Network Working Group
Request for Comments: 4853
Updates: 3852
Category: Standards Track

R. Housley
Vigil Security

April 2007

Cryptographic Message Syntax (CMS) Multiple Signer Clarification

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document updates the Cryptographic Message Syntax (CMS), which is published in RFC 3852. This document clarifies the proper handling of the SignedData protected content type when more than one digital signature is present.

1. Introduction

This document updates the Cryptographic Message Syntax [CMS]. The CMS SignedData protected content type allows multiple digital signatures, but the specification is unclear about the appropriate processing by a recipient of such a signed content. This document provides replacement text for a few paragraphs, making it clear that the protected content is validly signed by a given signer, if any of the digital signatures from that signer are valid.

This property is especially important in two cases. First, when the recipients do not all implement the same digital signature algorithm, a signer can sign the content with several different digital signature algorithms so that each of the recipients can find an acceptable signature. For example, if some recipients support RSA and some recipients support ECDSA, then the signer can generate two signatures, one with RSA and one with ECDSA, so that each recipient will be able to validate one of the signatures. Second, when a community is transitioning one-way hash functions or digital signature algorithms, a signer can sign the content with the older and the newer signature algorithms so that each recipient can find an acceptable signature, regardless of their state in the transition. For example, consider a transition from RSA with SHA-1 to RSA with SHA-256. The signer can generate two signatures, one with SHA-1 and one with SHA-256, so that each recipient will be able to validate at least one of the RSA signatures.

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 RFC 2119 [STDWORDS].

3. Update to RFC 3852, Section 5: Signed-data Content Type

RFC 3852, section 5, the next to the last paragraph says:

> A recipient independently computes the message digest. This message digest and the signer's public key are used to verify the signature value. The signer's public key is referenced either by an issuer distinguished name along with an issuer-specific serial number or by a subject key identifier that uniquely identifies the certificate containing the public key. The signer's certificate can be included in the SignedData certificates field.

This block of text is replaced with:

A recipient independently computes the message digest. This message digest and the signer's public key are used to verify the signature value. The signer's public key is referenced either by an issuer distinguished name along with an issuer-specific serial number or by a subject key identifier that uniquely identifies the certificate containing the public key. The signer's certificate can be included in the SignedData certificates field.

When more than one signature is present, the successful validation of one signature associated with a given signer is usually treated as a successful signature by that signer. However, there are some application environments where other rules are needed. An application that employs a rule other than one valid signature for each signer must specify those rules. Also, where simple matching of the signer identifier is not sufficient to determine whether the signatures were generated by the same signer, the application specification must describe how to determine which signatures were generated by the same signer. Support of different communities of recipients is the primary reason that signers choose to include more than one signature. For example, the signed-data content type might include signatures generated with the RSA signature algorithm and with the ECDSA signature algorithm. This allows recipients to verify the signature associated with one algorithm or the other.

4. Update to RFC 3852, Section 5.1: SignedData Type

RFC 3852, section 5.1, the next to the last paragraph says:

> signerInfos is a collection of per-signer information. There MAY be any number of elements in the collection, including zero. The details of the SignerInfo type are discussed in section 5.3. Since each signer can employ a digital signature technique and future specifications could update the syntax, all implementations MUST gracefully handle unimplemented versions of SignerInfo. Further, since all implementations will not support every possible signature algorithm, all implementations MUST gracefully handle unimplemented signature algorithms when they are encountered.

This block of text is replaced with:

> signerInfos is a collection of per-signer information. There MAY be any number of elements in the collection, including zero. When the collection represents more than one signature, the successful validation of one of signature from a given signer ought to be treated as a successful signature by that signer. However, there are some application environments where other rules are

needed. The details of the SignerInfo type are discussed in section 5.3. Since each signer can employ a different digital signature technique, and future specifications could update the syntax, all implementations MUST gracefully handle unimplemented versions of SignerInfo. Further, since all implementations will not support every possible signature algorithm, all implementations MUST gracefully handle unimplemented signature algorithms when they are encountered.

6. Security Considerations

The replacement text will reduce the likelihood of interoperability errors during the transition from MD5 and SHA-1 to stronger one-way hash functions, or to better signature algorithms.

7. Normative References

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

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

Author's Address

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.