EDHOC PSK-based authentication method draft-lopez-lake-edhoc-psk-01

Elsa Lopez-Perez, Inria

Göran Selander, Ericsson

John Preuß Mattsson, Ericsson

Rafael Marin-Lopez, University of Murcia

LAKE @ IETF 120 – 23/7/2024

Status

- Published -01 on 4 July 2024
- Goal of the presentation
  - Present the current status and the two proposed variants for PSK-based authentication in EDHOC

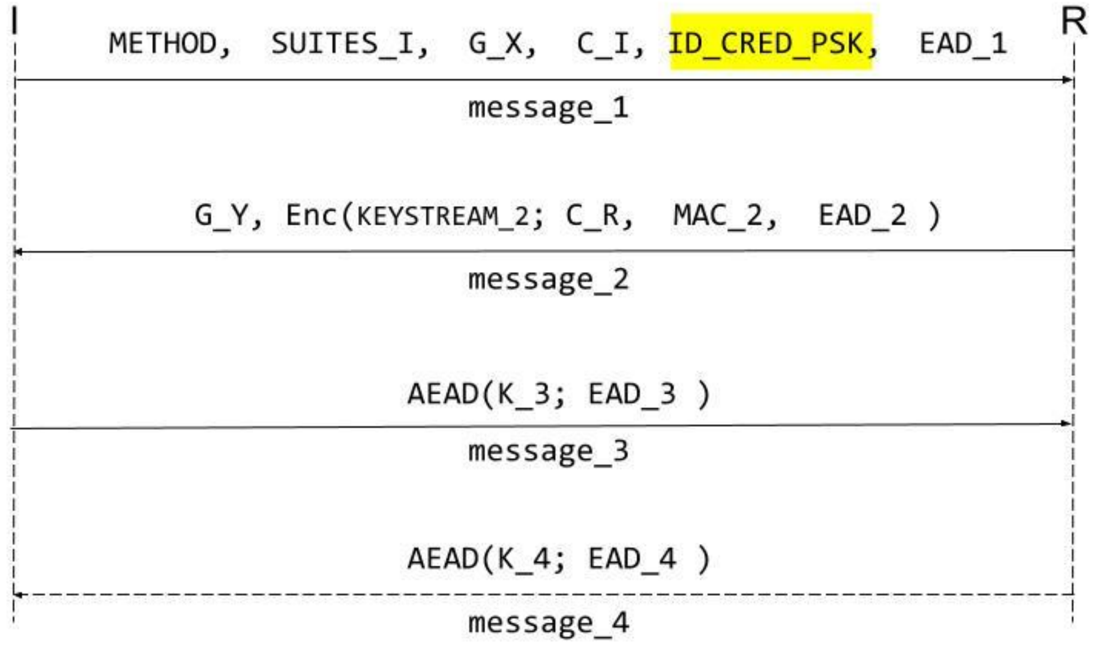
Motivation

- Working Group Charter alignment:
  - PSK authentication is a key objective in the IETF LAKE WG Charter
- Leveraging existing infrastructure:
  - Billions of SIM cards deployed worldwide.
  - Cost-effective: update software rather than replace hardware.
  - Preserves the investments in current technology.
- Gradual transition:
  - EDHOC + PSK supports adoption by older devices.
  - Bridges the gap between current and future security protocols.
  - Ensures backward compatibility while moving forward.

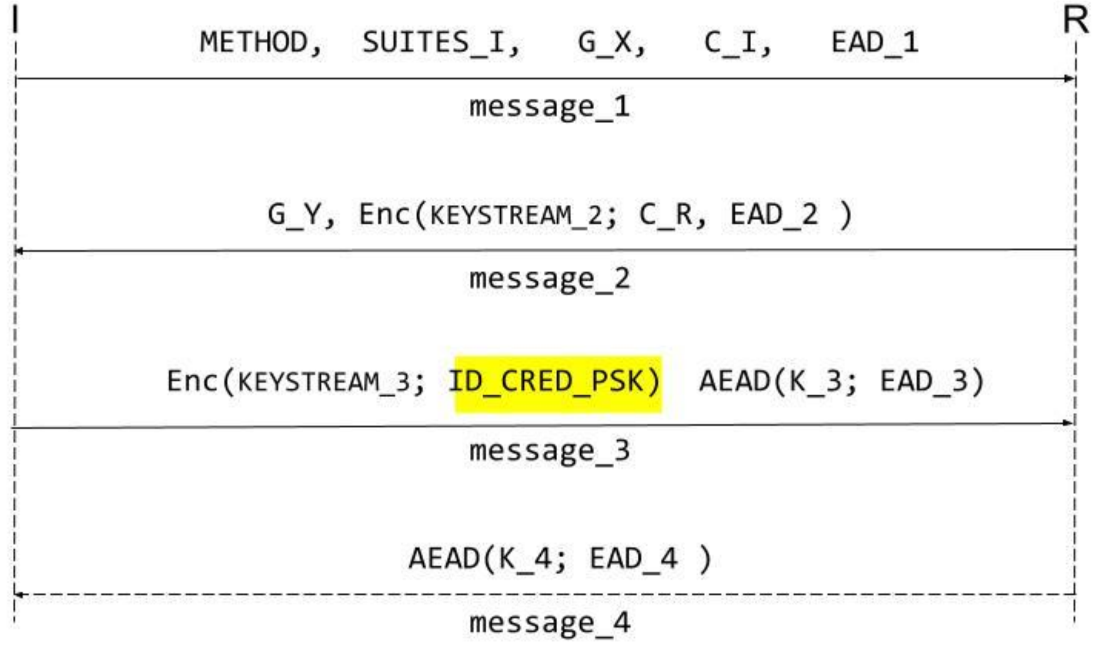
EDHOC with PSK offers a practical, cost-effective path to enhance IoT security while utilizing existing infrastructure

Proposed solutions

VARIANT 1

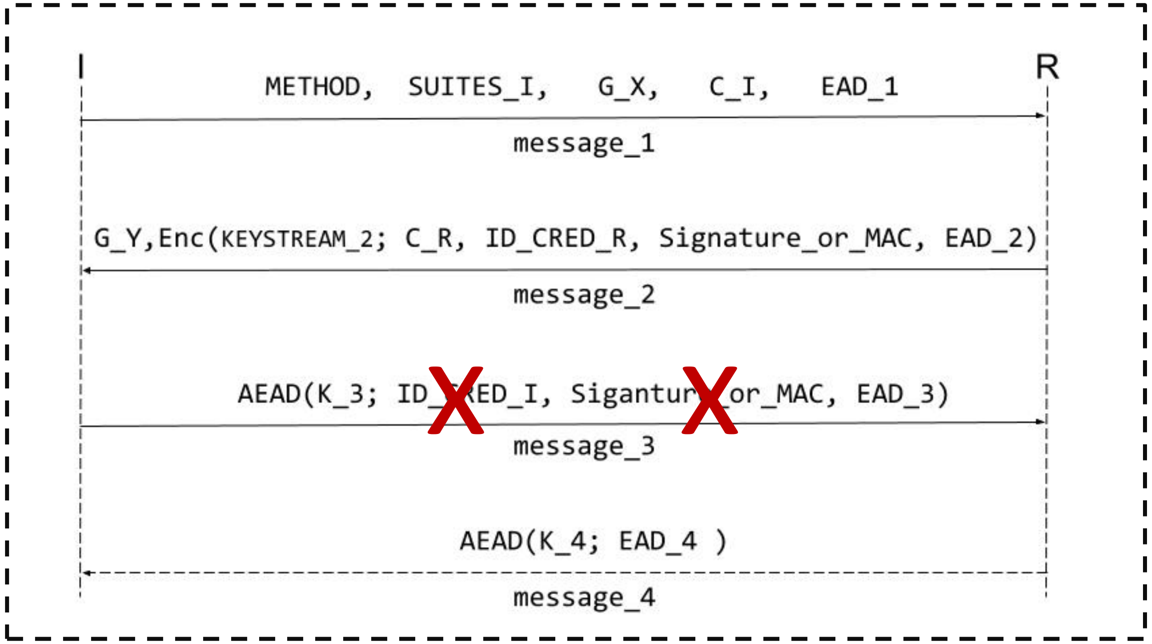


VARIANT 2

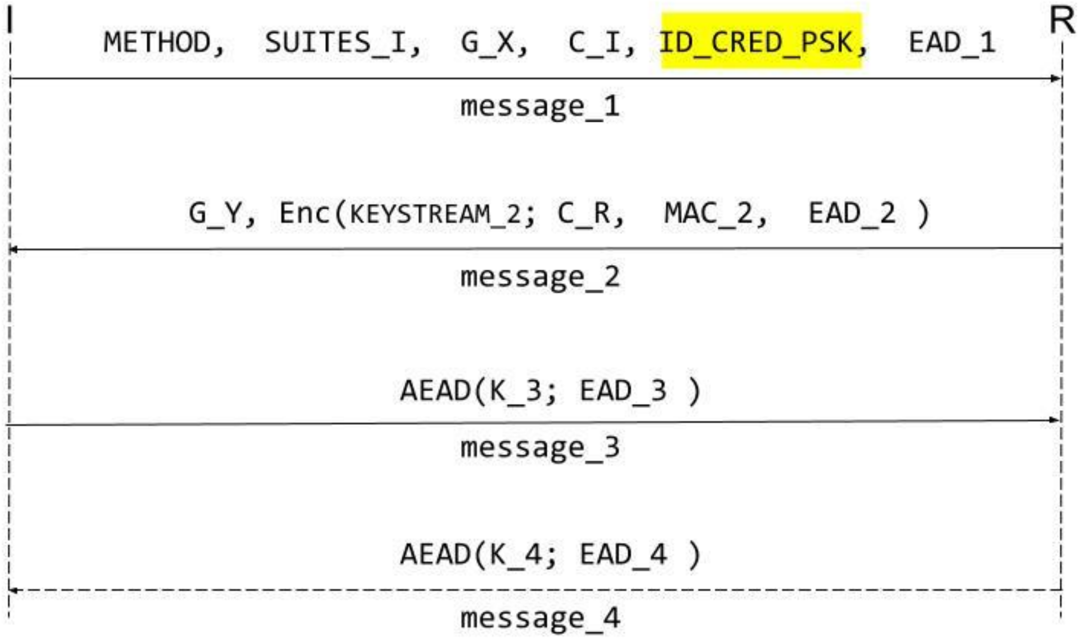


Variant 1: message flow

- Include ID_CRED_PSK in message_1 in cleartext.
- message_2 remains the same.
- Remove MAC_3 in message_3
- message_4 remains the same



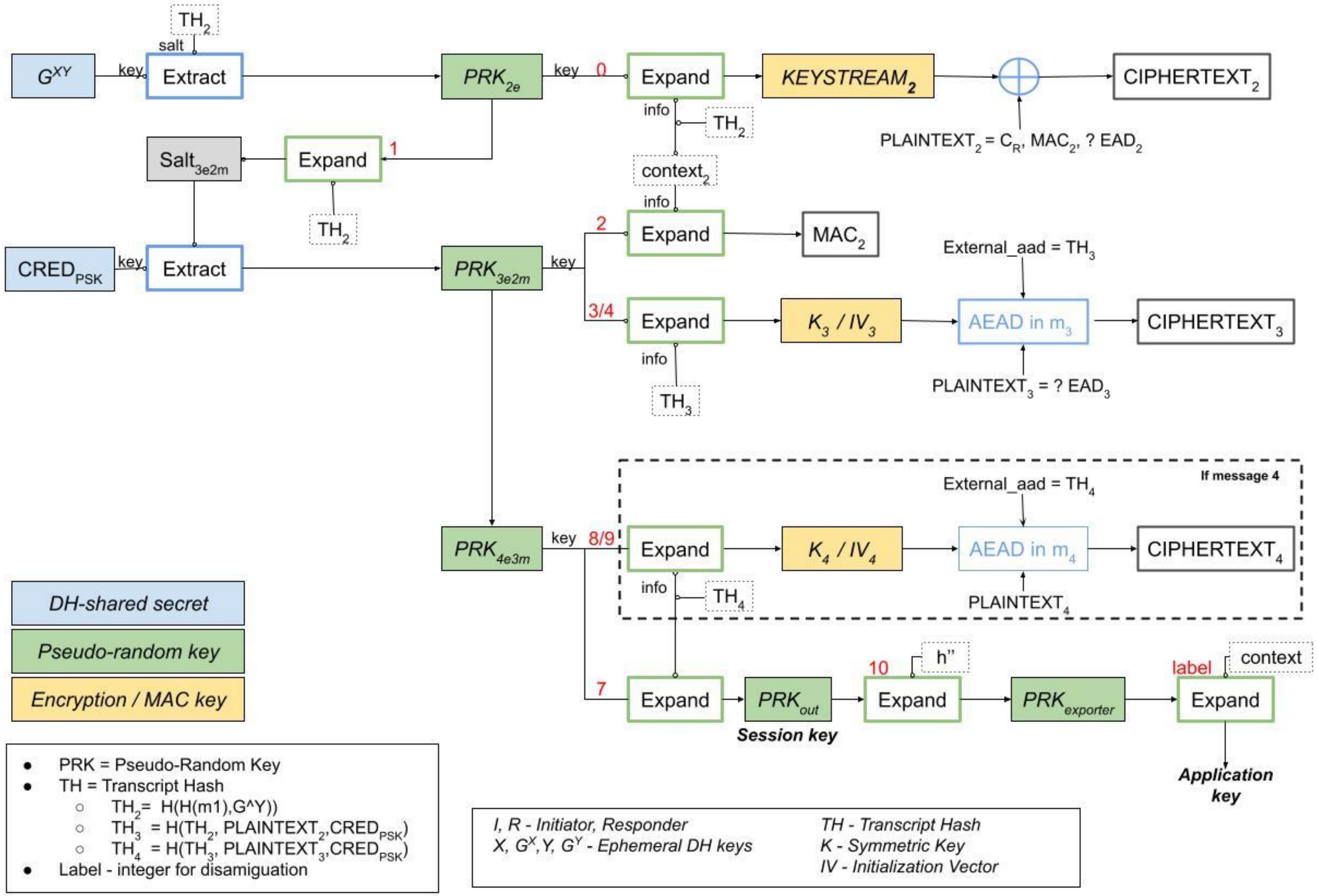
EDHOC message flow, as in RFC 9528



EDHOC PSK-authentication Variant 1 message flow

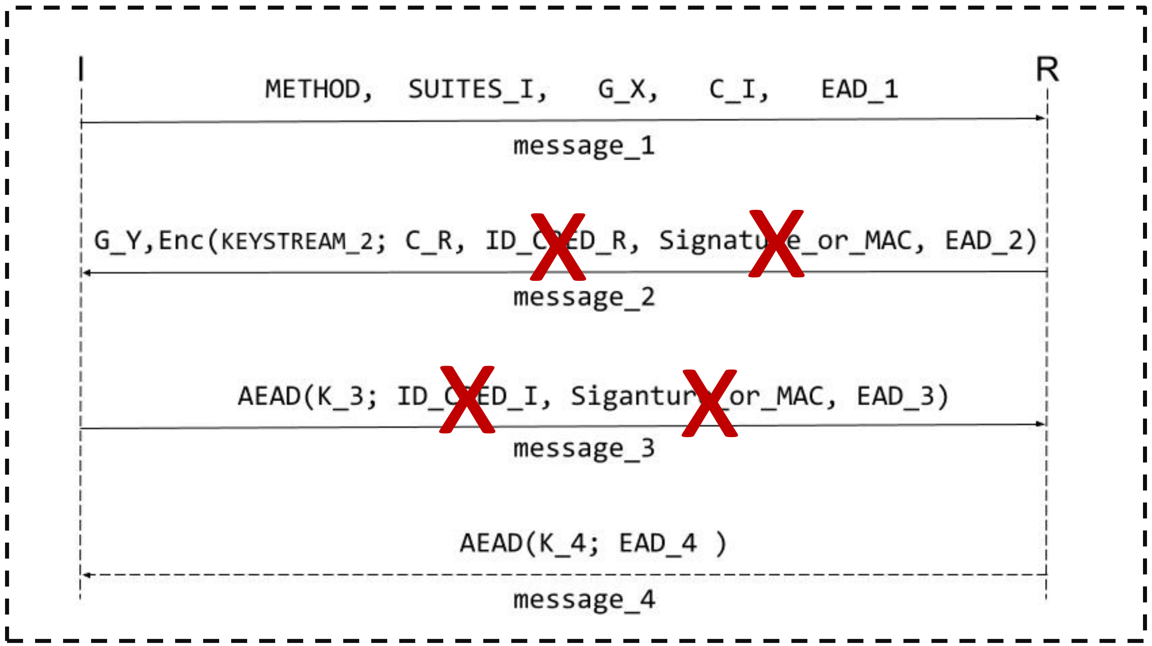
Variant 1: key schedule

- PRK_3e2m = EDHOC_Extract(salt3e_2m,
  CRED_PSK)
- PRK_4e3m = PRK_3e2m
- MAC_2 = EDHOC_KDF(PRK_3e2m, 2,
  context_2, mac_length_2)
- K_3 = EDHOC_KDF(PRK_4e3m, TBD, TH_3,
  key_length)
- IV_3 = EDHOC_KDF(PRK_4e3m, TBD,
  TH_3, iv_length)
- context_2 = <<C_R, ID_CRED_PSK, TH_2,
  CRED_PSK, ? EAD_2>>
- TH_3 = H(TH_2, PLAINTEXT_2, CRED_PSK)
- TH_4 = H(TH_3, PLAINTEXT_3, CRED_PSK)

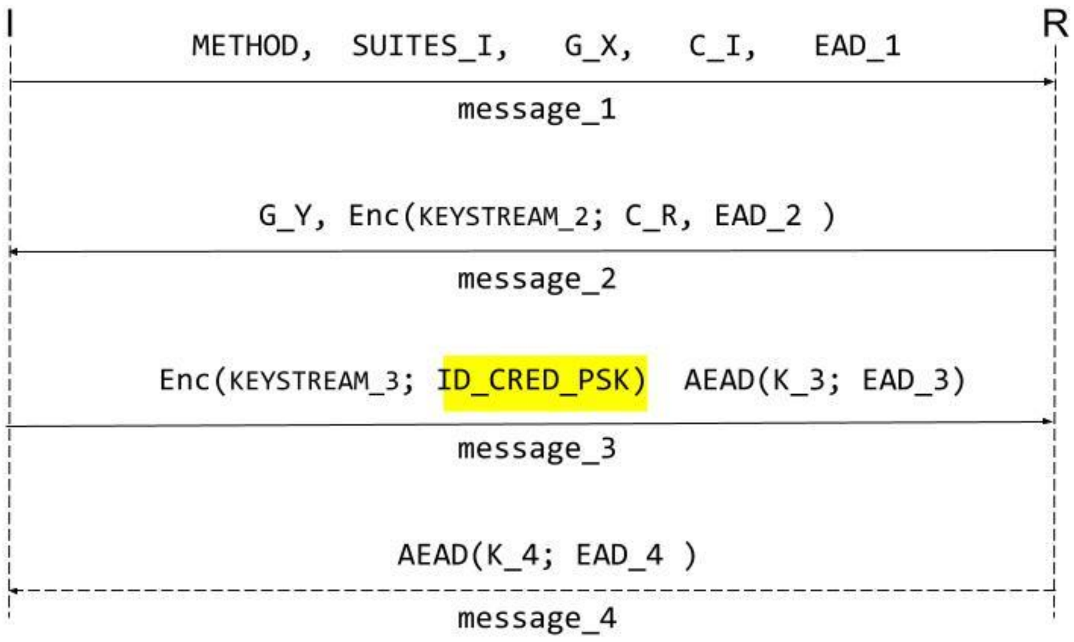


Variant 2: message flow

- Include ID_CRED_PSK in message_3 encrypted.
- Remove MAC_2.
- Message 3 consists of two ciphertexts concatenated:
  - Ciphertext_3a containing ID_CRED_PSK encrypted with keystream_3.
  - Ciphertext_3b containing AEAD with EAD_3.
- Remove MAC_3 in message_3
- External_aad in AEAD in message_3 includes the ID_CRED_PSK
- message_4 remains the same. It is needed for Repsonder's authentication (it can be replaced by an OSCORE message)



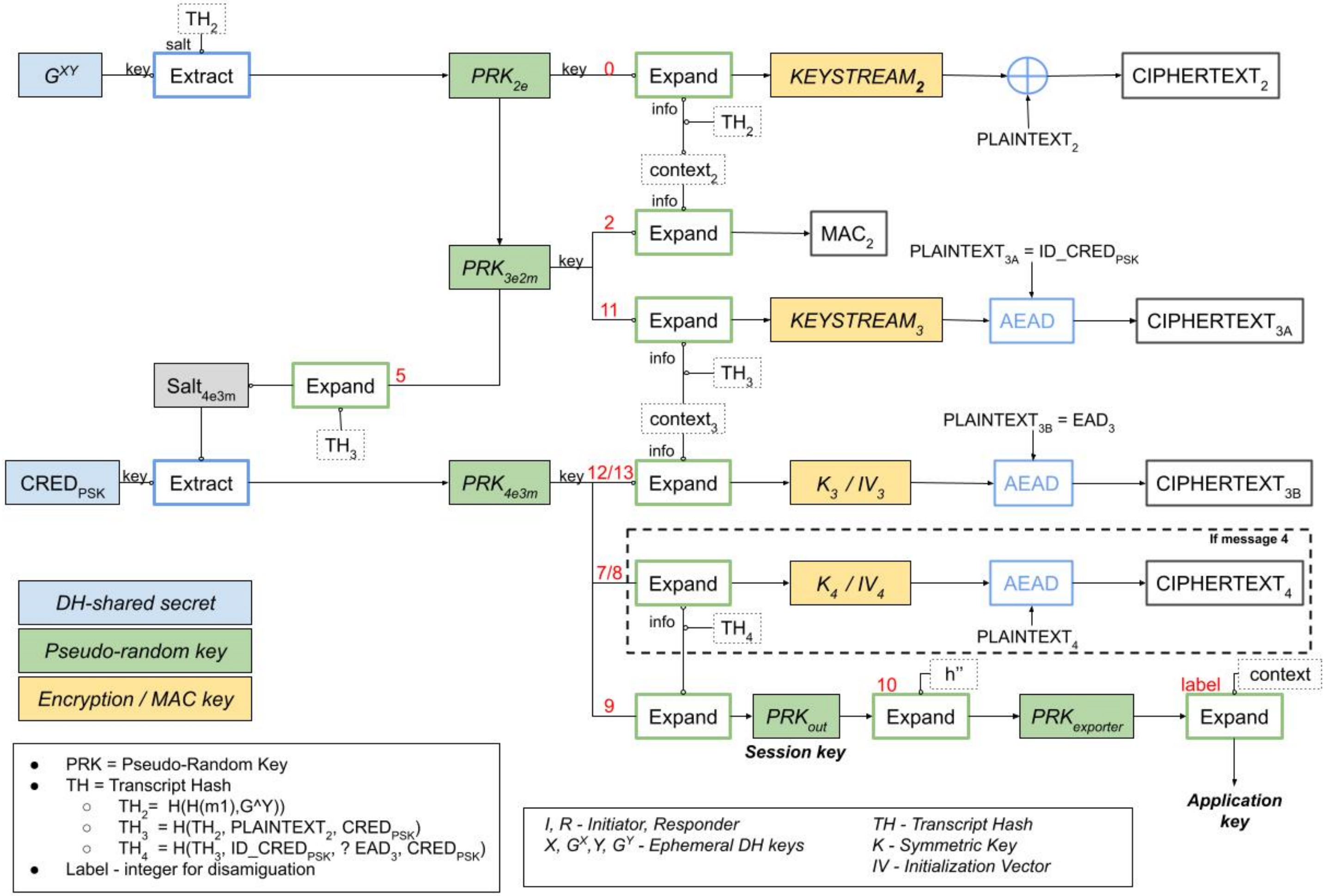
EDHOC message flow, as in RFC 9528



EDHOC PSK-authentication Variant 2 message flow

Variant 2: key schedule

- 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)



Comparison of Variant 1 and Variant 2

Aspect	Variant 1	Variant 2
Privacy	Lower: ID_CRED_PSK sent in the clear	Higher: ID_CRED_PSK encrypted in message_3
Identity Protection	Initiator exposed from message_1. Both I and R are vulnerable against passive and active attackers	Initiator protected until message_3. I and R's identities are protected against passive attackers.
Authentication Timing	Message_1	Message_3
Computational Efficiency	Slighlty higher (no encryption of ID_CRED_PSK)	Slightly lower (Encryption of ID_CRED_PSK)
Early access control	Possible from message_1	Possible from message_3
DoS Attack Vulnerability	Lower due to earlier authentication	Potentially higher
Resource allocation	Fewer resources allocated before authentication	More resources allocated before authentication
Key derivation timing	Earlier	Later
Completeness	Complete: achieves mutual authentication + implicit key authentication without message_4	A fourth message is needed for mutual authentication and key confirmation
Number of messages	Message_4 is only used for key confirmation (explicit key authentication) 3 + optional	A fourth message is needed for R's authentication and key confirmation 4
Num. of operations	2 Asym. 4 Sym.	2 Asym. 4Sym.

Next Steps

- Implementation of EDHOC_PSK in lakers
  - https://github.com/openwsn-berkeley/lakers
  - Merge PSK with the already supported StatStat method
- Evaluation and comparison of Variant 1 and Variant 2
  - Security
  - Privacy
  - Number of operations
  - Energy consumption
  - Latency
  - Memory consumption

Thank you!