#### Draft-ietf-anima-bootstrapping-keyinfra Versions 24-30

IETF 106 – Singapore

Slides from:
Michael Richardson
mcr+ietf@sandelman.ca

Revision to Christian Huiteam **SECDIR** review

#### Status of BRSKI IESG review

**Edits for Adam** Roach review

**Revision -21** posted

**IESG** review And DISCUSSes

Informal -23 Posted for Rfcdiff issue

**Revision -20** posted

une

Fr Sa We ľu 

Su Mo

We Th

2019

Sa Fr

3

5

Ben Kaduk review

Edits for first part of

10

14

12

16

18 19

20 21 22

16

30

19

0

23

25 26 27 28

29

28

23 24

18

30

Formal -23 And -24 **Posted** 

31

Finish reviews and post -25 document

**Revision -22** posted

**Edits for Alexey** review

**Edits for Magnus** review

**Edits for Mirja** review

Revision -25 posted

30

29

# Status of BRSKI IESG review

Revision -28 posted

RA

October

			Αι	ıgus					
Su		0	Tu	We	Th	Fr	Sa		
					1	2	3		
4		5	6	7	8	9 -	10	ВК	
11	1	2	1 <b>BI</b>	SCŲS	S\$IQI	<b>V\$</b> 6	17	EV:0	k
18	1	9	20	21	22	23	24		
25	2	6	27	28	29	30	31		

AR:ok</mark>Su Mo Tu We 2 5 9 Revision -296 posted 15 18 6 19 23 AC:Yang **Doctor** DISCUSSIONS1 AC:ok

Revision -26 mber-Period of posted pestering We Th FΥ Μo Τu Su of ADs 5 6 **AM** 12 10 13 18 19 24 25 26

Su Mo Tu We Th Fr

Revision -30
posted

1 5 6 7 8

11 12 13 14 15

17 18 19 20 21 22

24 25 26 27 28 29

AM:ok

Revision -27 posted

RA:?

**BK:?** 

AC:?

#### Summary of changes since -24

- https://www.ietf.org/rfcdiff?url1=draft-ietf-anima-bootstrapping-keyinfra-24&url2=draft-ietf-anima-bootstrapping-keyinfra-30
- 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 appologies 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 dependancy 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