EDHOC

draft-ietf-lake-edhoc-20
https://github.com/lake-wg/edhoc

IETF 117, LAKE WG, July 24, 2023

Photo by kallerna licensed under Creative Commons
Status

— Since IETF 116
  — edhoc-20
    — AD review
    — Clean up

— Next step
  — Last Call
edhoc-19 → edhoc-20

— Main changes:
  — Encryption of C_R in message_2
  — New error code for unknown referenced credential (Section 6.4)
— Minor changes
  — Error code 0 (success) explicitly reserved
  — Message deduplication moved from appendix to body (Section
— Terminology
  — protocol run / exchange -> session
  — discontinued -> aborted
— Clarifications, in particular
  — when to derive application keys
  — the role of the application for authentication
— Security considerations for kccs and kcwt
— Updated references
Encryption of C_R

— Connection identifiers C_I and C_R facilitate the retrieval of protocol state
— Change: C_R moved in under Enc()
  — Prepended C_R (if used) still in plaintext
  — Implied change to transcript hash TH_2
  — TH_3 unchanged

TH_2 = H( G_Y, C_R, H(message_1) )
TH_3 = H(TH_2, PLAINTEXT_2, CRED_R)
Contains C_R
## Error Codes

- Error codes defined to enable automated remediation

<table>
<thead>
<tr>
<th>ERR_CODE</th>
<th>ERR_INFO Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>This value is reserved</td>
</tr>
<tr>
<td>1</td>
<td>tstr</td>
<td>Unspecified error</td>
</tr>
<tr>
<td>2</td>
<td>suites</td>
<td>Wrong selected cipher suite</td>
</tr>
<tr>
<td>3</td>
<td>true</td>
<td>Unknown credential referenced</td>
</tr>
</tbody>
</table>

- New ERR_CODE = 3
- Can be used for indicating that the referenced credential is missing
  - Simplifies the use of credential by value only when needed

Explicitly reserved

New error code