# EDHOC with Pre-Shared Key (PSK) Authentication draft-ietf-lake-edhoc-psk-06

Elsa Lopez-Perez, Inria

Göran Selander, Ericsson

John Preuß Mattsson, Ericsson

Rafael Marin-Lopez, University of Murcia

Francisco Lopez-Gomez, University of Murcia

IETF-124 – 06/11/2025

# Status

- Correction of the Test Vectors
- Definition of Security Properties
- Call for Formal Analysis issued

# #Issue1: Test vectors

- Recap…
  - We define TWO credentials (CRED_I, CRED_R), containing the same symmetric key (PSK), and one single identifier (ID_CRED_PSK)

CRED_I

Identity 1

PSK

```
{                                              /CCS/
  2                                            /sub/
  8 : {                                        /cnf/
    1 : {                                      /COSE_Key/
      1 : 4,                                   /kty/
      2 : h'0f',                               /kid/
      -1 : h'50930FF462A77A3540CF546325DEA214'  /k/
    }
  }
}
```

CRED_R

Identity 2

PSK

```
{                                              /CCS/
  2 :                                          /sub/
  8 :                                          /cnf/
    1                                          /COSE_Key/
      1 : 4,                                   /kty/
      2 : h'0f',                               /kid/
      -1 : h'50930FF462A77A3540CF546325DEA214'  /k/
    }
  }
}
```

  - Changes in the key derivation of PRK_4e3m and transcript hash TH_4

| | |
|---|---|
| PRK_4E3M | EDHOC_Exporter(SALT_4e3m, **PSK**) |
| 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** >> |

# #Issue1: Test vectors

- To be compliant with the changes, we redefined the test vectors and verified them using two implementations (Rust and C)

# #Issue2: Security Properties

- We defined a new Section (Section 9) containing the Security Properties that the protocol claims to achieve to allow the formal analysis

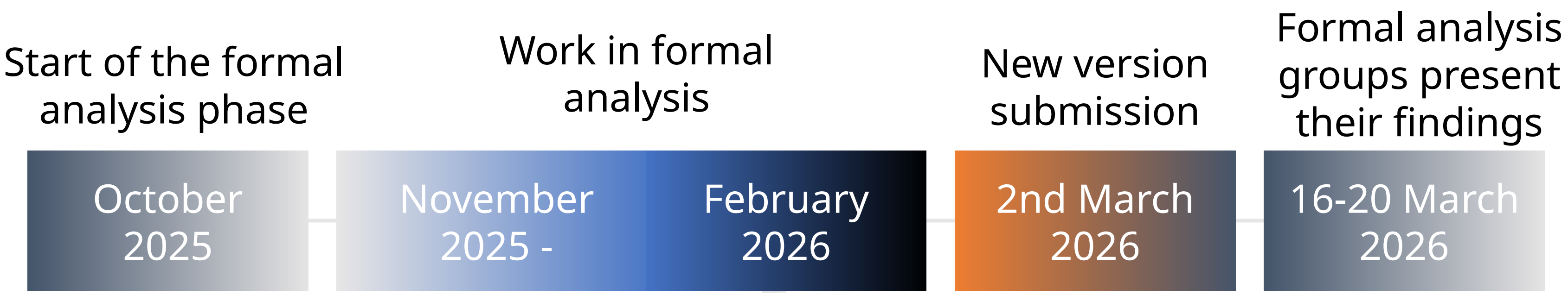
| Security Property | Claim |
|---|---|
| **Identity protection** | EDHOC-PSK protects both I and R against **passive** attackers |
| **Mutual Authentication** | EDHOC-PSK provides **mutual authentication** and **explicit key confirmation** through an additional message that demonstrates possession of the PSK. This may be message_4 or an application message |
| **Protection of EAD** | Unchanged with respect to EDHOC RFC 9528: EDHOC-PSK ensures the confidentiality and integrity of External Authorization Data (EAD). |
| **Cryptographic strength** | EDHOC-PSK provides **a minimum of 64-bit security** against online brute force attacks and, provided the PSK has sufficient entropy, a minimum of 128-bit security against offline brute force attacks |

# #Issue2: Security Properties

| Security Property | Claim |
| --- | --- |
| **Downgrade Protection** | Unchanged with respect to EDHOC RFC9528 |
| **Post Quantum Considerations** | - EDHOC-PSK derives authentication and session keys from a symmetric PSK -> quantum resistance<br>- EDHOC-PSK + quantum-resistant Key Encapsulation Mechanism (KEM) -> identity protection and PFS even against quantum-capable attackers. |
| **Confidentiality** | The protocol ensures key indistinguishability by relying on the security of the PSK and the ephemeral key shares |
| **Perfect Forward Secrecy** | Even if the PSK is compromised, an attacker is unable to decrypt the past sessions. |

# #Issue3: Call for Formal Analysis

- A call for formal analysis was issued -> check whether the claimed security properties hold in the symbolic and computational security models.




- Three groups interested
  - 1 Computational Proof: Loic Ferriera (Orange)
  - 2 Symbolic Analysis (Tamarin and SAPIC+): Elsa Lopez Perez (Inria Paris) and Vaishnavi Sundararajan (IIT Delhi)

# Thank you!