JOSE Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 25, 2013

M. Miller
Cisco Systems, Inc.
B. Campbell
Ping Identity Corp.
February 21, 2013

JavaScript Object Notation (JSON) Web Key (JWK) for Public Key Infrastructure (X.509) (PKIX) Certificates
draft-miller-jose-pkix-key-01

Abstract

This document defines a JavaScript Object Notation (JSON) Web Key (JWK) object to wrap Public Key Infrastructure (X.509) (PKIX) certificate chains, to allow for some interoperability between existing PKIX-based systems and newer JOSE-based systems.

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 August 25, 2013.

Table of Contents

1. Introduction

JavaScript Object Notation (JSON) Web Key ([JWK]) describes an abstract data structure to represent public keys using JSON [RFC4627]. The JSON Web Algorithms ([JWA]) define specific key representations for raw asymmetric key types, such as RSA [RFC3447] or Elliptic Curve [DSS]. However, there are times when it is desirable to represent a Public Key Infrastructure (X.509) (PKIX) certificate chain, such as to associate with a JSON Web Encryption ([JWE]) or JSON Web Signature ([JWS]) object. This document specifies an approach which encodes a chain of PKIX certificates as an array of strings within a JWK object.

PKIX certificates have a number of advantages, such as an established process of certification and attribution of entities. It is also sometimes desirable for JSON-based cryptographic operations to support the existing and widespread deployment of PKIX-based technologies.

2. Terminology

This document inherits JSON Web Algorithms (JWA)-related terminology from [JWA], JSON Web Encryption (JWE)-related terminology from [JWE], and JSON Web Key (JWK)-related terminology from [JWK]. Security-related terms are to be understood in the sense defined in [RFC4949].

The capitalized 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 [RFC2119].

3. PKIX Key Type

The "PKIX" key type is used to contain a chain of PKIX certificates. The following parameters are defined:

3.1. 'x5c' (X.509 Certificate Chain) Parameter

The REQUIRED "x5c" parameter contains a chain of one or more PKIX certificates [RFC5280]. The certificate chain is represented as an array of certificate value strings. Each string in the array is a DER [ITU.X690.1994] PKIX certificate encoded as base64 [RFC4648] (not base64url). The array MUST have at least one value, which MUST be the PKIX certificate of the actor (e.g., the singer of a [JWS], or a recipient of a [JWE]). Each additional value of the array (if any) MUST be the PKIX certificate that certifies the previous certificate.

4. Examples

The following is a non-normative example of a JWK Set containing a single JWK utilizing the PKIX Key Type ("kty") defined in this document.

```
{"keys":[
 {"kty":"PKIX",
  "x5c":[
   "MIIE3jCCA8agAwIBAgICAwEwDQYJKoZIhvcNAQEFBQAwYzELMAkGA1UEBhMCVVM
   xITAfBgNVBAoTGFRoZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR2
   8gRGFkZHkgQ2xhc3MgMiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0wNjExM
   TYwMTU0MzdaFw0yNjExMTYwMTU0MzdaMIHKMQswCQYDVQQGEwJVUzEQMA4GA1UE
   CBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEaMBgGA1UEChMRR29EYWR
   keS5jb20sIEluYy4xMzAxBgNVBAsTKmh0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29kYW
   RkeS5jb20vcmVwb3NpdG9yeTEwMC4GA1UEAxMnR28gRGFkZHkgU2VjdXJlIENlc
   nRpZmljYXRpb24gQXV0aG9yaXR5MREwDwYDVQQFEwgwNzk2OTI4NzCCASIwDQYJ
   KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMQt1RWMnCZM7DI161+4WQFapmGBWTt
   wY6vj3D3HKrjJM9N55DrtPDAjhI6zMBS2sofDPZVUBJ7fmd0LJR4h3mUpfjWoqV
   Tr9vcyOdQmVZWt7/v+WIbXnvQAjYwqDL1CBM6nPwT27oDyqu9SoWlm2r4arV3aL
```

GbqGmu75RpRSgAvSMeYddi5Kcju+GZtCpyz8/x4fKL4o/K1w/O5epHBp+YlLpyo
7RJlbmr2EkRTcDCVw5wrWCs9CHRK8r5RsL+H0EwnWGu1NcWdrxcx+AuP7q2BNgW
JCJjPOq8lh8BJ6qf9Z/dFjpfMFDniNoW1fho3/Rb2cRGadDAW/hOUoz+EDU8CAw
EAAaOCATIwggEuMB0GA1UdDgQWBBT9rGEyk2xF1uLuhV+auud2mWjM5zAfBgNVH
SMEGDAWgBTSxLDSkdRMEXGzYcs9of7dqGrU4zASBgNVHRMBAf8ECDAGAQH/AgEA
MDMGCCsGAQUFBwEBBCcwJTAjBggrBgEFBQcwAYYXaHR0cDovL29jc3AuZ29kYWR
keS5jb20wRgYDVR0fBD8wPTA7oDmgN4Y1aHR0cDovL2NlcnRpZmljYXRlcy5nb2
RhZGR5LmNvbS9yZXBvc2l0b3J5L2dkcm9vdC5jcmwwSwYDVR0gBEQwQjBABgRVH
SAAMDgwNgYIKwYBBQUHAgEWKmh0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29kYWRkeS5j
b20vcmVwb3NpdG9yeTAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQEFBQADggE
BANKGwOy9+aG2Z+5mC6IGOgRQjhVyrEp0lVPLN8tESe8HkGsz2ZbwlFalEzAFPI
UyIXvJxwqoJKSQ3kbTJSMUA2fCENZvD117esyfxVgqwcSeIaha86ykRvOe5GPLL
5CkKSkB2XIsKd83ASe8T+5o0yGPwLPk9Qnt0hCqU7S+8MxZC9Y7lhyVJEnfzuz9
p0iRFEUOOjZv2kWzRaJBydTXRE4+uXR21aITVSzGh6O1mawGhId/dQb8vxRMDsx
uxN89txJx9OjxUUAiKEngHUuHqDTMBqLdElrRhjZkAzVvb3du6/KFUJheqwNTrZ
EjYx8WnM25sgVjOuH0aBsXBTWVU+4=",
"MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Z
hbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIE
luYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb
24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8x
IDAeBgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDY
yMFoXDTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZS
BHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgM
iBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASAwDQYJKoZIhvcNAQEBBQADggEN
ADCCAQgCggEBAN6d1+pXGEmhW+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XC
APVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux
6wwdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLO
tXiEqITLdiOr18SPaAIBQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWo
riMYavx4A6lNf4DD+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZ
Eewo+YihfukEHU1jPEX44dMX4/7VpkI+EdOqXG68CAQOjggHhMIIB3TAdBgNVHQ
4EFgQU0sSw0pHUTBFxs2HLPaH+3ahq1OMwgdIGA1UdIwSByjCBx6GBwaSBvjCBu
zEkMCIGA1UEBxMbVmFsaUNlcnQgVmFsaWRhdGlvbiBOZXR3b3JrMRcwFQYDVQQK
Ew5WYWxpQ2VydCwgSW5jLjE1MDMGA1UECxMsVmFsaUNlcnQgQ2xhc3MgMiBQb2x
pY3kgVmFsaWRhdGlvbiBBdXRob3JpdHkxITAfBgNVBAMTGGh0dHA6Ly93d3cudm
FsaWNlcnQuY29tLzEgMB4GCSqGSIb3DQEJARYRaW5mb0B2YWxpY2VydC5jb22CA
QEwDwYDVR0TAQH/BAUwAwEB/zAzBggrBgEFBQcBAQQnMCUwIwYIKwYBBQUHMAGG
F2h0dHA6Ly9vY3NwLmdvZGFkZHkuY29tMEQGA1UdHwQ9MDswOaA3oDWGM2h0dHA
6Ly9jZXJ0aWZpY2F0ZXMuZ29kYWRkeS5jb20vcmVwb3NpdG9yeS9yb290LmNybD
BLBgNVHSAERDBCMEAGBFUdIAAwODA2BggrBgEFBQcCARYqaHR0cDovL2NlcnRpZ
mljYXRlcy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5MA4GA1UdDwEB/wQEAwIBBjAN
BgkqhkiG9w0BAQUFAAOBgQC1QPmnHfbq/qQaQlpE9xXUhUaJwL6e4+PrxeNYiY+
Sn1eocSxI0YGyeR+sBjUZsE4OWBsUs5iB0QQeyAfJg594RAoYC5jcdnplDQ1tgM
QLARzLrUc+cb53S8wGd9D0VmsfSxOaFIqII6hR8INMqzW/Rn453HWkrugp++85j
09VZw==",
"MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ
0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNT
AzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0a
G9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkq

hkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE
5MDYyNjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTm
V0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZ
XJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQD
ExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG9w0BCQEWEWluZm9
AdmFsaWNlcnQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOOnHK5a
vIWZJV16vYdA757tn2VUdZZUcOBVXc65g2PFxTXdMwzzjsvUGJ7SVCCSRrCl6zf
N1SLUzm1NZ9WlmpZdRJEy0kTRxQb7XBhVQ7/nHk01xC+YDgkRoKWzk2Z/M/VXwb
P7RfZHM047QSv4dk+NoS/zcnwbNDu+97bi5p9wIDAQABMA0GCSqGSIb3DQEBBQU
AA4GBADt/UG9vUJSZSWI4OB9L+KXIPqeCgfYrx+jFzug6EILLGACOTb2oWH+heQ
C1u+mNr0HZDzTuIYEZoDJJKPTEjlbVUjP9UNV+mWwD5MlM/Mtsq2azSiGM5bUMM
j4QssxsodyamEwCW/POuZ6lcg5Ktz885hZo+L7tdEy8W9ViH0Pd"],
"use":"sig",
"kid":"somekey"}]
}

5. IANA Considerations

5.1. JSON Web Key Type Registration

This document registers the following to the JSON Web Key Types registry:

- "kty" Paramater value: "PKIX"
- Implementation Requirements: OPTIONAL
- Change Controller: IETF
- Specification Document(s): Section 3 of [[this document]]

5.2. JSON Web Key Parameters Registration

This document registers the following to the JSON Web Key Parameters registry:

- Parameter Name: "x5c"
- Change Controller: IETF
- Specification Document(s): Section 3.1 of [[this document]]

6. Security Considerations

This document does not introduce any new considerations beyond those specified by [JWK].

7. References

7.1. Normative References

[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, July 2006.

[DSS] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-3, June 2009.

[ITU.X690.1994] International Telecommunications Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, 1994.

[JWA] Jones, M., "JSON Web Algorithms (JWA)", draft-ietf-jose-json-web-algorithms-08 (work in progress), December 2012.

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

[JWS] Jones, M., "JSON Web Signature (JWS)", draft-ietf-jose-json-web-signature-08 (work in progress), December 2012.

[JWK] Jones, M., "JSON Web Key (JWK)", draft-ietf-jose-json-web-key-08 (work in progress), December 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

7.2. Informative References

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 2898, February 2003.

Appendix A. Acknowledgements

Appendix B. Document History

-01 Minor typos and nits

-00 Initial revision

Authors' Addresses

Matthew Miller
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Phone: +1-303-308-3204
Email: mamille2@cisco.com

Brian Campbell
Ping Identity Corp.

Email: brian.d.campbell@gmail.com