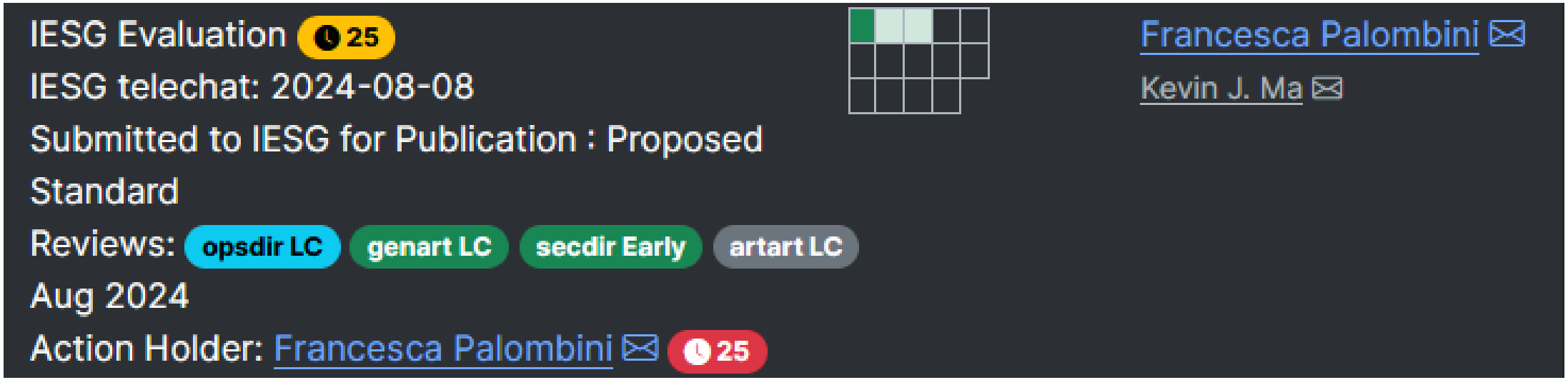
draft-ietf-cdni-https-delegation-subcerts-09

IETF 120 – CDNI WG

Christoph Neumann – July 23rd, 2023

Status

Under IESG evaluation



No major objections or concerns so far. Mostly nits, precisions and reformulations.

Recap of changes (since 05)

Many nits and reformulations.

References (RFC7336, RFC7337): normative versus informational?

- One reviewer: part of the terminology ➔ should be normative
- Another reviewer: generic framework and requirements documents➔ should be informational

Update in MI.DelegatedCredentials:

- Before IESG review: Usage of CertificateEntry as defined by RFC8446 (TLS) to encapsulate a delegated-credential structure as defined by RFC9345 (delegated credentials RFC). Allows also to encapsulate certificate chain.
- Reference to RFC46548 (Base64 encoding).

Recap of changes (since 05) – cont'd

Precisions on following SHOULD: "The uCDN SHOULD timely refresh dCDN credentials via the MI."

- Added reasons not to refresh: short-term one-shot deployments; deprovision of dCDN.
- Added consequences if not refreshed: dCDN refuses TLS connections of end-users.

Extended Security and Privacy Consideration discussion:

- Recall that, default maximum validity period of delegated credentials is set to 7 days in RFC9345.
- Recall that, if used, encryption is mandatory for private key in MI DelegatedCredentials object.
- Warning that a systematic retrieval of delegated credentials may allow to to decrypt data sent by end-user that may include PII.

Thank you.