

JOSE Working Group
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

C. Bormann
Universitaet Bremen TZI
October 27, 2014

Constrained Object Signing and Encryption (COSE)
draft-bormann-jose-cose-00

Abstract

COSE provides services similar to JSON Web Signature (JWS), JSON Web Encryption (JWE), and JSON Web Key (JWK), making use of JSON Web Algorithms (JWA), for data encoded in the Concise Binary Object Representation (CBOR).

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 <http://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 April 30, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
1.1. Objectives	3
1.2. COSE	3
1.3. Terminology	4
2. Specification	4
3. Examples	4
4. IANA considerations	5
5. Security considerations	5
6. Acknowledgments	5
7. References	5
7.1. Normative References	5
7.2. Informative References	5
7.3. URIs	6
Author's Address	6

1. Introduction

Constrained nodes and networks of constrained nodes [RFC7228] pose some specific requirements on data representation that may make it difficult to apply existing object security standards to this space.

In constrained node networks, message payloads are often small (by nature of the data exchanged), and both transmission systems (e.g., [RFC4944]) and application protocols (e.g., [RFC7252]) are optimized for these small interchanges. As a result, fixed-size overheads introduced by security protocols may be much more detrimental than in a traditional Web environment. Transmission/reception of messages requires power, turning a system that on average might consume ~100 [micro]W into a 50 mW consumer while communicating. This is a strong incentive to keep message sizes reasonably small. It is not often possible to rely on compression to achieve this, as compression requires CPU power, RAM, and code space, which all are rather constrained in these environments; compression also works better for larger messages.

Handling messages requires RAM, the total available size of which on a constrained node may be on the order of 10 KiB (note that apart from security, most of this RAM is already needed for operating system, network stack, sensor management, application processing, etc.). Protocols that require copying data, or, worse, re-encoding and escape processing, can double or triple those RAM requirements.

All the processing that is to be performed in a constrained node requires code space in Flash, the total available size of which on a constrained node may be on the order of 100 KiB (with the same note applying as above). This leads to a strong requirement to minimize

code complexity, and in particular to avoid having to implement multiple different ways to do the same thing.

Still, security is not optional.

1.1. Objectives

The JOSE set of specifications provides an attractive set of functions for the constrained space, even if its breadth of optional functionality may go beyond what is required there. The present specification aims to make use of the substantial amount of work that went into making JOSE such a comprehensive specification.

JOSE makes use of JSON [RFC7159], a text based data representation format. For applications in constrained nodes, the Concise Binary Object Representation format (CBOR) provides a more compact representation that is still largely based on the same principles.

By using CBOR, the present specification can:

- o avoid the use of base64 coding of binary data. Base64 coding causes message expansion, which is detrimental to energy requirements. In an implementation, it also causes the requirement for creating copies of some data, which increases RAM requirements.
- o avoid JSON-encoding of data. Again, this causes some message expansion, requires creating copies for escape processing, but also requires considerable code size, including for binary-to-decimal conversion.
- o potentially make use of CBOR's capability to minimize strings by enumerating frequently occurring member names. This again helps to reduce message sizes, but also can save some code space. (This is a secondary, but useful objective.)

1.2. COSE

COSE provides services similar to JSON Web Signature (JWS) [I-D.ietf-jose-json-web-signature], JSON Web Encryption (JWE) [I-D.ietf-jose-json-web-encryption], and JSON Web Key (JWK) [I-D.ietf-jose-json-web-key], making use of JSON Web Algorithms (JWA) [I-D.ietf-jose-json-web-algorithms], in conjunction with data encoding in the Concise Binary Object Representation (CBOR) [RFC7049].

1.3. Terminology

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 RFC 2119 [RFC2119].

The term "byte" is used in its now customary sense as a synonym for "octet".

2. Specification

Presently, we believe the entire specification of COSE can be reduced to the following:

COSE is exactly like JOSE, except that:

- o each use of JSON is replaced by the equivalent use of CBOR;
- o base64-encoding is never done:
 - * where the output of the base64url function was to be used as a JSON string, instead the input to the base64url function is represented as a byte string in CBOR
 - * where the output of the base64url function was to be used as an input to a cryptographic algorithm, instead the input is used directly
 - * where the output of the base64url function was to be joined by ASCII dots (".") with other such outputs, CBOR encoding of an array built from the inputs, each represented as a byte string, is used.
- o (probably:) certain member names ("alg"...) are replaced by a number of predefined numeric replacements only in the key positions of maps (JSON objects) defined by JOSE. Only the names most likely to be frequently occurring in constrained node networks are entered into a static table to be defined in this specification. (There is no future extension planned for this table.)

3. Examples

(TBD, to cover large parts of [I-D.ietf-jose-cookbook]).

4. IANA considerations

(TBD)

5. Security considerations

(TBD)

6. Acknowledgments

This document obviously owes a lot to the work of the entire JOSE working group, including the feedback during an initial presentation at IETF 90 [1]. Richard Barnes' Python implementation of JOSE was instrumental in confirming the feasibility of the COSE approach.

7. References

7.1. Normative References

- [I-D.ietf-jose-json-web-algorithms]
Jones, M., "JSON Web Algorithms (JWA)", draft-ietf-jose-json-web-algorithms-36 (work in progress), October 2014.
- [I-D.ietf-jose-json-web-encryption]
Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", draft-ietf-jose-json-web-encryption-36 (work in progress), October 2014.
- [I-D.ietf-jose-json-web-key]
Jones, M., "JSON Web Key (JWK)", draft-ietf-jose-json-web-key-36 (work in progress), October 2014.
- [I-D.ietf-jose-json-web-signature]
Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", draft-ietf-jose-json-web-signature-36 (work in progress), October 2014.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, October 2013.

7.2. Informative References

- [I-D.ietf-jose-cookbook]
Miller, M., "Examples of Protecting Content using
JavaScript Object Signing and Encryption (JOSE)", draft-
ietf-jose-cookbook-05 (work in progress), October 2014.
- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,
"Transmission of IPv6 Packets over IEEE 802.15.4
Networks", RFC 4944, September 2007.
- [RFC7159] Bray, T., "The JavaScript Object Notation (JSON) Data
Interchange Format", RFC 7159, March 2014.
- [RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for
Constrained-Node Networks", RFC 7228, May 2014.
- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained
Application Protocol (CoAP)", RFC 7252, June 2014.

7.3. URIs

- [1] <http://www.ietf.org/proceedings/90/slides/slides-90-jose-2.pdf>

Author's Address

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org