JOSE Working Group
Internet-Draft
Intended status: Informational
Expires: September 22, 2013

R. Barnes
BBN

March 21, 2013

JOSE Security Parameters Index
draft-barnes-jose-spi-00

Abstract

The use cases for JOSE include cases where a given sender and receiver use an out-of-band mechanism to negotiate cryptographic parameters, so that these parameters do not have to appear in a JOSE object. This document proposed a modification to the JOSE formats to allow for signaling that pre-negotiated parameters are being used, and if so, which parameters.

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 September 22, 2013.

Table of Contents

1. Introduction

The use cases for JOSE include cases where a given sender and receiver use an out-of-band mechanism to negotiate cryptographic parameters, such as OpenID Connect. This allows the sender and receiver to exchange JOSE objects without having to include all of the required security parameters, for example, algorithm names and public keys.

The current specifications for JSON Web Encryption (JWE) [I-D.ietf-jose-json-web-encryption] and JSON Web Signature (JWS) [I-D.ietf-jose-json-web-signature] accommodate these use cases by simply omitting requirements levels on some parameters. For exmaple, it should be REQUIRED for some sort of key or key identifier to be provided, so that the recipient of an object knows which key to use to process it. However, since two parties may have pre-negotiated which key to use, all key and key identifier fields are marked as OPTIONAL in the current specification. This leaves JWE and JWS without a good notion of what a well-formed object looks like.

A better approach would be to put hard requirements on parameters, but allow them to be omitted if they have been pre-negotiated. Thus, the specifications might REQUIRED that a "kid", "jwk", or "jku" field be present in an object, except if the object contains an indicator that some parameters have been pre-negotiated. Following the terminology from IPsec [RFC4301], we call this flag a "security parameters index", or SPI.

The addition of SPI would clarify the processing model for JWE to include an explicit provision for pre-negotiated parameters. Namely, if an object contains an "spi" value, then the recipient first the object to a normal JWE or JWS object by filling in the pre-negotiated parameters. Then it can process the object as normal.

This document proposes two main changes. First, we provide a definition of the "spi" header parameter, to be added to Section 4.1 of the JWE specification and the JWS specification. Second, we propose changes to the processing instructions in the respective specifications.

2. "spi" (Security Parameters Index) Header Parameter

The "spi" header parameter contains an opaque string, which refers to a set of pre-negotiated security parameters, established through some out-of-band negotiation protocol. The association of security parameters to SPI values is the responsibility of the negotiation protocol, as are other management considerations (e.g., the lifetime of a set of parameters).

When an object contains an SPI value, fields with pre-negotiated values MAY be omitted, even if they would otherwise be REQUIRED. If the recipient of an object encounters an SPI value references a known set of security parameters, then the recipient MUST populate them into relevant fields in the object before further processing. If the SPI value is unknown to a recipient, or the recipient does not support pre-negotiation of parameters, then the "spi" field MUST be ignored. (Implementations SHOULD issue a warning in this case, because of the risk that processing will fail due to missing parameters.)

3. Changes to Processing Steps

In JWE, Section 5.1, add the following text to step 10:

> If pre-negotiated parameters are used, add an "spi" field and remove any pre-negotiated parameters.

In JWE, Section 5.2. add the following step after step 3:

> The JWE Header SHOULD be examined for an "spi" parameter. If an "spi" parameter is present and contains a recognized value, add the corresponding pre-negotiated parameters to the Header object.

In JWS, Section 5.1, add the following text to step 3:

> If pre-negotiated parameters are used, add an "spi" field and remove any pre-negotiated parameters.

In JWS, Section 5.2., add the following step after step 3:

> The JWS Header SHOULD be examined for an "spi" parameter. If an "spi" parameter is present and contains a recognized value, add the corresponding pre-negotiated parameters to the Header object.

4. References

4.1. Normative References

[I-D.ietf-jose-json-web-encryption]
Jones, M., Rescorla, E., and J. Hildebrand, "JSON Web Encryption (JWE)", draft-ietf-jose-json-web-encryption-08 (work in progress), December 2012.

[I-D.ietf-jose-json-web-signature]
Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", draft-ietf-jose-json-web-signature-08 (work in progress), December 2012.

4.2. Informative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

Author's Address

Richard Barnes
BBN

Email: rlb@ipv.sx