

EDHOC with Pre-Shared Key (PSK) Authentication

draft-ietf-lake-edhoc-psk-07

Elsa Lopez-Perez, Inria

Göran Selander, Ericsson

John Preuß Mattsson, Ericsson

Rafael Marin-Lopez, University of Murcia

Francisco Lopez-Gomez, University of Murcia

IETF-125 – 16/03/2026

Status

- Correction of the Test Vectors
- Update of Security Properties after Formal Analysis
- Integration of EDHOC-PSK into *lakers*

#Issue1: Test Vectors

- We found an error in the computation of TH_4
- We redefined the test vectors and verified them using **two implementations** (Rust and C)

PRK_4E3M

EDHOC_Exporter(SALT_4e3m, **PSK**)

These values were missing
in the test vectors

TH_4

H(TH_3, ID_CRED_PSK, PLAINTEXT_3B, **CRED_I, CRED_R**)

External_aad in CIPHERTEXT_3B

<< ID_CRED_PSK, TH_3, **CRED_I, CRED_R** >>

#Issue2: Updates after Formal Analysis

Formal Verification of EDHOC-PSK: A Symbolic Approach with SAPIC+. Elsa Lopez Perez, Thomas Watteyne, Cristina Onete, Clement Papon, Dhekra Mahmoud, Pascal Lafourcade, Mališa Vučinić. **ACM ASIA Conference on Computer and Communications Security (ASIACCS)**, Bangalore, India, 1-5 June 2026.

Property	Lemma	Basic		LeakShare		LeakSKey		LeakShare & LeakSKey		PQ (SNDL)	
		Result	Time (s)	Result	Time (s)	Result	Time (s)	Result	Time (s)	Result	Time (s)
Authentication and Key Agreement	full_agreement_IR	✓	46.13	✓	47.30	✓	44.28	✓	42.93	✓	5.85
	full_agreement_RI	✓	45.11	✓	50.77	✓	45.97	✓	46.57	✓	7.581
Confidentiality	secretR_psk	✓	34.71	✓	48.15	✓	40.46	✓	44.07	✓	15.41
	secretI_psk	✓	41.37	✓	45.62	✓	43.24	✓	45.47	✓	10.66
	pfs	✓	107.58	✓	118.58	✓	116.05	✓	120.19	✗	-
	secret_psk	✓	73.81	✓	65.94	✓	67.37	✓	71.77	✓	18.11
Identity Protection	anonymity_I_active	✓	22.30	✓	81.45	✓	19.19	✓	84.61	✓	337.55
	anonymity_R_active	✓	24.63	✓	126.95	✓	21.94	✓	122.23	✓	569.38
	unlinkability_I_active	✗	-	✗	-	✗	-	✗	-	✗	-
	unlinkability_I_passive	✓	5.18	✓	7.90	✓	5.84	✓	8.25	✓	93.20
	unlinkability_R_active	✗	-	✗	-	✗	-	✗	-	✗	-
	unlinkability_R_passive	✗	-	✗	-	✗	-	✗	-	✗	-

Table 3: Summary of automated verification results of EDHOC-PSK across adversary capabilities. The classic results are computed using Tamarin. The Post-Quantum (PQ) results are computed using ProVerif.

#Issue2: Active Unlinkability Attack on Initiator Identity

- **Assumption:** Attacker is an active MitM between Initiator and Responder.
- **Attack:**
 - Initiator sends message_3, which contains the encrypted identity ID_CRED_PSK.
 - The attacker intercepts and modifies the ciphertext of ID_CRED_PSK.
 - The modified message_3 is forwarded to the Responder.
 - The Responder attempts to decrypt and verify the message.
 - Because the ciphertext was modified, AEAD verification fails... However, the observable failure behavior may depend on whether the manipulated identity corresponds to a valid credential:
 - different error types (e.g., unknown credential vs authentication failure)
 - timing differences during credential lookup

The attacker can test candidate identities and observe how the Responder fails.

#Issue3: Integration of EDHOC-PSK into *lakers*

- We are working on the integration of EDHOC-PSK into the *lakers* implementation of EDHOC (Rust)

Next steps

- Working Group Last Call?
- Address final comments/issues

Thank you!