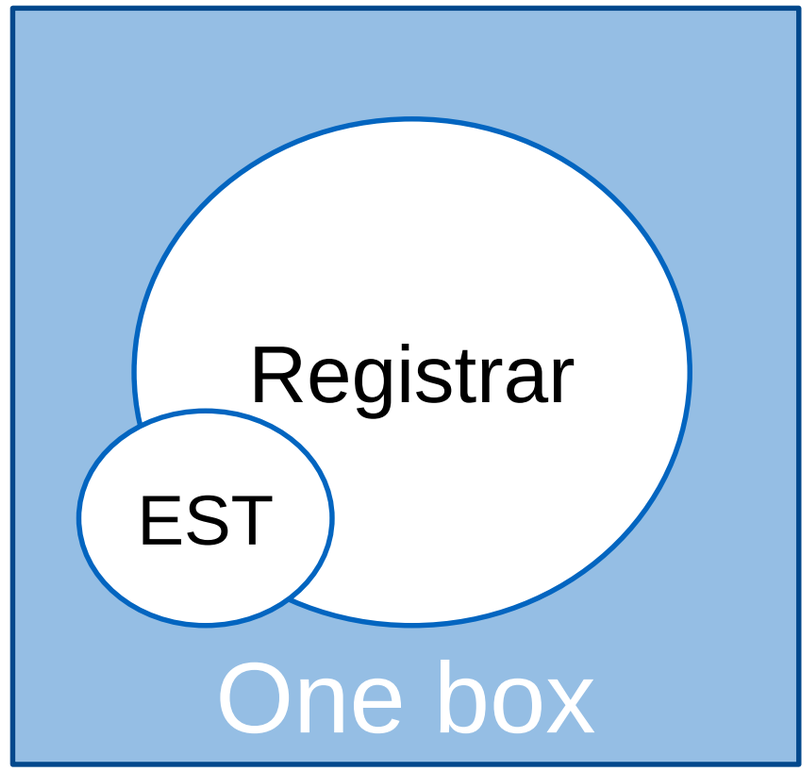
BACKground

BRSKI 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