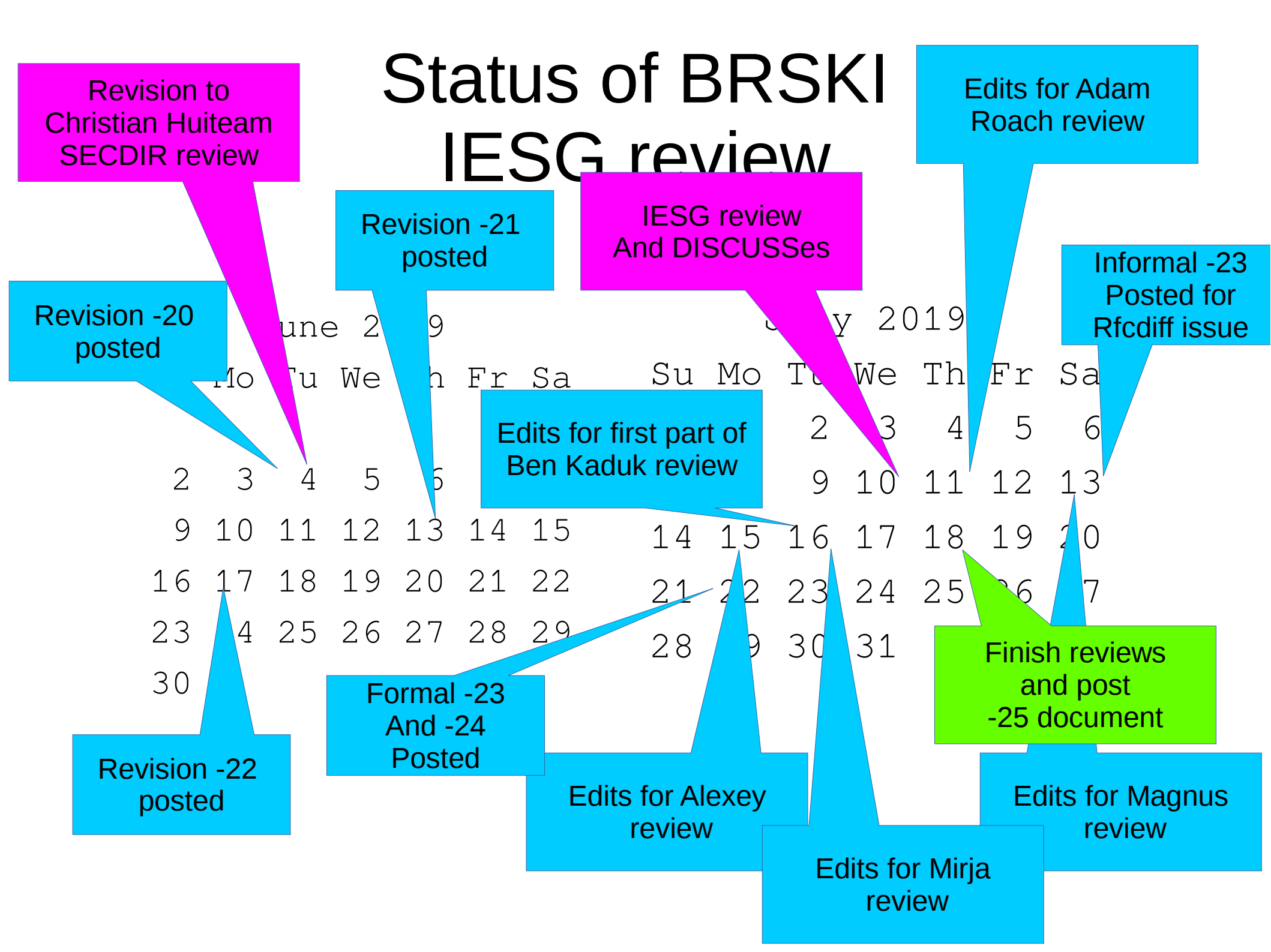
# Draft-ietf-anima-bootstrapping-keyinfra
# Versions 24-30

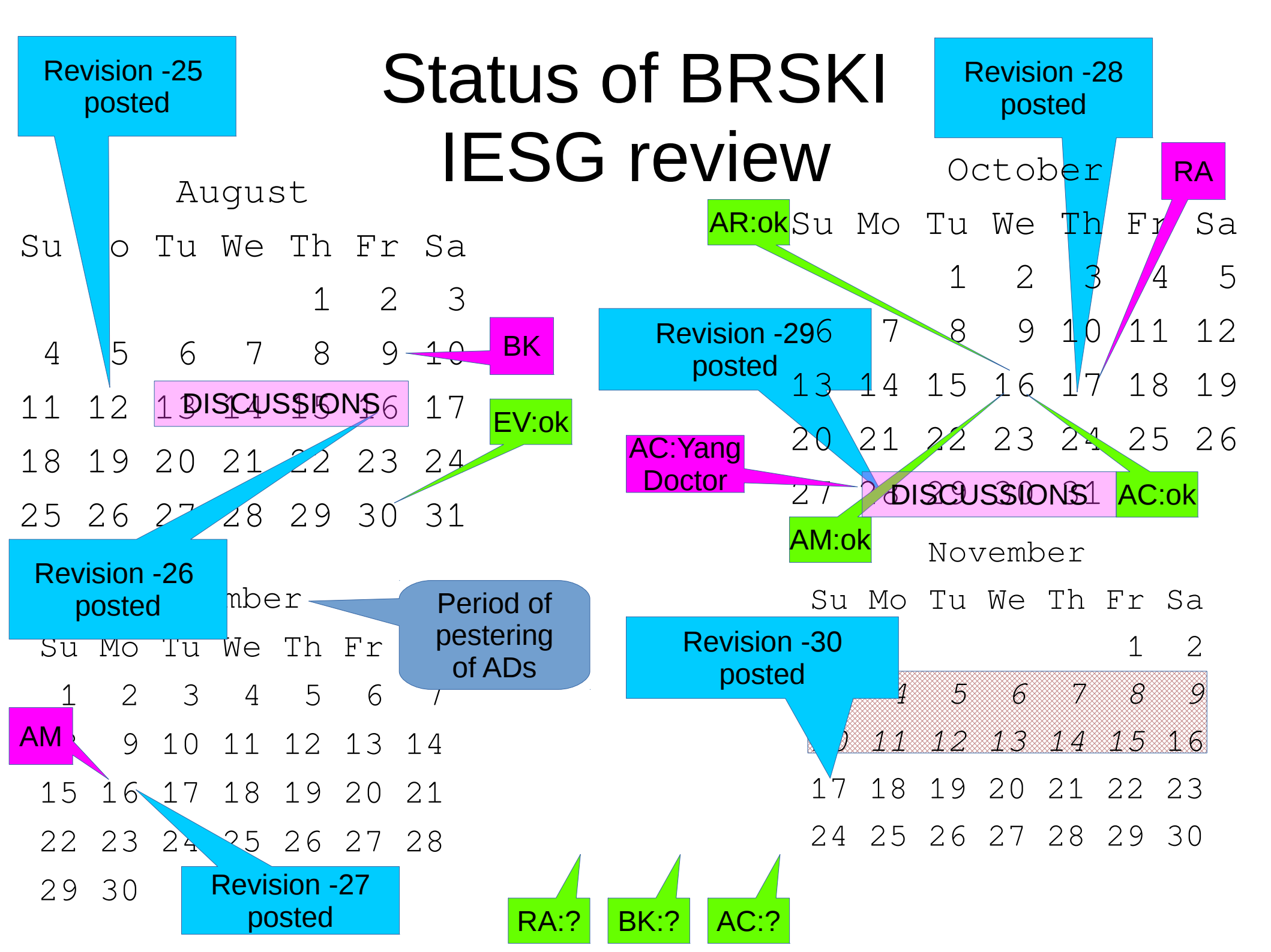
IETF 106 – Singapore

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

# Status of BRSKI IESG review



# Status of BRSKI IESG review



# 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