Status of BRSKI
IESG review

Revision to Christian Huiteam
SECDIR review

Revision -20 posted

IESG review
And DISCUSSes

Edits for first part of
Ben Kaduk review

Revision -21 posted

IESEG review
And DISCUSSes

Edits for Alexey
review

Formal -23
And -24
Posted

Edits for Adam
Roach review

Informal -23
Posted for
Rfcdiff issue

Edits for Magnus
review

Edits for Alexey
review

Edits for Mirja
review

Finish reviews
and post
-25 document
Status of BRSKI
IESG review

August
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31

September
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6 7 8 9 10 11 12
13 14 15 16 17 18 19 20 21 22 23 24 25 26
27

October
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6 7 8 9 10 11 12
13 14 15 16 17 18 19 20 21 22 23 24 25 26
27

November
Su Mo Tu We Th Fr Sa
1 2 3 4 5 6 7 8 9 10 11 12
13 14 15 16 17 18 19 20 21 22 23 24 25 26
27

Period of pester of ADs

Revision -25 posted
Revision -26 posted
Revision -27 posted
Revision -28 posted
Revision -29 posted
Revision -30 posted

DISCUSSIONS
AC: Yang
AR: ok
BK: ok
EV: ok
RA: ok
AM: ok

RA:?
BK:?
AC:?
Summary of changes since -24

- revised abstract
- expanded section 7.4: MASA security reductions, nonceless vouchers and adding voucher trust anchors
- added missing XML registry
- added section 9.1, Operational Requirements for ACP
  - MASA Operational Requirements
  - Domain Owner Operational Requirements
  - Device Operational Requirements
- Added “Death of a Manufacturer” (with apologies to Willy Loman)
Summary of changes since -24 (2)

- section 11.6 expanded to include consequences of loss of manufacturer keys
- sorted terminology rather than presenting in what was at some point a logical grouping
- fixed many TLAs that, after re-ordering were not expanded at first use
- [REST] reference added
- left 802.1AR reference at 2009 version, as 2018 version is not easily obtained, and changes are not relevant
- added description of figure 4 (time sequence)
Summary of changes since -24 (3)

- clarified comments about ignoring lifetime from broken CA systems
- MUD is RFC8520 (yeah!), updated reference
- clarified ACP use of IPv6 Link-Local for proxy connection
- fixed many examples vouchers to be correct,
- YANG doctor fixes, synchronized author list
- removed Steinthor, added Toerless as author
- describe MASA URL with URL rather than IRL terms
- added CDDL definition for Proxy GRASP Announcement, and for AN_Join_Registrar
Summary of changes since -24 (4)

- make it clear that TLS 1.2 suffices, but that TLS 1.3 is preferred. This is driven by (lack-of) availability of FIPS-140 certified TLS 1.3 implementations for router platforms.
- clarify RFC6125 checking of MASA ServerCertificate
- clarified when nonce is required and why serialNumber is required in voucher.
- clarified how MASA MAY authenticate the Registrar
- added 5.5.2: MASA pinning of registrar and 5.5.3: MASA checking of voucher request signature, deleted old: 5.5.4. MASA revocation checking of registrar (certificate)
- added CDDL for audit-log reply
Summary of changes since -24 (5)

- removed explicit SHA-1 dependency of domainID
- added CDDL for enrollment status and telemetry status messages

Hoping to get sign off from IESG this week
Started two new documents!

Operational Considerations for BRSKI Registrar
draft-richardson-anima-registrar-considerations-00
~ 20% done:
https://github.com/mcr/registrar-operational-considerations

Operational Considerations for Manufacturer Authorized Signing Authority
draft-richardson-anima-masa-considerations-00
~0% done.

Help sought