IP Security Maintenance and Extensions
(ipsecme)
Internet-Draft
Intended status: Informational
Expires: September 6, 2012

T. Kivinen
AuthenTec
P. Wouters
Red Hat
H. Tschofenig
Nokia Siemens Networks

March 5, 2012

More Raw Public Keys for IKEv2
draft-kivinen-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.

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 2 specifies this new encoding format.
- A new Certificate Encoding type needs to be allocated from the IANA registry. Section 5 contains this request to IANA.

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].

2. 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.

3. Old Raw RSA Key Certificate Type

After this there are two ways of sending Raw RSA public keys in the IKEv2: The already existing mechanisms, and the new format defined here. The IKEv2 protocol already supports a method to indicate which 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 which formats are supported and select one which is used to send Certificate back.

If the peer has raw non-RSA public key, it has no other option than to use the new format. If it has raw RSA public key, it can either use the old format or the new format, and it SHOULD indicate support

for both by sending both certificate encoding types inside Certificate Request payloads.

If a peer receives both old and new certificate endocing formats in the Certificate Request payloads, it is RECOMMENDED for new implementations to prefer this new format defined in this document, so the old Raw RSA public key format could possibly be phased out in the future.

To better support minimal implementations, it would be best to limit the code complexity of those versions, and in such implementations it might be better to implement only the new format as it supports all types of raw public keys.

4. 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. More information can be found in DNS-Based Authentication of Named Entitites (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.

5. IANA Considerations

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

TBD	Raw Public Key

6. Acknowledgements

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

7. References

7.1. 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.

7.2. Informative References

[I-D.ietf-tls-oob-pubkey]
Tschofenig, H., Gilmore, J., Wouters, P., Weiler, S., and T. Kivinen, "TLS Out-of-Band Public Key Validation", draft-ietf-tls-oob-pubkey-01 (work in progress), January 2012.

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

[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.

Authors' Addresses

Tero Kivinen
AuthenTec
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