EDHOC PSK-based authentication method draft-lopez-lake-edhoc-psk-02

Elsa Lopez-Perez, Inria

Göran Selander, Ericsson

John Preuß Mattsson, Ericsson

Rafael Marin-Lopez, University of Murcia

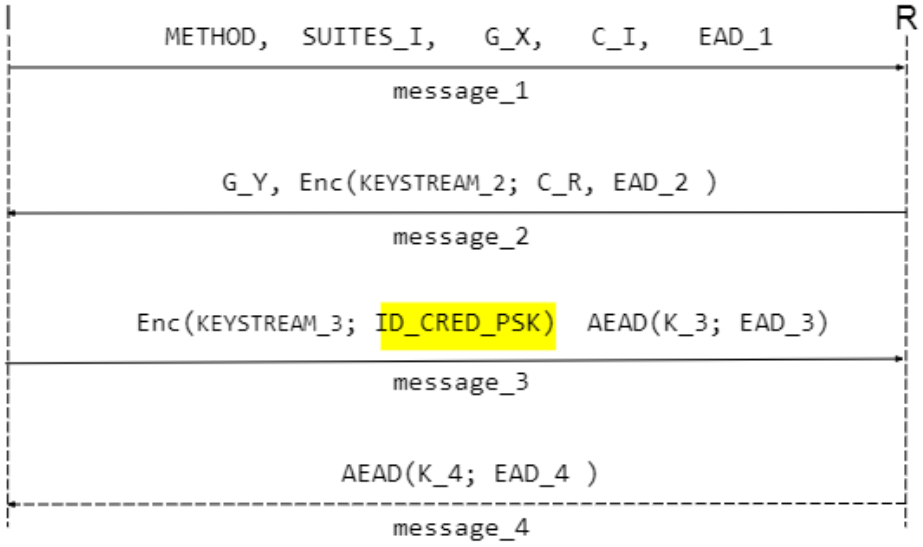
LAKE @ IETF 121 – 4/11/2024

Status

- Goal of the presentation
  - Present the current status of the draft.
  - Preliminary results of EDHOC PSK authentication with CryptoCell310
    - Added fourth message in PSK2 for mutual authentication

PSK Authentication for EDHOC [1]

- ID_CRED_PSK is sent encrypted in message 3
- No MAC_2 in message 2
- message 3 is a concatenation of two ciphertexts
- External_aad in AEAD in message 3 includes ID_CRED_PSK
- Message 4 remains the same but a fourth message is needed for Responder's authentication.



[1] draft-lopez-lake-edhoc-psk-01 - EDHOC PSK authentication (ietf.org)

Key schedule for EDHOC-PSK

PRK_3e2m = PRK_2e

PRK_4e3m = EDHOC_Extract(SALT_4e3m, CRED_PSK)

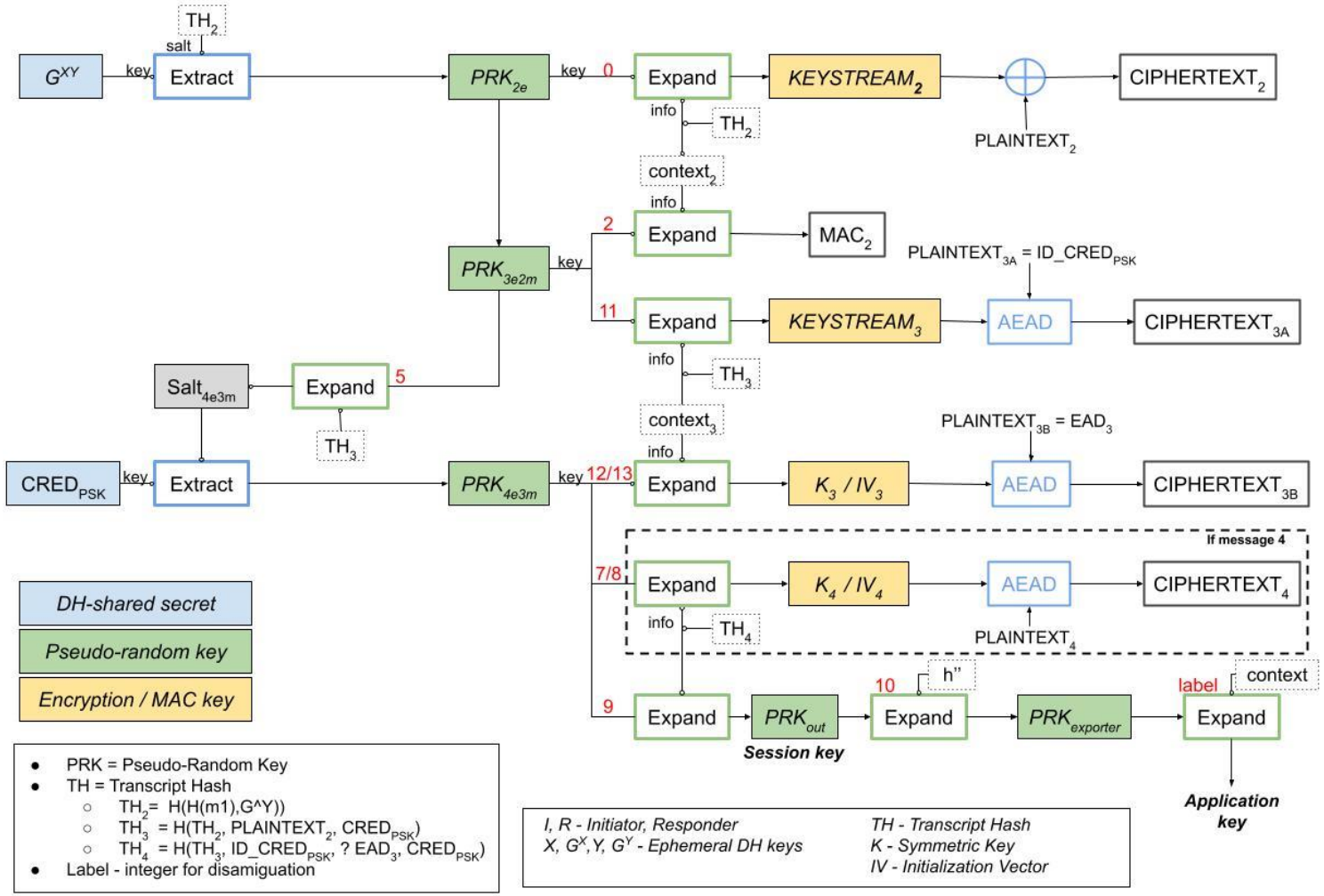
KEYSTREAM_3 = EDHOC_KDF(PRK_3e2m, TBD, TH_3, key_length)

K_3 = EDHOC_KDF(PRK_4e3m, TBD, TH_3, key_length)

IV_3 = EDHOC_KDF(PRK_4e3m, TBD, TH_3, iv_length)

TH_3 = H(TH_2, PLAINTEXT_2, CRED_PSK)

TH_4 = H(TH_3, ID_CRED_PSK, ? EAD_3, CRED_PSK)



Metrics

(comparison with previous variant)

NOTE:
- Crypto Cell 310 as backend
- Embassy framework

Message size:

Method	Message_1	Message_2	Message_3	Message_4	Total
PSK1	39	44	10	-	93
PSK2	38	35	15	9	97

Number of operations:

Method	Message_1	Message_2	Message_3	Message_4	Total
PSK1	1 Asym (DH)	1 Asym 2 Sym	1 Sym	1 Sym	2 Asym 4 Sym
PSK2	1 Asym (DH)	1 Asym 1 Sym	2 Sym	1 Sym	2 Asym 4 Sym

Metrics

(comparison with previous variant and StatStat method)

NOTE:
- Crypto Cell 310 as backend
- Embassy framework

Handshake duration and energy consumption:

Method Initiator	Avg. current (mA)	Time (ms)
PSK1	12.0	578
PSK2	13.0	485
STAT	12.9	519

Method Responder	Avg. current (mA)	Time (ms)
PSK1	8.5	266
PSK2	8.5	266
STAT	8.9	306

Memory consumption:

Method Initiator	Flash memory (kB)	Stack usage (kB)
PSK1	15.5	31
PSK2	17.8	31
STAT	18.8	31

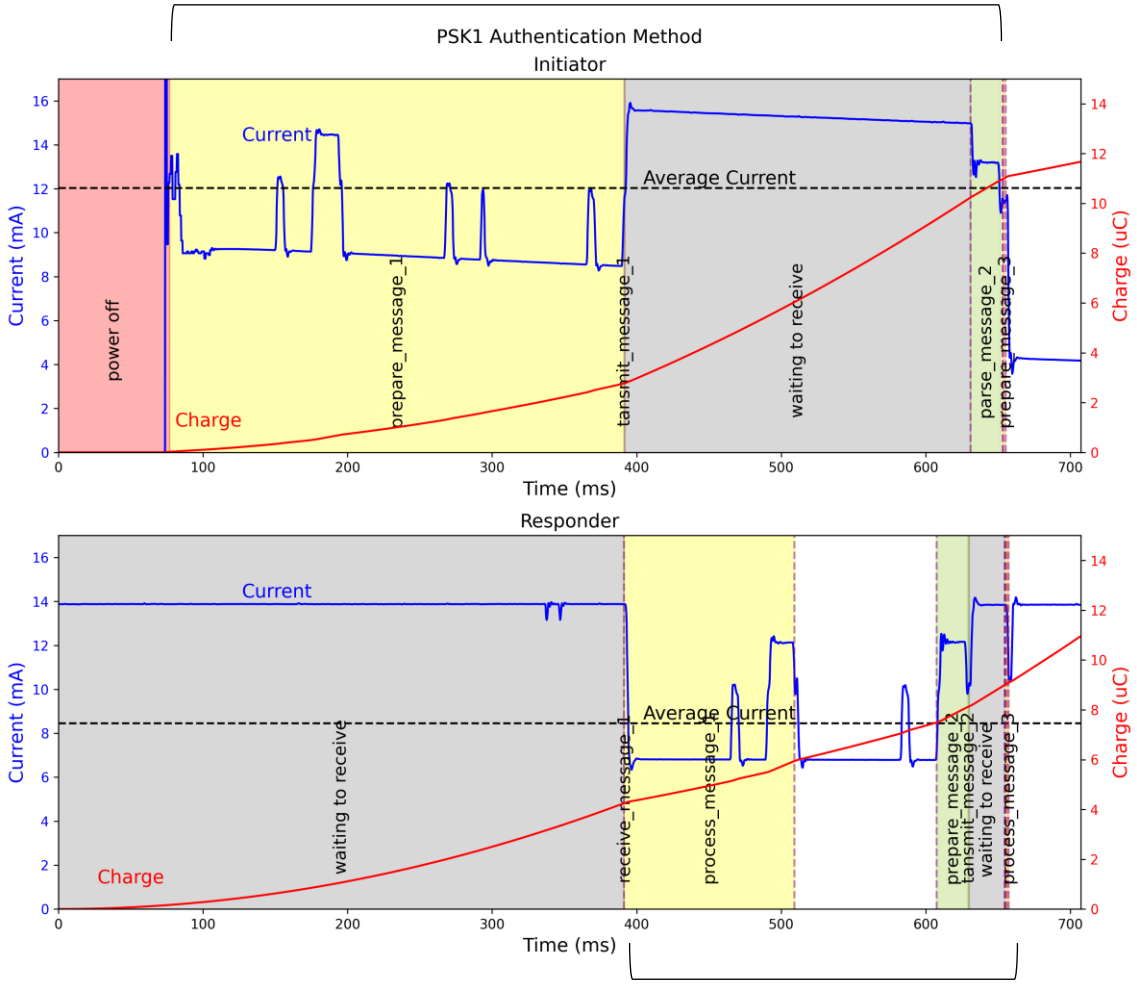
Method Responder	Flash memory (kB)	Stack usage (kB)
PSK1	17	30
PSK2	18	30
STAT	19	30

Metrics

(comparison with previous variant)

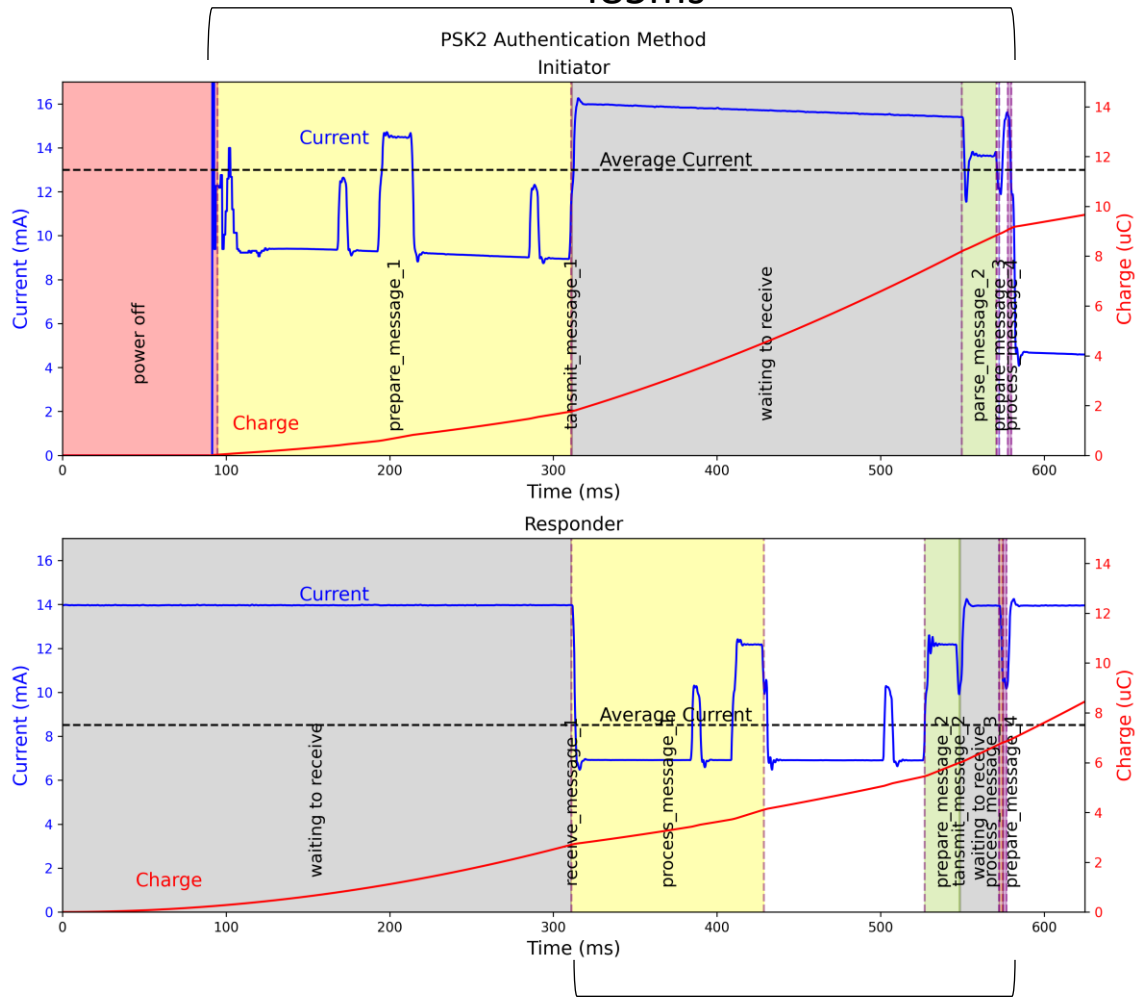
NOTE:
- Crypto Cell 310 as backend
- Embassy framework

587ms



266ms

485ms



266ms

Next Steps

- Call for adoption in the Working Group
- Integration in lakers Rust implementation

Thank you!