EDHOC

draft-ietf-lake-edhoc-20
https://github.com/lake-wg/edhoc

IETF 117, LAKE WG, July 24, 2023

Status

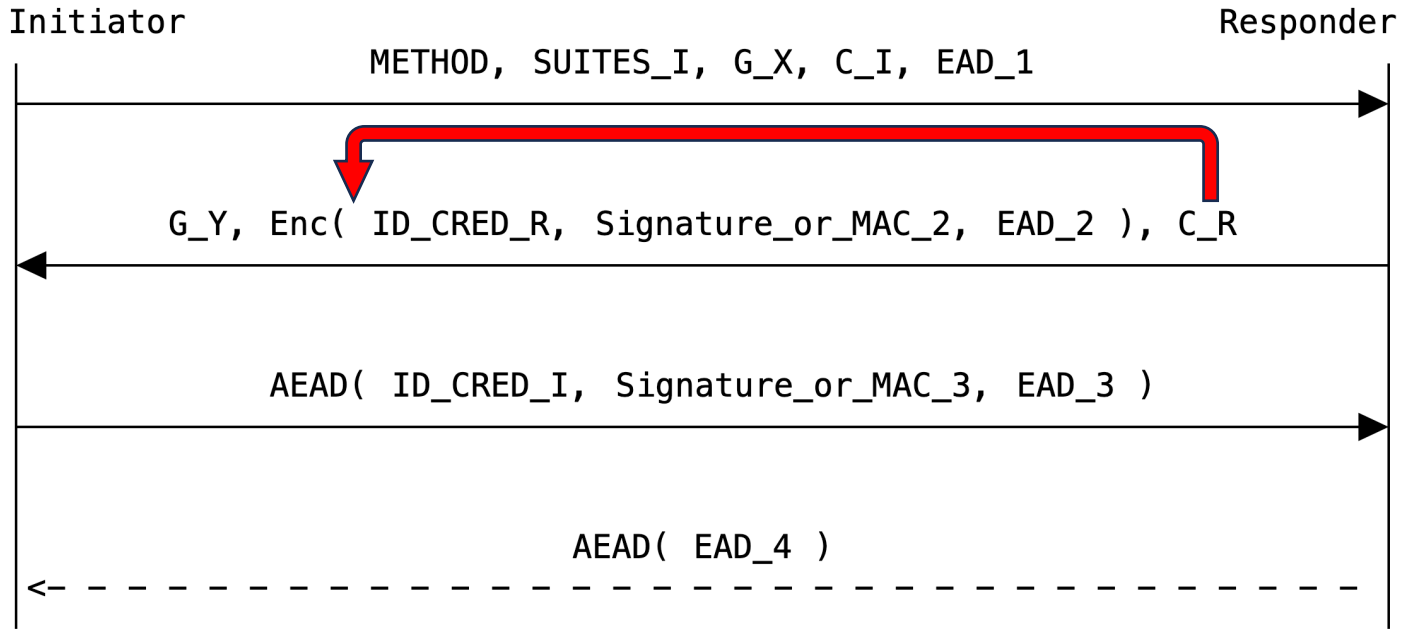
- Since IETF 116
  - edhoc-20
    - AD review
    - Clean up

- Next step
  - Last Call

edhoc-19 → edhoc-20

- Main changes:
  - Encryption of C_R in message_2
  - New error code for unknown referenced credential (Section 6.4)
- Minor changes
  - Error code 0 (success) explicitly reserved
  - Message deduplication moved from appendix to body (Section
  - Terminology
    - protocol run / exchange -> session
    - discontinued -> aborted
  - Clarifications, in particular
    - when to derive application keys
    - the role of the application for authentication
  - Security considerations for kccs and kcwt
  - Updated references

Encryption of C_R



TH_2 = H(G_Y, C_R, H(message_1))

TH_3 = H(TH_2, PLAINTEXT_2, CRED_R)

Contains C_R

- Connection identifiers C_I and C_R facilitate the retrieval of protocol state
- Change: C_R moved in under Enc( )
  - Prepended C_R (if used) still in plaintext
  - Implied change to transcript hash TH_2
  - TH_3 unchanged

Error Codes

— Error codes defined to enable automated remediation

ERR_CODE	ERR_INFO Type	Description
0		This value is reserved
1	tstr	Unspecified error
2	suites	Wrong selected cipher suite
3	true	Unknown credential referenced

Explicitly reserved

New error code

— New ERR_CODE = 3
— Can be used for indicating that the referenced credential is missing
  — Simplifies the use of credential by value only when needed