

Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)

draft-ietf-schc-8824-update-05

Marco Tiloca, RISE
Laurent Toutain, IMT Atlantique
Ivan Martínez, IRISA
Ana Minaburo

IETF 123 meeting – Madrid – July 23rd, 2025

Recap

- › **Document goal: obsolete RFC 8824**
- › **Document scope: same as RFC 8824, plus:**
 - Clarified and amended text originally from RFC 8824, also based on filed Errata
 - SCHC compression of CoAP options
 - › Clarified both in general and for specific CoAP options
 - › Defined for the Hop-Limit Option and for other recent options
 - › Updated for the OSCORE Option (extended by some CoRE documents)
 - Clarified SCHC compression for the CoAP payload marker
 - Spelled out SCHC compression in the presence of proxies, with examples provided
 - New IANA registry “SCHC Compression of CoAP Fields” for seamless extensibility
 - YANG data model extending the one defined in RFC 9363

From v -03 to v -04

- › **Various editorial improvements**
- › **Updated references:** I-D.ietf-core-oscore-edhoc → RFC 9668
- › **YANG data model in Appendix A:** now extractable from the Markdown source
- › **Harmonized style of tables with compression rules used in examples**
 - Single, deterministic order of OSCORE-related Field Descriptors
 - Single, consistent format of TV in Field Descriptors for the CoAP MID (0x notation)
 - When the unit for FL=var is bit, use (bit) instead of (b), per ISO/IEC 80000-13
- › **Harmonized phrasing for the formulation of functions**
 - E.g., “tkl” and “osc.x.m” used in FL of specific Field Descriptors

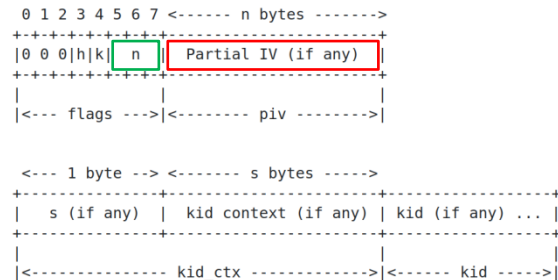
From v -03 to v -04

› Section 4.6 – Clarified the rationale for using the “tkl” function

- As suggested by Quentin before IETF 121 and confirmed there
- *“For the Token field, ... SCHC does not send the size of the residue resulting from the compression of the Token field, ... Instead, ... SCHC designates a specific function, “tkl”, that the Rule MUST use to complete the Field Descriptor. ... This construct avoids ambiguity with the Token Length field and results in a more efficient compression of the Token field.”*

› Defined the “osc.piv” function to use in the FL of SCHC Rules

- Proposed at IETF 121, analogous to the “tkl” function
- Input: bits 5-7 of the “flags” subfield
- Output: the length of the “piv” subfield in the OSCORE Option
- Updated examples of SCHC-compressed messages when using OSCORE



From v -03 to v -04

- › **Clarified requirement: Field Descriptors must be ordered in a deterministic way**
 - Same order that the corresponding fields have in the CoAP message to compress
 - Always taken for granted, now explicitly stated
 - In practice:
 - › Fields of the 4-byte header, in order of appearance
 - › Token field (if any)
 - › CoAP options in order of appearance (also for instances of the same repeatable option)
 - For structured options, e.g., the OSCORE Option ...
 - › Field Descriptors of subfields are in strict order of appearance
- › **Accordingly updated the tables with SCHC Rules used in the examples**

From v -04 to v -05

- › **New Github repo under the SCHC organization**

- Thanks, Pascal!
- <https://github.com/ietf-wg-schc/draft-ietf-schc-8824-update>

- › **Updated author's contact information**

- Affiliation and email address of Ivan

- › **Minor rephrasing and editorial improvements**

From v -04 to v -05

› Revised compression of the OSCORE Option

- (aligned with *draft-ietf-core-oscore-key-update*, i.e., KUDOS)
- Revised semantics of the “x” subfield, hence of its compression
- Removed moot subfields “y” and “old_nonce” related to KUDOS
- Hence removed the “osc.y.w” function
- Updated YANG data model accordingly
- Removed Field Descriptors from examples rules accordingly
- No impact on the examples: those fields were not considered

```
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 <---- n bytes ---->
+-----+-----+-----+-----+-----+-----+-----+-----+
|1|0|0|0|h|k| n | 0 | 0 | 0 | 0 | 0 | 0 | 0 | d | Partial IV (if any) |
+-----+-----+-----+-----+-----+-----+-----+-----+
|<----- flags ----->|<----- piv ----->|
```

```
<- 1 byte -> <----- s bytes ----->
+-----+-----+-----+-----+-----+-----+-----+-----+
| s (if any) | kid context (if any) |
+-----+-----+-----+-----+-----+-----+-----+-----+
|<----- kid_ctx ----->|
```

```
<----- 1 byte -----> <-- m + 1 bytes -->
+-----+-----+-----+-----+-----+-----+-----+-----+
| x (if any) | nonce (if any) |
+-----+-----+-----+-----+-----+-----+-----+-----+
|<----- x ----->|<----- nonce ----->|

0 1 2 3 4 5 6 7
+-----+-----+-----+-----+-----+-----+-----+-----+
|0|z|b|p| m |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| kid (if any) ... |
+-----+-----+-----+-----+-----+-----+-----+-----+
|<----- kid ----->|
```

› Clarified OSCORE compression when using the group mode of Group OSCORE

- Explicitly mentioned the signature at the end of the CoAP payload
- No changes in the SCHC compression/decompression process

From v -04 to v -05

Several clarifications on compressing CoAP options

› Explained structure of options:

– *Delta Length [Delta (Extended)] [Length (Extended)] Value*

› Definition of Field Descriptors in SCHC Rules (e.g., strict order etc.)

› Both the syntactic approach and the semantic approach are possible

- Conceptual overview of both approaches (see also *draft-ietf-schc-universal-option*)
- The semantic approach uses Field Descriptors that focus on compressing the Option Value
- Option Delta and Option Length are reconstructed leveraging the FID and FL in Field Descriptors
- Focus on the semantic approach, when discussing compression and showing examples

From v -04 to v -05

Several clarifications on compressing CoAP options

› Details on FIDs when using the semantic approach

- FID includes "CoAP" and the Option Number from the IANA registry "CoAP Option Numbers"
- E.g., "CoAP.option(3)" for the Uri-Host Option

› The Option Value can be composed of subfields (e.g., in the OSCORE Option)

- Field Descriptors in a SCHC Rule are ordered per the same appearance order of the subfields
- FID includes "CoAP", the Option Number, and the subfield name
 - › E.g., "CoAP.option(9).flags" for the “flags” subfield of the value of the OSCORE Option

› In the new registry "SCHC Compression of CoAP Fields"

- Updated naming and sorting of its initial entries

CoAP.MID	CoAP header field Message ID [RFC7252]
CoAP.Token	CoAP field Token [RFC7252][RFC8974]
CoAP.option(1)	CoAP option If-Match [RFC7252]
CoAP.option(3)	CoAP option Uri-Host [RFC7252]

...

...

Todo: update “tkl” function

› Use of the “tkl” function

- Specified in the **FL** of a SCHC Field Descriptor
- Output: the length of the **“Token”** field, in bytes

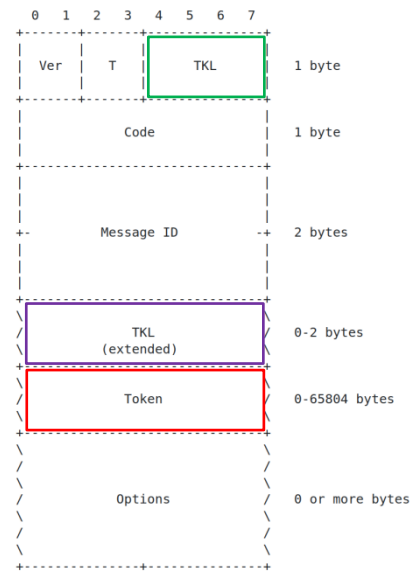
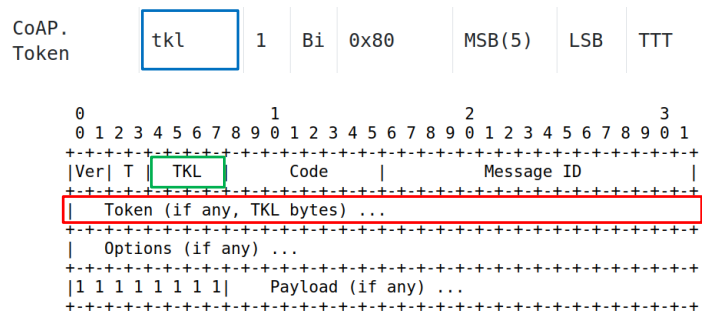
› Original definition – Consistent with RFC 7252

- Input: the “Token Length” (“TKL”) field

Planned updated definition

- Input: the “TKL” field and, if present, the “TKL (Extended)” field
- Consistent with RFC 8974, the length of “Token”, in bytes, is:
 - › “TKL”: 0-12 → Value in “TKL”, like in RFC 7252
 - › “TKL”: 13 → Value in the 8-bit “TKL (extended)”, minus 13
 - › “TKL”: 14 → Value in the 16-bit “TKL (extended)”, minus 269

- › Include “TKL (extended)” in the updated YANG data model



Reported errata for RFC 8824

› EID 8270

- https://www.rfc-editor.org/errata_search.php?eid=8270
- Section 7.3, use MSB(44) in a Field Descriptor
- Reviewed and confirmed by Laurent
 - › <https://mailarchive.ietf.org/arch/msg/lp-wan/b8va8LzRwLogWmXAuATJtiEHZII/>

› EID 8271

- https://www.rfc-editor.org/errata_search.php?eid=8271
- Section 7.3, length of compression residue on the wire, for the OSCORE Partial IV field
- Reviewed by Laurent
 - › <https://mailarchive.ietf.org/arch/msg/lp-wan/b8va8LzRwLogWmXAuATJtiEHZII/>
- Follow-up discussion at:
 - › <https://mailarchive.ietf.org/arch/msg/schc/j3EGVCSFrPKvYLsk1A5Gy8Kd588/>

Thank you!

Comments/questions?

<https://github.com/ietf-wg-schc/draft-ietf-schc-8824-update>