EST over coaps

Peter van der Stok, Panos Kampanakis
Shahid Raza, Michael Richardson

IETF 104 - ACE Working Group

EST over coaps

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

This draft proposes CoAP and DTLS
to support constrained devices

Application areas:

- Secure bootstrapping devices
- Distribution of identity (certificates)

WGLC updates

Many thanks to Jim, Esko, Klaus, and Carsten

1. Discovery and content-format negotiations clarified and corrected
2. Added application/pkix-cert Content-Format TBD287
3. Removed text that duplicates or contradicts RFC7252
4. Examples updated:

- *Accept options added, nits removed, inaccuracies fixed*

5. Merged DTLS sections
6. In general: cleaned up text and removed inaccuracies

Multipart payload

The addition of application/pkix-cert necessitates negotiation of PKCS#7 or application/pkix-cert.

Currently impossible for serverkeygen function that returns content-format 62 that includes two content formats

An additional path “/skc” has been generated such that:
/skg returns application/pkcs7 and application/pkcs8
/skc returns application/pkix-cert and application/pkcs8

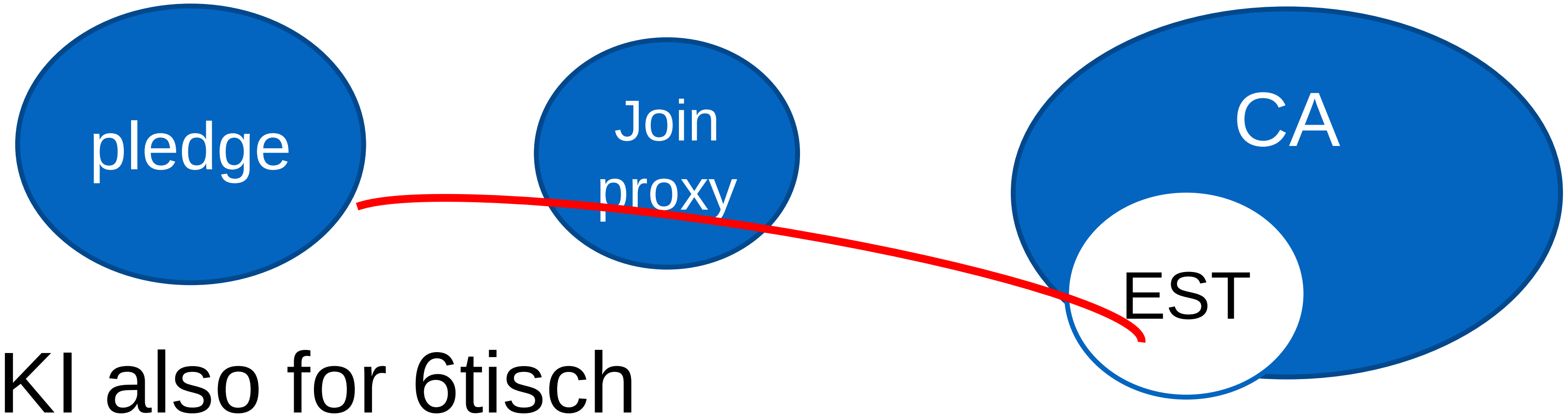
Continuation

Authors think they are done
All WGLC comments have been handled.

application/pkix, TBD287, still needs to be registered

REMINDER

Application areas

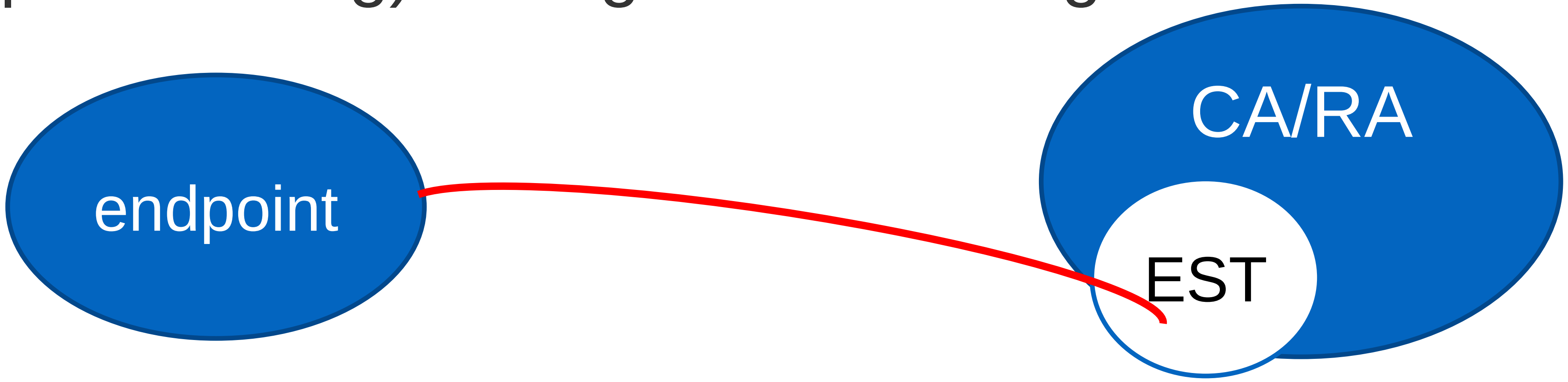


BRSKI also for 6tisch

Pledge and EST server exchange Certificates and Vouchers

BRSKI [anima]: Bootstrapping Remote Secure Key Infrastructures

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


endpoint
CA/RA
EST