

EDHOC with PSK-based authentication

John Preuß Mattsson, Ericsson

EDHOC with PSK-based authentication

- EDHOC and traces published as RFC 9528 and 9529.
- EMU WG charter is updated to add EAP-EDHOC.
 - EAP-EDHOC would like EDHOC with PSK-based authentication for resumption.
- Plan is to add a new method with PSK authentication as well as a new exporter label to derive a resumption PSK. Two identified issues:
 - PSK authentication has very bad privacy properties.
 - PSK key exchange has very bad security properties.



Old school keys from Uruguay by Addison Berry (CC BY-NC-SA 2.0 Deed)
<https://www.flickr.com/photos/add1sun/5544756684>

EDHOC with PSK-based authentication

- Likely need to differentiate between initial “handshake” and resumption.
 - Require ECDHE in initial handshake.
 - Allow PSK key exchange in resumption based on time and data?
(SSH e.g., requires “ECDHE” every 1 hour or 1 GB).
 - Derive a new resumption PSK for each resumption.
 - Privacy for initial “handshake” is a harder problem.
 - Forbid external PSKs?
 - Require that external PSK identifiers are only used once?
 - Trial decryption by Responder?
 - Require that Initiator has Responder’s ECDHE key and to ECIES encryption of PSK identifier.



Old school keys from Uruguay by Addison Berry (CC BY-NC-SA 2.0 Deed)
<https://www.flickr.com/photos/add1sun/5544756684>