Internet Engineering Task Force
Internet-Draft
Updates: 7517 (if approved)
Intended status: Standards Track
Expires: January 1, 2018

N. McCallum
Red Hat, Inc.
June 30, 2017

PKCS #11 for JSON Web Keys
draft-mccallum-jose-pkcs11-jwk-00

Abstract

This document updates RFC 7517 in order to specify an extension to the JSON Web Key (JWK) format so that private key material may be stored in cryptographic hardware using PKCS #11. It defines a new property for JWKs which contains the PKCS #11 URI identifying the location of the private key material. Implementations can use this URI to offload the cryptographic operations to the identified hardware.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Document Conventions 2
3. JWK PKCS #11 URI Property 2
4. Implementation Considerations 3
5. Security Considerations 3
6. IANA Considerations 4
7. Normative References 4
Author's Address 5

1. Introduction

JSON Web Key (JWK) [RFC7517] defines a format for keys which can be used to perform cryptographic operations. When these JWKs contain private key material, illegitimate access to this material creates the possibility for wide-scale security compromise.

As a defensive strategy, other key types will offload their private key material to cryptographic hardware or other secure storage using PKCS #11. The locations of these keys are communicated using PKCS #11 URIs [RFC7512]. Therefore, this document defines a method to replace the private key material of a JWK with a PKCS #11 URI.

2. Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. JWK PKCS #11 URI Property

JWKs that wish to offload their private key material using PKCS #11 will provide a JSON property named "p11" instead of the private key material. The "p11" property MUST contain a valid PKCS #11 URI [RFC7517] that points to a private key object (that is, type=private).

Private key material is defined by the Parameter Information Class of Section 8.1.1 of RFC 7517 [RFC7517]. JWKs MUST NOT provide both the "p11" property and other private key material. However, implementations SHOULD provide full public key material appropriate to the key type. This enables implementations to perform public key cryptographic operations without consulting PKCS #11.

4. Implementation Considerations

The PKCS #11 URI standard provides mappings to URI format for most metadata attributes available over PKCS #11. Some of these attributes may differ based on operating system, driver or even hardware implementations. The generation of URIs which can only be used in a specific context should be avoided for the sake of clarity.

The following path attributes are RECOMMENDED for general use:

- model
- manufacturer
- serial
- token
- id
- object
- type

The following query attributes are RECOMMENDED for general use:

- pin-value

Tools which generate PKCS #11 URIs for use in JWKs SHOULD NOT generate path or query attributes that are not recommended above. On the other hand, tools which process JWKs containing the "p11" property MAY process path or query attributes that are not recommended above.

Using PKCS #11 for cryptographic operations is usually associated with a performance penalty. Implementations SHOULD perform public key operations, such as asymmetric signature verification or asymmetric encryption, without using PKCS #11 in order to increase speed and should fall back to PKCS #11 where access to the private key material is required.

5. Security Considerations

Accessing a JWK containing the "p11" property in place of the private key material may still allow an attacker to perform operations using the private key while not obtaining the private key itself. This is particularly true when the "pin-value" query attribute is used.

Nevertheless, because the attacker does not learn the private key itself, the attacker's access to use of the key can be limited to a particular context; for example, only the host with direct access to the hardware. Because of this, the ability to remove the attacker's access to this context provides the option for significant damage mitigation strategies. Therefore, offloading the private key

material should not be misunderstood to be a cryptographic panacea but rather a way to reduce the cost of a compromise.

Exposing the "p11" property can leak institutional or configuration information to an attacker that could be used as part of a multifaceted attack. This is particularly true when the PKCS #11 URI contains the "pin-value" or "pin-source" query attributes since this PIN is used to protect access to the private key material. For this reason, the "p11" property MUST be treated as a private key material in its own right and care should be taken not to expose it.

It may be desirable to avoid the use of the "pin-value" query attribute altogether by passing in this value out of band. This strategy implies that the attacker will need to target the out of band delivery mechanism in addition to the JWK in order to use the private key material.

6. IANA Considerations

The following has been added to the "JSON Web Key Parameters" registry:

o Parameter Name: "p11"
o Parameter Description: The PKCS #11 URI
o Parameter Information Class: Private
o Used with "kty" Value(s): *
o Change Controller: IESG
o Specification Document(s): Section 3 of THIS DOCUMENT

7. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7512] Pechanec, J. and D. Moffat, "The PKCS #11 URI Scheme", RFC 7512, DOI 10.17487/RFC7512, April 2015, <http://www.rfc-editor.org/info/rfc7512>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <http://www.rfc-editor.org/info/rfc7517>.

Author's Address

Nathaniel McCallum
Red Hat, Inc.
100 East Davie Street
Raleigh, NC 27601
USA

EMail: npmccallum@redhat.com