Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 21 October 2025

A. Rundgren, Ed.
Independent

19 April 2025

CBOR Simple Value for CSF
draft-rundgren-cbor-simple-4-csf-00

Abstract

This document defines a CBOR "simple" value to be used as a unique label for a container map holding an embedded signature.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 October 2025.

Table of Contents

1. Introduction 2
2. Requirements Language 2
3. Description and Rationale 2
3.1. Current Solution 2
3.2. Enhanced Solution 3
4. IANA Considerations 3
5. Security Considerations 4
6. References 4
6.1. Normative References 4
6.2. Informative References 5
Document History 5
Acknowledgements 5
Author's Address 5

1. Introduction

This document defines a CBOR [RFC8949] "simple" value to be used as unique labels (map keys) to containers holding embedded signature constructs [CSF]. The primary purpose of the unique label is to securely decouple application-specific labels from the signature container. In addition to eliminating the need for application-specific labels for embedded signature containers, the net result includes simplified signature APIs as well.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Description and Rationale

This section describes the problem and its possible solution.

The CBOR examples are provided in "Extended Diagnostic Notation (EDN)" [I-D.ietf-cbor-edn-literals].

3.1. Current Solution

The [CSF] embedded signature scheme currently depends on an application-specific label holding the embedded signature container.

The following CBOR code shows a very simple example using an HMAC signature:

```
{
  1: "data",          # Application data
  2: "more data",     # Application data
  -1: {               # Embedded signature (CSF container)
    1: 5,
    6: h'4853d7730cc1340682b1748dc346cf627a5e91ce62c67fff15c40257ed2a37a1'
  }
}
```

Having to define an application-specific ("custom") label for the embedded signature container is certainly not a showstopper, but it lacks "finesse". In addition, signature APIs need to deal with such labels like the following:

```
sign(_signatureLabel_, _applicationMap_).
```

3.2. Enhanced Solution

Replacing the application-specific label with a CBOR simple value, would yield the following:

```
{
  1: "data",          # Application data
  2: "more data",     # Application data
  simple(99): {       # Embedded signature (CSF container)
    1: 5,
    6: h'237e674c7be1818ddd7eaacf40ca80415b9ad816880751d2136c45385207420c'
  }
}
```

The advantages with using simple(99) include:

* Eliminates the need for application-specific labels for signature containers.

* Simplifies signature APIs: sign(_applicationMap_).

* Using deterministic encoding (a [CSF] prerequisite), CBOR simple types lexicographically follow after other CBOR elements. This makes perfect sense for embedded signatures, since they usually "attest" the application data that is (list-wise), situated above the signature container, like in the example.

4. IANA Considerations

In the registry [IANA.cbor-simple-values], IANA is requested to allocate the simple value defined in Table 1.

Value	Semantics	Reference
99^(*)	Unique label	draft-rundgren-cbor-simple-4-csf-XX

Table 1: Simple Values

* TBD. The actual number is of no importance. The following are some musical inspirations:

* NENA - 99 Luftballons

* Chuck Berry - (Get Your Kicks on) Route 66

* Niska - 44

5. Security Considerations

The proposed enhanced solution does not reduce security compared to the current solution because duplicate labels SHOULD in both cases be rejected by conforming CBOR encoders and decoders.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[IANA.cbor-simple-values]
IANA, "Concise Binary Object Representation (CBOR) Simple Values",
<https://www.iana.org/assignments/cbor-simple-values>.

6.2. Informative References

[I-D.ietf-cbor-edn-literals]
Bormann, C., "CBOR Extended Diagnostic Notation (EDN)", Work in Progress, Internet-Draft, draft-ietf-cbor-edn-literals-16, 8 January 2025,
<https://datatracker.ietf.org/doc/html/draft-ietf-cbor-edn-literals-16>.

[CSF] Rundgren, A., "CBOR Signature Format (CSF)",
<https://cyberphone.github.io/javaapi/org/webpki/cbor/doc-files/signatures.html>.

Document History

* 00. First cut.

Acknowledgements

TBD

Author’s Address

Anders Rundgren (editor)
Independent
Montpellier
France
Email: anders.rundgren.net@gmail.com
URI: https://www.linkedin.com/in/andersrundgren/