

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: July 28, 2011

J. Schaad
Soaring Hawk Consulting
January 24, 2011

Experiment: Hash functions with parameters in CMS and S/MIME
draft-schaad-smime-hash-experiment-06

Abstract

New hash algorithms are being developed and these algorithms may include parameters. CMS has not currently defined any hash algorithms with parameters, but anecdotal evidence suggests that defining one could cause major problems. In this document we define just such an algorithm and describe how to use it so that we can run experiments to find out how bad including hash parameters will be.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 28, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as

Internet-Draft

CMS Parameterized Hash

January 2011

described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Notation	5
2.	XOR-MD5 Digest Algorithm	6
3.	ASN.1 Encoding	7
4.	CMS ASN.1 Handling	8
5.	MIME handling	9
6.	IANA Considerations	10
7.	Security Considerations	11
8.	References	12
8.1.	Normative References	12
8.2.	Informational References	12
Appendix A.	Examples	13
A.1.	Encapsulated Signed Data Example	13
A.2.	Multipart Signed Message	15
A.3.	Authenticated Data Example	17
Appendix B.	2008 ASN.1 Module	18
	Author's Address	19

[1.](#) Introduction

At the present time, all hash algorithms that are used in Cryptographic Message Syntax (CMS) implementations are defined as having no parameters. Anecdotal evidence suggests that if a hash algorithm is defined that does require the presence of parameters there may be extensive problems. This document presents the details needed to run an experiment so that we can find out just how bad the situation really is and, if we need to, either make drastic changes in implementations or make sure that any hash algorithms chosen do not have parameters.

In CMS data structures, hash algorithms currently exist in the following locations:

- o `SignerInfo.digestAlgorithm` -- holds the digest algorithm used to compute the hash value over the content.
- o `DigestedData.digestAlgorithm` -- holds the digest algorithm used to compute the hash value over the content
- o `AuthenticatedData.digestAlgorithm` -- holds the digest algorithm used to compute the hash value over the content
- o `SignedData.digestAlgorithms` -- an optional location to place information about the set of digest algorithms used in computing the hash value over the content.
- o `multipart/signed micalg` - Holds a textual indicator of the hash algorithm for multipart signed MIME messages.

The first three locations hold the identification of a single hash, and would hold the parameters for that hash. These fields are mandatory to be filled in.

The ASN.1 defined for the types `DigestedData` and `AuthenticatedData`

are defined by placing the digest algorithm before the encapsulated data. This means that the hash algorithm (including the parameters) is fully defined before the hash function would start hashing the encapsulated data.

In the ASN.1 defined for the SignedData type, the value of SignerInfo.digestAlgorithm is not seen until the content has been processed. This is the reason for the existence of the SignedData.digestAlgorithms field, so that the set of all digest algorithms used can be seen prior to the content being processed. It is not currently a mandatory to fill in this field, and the signature validation process is supposed to succeed even if this field is

absent. ([RFC 5652](#) says signature validation MAY fail if the digest algorithm is absent.)

For the case of detached content, the ASN.1 structures need to be processed before processing the detached content in order to obtain the parameters of the hash function. The MIME multipart/signature content type attempts to avoid this problem by defining a micalg field which contains the set of hash algorithms (with parameters) so that the hash functions can be setup prior to processing the content.

When processing multipart/signed messages two paths exists:

1. Process the message content before the ASN.1. The steps involved are:
 - * Get a set of hash functions by looking at the micalg parameter and potentially add a set of generic algorithms
 - * Create a hasher for each of those algorithms
 - * Hash the message content (the first part of the multipart)
 - * Process the ASN.1 and have a potential failure point if a hash algorithm is required which was not computed.
2. Process the message content after the ASN.1. The steps involved are:
 - * Save the message content for later processing

- * Parse the ASN.1 and build a list of hash functions based on it's content
- * Create a hasher for each of those algorithms
- * Hash the saved message content
- * Perform the signature validation.

The first path allows for single pass processing, but has the potential that a fallback path needs to be added in some cases. The second path does not need a fallback path, but does not allow for single pass processing.

The fallback path above may also be needed for the encapsulated content case. Since it is optional to place hash algorithms in the SignedData.digestAlgorithms field, the content will be completely parsed before the set of hash algorithms used in the various

SignerInfo structures are determined. It may be that we need to require population of the SignedData.digestAlgorithms field if we adopt a parameterized hash field.

In this document a new hash function is created that is based on the XOR operator and on MD5. MD5 was deliberately used as the basis of this digest algorithm since it is known to be insecure and I do not want to make any statements that the hash algorithm designed here is in any way secure. This hash function MUST NOT be released as shipping code, it is designed only for use in experimentation. An example of a parameterized hash algorithm that might be standardized is a scheme developed by Shai Halevi and others [[Random-Hash](#)].

1.1. Notation

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. XOR-MD5 Digest Algorithm

The XOR-MD5 digest algorithm has been designed to use two existing operators, XOR and the MD5 hash algorithm [[MD5](#)]. The hash algorithm works as follows:

1. A random XOR string consisting of exactly 64 bytes is created.
2. The input content is broken up into 64 byte blocks. The last block may be less than 64 bytes.
3. Each block is XOR-ed with the random string. The last block uses the same number of bits from the random string as it contains.
4. The resulting string is run through the MD5 hash function.

The length of the XOR string was designed to match the barrel size of the MD5 hash function.

[3.](#) ASN.1 Encoding

The following ASN.1 is used to define the algorithm:

```
mda-xor-md5-EXPERIMENT DIGEST-ALGORITHM ::= {  
    IDENTIFIER id-alg-MD5-XOR-EXPERIMENT  
    PARAMS TYPE MD5-XOR-EXPERIMENT ARE required  
}
```

```
id-alg-MD5-XOR-EXPERIMENT OBJECT IDENTIFIER ::= {  
    iso(1) member-body(2) us(840) rsadsi(113549)  
    pkcs(1) pkcs-9(9) smime(16) id-alg(3) 13  
}
```

```
MD5-XOR-EXPERIMENT ::= OCTET STRING (SIZE(64))
```

The octet string holds the value of the random XOR string.

The algorithm is added to the DigestAlgorithmSet in [[CMS](#)].

When this algorithm is used in a signed message, it is REQUIRED that the algorithm be placed in the SignedData.digestAlgorithms sequence. The algorithm MUST appear in the sequence at least once for each unique set of parameters. The algorithm SHOULD NOT appear multiple times with the same set of parameters.

[5.](#) MIME handling

This section defines the string that appears in the micalg parameter.

The algorithm is identified by the string xor-md5. The parameters for the algorithm are the hex encoded DER ASN.1 encoding. The parameters and the identifier string are separated by a colon. One of the issues that needs to be addressed is the fact this this will generate very long data values for parameters. These will be too long for many systems to deal with. The issue of how to deal with this has been addressed by creating a method to fragment values in [\[RFC2231\]](#). An example content-type string that has been fragmented is:

```
Content-Type: multipart/signed;  
  protocol="application/pkcs7-signature";  
  micalg*0="sha1, xor-md5:04400102030405060708090a0b0c0d0e0f0011";  
  micalg*1="12131415161718191a1b1c1d1e1f102122232425262728292a2b";  
  micalg*2="2c2d2e2f203132333435363738";  
  micalg*3="393a3b3c3d3e3f30";  boundary=boundar42
```

Arguments could be made that the string should be base64 encoded rather than hex encoding the string. The advantage is that the resulting encoding is shorter. This could be significant if there are a substantial number of parameters and of a substantial size. Even with the above example we needed to break the encoding across multiple lines. The downside would be the requirement that the micalg parameter always be quoted.

It may be reasonable to require that whitespace be inserted only on encoding boundaries, but it seems to be overly restrictive.

[6.](#) IANA Considerations

There are no IANA considerations. All identifiers are assigned out of the S/MIME OID arc.

[7.](#) Security Considerations

The algorithm XOR-MD5 is not designed for general purpose use. The hash algorithm included here is designed for running this experiment and nothing more.

This document makes no representation that XOR-MD5 is a secure digest algorithm. I believe that the algorithm is no more secure than MD5, and I consider MD5 to be a broken hash algorithm for many purposes.

One known issue with the algorithm as present is the fact that the xor pattern is always 64 bytes long, even if the data is shorter. This means that there is a section of the data than can be manipulated without changing the hash. In a real algorithm this should either be truncated or forced to a known value.

[8.](#) References

[8.1.](#) Normative References

- [MD5] Rivest, R., "The MD5 Message-Digest Algorithm", [RFC 1321](#), April 1992.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2231] Freed, N. and K. Moore, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", [RFC 2231](#), November 1997.
- [CMS] Housley, R., "Cryptographic Message Syntax (CMS)", [RFC 5652](#), September 2009.
- [SMIME-MSG] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", [RFC 5751](#), January 2010.
- [ASN.1-2008] ITU-T, "ITU-T Recommendations X.680, X.681, X.682, and

X.683", 2008.

[8.2.](#) Informational References

[SMIME-EXAMPLES]

Hoffman, P., "Examples of S/MIME Messages", [RFC 4134](#), July 2005.

[CMS-ASN] Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", [RFC 5911](#), June 2010.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", [RFC 5912](#), June 2010.

[Random-Hash]

Halevi, S., Shao, W., Krawczyk, H., Boneh, D., and M. McIntosh, "Implementing the Halevi-Krawczyk Randomized Hashing Scheme".

Schaad

Expires July 28, 2011

[Page 12]

Internet-Draft

CMS Parameterized Hash

January 2011

[Appendix A.](#) Examples

Provided here are a set of simple S/MIME messages [[SMIME-MSG](#)] that are provided for testing. The content used is the same as that found in Section 2.1 of [[SMIME-EXAMPLES](#)]. The certificates and key pairs found in [[SMIME-EXAMPLES](#)] are also used here.

The perl script in [Appendix A](#) of [[SMIME-EXAMPLES](#)] can be used to extract the binary examples from this file. The mime examples can be extracted with a standard text editor.

Note: The examples presented here have not been independently verified. I was unable to use the Microsoft APIs because of the new cryptographic hash algorithm. However, for the purposes of this experiment I believe that the form of the messages, which can be verified visually as correct, is more important than the question of the message validating.

NOTE FOR RFC EDITOR: The | character needs to be in column #1 in order for the extraction script to work. I would suggest that all of the examples below (inside of the artwork) start in column #1.

[A.1.](#) Encapsulated Signed Data Example

This section contains a detached signed data example. The content was hashed with the md5-xor algorithm defined in this document. The signature is performed using RSA with MD5. The signature is wrapped as an embedded signed mime message.

```
MIME-Version: 1.0
To: BobRSA@example.com
From: AliceDss@example.com
Subject: MD5-XOR example message
Message-Id: <34567809323489fd.esc@example.com>
Date: Wed, 16 Dec 2010 23:13:00 -0500
Content-Type: application/pkcs7-mime; smime-type=signed-data;
  name=smime.p7m;
  micalg*0="xor-md5: 0440010203405060708090a0b0c0d0e0f10";
  micalg*1="111213415161718191a1b1c1d1e1f20212223425262728292a2b2c";
  micalg*2="2d2e2f30313233435363738393a3b3c3d3e3f40"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
```

```
MIIEqAYJKoZIhvcNAQcCoIIEmTCCBJUCAQEExUTBPBgsqhkiG9w0BCRADDQRAAQIDBAUGBw
gJCgsMDQ4PEBESEwQVFhcYGRobHB0eHyAhIiMEJSYnKCKqKywtLi8wMTIzBDU2Nzg5Ojs8
PT4/QDARBgkqhkiG9w0BBwGgHgQcVGhpcyBpcyBzb21lIHh0eXBsZSBjb250ZW50LQCCAi
swggInMIIBKkADAgECAhBGNGvHgABWvBHTbi7NXXHQMA0GCSqGSIb3DQEBBQUAMBIxEDAO
BgNVBAMTB0NhcmxSU0EwHhcNOTkwOTE5MDEwOTAYWhcNMzkxMjMxMjM1OTU5WjARMQ8wDQ
```

```
YDVQQDEwZC2JSU0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKnhZ5g/OdVf8qCT
QV6meYmFyDVdmpFb+x0B2hlwJhcPvaUi0DWFbXqYZhRBXM+3twg7CcmRuB1pN235ZR572a
kzJKN/07uvRgGGNjQyywcDWVL8hYsxBLjMGAUSOZPHPTdYMTgXB9T039T2GkB8QX4enDR
voPGXzjPHCyqaqfrAgMBAAGj fzb9MAwGA1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgUGMB
8GA1UdIwQYMBaAF0ngkCeseCB6mtNM8kI3TiKunji7MB0GA1UdDgQWBBTo9Lhn2LOWpCrz
Eaop05Vahha0JDAdBgNVHREEFjAugRJCb2JSU0FAZXhhbXBsZS5jb20wDQYJKoZIhvcNAQ
EFBQADgYEAE45mxfEQPxAgTIhxq3tAayEz+kqV3p00W2uUIQXA8uF+Ks2ck4iH+4u3fn1B
YeHk1m354gRVYUW8ZCdEwKG9WXnZHWQ8IdZFsf1oM5LqrPFX5YF9m0Y1kaM53nf06Bw7Kd
x/UQeX8zbwUArmd962XjgRK/tX6oltrcmI2I/PK9MxggHfMIIB2wIBATAmMBIxEDA0BgNV
BAMTB0NhcmxSU0ECEY0a8eAAFa8EdNuLs1dcdAwTwYlKoZIhvcNAQkQAww0EQAECawQFBg
cICQoLDA00DxAREhMEFRYXGBkaGxwdHh8gISIjBCUmJygpKissLS4vMDEyMwQ1Njc40To7
```

PD0+P0CggcowGAYJKoZIhvcNAQkDMQsGCSqGSIB3DQEHATAcBgkqhkiG9w0BCQUxDxcNMD
kxMjEwMjMyNTAwWjAfbGkqhkiG9w0BCQQxEgQQLmmuYRtXnoPqECtrSd3A+TBvBgkqhkiG
9w0BCTQxYjBgME8GCyqGSIB3DQEJEAMNBEABAgMEBQYHCAkKCwwNDg8QERITBBUWFxgZGh
schr4fICEiIwQlJicoKSorLC0uLzAxMjMENTY30Dk60zw9Pj9AoQ0GCSqGSIB3DQEBBAUA
MA0GCSqGSIB3DQEBBAUABIGAClmpfG4IL1yAdRxWdvYKbtuFz1XKnFqo9ui7V5PndjlDut
yib02knY7UtGNhg6oVEkiZHxYh/iLuoLOHSFA1P4ZacTYrEKChF4K18dsqvlFip1vn8BG/
ysFUDfbx5VcTG2Md0/NHV+qj5ihqM+Pye6Urp+5jbqVgpZ0XSLfP+pI=

|>sd.bin

|MIIeQAYJKoZIhvcNAQcCoIIEmTCCBJUCAQEExUTBPBgsqhkiG9w0BCRADDQRAAQIDBAUGBw
|gJCgsMDQ4PEBESEwQVFhcYGRobHB0eHyAhIiMEJSYnKCkqKywtLi8wMTIzBDU2Nzg50js8
|PT4/QDARBgkqhkiG9w0BBwGgHgQcVGhpcyBpcyBzb21lIHNBhXBsZSBjb250ZW50LQCCAi
|swggInMIIbKADAgECAhBGNGvHgABWvBHTbi7NXXHQMA0GCSqGSIB3DQEBBQUAMBIxEDA0
|BgNVBAMTB0NhcmxSU0EwHhcNOTkwOTE5MDEwOTAYWhcNMzkxMjM1OTU5WjARMQ8wDQ
|YDVQQDEwZCb2JSU0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKnhZ5g/Odvf8qCT
|QV6meYmFyDVdmpFb+x0B2hlwJhcPvaUi0DWfBxqYZhRBXM+3twg7CcmRuBlpN235ZR572a
|kzJKN/07uvRgGGNjQyywcDWVL8hYsXBLjMGAUSOZPHPtYMTgXB9T039T2Gk8QX4enDR
|voPGXzjPHCYqaqfrAgMBAAGjfbzB9MAwGA1UdEwEB/wQCMAAwDgYDVR0PAAQH/BAQDAgUGMB
|8GA1UdIwQYMBaAFongkCeseCB6mtNM8kI3TiKunji7MB0GA1UdDgQWBbTo9Lhn2LOWpCrz
|Eaop05Vahha0JDAdBgNVHREEfjAUGrJCb2JSU0FAZXhbbXBsZS5jb20wDQYJKoZIhvcNAQ
|EFBQADgYEAe45mxfEQPxAgTIhxq3tAayEz+kqV3p00W2uUIQXA8uF+Ks2ck4iH+4u3fn1B
|YeHk1m354gRVYUW8ZCdEwKG9WXnZHWQ8IdZFsf1oM5LqrPFX5YF9mOY1kaM53nf06Bw7Kd
|x/UQeX8zbwUArDm962XjgRK/tX6o1trcmI2I/PK9MxggHfMIIb2wIBATAmMBIxEDA0BgNV
|BAMTB0NhcmxSU0ECEY0a8eAAFa8EdNuLs1dcdAwTwYLKoZIhvcNAQkQAw0EQAECawQFBg
|cICQoLDA00DxAREhMEFRYXGBkaGxwdHh8gISIjBCUmJygpKissLS4vMDEyMwQ1Njc40To7
|PD0+P0CggcowGAYJKoZIhvcNAQkDMQsGCSqGSIB3DQEHATAcBgkqhkiG9w0BCQUxDxcNMD
|kxMjEwMjMyNTAwWjAfbGkqhkiG9w0BCQQxEgQQLmmuYRtXnoPqECtrSd3A+TBvBgkqhkiG
|9w0BCTQxYjBgME8GCyqGSIB3DQEJEAMNBEABAgMEBQYHCAkKCwwNDg8QERITBBUWFxgZGh
|schr4fICEiIwQlJicoKSorLC0uLzAxMjMENTY30Dk60zw9Pj9AoQ0GCSqGSIB3DQEBBAUA
|MA0GCSqGSIB3DQEBBAUABIGAClmpfG4IL1yAdRxWdvYKbtuFz1XKnFqo9ui7V5PndjlDut
|yib02knY7UtGNhg6oVEkiZHxYh/iLuoLOHSFA1P4ZacTYrEKChF4K18dsqvlFip1vn8BG/
|ysFUDfbx5VcTG2Md0/NHV+qj5ihqM+Pye6Urp+5jbqVgpZ0XSLfP+pI=

|<sd.bin

[A.2.](#) Multipart Signed Message

This section contains a detached signed data example. The content was hashed with the md5-xor algorithm defined in this document. The

signature is performed using RSA with MD5. The signature is wrapped as a detached signed mime message.

-----=_NextBoundry____Fri,_18_Dec_2009_00:25:21--

Schaad

Expires July 28, 2011

[Page 16]

Internet-Draft

CMS Parameterized Hash

January 2011

[A.3.](#) Authenticated Data Example

This section contains an authenticated data example. The content was hashed with the md5-xor algorithm defined in this document. The authentication was done with the HMAC-SHA1 algorithm. The key is transported using RSA encryption to BobRSASignByCarl certificate.

MIME-Version: 1.0
To: BobRSA@example.com
From: AliceDss@example.com
Subject: MD5-XOR example message
Message-Id: <34567809323489fd.esc@example.com>
Date: Wed, 16 Dec 2010 23:13:00 -0500
Content-Type: application/pkcs7-mime; smime-type=authenticated-data;
 name=smime.p7m;
 micalg*0="xor-md5: 0440010203405060708090a0b0c0d0e0f10";
 micalg*1="111213415161718191a1b1c1d1e1f20212223425262728292a2b2c2d2e";
 micalg*2="2f30313233435363738393a3b3c3d3e3f40"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

MIICRQYLKoZIhvcNAQkQAQKgggI0MIICMAIBADGBwDCBvQIBADAmMBIxEDA0BgNVBAMMB0
NhcmxSU0ECEEEY0a8eAAFa8EdNuLs1dcdAwDQYJKoZIhvcNAQEBBQAEGYCH70EpEikY7deb
859YJRAWfFondQv1D4NFltw6C1ceheWnLAU0C2WEXr3LUBXZp1/PSte29FnJxu5bXCTn1g
eLmM6zNLZNWNd0KadVBcaxi1n8L52tVM5sWFGJP05cSt0yAka2ucuZM6iAnCSkn1Ju7fgU
5j2g3bZ/IM8nHTcygjAKBggrBgEFBQgBAqFPBgshkiG9w0BCRADDQRAAQIDBAUGBwgJCg
sMDQ4PEBESEwQVFhcYGRobHB0eHyAhIiMEJSYnKCKqKywtLi8wMTIzBDU2Nzg50js8PT4/
QDARBgkqhkiG9w0BBwGgHgQcVGhpcyBpcyBzb21lIHhnbXBsZSBjb250ZW50LqKBxzAYBg
kqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0wOTEyMTAyMzI1MDBa
MB8GCSqGSIb3DQEJBDESBBCWaa5hG1eeg+oQK2tJ3cD5MGwGCSqGSIb3DQEJNDFmF0wTw
YLKoZIhvcNAQkQAww0EQAECawQFBgcICQoLDA0ODxAREhMEFRYXGBkaGxwdHh8gISIjBCUm
JygpKissLS4vMDEyMwQ1Njc4OT07PD0+P0CiCgYIKwYBBQUIAQIEFLjUxQ9PJFzFnWraxb
EIbVbg2xql

|>ad.bin

|MIICRQYLKoZIhvcNAQkQAQKgggI0MIICMAIBADGBwDCBvQIBADAmMBIxEDA0BgNVBAMMB0
|NhcmxSU0ECEEEY0a8eAAFa8EdNuLs1dcdAwDQYJKoZIhvcNAQEBBQAEGYCH70EpEikY7deb
|859YJRAWfFondQv1D4NFltw6C1ceheWnLAU0C2WEXr3LUBXZp1/PSte29FnJxu5bXCTn1g
|eLmM6zNLZNWNd0KadVBcaxi1n8L52tVM5sWFGJP05cSt0yAka2ucuZM6iAnCSkn1Ju7fgU
|5j2g3bZ/IM8nHTcygjAKBggrBgEFBQgBAqFPBgshkiG9w0BCRADDQRAAQIDBAUGBwgJCg

```
|sMDQ4PEBESEwQVFhcYGRobHB0eHyAhIiMEJSYnKCKqKywtLi8wMTIzBDU2Nzg50js8PT4/  
|QDArBgkqhkiG9w0BBWgGgHgQcVGhpcyBpcyBzb21lIHhnbXBsZSBjb250ZW50LqKBxzAYBg  
|kqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0wOTEyMTAyMzI1MDBa  
|MB8GCSqGSIb3DQEJBDESBBCWaa5hG1eeg+oQK2tJ3cD5MGwGCSqGSIb3DQEJNDFfMF0wTw  
|YLKoZIhvcNAQkQAww0EQAECawQFBgcICQoLDA0ODxAREhMEFRYXGBkaGxwdHh8gISIjBCUm  
|JygpKissLS4vMDEyMwQ1Njc4OT07PD0+P0CiCgYIKwYBBQUIAQIEFLjUxQ9PJFzFnWraxb  
|EibVbg2xql  
|<ad.bin
```

Schaad

Expires July 28, 2011

[Page 17]

Internet-Draft

CMS Parameterized Hash

January 2011

[Appendix B](#). 2008 ASN.1 Module

The ASN.1 module defined uses the 2008 ASN.1 definitions found in [\[ASN.1-2008\]](#). This module contains the ASN.1 module which contains the required definitions for the types and values defined in this document. The module uses the class defined in [\[CMS-ASN\]](#) and [\[RFC5912\]](#).

MD5-HASH-EXPERIMENT

```
{ iso(1) member-body(2) us(840) rsadsi(113549)  
  pkcs(1) pkcs-9(9) smime(16) modules(0)  
  id-mod-MD5-XOR-EXPERIMENT(999) }
```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

-- Cryptographic Message Syntax (CMS) [\[CMS\]](#)

DigestAlgorithmIdentifier, MessageAuthenticationCodeAlgorithm,
SignatureAlgorithmIdentifier, DIGEST-ALGORITHM
FROM CryptographicMessageSyntax-2009

```
{ iso(1) member-body(2) us(840) rsadsi(113549)  
  pkcs(1) pkcs-9(9) smime(16) modules(0) id-mod-cms-2004-02(41) }
```

-- Common PKIX structures [\[RFC5912\]](#)

ATTRIBUTE

FROM PKIX-CommonTypes-2009

```
{ iso(1) identified-organization(3) dod(6) internet(1)  
  security(5) mechanisms(5) pkix(7) id-mod(0)  
  id-mod-pkixCommon-02(57)};
```

mda-xor-md5-EXPERIMENT DIGEST-ALGORITHM ::= {

```
IDENTIFIER id-alg-MD5-XOR-EXPERIMENT
PARAMS TYPE MD5-XOR-EXPERIMENT ARE required
}

id-alg-MD5-XOR-EXPERIMENT OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs-9(9) smime(16) id-alg(3) 13
}

MD5-XOR-EXPERIMENT ::= OCTET STRING (SIZE(64))

END
```

Schaad

Expires July 28, 2011

[Page 18]

Internet-Draft

CMS Parameterized Hash

January 2011

Author's Address

Jim Schaad
Soaring Hawk Consulting

Email: ietf@augustcellars.com

