Clarifications and Updates on using Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)

draft-tiloca-lpwan-8824-update-00

Marco Tiloca, RISE
Laurent Toutain, IMT Atlantique
Ivan Martinez, IMT Atlantique

IETF 116 meeting – Yokohama – March 30th, 2023
Motivation

› RFC 8824 – SCHC compression of CoAP headers (June 2021)
  – Covering all the CoAP options defined at the time (except for Hop-Limits)
  – CoAP messages unprotected or protected end-to-end with OSCORE (RFC 8613)

› Had a close reading with fresh eyes and noticed:
  – Of course, some very recent CoAP options are missing
  – The CoAP payload marker is always *tacitly* “not-sent” (i.e., it’s never in the rules)
  – How does this work with CoAP proxies?
    › No processing workflow, no examples
    › Non trivial to “just figure out” in case OSCORE is used
Contribution

› Proposed update to RFC 8824
  – Clarifications on CoAP options Size1, Size2, Proxy-URI, Proxy-Scheme
    › See Errata at https://www.rfc-editor.org/errata/eid7391
  – Defined SCHC compression for the CoAP option Hop-Limit
  – Defined SCHC compression for recent CoAP options
  – Defined SCHC compression for the updated CoAP option OSCORE
  – Clarified handling of CoAP payload marker 0xFF
    › Both with and without OSCORE end-to-end security
  – Defined SCHC compression with CoAP proxies
    › Both with and without OSCORE end-to-end security

› Approach, design choices and features of SCHC compression are not changed
CoAP options

› Hop-Limit (RFC 8768)
  – TV: empty; MO: "ignore"; CDA: "value-sent"

› Echo and Request-Tag (RFC 9175)
  – TV: empty; MO: "ignore"; CDA: "value-sent"

› Q-Block1 and Q-Block2 (RFC 9177)
  – TV: empty; MO: "ignore"; CDA: "value-sent"

› EDHOC (draft-ietf-core-oscore-edhoc)
  – TV: empty; MO: "equal"; CDA: "not-sent"
CoAP options

› **OSCORE (RFC 8613)**
  – Updated by related documents

› **Defined new flag bits in the first byte**
  – draft-ietf-core-oscore-key-update
  – draft-ietf-core-oscore-groupcomm

› **Defined new, second flag byte**
  – draft-ietf-core-oscore-key-update

› **Defined new fields ‘x’ and ‘nonce’**
  – draft-ietf-core-oscore-key-update

**OSCORE option value**

(when running the KUDOS key update protocol)

CoAP options

---

**OSCORE Flags**

<table>
<thead>
<tr>
<th>Bit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>empty</td>
</tr>
<tr>
<td>1</td>
<td>ignore</td>
</tr>
<tr>
<td>2</td>
<td>value-sent</td>
</tr>
</tbody>
</table>

**OSCORE KidCTX**

<table>
<thead>
<tr>
<th>Bit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>pre-agreed</td>
</tr>
<tr>
<td>1</td>
<td>equal</td>
</tr>
<tr>
<td>2</td>
<td>not-sent</td>
</tr>
<tr>
<td>3</td>
<td>empty</td>
</tr>
<tr>
<td>4</td>
<td>ignore</td>
</tr>
<tr>
<td>5</td>
<td>value-sent</td>
</tr>
<tr>
<td>6</td>
<td>match-mapping</td>
</tr>
<tr>
<td>7</td>
<td>matching-sent</td>
</tr>
</tbody>
</table>

---

draft-tiloca-lpwan-8824-update | IETF 116 meeting – Yokohama | 2023-03-30 | Page 5
CoAP payload marker 0xFF

- **Never** included in a compressed message
  - Neither in the compression residue, ...
  - ... nor before the payload (if any)
  - (... nor in the compression rules!)

- Compression result without end-to-end security
  - Rule ID | Compression residue | Payload

- Compression result with end-to-end security
  - Rule ID' | Compression residue' | OSCORE ciphertext
  - Following the second, outer compression
Compression with CoAP proxies

› **Without end-to-end security**
  – Compression based on hop-by-hop rules
  – C compresses for P, then P compresses for S

› **With end-to-end security**
  – The inner compression is end-to-end
  – The outer compression is hop-by-hop
  – @C: inner C<->S compression, then
    outer C<->P compression
  – @P: outer C<->P decompression, then
    outer P<->S compression
  – @S: outer P<->S decompression, then
    inner C<->S decompression
Input on security considerations

Comment from Carles Gomez Montenegro [1]
– *draft-ietf-6lo-schc-15dot4* relies on RFC 8824

Security considerations from RFC 8824:
– *If an LPWAN is the Layer 2 technology being used, the SCHC security considerations discussed in [RFC8724] continue to apply. When using another Layer 2 protocol, the use of a cryptographic integrity-protection mechanism to protect the SCHC headers is REQUIRED*. Such cryptographic integrity protection is necessary in order to continue to provide the properties that [RFC8724] relies upon.

Could an update to RFC 8824 change the REQUIRED to a SHOULD?
– IEEE 802.15.4 can be used in “no security” mode, and still benefit of compression
– The same may apply to further L2 technologies

[1] https://mailarchive.ietf.org/arch/msg/lp-wan/0IYD-1j5-w6rEKJPNiRiK3vPSs/
Summary and next steps

› Update to RFC 8824 (use of SCHC for CoAP messages)
   – Compression of CoAP options recently defined or extended
   – Clarifications on SCHC handling of the CoAP payload marker 0xFF
   – SCHC compression in the presence of CoAP proxies

› Next steps for version -01 (*)
   – Examples of compression with CoAP proxies
   – YANG data model for compression of new CoAP options
     › https://gitlab.com/crimson84/draft-tiloca-lpwan-8824-update/-/blob/main/ietf-schc-coap@2023-03-07.yang
   – Require that new/extended CoAP options also define/revise how they are compressed

› Comments and feedback are welcome!

(*) As draft-tiloca-schc-8824-update
Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-lpwan-8824-update