LAMPS
Internet-Draft
Updates: {"RFC5280"=>nil} (if approved)
Intended status: Standards Track
Expires: September 22, 2021

M. Ounsworth
Entrust
M. Saarinen
PQShield

March 21, 2021

External Keys And Signatures For Use In Internet PKI
draft-ounsworth-pq-external-pubkeys-00

Abstract

Many of the post quantum cryptographic algorithms have either large public keys or signatures. In the interest of reducing bandwidth of transitting X.509 certificates, this document defines new public key and signature algorithms for referencing external public key and signature data by hash, URL, etc. This mechanism is designed to mimic the behaviour of an Authority Information Access extension.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. External Value 2
  2.1. External Public Key 3
  2.2. External Signature 3
3. IANA Considerations 3
4. Security Considerations 3
  4.1. CSRs and CT logs 3
5. Appendices 4
  5.1. ASN.1 Module 4
  5.2. Intellectual Property Considerations 4
6. Contributors and Acknowledgements 4
  6.1. Making contributions 4
7. Normative References 4
Authors' Addresses 5

1. Introduction

2. External Value

The id-external-value algorithm identifier is used for identifying a public key or signature which is provided as a reference to external data.

```
id-external-value ::= < OID >
```

The corresponding subjectPublicKey is the DER encoding of the following structure:

```
ExternalValue ::= SEQUENCE {
  location     GeneralName,
  hashAlg      AlgorithmIdentifier,
  hashVal      BIT STRING
}
```

Upon retrieval of the referenced data, the hash of the OCTET STRING of the retrieved data (removing base64 encoding as per [RFC4648] if necessary) MUST be verified using hashAlg to match the ExternalPublicKey.hash value.

2.1. External Public Key

When used with a public key, algorithm parameters for id-external-value are absent.

When ExternalValue is placed into a SubjectPublicKeyInfo.subjectPublicKey, the ExternalValue.location MUST refer to a DER-encoded SubjectPublicKeyInfo, which MAY be base64 encoded as per [RFC4648] for easier transport over text protocols.

2.2. External Signature

When used with a signatureAlgorithm, algorithm parameters are to contain the AlgorithmIdentifier of the signature that is being externalized.

When ExternalValue is placed into a signatureValue, the location MUST refer to the BIT STRING of a signatureValue, which MAY be base64 encoded as per [RFC4648] for easier transport over text protocols.

3. IANA Considerations

The ASN.1 module OID is TBD. The id-alg-composite OID is to be assigned by IANA.

4. Security Considerations

4.1. CSRs and CT logs

In practice, situations will arise where the ExternalPublicKey.location refers to a location which is not publicly available either because it is in a local keystore, on a private network, or no longer being hosted.

Not having the public key in a certificate signing request (CSR) could make it substantially harder for CAs to perform vetting of the key, for example for cryptographic strength or checking for prior revocation due to key compromise. A certificate requester MUST make the full public key available to the CA at the time of certificate request either by ensuring that the link in the ExternalPublicKey.location is visible to the CA, or by supplying the full public key to the CA out of band.

Not having the public key in Certificate Transparency (CT) logs could make it substantially harder for researchers to perform auditing tasks on CT logs. This may require additional CT mechanisms.

5. Appendices

5.1. ASN.1 Module

5.2. Intellectual Property Considerations

The following IPR Disclosure relates to this draft:

https://datatracker.ietf.org/ipr/3588/

6. Contributors and Acknowledgements

This document incorporates contributions and comments from a large group of experts. The Editors would especially like to acknowledge the expertise and tireless dedication of the following people, who attended many long meetings and generated millions of bytes of electronic mail and VOIP traffic over the past year in pursuit of this document:

John Gray (Entrust), Serge Mister (Entrust), Scott Fluhrer (Cisco Systems), Panos Kampanakis (Cisco Systems), Daniel Van Geest (ISARA), and Tim Hollebeek (Digicert).

We are grateful to all, including any contributors who may have been inadvertently omitted from this list.

This document borrows text from similar documents, including those referenced below. Thanks go to the authors of those documents. "Copying always makes things easier and less error prone" - [RFC8411].

6.1. Making contributions

Additional contributions to this draft are weclome. Please see the working copy of this draft at, as well as open issues at:

https://github.com/EntrustCorporation/draft-ounsworth-pq-external-keys

7. Normative References

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[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, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8411] Schaad, J. and R. Andrews, "IANA Registration for the Cryptographic Algorithm Object Identifier Range", RFC 8411, DOI 10.17487/RFC8411, August 2018, <https://www.rfc-editor.org/info/rfc8411>.

Authors' Addresses

Mike Ounsworth
Entrust Limited
1000 Innovation Drive
Ottawa, Ontario K2K 1E3
Canada

Email: mike.ounsworth@entrust.com

Markku-Juhani O. Saarinen
PQShield

Email: mjos@pqshield.com