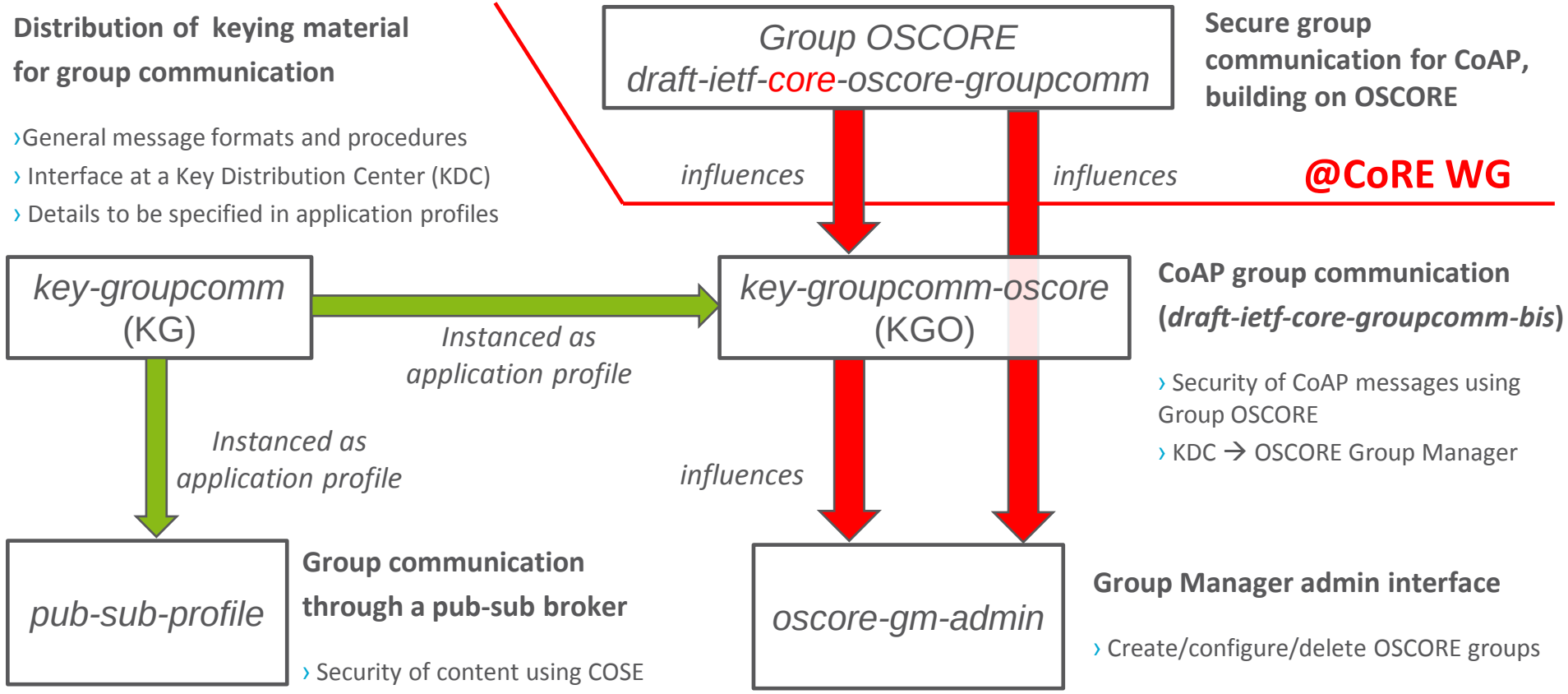
Key Provisioning for Group Communication Using ACE

draft-ietf-ace-key-groupcomm-13

Francesca Palombini, Ericsson
Marco Tiloca, RISE

IETF 111, ACE WG, July 29th, 2021

Recap of groupcomm documents



Updates from v -13

- Proof-of-possession (PoP) of a node's private key
  - When joining the group at the KDC, or when uploading a new public key at the KDC
  - OLD: always achieved through a signature
  - NEW: achieved through a "PoP evidence", that profiles must specify how to compute
- Format of public keys used in the group
  - Indicated by the 'pub_key_enc' parameter, in different messages
  - OLD: COSE Key as default format; practically, the one to use
  - NEW: any suitable format with a codepoint in the "COSE Header Parameters" registry
    - E.g.: X.509/C509 certificates; CWTs; unprotected CWT claim set – Some under pending registration
    - Profiles must specify the public key formats accepted in the group
- Explicit indication of a node identifier, associated to a public key owner
  - OLD: use the 'kid' header parameter of the COSE Key
  - NEW: use the key-groupcomm parameter 'peer_identifiers' (was optional, for other key formats)

Summary and next steps

- The latest version -13 is stable
  - All required updates pertaining to this document have been made
  - Consistency fixes and overall document revision

- The work on Group OSCORE in CoRE is not finished, but …
  - *ace-key-groupcomm* should not be impacted further
  - Side-effects will be on *ace-key-groupcomm-oscore* (mostly) and *ace-oscore-gm-admin*

- *draft-ace-key-groupcomm-13* ready for WGLC

Thank you!

Comments/questions?

https://github.com/ace-wg/ace-key-groupcomm