IP Security Maintenance and Extensions (ipsecme)
Internet-Draft
Updates: RFC 5996 (if approved)
Intended status: Standards Track
Expires: October 10, 2013

T. Kivinen
INSIDE Secure
P. Wouters
Red Hat
H. Tschofenig
Nokia Siemens Networks
April 08, 2013

More Raw Public Keys for IKEv2
draft-ietf-ipsecme-oob-pubkey-00.txt

Abstract

The Internet Key Exchange Version 2 (IKEv2) protocol currently only supports raw RSA keys. In some environments it is useful to make use of other types of public keys, such as those based on Elliptic Curve Cryptography. This documents adds support for other types of raw public keys to IKEv2 and obsoletes the old raw RSA key format.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Secure DNS allows public keys to be associated with domain names for usage with security protocols like Internet Key Exchange Version 2 (IKEv2) [RFC5996] and Transport Layer Security (TLS) but it relies on extensions in those protocols to be specified.

IKEv2 already offers support for PKCS #1 encoded RSA keys, i.e., a DER- encoded RSAPublicKey structure (see [RSA] and [RFC3447]). Other raw public keys types are, however, not supported.

The TLS Out-of-Band Public Key Validation specification ([I-D.ietf-tls-oob-pubkey]) adds generic support for raw public keys to TLS by re-using the SubjectPublicKeyInfo format from the X.509 Public Key Infrastructure Certificate profile [RFC5280].

This document is similar than the TLS Out-of-Band Public Key Validation specification, and applies the concept to IKEv2 to support all public key formats defined by PKIX. This approach also allows future public key extensions to be supported without the need to introduce further enhancements to IKEv2.

To support new types of public keys in IKEv2 the following changes are needed:

- A new Certificate Encoding format needs to be defined for carrying the SubjectPublicKeyInfo structure. Section 3 specifies this new encoding format.

- A new Certificate Encoding type needs to be allocated from the IANA registry. Section 6 contains this request to IANA.

2. Terminology

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 [RFC2119].

3. Certificate Encoding Payload

Section 3.6 of RFC 5996 defines the Certificate payload format as shown in Figure 1.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cert Encoding |                                               |
+-+-+-+-+-+-+-+-+                                               |
~                       Certificate Data                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Certificate Payload Format.

- Certificate Encoding (1 octet) - This field indicates the type of certificate or certificate-related information contained in the Certificate Data field.

Certificate Encoding	Value
Raw Public Key	TBD

- Certificate Data (variable length) - Actual encoding of the certificate data. The type of certificate is indicated by the Certificate Encoding field.

When the certificate encoding type 'Raw Public Key' is used then the Certificate Data only contains the SubjectPublicKeyInfo part of the PKIX certificate.

In the case of the Certificate Request payload the Certification Authority field MUST be empty if the "Raw Public Key" certificate encoding is used.

Note, that we do follow public key processing rules of the section 1.2 of the Additional Algorithms and Identifiers for RSA Cryptography for PKIX ([RFC4055]) even when the SubjectPublicKeyInfo is not part of the certificate, but sent here. This means RSASSA-PSS and RSASSA-PSS-params inside the SubjectPublicKeyInfo needs to followed.

4. Old Raw RSA Key Certificate Type

After this there would be two ways of sending Raw RSA public keys in the IKEv2: The original IKEv2 mechanism (Raw RSA Key, encoding value 11), and the new format defined here. The old Raw RSA Key encoding has not been widely used. The IKEv2 protocol already supports a method to indicate what certificate encoding formats are supported, i.e. a peer can send one or multiple Certificate Request payload with the certificate encoding types it supports. From this list the recipient can see what formats are supported and select one which is used to send Certificate back.

Implementations conforming to this document MUST use the new format defined here for the raw public keys, regardless of the key type. This means that old Raw RSA Key encoding value 11 MUST NOT be used for certificate or certificate request payloads.

Note, that recipients can simply process the old Raw RSA key encodings just like any other unsupported or unknown certificate encoding type, i.e. skip over it, recipients MUST NOT consider receiving such payloads as fatal error (if other end sends such payloads, it is completely possible that the peers do not have common format for certificate encoding and the authentication will fail because of that).

5. Security Considerations

An IKEv2 deployment using raw public keys needs to utilize an out-of-band public key validation procedure to be confident in the authenticity of the keys being used. One such mechanism is to use a configuration mechanism for provisioning raw public keys into the IKEv2 software. A suitable deployment is likely to be found with smart objects. Yet another approach is to rely on secure DNS to associate public keys to be associated with domain names using the IPSECKEY DNS RRtype [RFC4025]. More information can be found in DNS-Based Authentication of Named Entities (DANE) [RFC6394].

This document does not change the assumptions made by the IKEv2 specifications since "Raw RSA Key" support is already available in IKEv2. This document only generalizes the raw public key support and obsoletes the old "Raw RSA Key" format.

6. IANA Considerations

This document allocates a new value from the IKEv2 Certificate Encodings registry:

TBD   Raw Public Key

This document also obsoletes the old value in the same registry, and the entry for "Raw RSA Key" should be changed to:

11   Obsoleted (was Raw RSA Key)

7. Acknowledgements

This document copies parts from the similar TLS document ([I-D.ietf-tls-oob-pubkey]).

8. References

8.1. Normative References

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

[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.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

8.2. Informative References

[I-D.ietf-tls-oob-pubkey]
Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Out-of-Band Public Key Validation for Transport Layer Security (TLS)", draft-ietf-tls-oob-pubkey-07 (work in progress), February 2013.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS", RFC 4025, March 2005.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

[RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 4754, January 2007.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[RFC6394] Barnes, R., "Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)", RFC 6394, October 2011.

[RSA] R. Rivest, , A. Shamir, , and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", February 1978.

Appendix A. Examples

This appendix provides examples of the actual packets sent on the wire. This uses the 256-bit ECDSA private/public key pair defined in the section 8.1. of the IKEv2 ECDSA document [RFC4754].

The public key is as followed:

o Algorithm : id-ecPublicKey (1.2.840.10045.2.1)

o Fixed curve: secp256r1 (1.2.840.10045.3.1.7)

o Public key x coordinate : cb28e099 9b9c7715 fd0a80d8 e47a7707
  9716cbbf 917dd72e 97566ea1 c066957c

o Public key y coordinate : 2b57c023 5fb74897 68d058ff 4911c20f
  dbe71e36 99d91339 afbb903e e17255dc

The SubjectPublicKeyInfo ASN.1 object is as follows:

```
0000 :     SEQUENCE
0002 :       SEQUENCE
0004 :         OBJECT IDENTIFIER  id-ecPublicKey (1.2.840.10045.2.1)
```

```
000d :         OBJECT IDENTIFIER  secp256r1 (1.2.840.10045.3.1.7)
0017 :       BIT STRING  (66 bytes)
00000000: 0004 cb28 e099 9b9c 7715 fd0a 80d8 e47a
00000010: 7707 9716 cbbf 917d d72e 9756 6ea1 c066
00000020: 957c 2b57 c023 5fb7 4897 68d0 58ff 4911
00000030: c20f dbe7 1e36 99d9 1339 afbb 903e e172
00000040: 55dc
```

The first byte (00) of the bit string indicates that there is no "number of unused bits", and the second byte (04) indicates uncompressed form ([RFC5480]). Those two octets are followed by the values of X and Y.

The final encoded SubjectPublicKeyInfo object is as follows:

```
00000000: 3059 3013 0607 2a86 48ce 3d02 0106 082a
00000010: 8648 ce3d 0301 0703 4200 04cb 28e0 999b
00000020: 9c77 15fd 0a80 d8e4 7a77 0797 16cb bf91
00000030: 7dd7 2e97 566e a1c0 6695 7c2b 57c0 235f
00000040: b748 9768 d058 ff49 11c2 0fdb e71e 3699
00000050: d913 39af bb90 3ee1 7255 dc
```

This will result the final IKEv2 Certificate Payload to be:

```
00000000: NN00 0060 XX30 5930 1306 072a 8648 ce3d
00000010: 0201 0608 2a86 48ce 3d03 0107 0342 0004
00000020: cb28 e099 9b9c 7715 fd0a 80d8 e47a 7707
00000030: 9716 cbbf 917d d72e 9756 6ea1 c066 957c
00000040: 2b57 c023 5fb7 4897 68d0 58ff 4911 c20f
00000050: dbe7 1e36 99d9 1339 afbb 903e e172 55dc
```

Where the NN will be the next payload type (i.e. that value depends on what is the next payload after this certificate payload).

Note to the RFC editor / IANA, replace the XX above with the newly allocated Raw Public Key number, and remove this note.

Authors' Addresses

Tero Kivinen
INSIDE Secure
Eerikinkatu 28
HELSINKI FI-00180
FI

Email: kivinen@iki.fi

Paul Wouters
Red Hat

Email: pwouters@redhat.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at