CMS (RFC 3852) Implementation Report

Submitted by Sean Turner, IECA, Inc.
30 March 2009

1 Summary

This document provides an implementation report for Cryptographic Message Syntax (CMS) [CMS]. The methodology used to develop this document is explained, the questionnaire used to develop some of the report is included, and the eight different "products" are listed, the results of the questionnaire is included, and a conclusion is provided. The editor makes no claim as to the accuracy of the information provided.

2 Methodology

Russ Housley and Tim Polk challenged/tasked the author of this document to move [CMS] to draft standard. Russ and Tim suggested that Guidance on Interoperation and Implementation Reports [IMPREP] be consulted. Russ, Tim, and myself developed a questionnaire that identified features necessary to move [CMS] from proposed standard to draft standard. Additionally, some "bonus" questions were asked that are not used to move the standard along but were considered interesting to know.

Five implementations responded to the questionnaire. 1 has been in existence for 10 years (crytplib 3.2.2) and multiple versions are freely available (cryptlb 3.2.2 and OpenSSL). More than one of the implementations are programming toolkits and not end-user application (i.e., they are not mail clients).

Additional input has been derived from Jim Schaad's interoperability matrix developed long, long ago in a far, far away galaxy to test a previous version of CMS [CMSOLD]. That effort was abandoned because the old rules required that all normative references be at the same standardization level, and there was little chance [PKIX-1] would have made it.

3 Questionnaire

The following questionnaire was distributed on 26 January 2009 and 11 February 2009 to ietf-smime@imc.org:

What evidence do you have that you can interop with other implementations?
Have you worked through the examples draft?

Which of the following content types did you implement:

- ContentInfo,
- id-data,
- id-signed-data,
- id-enveloped-data?

For those that implemented SignedData:

- which version(s): v1, v3, v4, v5?
- without Certificates & CRLs?
- with Certificates?
- with CRL?
- with embedded content?
- with detached content?
- SignerInfo without signed attributes?
- SignerInfo with signed attributes: id-messageDigest, id-contentType, id-signingTime, id-counterSignature?
- SignerInfo with unsigned attributes?
- SignerInfo with SKI, issuer/serialnumber, or both?

For those that implemented EnvelopedData:

- which version(s): v0, v2, v3, v4?
- with unprotected attributes?
- which RecipientInfo: ktri, kari, kekri, pwri, ori?
- for ktri, which identifier issuer/serial, SKI, or both?
- for kari, which identifier issuer/serial, SKI, or both?
- for kari, was ukm supported?
- for kekri, is date, other or both supported in KEKIdentifier?

For those that implemented both SignedData and EnvelopedData, can you support receiving a triple wrapped message: An id-signedData encapsulated in an id-envelopedData encapsulated in id-envelopedData?

Bonus questions, which are not going to be included in the CMS interop report:

- for SignedData, do you support the multisig ID?
- for AuthenticatedData, do you support DigestedData, CompressedData, EncryptedData, and/or AuthEnvelopedData?
- for SignedData what do you do when you encounter an attribute that you don't support?

4 Implementations

As noted earlier, results from 9 implementations were received. The implementations are as follow:

1. OpenSSL 0.9.8h and later when compiled to enable CMS support <http://www.openssl.org/>
2. cryptlib 3.3.2 <http://www.cs.auckland.ac.nz/~pgut001/cryptlib/>
3. CryptoSys PKI Toolkit v3.2 <http://www.cryptosys.net/pki/>
4. IAIK-CMS with S/MIMEv3" Java Toolkit, version 4.01 <http://jce.iaik.tugraz.at/sic/products/communication_messaging_security/cms_s_mime>
5. Simple Cisco Enrollment Protocol (SCEP) Server

6. Outlook 2000
7. S/MIME Freeware Library (SFL)
8. Deming/Tumbleweed
9. Jim Schaad's hacked up code base

The numbers above correspond to the tables in the following section. This was done for brevity.

5 Supported Features

5.1 Demonstration of Interoperability

The following summarizes the replies to evidence of interoperability:

- OpenSSL was tested against Microsoft Outlook Express and Thunderbird. Where OpenSSL included features not supported by Microsoft Outlook Express or Thunderbird, testing was performed using OpenSSL as both sender and receiver.
- The latest versions of crytolib and IAIK were not checked against [EXAMPLES], but earlier version were.
- CryptoSys, Microsoft Outlook, Deming/Tumbleweed, Jim's code, and SFL were all tested against [EXAMPLES].
- SCEP was not tested against [EXAMPLES].

5.2 Distilled Questionnaire Data

Y=Yes, N=No, and -=Not Applicable. When referring to version the #s are the version #.

Support for:	1	2	3	4	5	6	7	8	9
Content-Info	Y	Y	-	Y	Y	Y	Y	-	Y
id-data	Y	Y	-	Y	Y	Y	Y	-	Y
id-signed-data	Y	Y	Y	Y	Y	Y	Y	Y	Y
Id-encrytped-data	Y	Y	Y	Y	Y	Y	Y	Y	Y

For id-signed-data:	1	2	3	4	5	6	7	8	9
Which version	1, 3, 4, 5	1, 3	1	1, 3, 4, 5	1	1, 3, 5	1, 3	-	1, 3, 4, 5
Without certificates & CRLs	Y	Y	Y	Y	-	Y	Y	-	Y
With certificates	Y	Y	Y	Y	Y	Y	Y	-	Y
With CRLs	Y	N	N	Y	N	Y	Y	-	Y
With embedded content	Y	Y	Y	Y	Y	Y	Y	Y	Y
With detached content	Y	Y	Y	Y	N	Y	Y	Y	Y
Without signed attributes	Y	Y	Y	Y	N	Y	Y	-	Y
With id-messageDigest	Y	Y	Y	Y	Y	Y	Y	Y	Y
With id-contentType	Y	Y	Y	Y	Y	Y	Y	Y	Y
With id-signingTime	Y	Y	Y	Y	N	Y	Y	Y	Y
With id-counterSignature?	Y	Y	N	Y	N	Y	Y	-	Y

With unsigned attributes?	Y	Y	Y	Y	Y	Y	Y	-	Y
With identifier: subject key id	Y	Y	N	Y	N	Y	Y	-	Y
With issuer & serial #	Y	Y	Y	Y	Y	Y	Y	-	Y

For id-enveloped-data	1	2	3	4	5	6	7	8	9
Which version	0, 2, 3, 4	0, 2, 3	0	0, 2, 3, 4	0	0, 2	0, 2	0	0, 2, 3, 4
With unprotected attributes	Y	Y	N	Y	-	Y	Y	-	Y
With ktri	Y	Y	Y	Y	Y	Y	Y	Y	Y
With kari	N	N	N	Y	N	Y	Y	-	Y
With kekri	Y	N	N	Y	N	Y	Y	-	Y
With pwri	N	Y	N	Y	N	N	N	-	Y
With ori	N	N	N	Y	N	N	N	-	Y
With ktri identifier: issuer & serial number	Y	Y	Y	Y	Y	Y	Y	Y	Y
With ktri identifier: subject key identifier	Y	Y	N	Y	N	Y	Y	Y	Y
With kari identifier: issuer & serial number	N	N	N	Y	N	Y	Y	-	Y
With kari identifier SKI	N	N	N	Y	N	Y	Y	-	Y
With kari ukm	N	N	N	Y	N	Y	Y	-	Y
With kekri date	Y	N	N	Y	N	Y	Y	-	Y
With kekri other	Y	N	N	Y	N	Y	Y	-	Y

Support for Wrappings	1	2	3	4	5	6	7	8	9
Triple wrapped	Y	Y	Y	Y	N	Y	Y	Y	Y

6 Analyzed Results

id-signed-data versions 4 and 5 were not universally supported. Version 5 supports non-X.509 certificates and CRLs. Version 4 supports version 2 attribute certificates. These versions should be retained to support PGP and future support for attribute certificates.

id-encrypted-data versions 3 and 4 were not universally supported. Version 4 supports non-X.509 certificates and CRLs. Version 3 version 2 certificates, pwri, and ori. These versions should be retained to support PGP and future support for attribute certificates. Further, it is believed pwri would be interoperable if tested.

7 Conclusion

This document shows that there are at least independent implementations of the relevant CMS [CMS] features. Additionally, there are two sets of implementations that interoperate with all of these features. Finally, CMS [CMS] implementations are very widely deployed. Based on these conclusions, CMS [CMS] should be progressed to draft standard. Note that no changes to CMS [CMS] are proposed (i.e., no need to republish RFC).

8 Acknowledgments

Thanks, in no particular order, to Peter Gutmann, David Ireland, Jean-Paul Lemaire, Dr. Stephen Henson, Dietre Bratko, Jim Schaad, Russ Housley, Tim Polk, and all those who participated in the development of [CMS] and [EXAMPLES].

9 References

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

[CMSOLD] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 2630, June 1999.

[EXAMPLES] Hoffman, P., "Examples of S/MIME", RFC 4134, July 2005.

[IMPREP] Dusseault, L. "Guidance on Interoperation and Implementation Reports", draft-dusseault-impl-reports-00.txt.