



EDHOC + Traces

draft-ietf-lake-edhoc-23

draft-ietf-lake-traces-09

IETF LAKE WG, Interim, Feb 13, 2024

Since IETF 118

- edhoc-23:
 - Include the connection identifier C_R in MAC_2 (following slides)
 - Clarification of use of deterministic CBOR
 - Check of all-zero output of in X25519/448
- traces-09:
 - new test vectors reflecting the change in MAC_2

Include C_R in MAC_2

1(2)

— Recap change made when we added encryption of C_R : Before $\rightarrow$ After

— $message_2 =$ $G_Y, \text{Enc}(ID_CRED_R, \text{Signature_or_MAC}_2, EAD_2), C_R \rightarrow$
 $G_Y, \text{Enc}(C_R, ID_CRED_R, \text{Signature_or_MAC}_2, EAD_2)$

— In other words:

— $PLAINTEXT_2 =$ $ID_CRED_R, \dots \rightarrow$
 $C_R, ID_CRED_R, \dots$

— Consequential change:

— $TH_2 =$ $H(G_Y, C_R, H(message_1)) \rightarrow$
 $H(G_Y, H(message_1))$

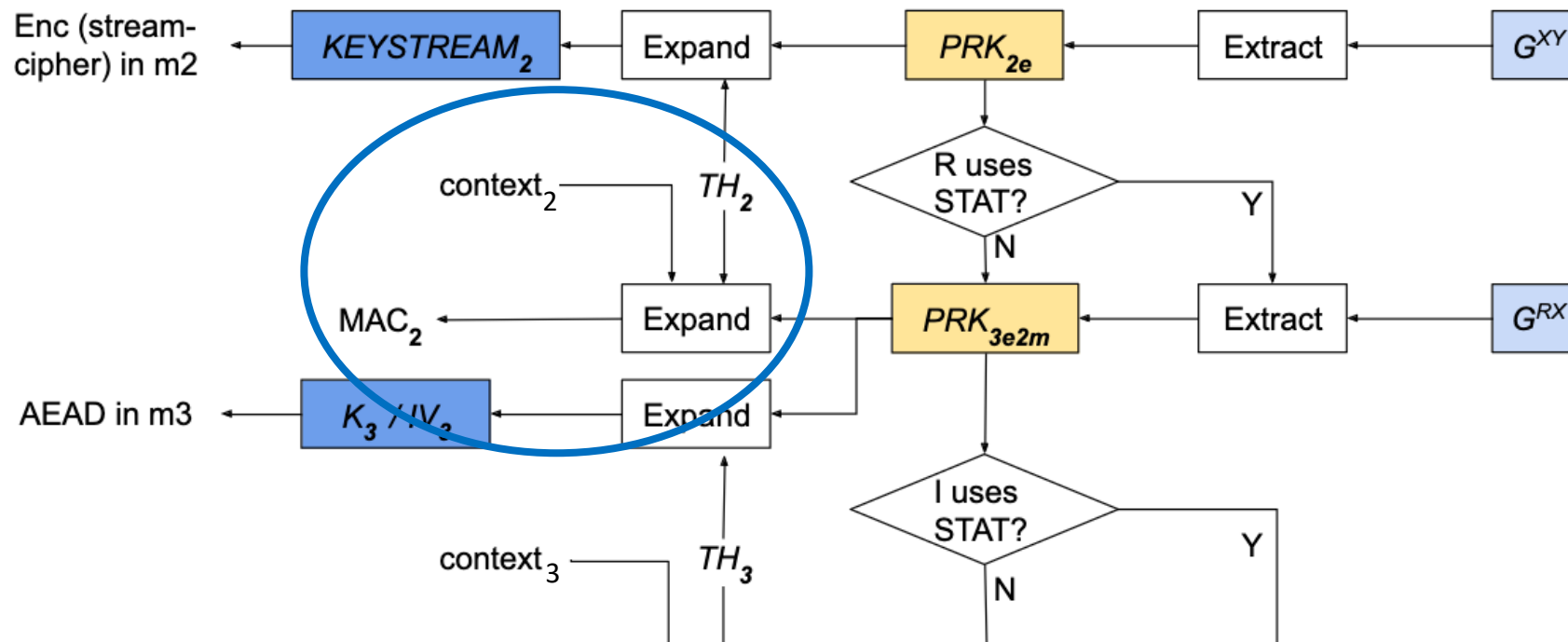
— $TH_3 =$ $H(TH_2, PLAINTEXT_2, CRED_R)$ (unchanged)

— Before encryption of C_R , TH_2 was dependent of C_R

— After encryption of C_R , TH_3 was dependent of C_R (because of $PLAINTEXT_2$)

Include C_R in MAC_2

2(2)



- So, after encryption of C_R , C_R was not covered by MAC_2
- Not a major issue, connection ids only facilitate the retrieval of protocol state
- But undesirable since application may take actions after message₂
- Fixed in -23: included C_R in $context_2$
- Thanks to Loïc Ferreira!

Next steps

- Wait for RFC Editor
- Currently both drafts are in RFC Editor state "RFC-EDITOR"
 - "Awaiting final RFC Editor review before AUTH48"