Additional XML Security Uniform Resource Identifiers (URIs)

Abstract

This document expands, updates, and establishes an IANA registry for the list of URIs intended for use with XML digital signatures, encryption, canonicalization, and key management. These URIs identify algorithms and types of information. This document obsoletes RFC 4051.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6931.

Copyright Notice

Copyright (c) 2013 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 described in the Simplified BSD License.
Table of Contents

1. Introduction ....................................................3
   1.1. Terminology ................................................4
   1.2. Acronyms ...................................................4
2. Algorithms ......................................................5
   2.1. DigestMethod (Hash) Algorithms .............................5
       2.1.1. MD5 .................................................5
       2.1.2. SHA-224 .............................................6
       2.1.3. SHA-384 .............................................6
       2.1.4. Whirlpool ...........................................6
       2.1.5. New SHA Functions ...................................7
   2.2. SignatureMethod MAC Algorithms .............................7
       2.2.1. HMAC-MD5 ............................................7
       2.2.2. HMAC SHA Variations ................................8
       2.2.3. HMAC-RIPemd160 .....................................8
   2.3. SignatureMethod Public-Key Signature Algorithms ............9
       2.3.1. RSA-MD5 .............................................9
       2.3.2. RSA-SHA256 .........................................10
       2.3.3. RSA-SHA384 .........................................10
       2.3.4. RSA-SHA512 .........................................10
       2.3.5. RSA-RIPemd160 ......................................11
       2.3.6. ECDSA-SHA*, ECDSA-RIPemd160, ECDSA-Whirlpool ......11
       2.3.7. ESIGN-SHA* .........................................12
       2.3.8. RSA-Whirlpool ......................................12
       2.3.9. RSASSA-PSS with Parameters ..........................13
       2.3.10. RSASSA-PSS without Parameters ......................14
       2.3.11. RSA-SHA224 ........................................15
   2.4. Minimal Canonicalization ..................................15
2.5. Transform Algorithms ......................................16
   2.5.1. XPointer ...........................................16
2.6. EncryptionMethod Algorithms ...............................17
   2.6.1. ARCFour Encryption Algorithm ..........................17
   2.6.2. Camellia Block Encryption .............................17
   2.6.3. Camellia Key Wrap ....................................17
   2.6.4. P SEC-KEM ...........................................18
   2.6.5. SEED Block Encryption ................................19
   2.6.6. SEED Key Wrap .......................................19
3. KeyInfo ........................................................19
   3.1. PKCS #7 Bag of Certificates and CRLs ......................20
   3.2. Additional RetrievalMethod Type Values ....................20
4. Indexes ........................................................20
   4.1. Fragment Index ..........................................21
   4.2. URI Index .................................................24
5. Allocation Considerations ......................................27
   5.1. W3C Allocation Considerations ............................27
   5.2. IANA Considerations .....................................28
6. Security Considerations ........................................28
1. Introduction

XML digital signatures, canonicalization, and encryption have been standardized by the W3C and by the joint IETF/W3C XMLDSIG working group [W3C]. All of these are now W3C Recommendations and some are also RFCs. They are available as follows:

<table>
<thead>
<tr>
<th>RFC</th>
<th>W3C REC</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>[RFC3275]</td>
<td>[XMLDSIG10]</td>
<td>XML Digital Signatures</td>
</tr>
<tr>
<td>Draft Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[RFC3076]</td>
<td>[CANON10]</td>
<td>Canonical XML</td>
</tr>
<tr>
<td>Informational</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- - - - -</td>
<td>[XMLENC10]</td>
<td>XML Encryption 1.0</td>
</tr>
<tr>
<td>[RFC3741]</td>
<td>[XCANON]</td>
<td>Exclusive XML Canonicalization 1.0</td>
</tr>
<tr>
<td>Informational</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All of these documents and recommendations use URIs [RFC3986] to identify algorithms and keying information types. The W3C has subsequently produced updated XML Signature 1.1 [XMLDSIG11], Canonical XML 1.1 [CANON11], and XML Encryption 1.1 [XMLENC11] versions, as well as a new XML Signature Properties specification [XMLDSIG-PROP].

All camel-case element names herein, such as DigestValue, are from these documents.

This document is an updated convenient reference list of URIs and corresponding algorithms in which there is expressed interest. Since the previous list [RFC4051] was issued in 2005, significant new cryptographic algorithms of interest to XML security, for some of which the URI is only specified in this document, have been added. This document obsoletes [RFC4051]. All of the URIs appear in the indexes in Section 4. Only the URIs that were added by [RFC4051] or this document have a subsection in Section 2 or 3, with the exception of Minimal Canonicalization (Section 2.4), for example, use of
SHA-256 is defined in [XMLENC11] and hence there is no subsection on that algorithm here, but its URI is included in the indexes in Section 4.

Specification in this document of the URI representing an algorithm does not imply endorsement of the algorithm for any particular purpose. A protocol specification, which this is not, generally gives algorithm and implementation requirements for the protocol. Security considerations for algorithms are constantly evolving, as documented elsewhere. This specification simply provides some URIs and relevant formatting for when those URIs are used.

Note that progressing XML Digital Signature [RFC3275] along the Standards Track required removal of any algorithms from the original version [RFC3075] for which there was not demonstrated interoperability. This required removal of the Minimal Canonicalization algorithm, in which there appears to be continued interest. The URI for Minimal Canonicalization was included in [RFC4051] and is included here.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document is not intended to change the algorithm implementation requirements of any IETF or W3C document. Use of [RFC2119] terminology is intended to be only such as is already stated or implied by other authoritative documents.

1.2. Acronyms

The following acronyms are used in this document:

HMAC - Keyed-Hashing MAC [RFC2104]

IETF - Internet Engineering Task Force <www.ietf.org>

MAC - Message Authentication Code

MD - Message Digest

NIST - United States National Institute of Standards and Technology <www.nist.gov>

RC - Rivest Cipher
2. Algorithms

The URI [RFC3986] that was dropped from the XML Digital Signature standard due to the transition from Proposed Standard to Draft Standard [RFC3275] is included in Section 2.4 below with its original http://www.w3.org/2000/09/xmldsig# prefix so as to avoid changing the XMLDSIG standard’s namespace.

Additional algorithms in [RFC4051] were given URIs that start with http://www.w3.org/2001/04/xmldsig-more# while further algorithms added in this document are given URIs that start with http://www.w3.org/2007/05/xmldsig-more#

In addition, for ease of reference, this document includes in the indexes in Section 4 many cryptographic algorithm URIs from several XML security documents using the namespaces with which they are defined in those documents. For example, 2000/09/xmldsig# for some URIs specified in [RFC3275] and 2001/04/xmlenc# for some URIs specified in [XMLENC10].

See also [XMLSECXREF].

2.1. DigestMethod (Hash) Algorithms

These algorithms are usable wherever a DigestMethod element occurs.

2.1.1. MD5

Identifier:
http://www.w3.org/2001/04/xmldsig-more#md5
The MD5 algorithm [RFC1321] takes no explicit parameters. An example of an MD5 DigestAlgorithm element is:

```
<DigestAlgorithm
  Algorithm="http://www.w3.org/2001/04/xmlsig-more#md5"/>
```

An MD5 digest is a 128-bit string. The content of the DigestValue element SHALL be the base64 [RFC2045] encoding of this bit string viewed as a 16-octet stream. See [RFC6151] for MD5 security considerations.

### 2.1.2. SHA-224

**Identifier:**
http://www.w3.org/2001/04/xmlsig-more#sha224

The SHA-224 algorithm [FIPS180-4] [RFC6234] takes no explicit parameters. An example of a SHA-224 DigestAlgorithm element is:

```
<DigestAlgorithm
  Algorithm="http://www.w3.org/2001/04/xmlsig-more#sha224" />
```

A SHA-224 digest is a 224-bit string. The content of the DigestValue element SHALL be the base64 [RFC2045] encoding of this string viewed as a 28-octet stream.

### 2.1.3. SHA-384

**Identifier:**
http://www.w3.org/2001/04/xmlsig-more#sha384

The SHA-384 algorithm [FIPS180-4] takes no explicit parameters. An example of a SHA-384 DigestAlgorithm element is:

```
<DigestAlgorithm
  Algorithm="http://www.w3.org/2001/04/xmlsig-more#sha384" />
```

A SHA-384 digest is a 384-bit string. The content of the DigestValue element SHALL be the base64 [RFC2045] encoding of this string viewed as a 48-octet stream.

### 2.1.4. Whirlpool

**Identifier:**
http://www.w3.org/2007/05/xmlsig-more#whirlpool
The Whirlpool algorithm [10118-3] takes no explicit parameters. A Whirlpool digest is a 512-bit string. The content of the DigestValue element SHALL be the base64 [RFC2045] encoding of this string viewed as a 64-octet stream.

2.1.5. New SHA Functions

Identifiers:
- http://www.w3.org/2007/05/xmldsig-more#sha3-224
- http://www.w3.org/2007/05/xmldsig-more#sha3-256
- http://www.w3.org/2007/05/xmldsig-more#sha3-384
- http://www.w3.org/2007/05/xmldsig-more#sha3-512

NIST has recently completed a hash function competition for an alternative to the SHA family. The Keccak-f[1600] algorithm was selected [Keccak] [SHA-3]. This hash function is commonly referred to as "SHA-3", and this section is a space holder and reservation of URIs for future information on Keccak use in XML security.

A SHA-3 224, 256, 384, and 512 digest is a 224-, 256-, 384-, and 512-bit string, respectively. The content of the DigestValue element SHALL be the base64 [RFC2045] encoding of this string viewed as a 28-, 32-, 48-, and 64-octet stream, respectively.

2.2. SignatureMethod MAC Algorithms

This section covers SignatureMethod MAC (Message Authentication Code) Algorithms.

Note: Some text in this section is duplicated from [RFC3275] for the convenience of the reader. RFC 3275 is normative in case of conflict.

2.2.1. HMAC-MD5

Identifier:
- http://www.w3.org/2001/04/xmldsig-more#hmac-md5

The HMAC algorithm [RFC2104] takes the truncation length in bits as a parameter; if the parameter is not specified, then all the bits of the hash are output. An example of an HMAC-MD5 SignatureMethod element is as follows:

```xml
<SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-md5">
  <HMACOutputLength>112</HMACOutputLength>
</SignatureMethod>
```
The output of the HMAC algorithm is ultimately the output (possibly truncated) of the chosen digest algorithm. This value SHALL be base64 [RFC2045] encoded in the same straightforward fashion as the output of the digest algorithms. Example: the SignatureValue element for the HMAC-MD5 digest

9294727A 3638BB1C 13F48EF8 158BFC9D

from the test vectors in [RFC2104] would be

kpRyejY4uxwT9I74FYv8nQ==

Schema Definition:

```xml
<simpleType name="HMACOutputLength">
  <restriction base="integer"/>
</simpleType>
```

DTD:

```xml
<!ELEMENT HMACOutputLength (#PCDATA) >
```

The Schema Definition and DTD immediately above are copied from [RFC3275].

See [RFC6151] for HMAC-MD5 security considerations.

2.2.2. HMAC SHA Variations

Identifiers:

- http://www.w3.org/2001/04/xmldsig-more#hmac-sha224
- http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
- http://www.w3.org/2001/04/xmldsig-more#hmac-sha384
- http://www.w3.org/2001/04/xmldsig-more#hmac-sha512

SHA-224, SHA-256, SHA-384, and SHA-512 [FIPS180-4] [RFC6234] can also be used in HMAC as described in Section 2.2.1 above for HMAC-MD5.

2.2.3. HMAC-RIPEMD160

Identifier:

- http://www.w3.org/2001/04/xmldsig-more#hmac-ripemd160

RIPEMD-160 [10118-3] can also be used in HMAC as described in Section 2.2.1 above for HMAC-MD5.
2.3. SignatureMethod Public-Key Signature Algorithms

These algorithms are distinguished from those in Section 2.2 above in that they use public-key methods. That is to say, the verification key is different from and not feasibly derivable from the signing key.

2.3.1. RSA-MD5

Identifier: http://www.w3.org/2001/04/xmldsig-more#rsa-md5

This implies the PKCS#1 v1.5 padding algorithm described in [RFC3447]. An example of use is

```xml
<SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-md5"/>
```

The SignatureValue content for an RSA-MD5 signature is the base64 [RFC2045] encoding of the octet string computed as per [RFC3447], Section 8.2.1, signature generation for the RSASSA-PKCS1-v1_5 signature scheme. As specified in the EMSA-PKCS1-V1_5-ENCODE function in [RFC3447], Section 9.2, the value input to the signature function MUST contain a pre-pended algorithm object identifier for the hash function, but the availability of an ASN.1 parser and recognition of OIDs is not required of a signature verifier. The PKCS#1 v1.5 representation appears as:

```
CRYPT (PAD (ASN.1 (OID, DIGEST (data))))
```

Note that the padded ASN.1 will be of the following form:

```
01 | FF* | 00 | prefix | hash
```

Vertical bar ("|") represents concatenation. "01", "FF", and "00" are fixed octets of the corresponding hexadecimal value, and the asterisk ("*") after "FF" indicates repetition. "hash" is the MD5 digest of the data. "prefix" is the ASN.1 BER MD5 algorithm designator prefix required in PKCS #1 [RFC3447], that is,

```
hex 30 20 30 0c 06 08 2a 86 86 f7 0d 02 05 04 10
```

This prefix is included to make it easier to use standard cryptographic libraries. The FF octet MUST be repeated enough times that the value of the quantity being CRYPTed is exactly one octet shorter than the RSA modulus.

See [RFC6151] for MD5 security considerations.
2.3.2. RSA-SHA256

Identifier:
  http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

This implies the PKCS#1 v1.5 padding algorithm [RFC3447] as described in Section 2.3.1, but with the ASN.1 BER SHA-256 algorithm designator prefix. An example of use is

<SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />

2.3.3. RSA-SHA384

Identifier:
  http://www.w3.org/2001/04/xmldsig-more#rsa-sha384

This implies the PKCS#1 v1.5 padding algorithm [RFC3447] as described in Section 2.3.1, but with the ASN.1 BER SHA-384 algorithm designator prefix. An example of use is

<SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha384" />

Because it takes about the same effort to calculate a SHA-384 message digest as it does a SHA-512 message digest, it is suggested that RSA-SHA512 be used in preference to RSA-SHA384 where possible.

2.3.4. RSA-SHA512

Identifier:
  http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

This implies the PKCS#1 v1.5 padding algorithm [RFC3447] as described in Section 2.3.1, but with the ASN.1 BER SHA-512 algorithm designator prefix. An example of use is

<SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512" />
2.3.5. RSA-RIPEMD160

Identifier:
   http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160

This implies the PKCS#1 v1.5 padding algorithm [RFC3447] as described in Section 2.3.1, but with the ASN.1 BER RIPEMD160 algorithm designator prefix. An example of use is

   <SignatureMethod
      Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160"
/>  

2.3.6. ECDSA-SHA*, ECDSA-RIPEMD160, ECDSA-Whirlpool

Identifiers:
   http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1
   http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha224
   http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
   http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384
   http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512
   http://www.w3.org/2007/05/xmldsig-more#ecdsa-ripemd160
   http://www.w3.org/2007/05/xmldsig-more#ecdsa-whirlpool

The Elliptic Curve Digital Signature Algorithm (ECDSA) [FIPS180-4] is the elliptic curve analogue of the Digital Signature Algorithm (DSA) signature method, i.e., the Digital Signature Standard (DSS). It takes no explicit parameters. For detailed specifications of how to use it with SHA hash functions and XML Digital Signature, please see [X9.62] and [RFC4050]. The #ecdsa-ripemd160 and #ecdsa-whirlpool fragments in the new namespace identifies a signature method processed in the same way as specified by the #ecdsa-sha1 fragment of this namespace, with the exception that RIPEMD160 or Whirlpool is used instead of SHA-1.

The output of the ECDSA algorithm consists of a pair of integers usually referred by the pair \((r, s)\). The signature value consists of the base64 encoding of the concatenation of two octet streams that respectively result from the octet-encoding of the values \(r\) and \(s\) in that order. Conversion from integer to octet stream must be done according to the I2OSP operation defined in the [RFC3447] specification with the \(l\) parameter equal to the size of the base point order of the curve in bytes (e.g., 32 for the P-256 curve and 66 for the P-521 curve [FIPS186-3]).

For an introduction to elliptic curve cryptographic algorithms, see [RFC6090] and note the errata (Errata ID 2773-2777).
2.3.7. ESIGN-SHA*

Identifiers:
http://www.w3.org/2001/04/xmldsig-more#esign-sha1
http://www.w3.org/2001/04/xmldsig-more#esign-sha224
http://www.w3.org/2001/04/xmldsig-more#esign-sha256
http://www.w3.org/2001/04/xmldsig-more#esign-sha384
http://www.w3.org/2001/04/xmldsig-more#esign-sha512

The ESIGN algorithm specified in [IEEEP1363a] is a signature scheme based on the integer factorization problem. It is much faster than previous digital signature schemes, so ESIGN can be implemented on smart cards without special co-processors.

An example of use is

  <SignatureMethod
      Algorithm="http://www.w3.org/2001/04/xmldsig-more#esign-sha1" />

2.3.8. RSA-Whirlpool

Identifier:
http://www.w3.org/2007/05/xmldsig-more#rsa-whirlpool

As in the definition of the RSA-SHA algorithm in [XMLDSIG1], the designator "RSA" means the RSASSA-PKCS1-v1_5 algorithm as defined in [RFC3447]. When identified through the #rsa-whirlpool fragment identifier, Whirlpool is used as the hash algorithm instead. Use of the ASN.1 BER Whirlpool algorithm designator is implied. That designator is

  hex 30 4e 30 0a 06 06 28 cf 06 03 00 37 05 00 04 40
as an explicit octet sequence. This corresponds to OID 1.0.10118.3.0.55 defined in [10118-3].

An example of use is

  <SignatureMethod
      Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-whirlpool" />

2.3.9. RSASSA-PSS with Parameters

Identifiers:
http://www.w3.org/2007/05/xmldsig-more#rsa-pss
http://www.w3.org/2007/05/xmldsig-more#MGF1

These identifiers imply the PKCS#1 EMSA-PSS encoding algorithm
[RFC3447]. The RSASSA-PSS algorithm takes the digest method (hash
function), a mask generation function, the salt length in bytes
(SaltLength), and the trailer field as explicit parameters.

Algorithm identifiers for hash functions specified in XML encryption
[XMLENC11] [XMLDSIG11] and in Section 2.1 are considered to be valid
algorithm identifiers for hash functions. According to [RFC3447],
the default value for the digest function is SHA-1, but due to the
discovered weakness of SHA-1 [RFC6194], it is recommended that
SHA-256 or a stronger hash function be used. Notwithstanding
[RFC3447], SHA-256 is the default to be used with these
SignatureMethod identifiers if no hash function has been specified.

The default salt length for these SignatureMethod identifiers if the
SaltLength is not specified SHALL be the number of octets in the hash
value of the digest method, as recommended in [RFC4055]. In a
parameterized RSASSA-PSS signature the ds:DigestMethod and the
SaltLength parameters usually appear. If they do not, the defaults
make this equivalent to
http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1 (see Section
2.3.10). The TrailerField defaults to 1 (0xBC) when omitted.
2.3.10. RSASSA-PSS without Parameters

[RFC3447] currently specifies only one mask generation function MGF1 based on a hash function. Although [RFC3447] allows for parameterization, the default is to use the same hash function as the digest method function. Only this default approach is supported by this section; therefore, the definition of a mask generation function type is not needed yet. The same applies to the trailer field. There is only one value (0xBC) specified in [RFC3447]. Hence, this default parameter must be used for signature generation. The default salt length is the length of the hash function.

Identifiers:
- http://www.w3.org/2007/05/xmldsig-more#sha3-224-rsa-MGF1
- http://www.w3.org/2007/05/xmldsig-more#sha3-256-rsa-MGF1
- http://www.w3.org/2007/05/xmldsig-more#sha3-384-rsa-MGF1
- http://www.w3.org/2007/05/xmldsig-more#sha3-512-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#md2-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#md5-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#sha1-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#sha224-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#sha384-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#sha512-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#ripemd128-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#ripemd160-rsa-MGF1
http://www.w3.org/2007/05/xmldsig-more#whirlpool-rsa-MGF1

An example of use is

```xml
<SignatureMethod
  Algorithm="http://www.w3.org/2007/05/xmldsig-more#SHA3-256-rsa-MGF1"
/>
```

### 2.3.11. RSA-SHA224

Identifier:
http://www.w3.org/2007/05/xmldsig-more#rsa-sha224

This implies the PKCS#1 v1.5 padding algorithm [RFC3447] as described in Section 2.3.1, but with the ASN.1 BER SHA-224 algorithm designator prefix. An example of use is

```xml
<SignatureMethod
  Algorithm="http://www.w3.org/2007/05/xmldsig-more#rsa-sha224"
/>
```

Because it takes about the same effort to calculate a SHA-224 message digest as it does a SHA-256 message digest, it is suggested that RSA-SHA256 be used in preference to RSA-SHA224 where possible.

### 2.4. Minimal Canonicalization

Thus far, two independent interoperable implementations of Minimal Canonicalization have not been announced. Therefore, when XML Digital Signature was advanced along the Standards Track from [RFC3075] to [RFC3275], Minimal Canonicalization was dropped. However, there is still interest. For its definition, see Section 6.5.1 of [RFC3075].

For reference, its identifier remains:
http://www.w3.org/2000/09/xmldsig#minimal
2.5. Transform Algorithms

Note that all CanonicalizationMethod algorithms can also be used as transform algorithms.

2.5.1. XPointer

Identifier:
http://www.w3.org/2001/04/xmlsig-more#xptr

This transform algorithm takes an [XPointer] as an explicit parameter. An example of use is:

```xml
<Transform
  Algorithm="http://www.w3.org/2001/04/xmlsig-more/xptr">
  <XPointer
    xmlns="http://www.w3.org/2001/04/xmlsig-more/xptr">
    xpointer(id("foo")) xmlns(bar=http://foobar.example)
    xpointer(//bar:Zab[@Id="foo"])</XPointer>
</Transform>
```

Schema Definition:

```xml
<element name="XPointer" type="string"/>
```

DTD:

```xml
<!ELEMENT XPointer (#PCDATA) >
```

Input to this transform is an octet stream (which is then parsed into XML).

Output from this transform is a node set; the results of the XPointer are processed as defined in the XMLDSIG specification [RFC3275] for a same-document XPointer.
2.6. EncryptionMethod Algorithms

This subsection gives identifiers and information for several EncryptionMethod Algorithms.

2.6.1. ARCFOUR Encryption Algorithm

Identifier:
http://www.w3.org/2001/04/xmldsig-more#arcfour

ARCFOUR is a fast, simple stream encryption algorithm that is compatible with RSA Security's RC4 algorithm [RC4]. An example EncryptionMethod element using ARCFOUR is

<EncryptionMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#arcfour">
  <KeySize>40</KeySize>
</EncryptionMethod>

Note that Arcfour makes use of the generic KeySize parameter specified and defined in [XMLENC11].

2.6.2. Camellia Block Encryption

Identifiers:
http://www.w3.org/2001/04/xmldsig-more#camellia128-cbc
http://www.w3.org/2001/04/xmldsig-more#camellia192-cbc
http://www.w3.org/2001/04/xmldsig-more#camellia256-cbc

Camellia is a block cipher with the same interface as the AES [Camellia] [RFC3713]; it has a 128-bit block size and 128-, 192-, and 256-bit key sizes. In XML encryption, Camellia is used in the same way as the AES: it is used in the Cipher Block Chaining (CBC) mode with a 128-bit initialization vector (IV). The resulting cipher text is prefixed by the IV. If included in XML output, it is then base64 encoded. An example Camellia EncryptionMethod is as follows:

<EncryptionMethod
  Algorithm="http://www.w3.org/2001/04/xmldsig-more#camellia128-cbc" />

2.6.3. Camellia Key Wrap

Identifiers:
http://www.w3.org/2001/04/xmldsig-more#kw-camellia128
http://www.w3.org/2001/04/xmldsig-more#kw-camellia192
http://www.w3.org/2001/04/xmldsig-more#kw-camellia256
Camellia [Camellia] [RFC3713] key wrap is identical to the AES key wrap algorithm [RFC3394] specified in the XML Encryption standard with "AES" replaced by "Camellia". As with AES key wrap, the check value is 0xA6A6A6A6A6A6A6A6.

The algorithm is the same whatever the size of the Camellia key used in wrapping, called the "key encrypting key" or "KEK". If Camellia is supported, it is particularly suggested that wrapping 128-bit keys with a 128-bit KEK and wrapping 256-bit keys with a 256-bit KEK be supported.

An example of use is:

```xml
<EncryptionMethod
   Algorithm=
      "http://www.w3.org/2001/04/xmlenc-more#kw-camellia128"
/>
```

2.6.4.  PSEC-KEM

Identifier:
http://www.w3.org/2001/04/xmlenc-more#psec-kem

The PSEC-KEM algorithm, specified in [18033-2], is a key encapsulation mechanism using elliptic curve encryption.

An example of use is:

```xml
<EncryptionMethod
   Algorithm="http://www.w3.org/2001/04/xmlenc#psec-kem">
   <ECParameters>
      <Version>version</Version>
      <FieldID>id</FieldID>
      <Curve>curve</Curve>
      <Base>base</Base>
      <Order>order</Order>
      <Cofactor>cofactor</Cofactor>
   </ECParameters>
</EncryptionMethod>
```

See [18033-2] for information on the parameters above.
2.6.5. SEED Block Encryption

Identifier:
http://www.w3.org/2007/05/xmldsig-more#seed128-cbc

SEED [RFC4269] is a 128-bit block size with 128-bit key sizes. In XML Encryption, SEED can be used in the Cipher Block Chaining (CBC) mode with a 128-bit initialization vector (IV). The resulting cipher text is prefixed by the IV. If included in XML output, it is then base64 encoded.

An example SEED EncryptionMethod is as follows:

```xml
<EncryptionMethod
   Algorithm="http://www.w3.org/2007/05/xmldsig-more#seed128-cbc" />
```

2.6.6. SEED Key Wrap

Identifier:
http://www.w3.org/2007/05/xmldsig-more#kw-seed128

Key wrapping with SEED is identical to Section 2.2.1 of [RFC3394] with "AES" replaced by "SEED". The algorithm is specified in [RFC4010]. The implementation of SEED is optional. The default initial value is 0xA6A6A6A6A6A6A6A6.

An example of use is:

```xml
<EncryptionMethod
   Algorithm="http://www.w3.org/2007/05/xmldsig-more#kw-seed128"
/>`

3. KeyInfo

In Section 3.1 below a new KeyInfo element child is specified, while in Section 3.2 additional KeyInfo Type values for use in RetrievalMethod are specified.
3.1. PKCS #7 Bag of Certificates and CRLs

A PKCS #7 [RFC2315] "signedData" can also be used as a bag of certificates and/or certificate revocation lists (CRLs). The PKCS7signedData element is defined to accommodate such structures within KeyInfo. The binary PKCS #7 structure is base64 [RFC2045] encoded. Any signer information present is ignored. The following is an example [RFC3092], eliding the base64 data:

```
<foo:PKCS7signedData
    xmlns:foo="http://www.w3.org/2001/04/xmldsig-more">
    ...
</foo:PKCS7signedData>
```

3.2. Additional RetrievalMethod Type Values

The Type attribute of RetrievalMethod is an optional identifier for the type of data to be retrieved. The result of dereferencing a RetrievalMethod reference for all KeyInfo types with an XML structure is an XML element or document with that element as the root. The various "raw" key information types return a binary value. Thus, they require a Type attribute because they are not unambiguously parsable.

Identifiers:
- http://www.w3.org/2001/04/xmlsig-more#KeyName
- http://www.w3.org/2001/04/xmlsig-more#KeyValue
- http://www.w3.org/2001/04/xmlsig-more#PKCS7signedData
- http://www.w3.org/2001/04/xmlsig-more#rawPGPKeyPacket
- http://www.w3.org/2001/04/xmlsig-more#rawPKCS7signedData
- http://www.w3.org/2001/04/xmlsig-more#rawSPKISexp
- http://www.w3.org/2001/04/xmlsig-more#rawX509CRL
- http://www.w3.org/2001/04/xmlsig-more#RetrievalMethod

4. Indexes

The following subsections provide an index by URI and by fragment identifier (the portion of the URI after "#") of the algorithm and KeyInfo URIs defined in this document and in the standards (plus the one KeyInfo child element name defined in this document). The "Sec/Doc" column has the section of this document or, if not specified in this document, the document where the item is specified. See also [XMLSECXREF].
4.1. Fragment Index

The initial "http://www.w3.org/" part of the URI is not included below. The first six entries have a null fragment identifier or no fragment identifier.

<table>
<thead>
<tr>
<th>Fragment</th>
<th>URI</th>
<th>Sec/Doc</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>--------</td>
</tr>
<tr>
<td>2002/06/xmldsig-filter2</td>
<td></td>
<td>[XPATH]</td>
</tr>
<tr>
<td>2006/12/xmlc12n11#</td>
<td></td>
<td>[CANON11]</td>
</tr>
<tr>
<td>TR/1999/REC-xslt-19991116</td>
<td></td>
<td>[XSLT]</td>
</tr>
<tr>
<td>TR/1999/REC-xpath-19991116</td>
<td></td>
<td>[XPATH]</td>
</tr>
<tr>
<td>TR/2001/06/xml-exc-c14n#</td>
<td></td>
<td>[XCANON]</td>
</tr>
<tr>
<td>TR/2001/REC-xml-c14n-20010315</td>
<td></td>
<td>[CANON10]</td>
</tr>
<tr>
<td>TR/2001/REC-xmlschema-1-20010502</td>
<td></td>
<td>[Schema]</td>
</tr>
<tr>
<td>aes128-cbc</td>
<td>2001/04/xmlenc#aes128-cbc</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>aes128-gcm</td>
<td>2009/xmlenc11#aes128-gcm</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>aes192-cbc</td>
<td>2001/04/xmlenc#aes192-cbc</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>aes192-gcm</td>
<td>2009/xmlenc11#aes192-gcm</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>aes256-cbc</td>
<td>2001/04/xmlenc#aes256-cbc</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>aes256-gcm</td>
<td>2009/xmlenc11#aes256-gcm</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>arcfour</td>
<td>2001/04/xmldsig-more#arcfour</td>
<td>2.6.1</td>
</tr>
<tr>
<td>base64</td>
<td>2000/09/xmldsig#base64</td>
<td>[RFC3275]</td>
</tr>
<tr>
<td>camellia128-cbc</td>
<td>2001/04/xmldsig-more#camellia128-cbc</td>
<td>2.6.2</td>
</tr>
<tr>
<td>camellia192-cbc</td>
<td>2001/04/xmldsig-more#camellia192-cbc</td>
<td>2.6.2</td>
</tr>
<tr>
<td>camellia256-cbc</td>
<td>2001/04/xmldsig-more#camellia256-cbc</td>
<td>2.6.2</td>
</tr>
<tr>
<td>ConcatKDF</td>
<td>2009/xmlenc11#ConcatKDF</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>decrypt#XML</td>
<td>2002/07/decrypt#XML</td>
<td>[DECRYPT]</td>
</tr>
<tr>
<td>decrypt#Binary</td>
<td>2002/07/decrypt#Binary</td>
<td>[DECRYPT]</td>
</tr>
<tr>
<td>DEREncodedKeyValue</td>
<td>2009/xmldsig11#DEREncodedKeyValue</td>
<td>[XMLSIG11]</td>
</tr>
<tr>
<td>dh</td>
<td>2001/04/xmlenc#dh</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>dsa-sha1</td>
<td>2000/09/xmldsig#dsa-sha1</td>
<td>[RFC3275]</td>
</tr>
<tr>
<td>dsa-sha256</td>
<td>2009/xmldsig11#dsa-sha256</td>
<td>[XMLSIG11]</td>
</tr>
<tr>
<td>DSAKeyValue</td>
<td>2000/09/xmldsig#DSAKeyValue</td>
<td>[XMLSIG11]</td>
</tr>
<tr>
<td>ECDH-ES</td>
<td>2009/xmlenc11#ECDH-ES</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>ecdsa-rippedm160</td>
<td>2007/05/xmldsig-more#ecdsa-rippedm160</td>
<td>2.3.6</td>
</tr>
<tr>
<td>ecdsa-sha1</td>
<td>2001/04/xmldsig-more#ecdsa-sha1</td>
<td>2.3.6</td>
</tr>
<tr>
<td>ecdsa-sha224</td>
<td>2001/04/xmldsig-more#ecdsa-sha224</td>
<td>2.3.6</td>
</tr>
<tr>
<td>ecdsa-sha256</td>
<td>2001/04/xmldsig-more#ecdsa-sha256</td>
<td>2.3.6</td>
</tr>
<tr>
<td>ecdsa-sha384</td>
<td>2001/04/xmldsig-more#ecdsa-sha384</td>
<td>2.3.6</td>
</tr>
<tr>
<td>ecdsa-sha512</td>
<td>2001/04/xmldsig-more#ecdsa-sha512</td>
<td>2.3.6</td>
</tr>
</tbody>
</table>
ecdsa-whirlpool 2007/05/xmldsig-more#ecdsa-whirlpool 2.3.5
ecies-kem 2010/xmlsec-ghc#ecies-kem  [GENERIC]
ECKeyValue 2009/xmldsig11#ECKeyValue  [XMLSIG11]
enveloped-signature 2000/09/xmldsig#enveloped-signature  [RFC3275]
esign-sha1 2001/04/xmldsig-more#esign-sha1 2.3.7
esign-sha224 2001/04/xmldsig-more#esign-sha224 2.3.7
esign-sha256 2001/04/xmldsig-more#esign-sha256 2.3.7
esign-sha384 2001/04/xmldsig-more#esign-sha384 2.3.7
esign-sha512 2001/04/xmldsig-more#esign-sha512 2.3.7
generic-hybrid 2010/xmlsec-ghc#generic-hybrid  [GENERIC]
hmac-md5 2001/04/xmldsig-more#hmac-md5 2.2.1
hmac-ripemd160 2001/04/xmldsig-more#hmac-ripemd160 2.2.3
hmac-shal 2000/09/xmldsig#hmac-shal  [RFC3275]
hmac-sha224 2001/04/xmldsig-more#hmac-sha224 2.2.2
hmac-sha256 2001/04/xmldsig-more#hmac-sha256 2.2.2
hmac-sha384 2001/04/xmldsig-more#hmac-sha384 2.2.2
hmac-sha512 2001/04/xmldsig-more#hmac-sha512 2.2.2

KeyName 2001/04/xmldsig-more#KeyName 3.2
KeyValue 2001/04/xmldsig-more#KeyValue 3.2
ekw-aes128 2001/04/xmlenc#kw-aes128  [XMLENC11]
kw-aes192 2001/04/xmlenc#kw-aes192  [XMLENC11]
kw-aes256 2001/04/xmlenc#kw-aes256  [XMLENC11]
kw-aes256-pad 2009/xmlenc11#kw-aes-256-pad  [XMLENC11]
kw-camellia128 2001/04/xmlsig-more#kw-camellia128 2.6.3
kw-camellia192 2001/04/xmlsig-more#kw-camellia192 2.6.3
kw-camellia256 2001/04/xmlsig-more#kw-camellia256 2.6.3
kw-seed128 2007/05/xmldsig-more#kw-seed128 2.6.6

md2-rsa-MGF1 2007/05/xmldsig-more#md2-rsa-MGF1 2.3.10
md5 2001/04/xmldsig-more#md5 2.1.1
md5-rsa-MGF1 2007/05/xmldsig-more#md5-rsa-MGF1 2.3.10
MGF1 2007/05/xmldsig-more#MGF1 2.3.9
mgf1sha1 2009/xmlenc11#mgf1sha1  [XMLENC11]
mgf1sha224 2009/xmlenc11#mgf1sha224  [XMLENC11]
mgf1sha256 2009/xmlenc11#mgf1sha256  [XMLENC11]
mgf1sha384 2009/xmlenc11#mgf1sha384  [XMLENC11]
mgf1sha512 2009/xmlenc11#mgf1sha512  [XMLENC11]
MgmtData 2000/09/xmldsig#MgmtData  [XMLSIG11]
minimal 2000/09/xmldsig#minimal 2.4

pbkdf2 2009/xmlenc11#pbkdf2  [XMLENC11]
PGPData 2000/09/xmldsig#PGPData  [XMLSIG11]
PKCS7signedData 2001/04/xmldsig-more#PKCS7signedData 3.1
<table>
<thead>
<tr>
<th>URI Type</th>
<th>URI</th>
<th>Version</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS7signedData</td>
<td>2001/04/xmldsig-more#PKCS7signedData</td>
<td>3.2</td>
<td>3.2</td>
</tr>
<tr>
<td>psec-kem</td>
<td>2001/04/xmldsig-more#psec-kem</td>
<td>2.6.4</td>
<td></td>
</tr>
<tr>
<td>rawPGPKKeyPacket</td>
<td>2001/04/xmldsig-more#rawPGPKKeyPacket</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>rawPKCS7signedData</td>
<td>2001/04/xmldsig-more#rawPKCS7signedData</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>rawSPKISexp</td>
<td>2001/04/xmldsig-more#rawSPKISexp</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>rawX509CRL</td>
<td>2001/04/xmldsig-more#rawX509CRL</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>RetrievalMethod</td>
<td>2001/04/xmldsig-more#RetrievalMethod</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>ripemd128-rsa-MGF1</td>
<td>2007/05/xmldsig-more#ripemd128-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>ripemd160</td>
<td>2001/04/xmlenc#ripemd160</td>
<td>[XMLENC11]</td>
<td></td>
</tr>
<tr>
<td>rsa-1_5</td>
<td>2001/04/xmlenc#rsa-1_5</td>
<td>[XMLENC11]</td>
<td></td>
</tr>
<tr>
<td>rsa-md5</td>
<td>2001/04/xmldsig-more#rsa-md5</td>
<td>2.3.1</td>
<td></td>
</tr>
<tr>
<td>rsa-oaep</td>
<td>2009/xmlenc11#rsa-oaep</td>
<td>[XMLENC11]</td>
<td></td>
</tr>
<tr>
<td>rsa-oaep-mgf1p</td>
<td>2001/04/xmlenc#rsa-oaep-mgf1p</td>
<td>[XMLENC11]</td>
<td></td>
</tr>
<tr>
<td>rsa-pss</td>
<td>2007/05/xmldsig-more#rsa-pss</td>
<td>2.3.9</td>
<td></td>
</tr>
<tr>
<td>rsa-ripemd160</td>
<td>2001/04/xmldsig-more#rsa-ripemd160</td>
<td>2.3.5</td>
<td></td>
</tr>
<tr>
<td>rsa-shal</td>
<td>2000/09/xmlsig#rsa-shal</td>
<td>[RFC3275]</td>
<td></td>
</tr>
<tr>
<td>rsa-sha224</td>
<td>2007/05/xmldsig-more#rsa-sha224</td>
<td>2.3.11</td>
<td></td>
</tr>
<tr>
<td>rsa-sha256</td>
<td>2001/04/xmldsig-more#rsa-sha256</td>
<td>2.3.2</td>
<td></td>
</tr>
<tr>
<td>rsa-sha384</td>
<td>2001/04/xmldsig-more#rsa-sha384</td>
<td>2.3.3</td>
<td></td>
</tr>
<tr>
<td>rsa-sha512</td>
<td>2001/04/xmldsig-more#rsa-sha512</td>
<td>2.3.4</td>
<td></td>
</tr>
<tr>
<td>rsa-whirlpool</td>
<td>2007/05/xmldsig-more#rsa-whirlpool</td>
<td>2.3.5</td>
<td></td>
</tr>
<tr>
<td>rsaes-kem</td>
<td>2010/xmlsec-ghc#rsaes-kem</td>
<td>[GENERIC]</td>
<td></td>
</tr>
<tr>
<td>RSAKeyValue</td>
<td>2000/09/xmlsig#RSAKeyValue</td>
<td>[XMLDSIG11]</td>
<td></td>
</tr>
<tr>
<td>seed128-cbc</td>
<td>2007/05/xmldsig-more#seed128-cbc</td>
<td>2.6.5</td>
<td></td>
</tr>
<tr>
<td>sha1</td>
<td>2000/09/xmldsig#sha1</td>
<td>[RFC3275]</td>
<td></td>
</tr>
<tr>
<td>sha1-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha1-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha224</td>
<td>2001/04/xmldsig-more#sha224</td>
<td>2.1.2</td>
<td></td>
</tr>
<tr>
<td>sha224-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha224-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha256</td>
<td>2001/04/xmlenc#sha256</td>
<td>[XMLENC11]</td>
<td></td>
</tr>
<tr>
<td>sha256-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha256-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha3-224</td>
<td>2007/05/xmldsig-more#sha3-224</td>
<td>2.1.5</td>
<td></td>
</tr>
<tr>
<td>sha3-224-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha3-224-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha3-256</td>
<td>2007/05/xmldsig-more#sha3-256</td>
<td>2.1.5</td>
<td></td>
</tr>
<tr>
<td>sha3-256-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha3-256-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha3-384</td>
<td>2007/05/xmldsig-more#sha3-384</td>
<td>2.1.5</td>
<td></td>
</tr>
<tr>
<td>sha3-384-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha3-384-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha3-512</td>
<td>2007/05/xmldsig-more#sha3-512</td>
<td>2.1.5</td>
<td></td>
</tr>
<tr>
<td>sha3-512-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha3-512-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha384</td>
<td>2001/04/xmldsig-more#sha384</td>
<td>2.1.3</td>
<td></td>
</tr>
<tr>
<td>sha384-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha384-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>sha512</td>
<td>2001/04/xmlenc#sha512</td>
<td>[XMLENC11]</td>
<td></td>
</tr>
<tr>
<td>sha512-rsa-MGF1</td>
<td>2007/05/xmldsig-more#sha512-rsa-MGF1</td>
<td>2.3.10</td>
<td></td>
</tr>
<tr>
<td>SPKIData</td>
<td>2000/09/xmldsig#SPKIData</td>
<td>[XMLDSIG11]</td>
<td></td>
</tr>
</tbody>
</table>

Eastlake Standards Track [Page 23]
<table>
<thead>
<tr>
<th>URI</th>
<th>Sec/Doc</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000/09/xmldsig#base64</td>
<td>[RFC3275]</td>
<td>Transform</td>
</tr>
<tr>
<td>2000/09/xmldsig#DSAKeyValue</td>
<td>[RFC3275]</td>
<td>Retrieval type</td>
</tr>
<tr>
<td>2000/09/xmldsig#dsal-shal</td>
<td>[RFC3275]</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2000/09/xmldsig#enveloped-signature</td>
<td>[RFC3275]</td>
<td>Transform</td>
</tr>
<tr>
<td>2000/09/xmldsig#hmac-shal</td>
<td>[RFC3275]</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2000/09/xmldsig#MgmtData</td>
<td>[RFC3275]</td>
<td>Retrieval type</td>
</tr>
<tr>
<td>2000/09/xmldsig#minimal</td>
<td>2.4</td>
<td>Canonicalization</td>
</tr>
<tr>
<td>2000/09/xmldsig#PGPData</td>
<td>[RFC3275]</td>
<td>Retrieval type</td>
</tr>
<tr>
<td>2000/09/xmldsig#rsa-shal</td>
<td>[RFC3275]</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2000/09/xmldsig#SPKIData</td>
<td>[RFC3275]</td>
<td>Retrieval type</td>
</tr>
<tr>
<td>2000/09/xmldsig#X509Data</td>
<td>[RFC3275]</td>
<td>Retrieval type</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#arcfour</td>
<td>2.6.1</td>
<td>EncryptionMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#camellia128-cbc</td>
<td>2.6.2</td>
<td>EncryptionMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#camellia192-cbc</td>
<td>2.6.2</td>
<td>EncryptionMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#camellia256-cbc</td>
<td>2.6.2</td>
<td>EncryptionMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#ecdsa-shal</td>
<td>2.3.6</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#ecdsa-sha224</td>
<td>2.3.6</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#ecdsa-sha256</td>
<td>2.3.6</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#ecdsa-sha384</td>
<td>2.3.6</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#ecdsa-sha512</td>
<td>2.3.6</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2001/04/xmldsig-more#esign-shal</td>
<td>2.3.7</td>
<td>SignatureMethod</td>
</tr>
</tbody>
</table>

The initial "http://www.w3.org/" part of the URI is not included above.

4.2. URI Index

The initial "http://www.w3.org/" part of the URI is not included below.

<table>
<thead>
<tr>
<th>URI</th>
<th>Sec/Doc</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001/04/xmldsig#tripledes-cbc</td>
<td>2001/04/xmlenc#tripledes-cbc</td>
<td>[XMLENC11]</td>
</tr>
<tr>
<td>whirlpool</td>
<td>2007/05/xmldsig-more#whirlpool</td>
<td>2.1.4</td>
</tr>
<tr>
<td>whirlpool-rsa-MGF1</td>
<td>2007/05/xmldsig-more#whirlpool-rsa-MGF1</td>
<td>2.3.10</td>
</tr>
<tr>
<td>WithComments</td>
<td>2006/12/xmlc14n11#WithComments</td>
<td>[CANON11]</td>
</tr>
<tr>
<td>WithComments</td>
<td>TR/2001/06/xml-exc-c14n#WithComments</td>
<td>[XCANON]</td>
</tr>
<tr>
<td>WithComments</td>
<td>TR/2001/REC-xml-c14n-20010315#WithComments</td>
<td>[CANON10]</td>
</tr>
<tr>
<td>X509Data</td>
<td>2000/09/xmldsig#X509Data</td>
<td>[XMLSIG11]</td>
</tr>
<tr>
<td>xptr</td>
<td>2001/04/xmldsig-more#xptr</td>
<td>2.5.1</td>
</tr>
</tbody>
</table>
2001/04/xmldsig-more#esign-sha224  2.3.7 SignatureMethod
2001/04/xmldsig-more#esign-sha256  2.3.7 SignatureMethod
2001/04/xmldsig-more#esign-sha384  2.3.7 SignatureMethod
2001/04/xmldsig-more#esign-sha512  2.3.7 SignatureMethod
2001/04/xmldsig-more#hmac-md5      2.2.1 SignatureMethod
2001/04/xmldsig-more#hmac-ripemd160 2.2.3 SignatureMethod
2001/04/xmldsig-more#hmac-sha224   2.2.2 SignatureMethod
2001/04/xmldsig-more#hmac-sha256   2.2.2 SignatureMethod
2001/04/xmldsig-more#hmac-sha384   2.2.2 SignatureMethod
2001/04/xmldsig-more#hmac-sha512   2.2.2 SignatureMethod
2001/04/xmldsig-more#KeyName       3.2 Retrieval type
2001/04/xmldsig-more#KeyValue      3.2 Retrieval type
2001/04/xmldsig-more#kw-camellia128 2.6.3 EncryptionMethod
2001/04/xmldsig-more#kw-camellia192 2.6.3 EncryptionMethod
2001/04/xmldsig-more#kw-camellia256 2.6.3 EncryptionMethod
2001/04/xmldsig-more#md5           2.1.1 DigestAlgorithm
2001/04/xmldsig-more#PKCS7signedData   3.2 Retrieval type
2001/04/xmldsig-more#psec-kem      2.6.4 EncryptionMethod
2001/04/xmldsig-more#rawPGPKeyPacket 3.2 Retrieval type
2001/04/xmldsig-more#rawPKCS7signedData 3.2 Retrieval type
2001/04/xmldsig-more#rawPKCS7signedData 3.2 Retrieval type
2001/04/xmldsig-more#rawPKCS7signedData 3.2 Retrieval type
2001/04/xmldsig-more#rawPKCS7signedData 3.2 Retrieval type
2001/04/xmldsig-more#rawPKCS7signedData 3.2 Retrieval type
2001/04/xmldsig-more#rawPKCS7signedData 3.2 Retrieval type
2001/04/xmldsig-more#rsa-md5       2.3.1 SignatureMethod
2001/04/xmldsig-more#rsa-sha256    2.3.2 SignatureMethod
2001/04/xmldsig-more#rsa-sha384    2.3.3 SignatureMethod
2001/04/xmldsig-more#rsa-sha512    2.3.4 SignatureMethod
2001/04/xmldsig-more#rsa-ripemd160 2.3.5 SignatureMethod
2001/04/xmldsig-more#sha224        2.1.2 DigestAlgorithm
2001/04/xmldsig-more#sha256        2.1.3 DigestAlgorithm
2001/04/xmldsig-more#sha384        2.1.3 DigestAlgorithm
2001/04/xmldsig-more#sha512        2.1.3 DigestAlgorithm
2001/04/xmldsig-more#xptr          2.5.1 Transform
2001/04/xmldsig-more#PKCS7signedData   3.1 KeyInfo child
2001/04/xmlenc#kw-aes256       [XMLENC11] EncryptionMethod
2001/04/xmlenc#ripemd160       [XMLENC11] DigestAlgorithm
2001/04/xmlenc#rsa-1_5          [XMLENC11] EncryptionMethod
2001/04/xmlenc#rsa-oaep-mgf1p   [XMLENC11] EncryptionMethod
2001/04/xmlenc#sha256          [XMLENC11] DigestAlgorithm
2001/04/xmlenc#sha512          [XMLENC11] DigestAlgorithm
2002/06/xmldsig-filter2        [XPATH] Transform
2002/07/decrypt#XML [DECRYPT] Transform
2002/07/decrypt#Binary [DECRYPT] Transform

2006/12/xmlc12n11# [CANON11] Canonicalization
2006/12/xmlc14n11#WithComments [CANON11] Canonicalization

2007/05/xmldsig-more#ecdsa-ripemd160 2.3.6 SignatureMethod
2007/05/xmldsig-more#ecdsa-whirlpool 2.3.5 SignatureMethod
2007/05/xmldsig-more#kw-seed128 2.6.6 EncryptionMethod
2007/05/xmldsig-more#md2-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#md5-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#MGF1 2.3.9 SignatureMethod
2007/05/xmldsig-more#ripemd128-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#ripemd160-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#rsa-pss 2.3.9 SignatureMethod
2007/05/xmldsig-more#rsa-sha224 2.3.11 SignatureMethod
2007/05/xmldsig-more#rsa-whirlpool 2.3.5 SignatureMethod
2007/05/xmldsig-more#seed128-cbc 2.6.5 EncryptionMethod
2007/05/xmldsig-more#sha1-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha224-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha256-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha3-224 2.1.5 DigestAlgorithm
2007/05/xmldsig-more#sha3-224-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha3-256 2.1.5 DigestAlgorithm
2007/05/xmldsig-more#sha3-256-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha3-384 2.1.5 DigestAlgorithm
2007/05/xmldsig-more#sha3-384-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha3-512 2.1.5 DigestAlgorithm
2007/05/xmldsig-more#sha3-512-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#sha384-rsa-MGF1 2.3.10 SignatureMethod
2007/05/xmldsig-more#whirlpool 2.1.4 DigestAlgorithm
2007/05/xmldsig-more#whirlpool-rsa-MGF1 2.3.10 SignatureMethod
2009/xmldsig11#dsa-sha256 [XMLDSIG11] SignatureMethod
2009/xmldsig11#ECKKeyValue [XMLDSIG11] Retrieval type
2009/xmldsig11#DEREncodedKeyValue [XMLDSIG11] Retrieval type
2009/xmlenc11#mgf1sha1 [XMLENC11] SignatureMethod
2009/xmlenc11#mgf1sha224 [XMLENC11] SignatureMethod
2009/xmlenc11#mgf1sha256 [XMLENC11] SignatureMethod
<table>
<thead>
<tr>
<th>URI</th>
<th>Category</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009/xmlenc11#mgf1sha384</td>
<td>[XMLENC11]</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2009/xmlenc11#mgf1sha512</td>
<td>[XMLENC11]</td>
<td>SignatureMethod</td>
</tr>
<tr>
<td>2010/xmlsec-ghc#generic-hybrid</td>
<td>[GENERIC]</td>
<td>Generic Hybrid</td>
</tr>
<tr>
<td>2010/xmlsec-ghc#rsaes-kem</td>
<td>[GENERIC]</td>
<td>Generic Hybrid</td>
</tr>
<tr>
<td>2010/xmlsec-ghc#ecies-kem</td>
<td>[GENERIC]</td>
<td>Generic Hybrid</td>
</tr>
<tr>
<td>TR/1999/REC-xpath-19991116</td>
<td>[XPATH]</td>
<td>Transform</td>
</tr>
<tr>
<td>TR/1999/REC-xslt-19991116</td>
<td>[XSLT]</td>
<td>Transform</td>
</tr>
<tr>
<td>TR/2001/06/xml-exc-c14n#</td>
<td>[XCANON]</td>
<td>Canonicalization</td>
</tr>
<tr>
<td>TR/2001/06/xml-exc-c14n#WithComments</td>
<td>[XCANON]</td>
<td>Canonicalization</td>
</tr>
<tr>
<td>TR/2001/REC-xmcl-c14n-2001315</td>
<td>[CANON10]</td>
<td>Canonicalization</td>
</tr>
<tr>
<td>TR/2001/REC-xmcl-c14n-20010315#WithComments</td>
<td>[CANON10]</td>
<td>Canonicalization</td>
</tr>
</tbody>
</table>

The initial "http://www.w3.org/" part of the URI is not included above.

5. Allocation Considerations

W3C and IANA allocation considerations are given below.

5.1. W3C Allocation Considerations

As it is easy for people to construct their own unique URIs [RFC3986] and, if appropriate, to obtain a URI from the W3C, it is not intended that any additional "http://www.w3.org/2007/05/xmldsig-more#" URIs be created beyond those enumerated in this RFC. (W3C Namespace stability rules prohibit the creation of new URIs under "http://www.w3.org/2000/09/xmldsig#" and URIs under "http://www.w3.org/2001/04/xmldsig-more#" were frozen with the publication of [RFC4051].)

An "xmldsig-more" URI does not imply any official W3C or IETF status for these algorithms or identifiers nor does it imply that they are only useful in digital signatures. Currently, dereferencing such URIs may or may not produce a temporary placeholder document. Permission to use these URI prefixes has been given by the W3C.
5.2. IANA Considerations

IANA has established a registry entitled "XML Security URIs". The initial contents correspond to Section 4.2 of this document with each section number in the "Sec/Doc" column augmented with a reference to this RFC (for example, "2.6.4" means "[RFC6931], Section 2.6.4"). New entries, including new Types, will be added based on Expert Review [RFC5226]. Criterion for inclusion are (1) documentation sufficient for interoperability of the algorithm or data type and the XML syntax for its representation and use and (2) sufficient importance as normally indicated by inclusion in (2a) an approved W3C Note, Proposed Recommendation, or Recommendation or (2b) an approved IETF Standards Track document. Typically, the registry will reference a W3C or IETF document specifying such XML syntax; that document will either contain a more abstract description of the algorithm or data type or reference another document with a more abstract description.

6. Security Considerations

This RFC is concerned with documenting the URIs that designate algorithms and some data types used in connection with XML security. The security considerations vary widely with the particular algorithms, and the general security considerations for XML security are outside of the scope of this document but appear in [XMLSIG11], [XMLENC11], [CANON10], [CANON11], and [GENERIC].

[RFC6151] should be consulted before considering the use of MD5 as a DigestMethod or RSA-MD5 as a SignatureMethod.

See [RFC6194] for SHA-1 security considerations and [RFC6151] for MD5 security considerations.

Additional security considerations are given in connection with the description of some algorithms in the body of this document.

Implementers should be aware that cryptographic algorithms become weaker with time. As new cryptoanalysis techniques are developed and computing performance improves, the work factor to break a particular cryptographic algorithm will reduce. Therefore, cryptographic implementations should be modular, allowing new algorithms to be readily inserted. That is, implementers should be prepared for the set of mandatory-to-implement algorithms to change over time.
7. Acknowledgements

The contributions to this document by the following people, listed in alphabetic order, are gratefully acknowledged: Benoit Claise, Adrian Farrel, Stephen Farrell, Ernst Giessmann, Frederick Hirsch, Bjoern Hoehrmann, Russ Housley, Satoru Kanno, Charlie Kaufman, Konrad Lanz, HwanJin Lee, Barry Leiba, Peter Lipp, Subramanian Moonesamy, Thomas Roessler, Hanseong Ryu, Peter Saint-Andre, and Sean Turner.

The following contributors to [RFC4051], on which this document is based, are gratefully acknowledged: Glenn Adams, Merlin Hughs, Gregor Karlinger, Brian LaMachia, Shiho Moriai, Joseph Reagle, Russ Housley, and Joel Halpern.
Appendix A. Changes from RFC 4051

The following changes have been made in RFC 4051 to produce this document.

1. Updated and added numerous RFC, W3C, and Internet-Draft references.
2. Added #ecdsa-ripemd160, #whirlpool, #ecdsa-whirlpool, #rsa-whirlpool, #seed128-cbc, and #kw-seed128.
3. Incorporated RFC 4051 errata [Errata191].
4. Added URI and fragment index sections.
5. For MD5 and SHA-1, added references to [RFC6151] and [RFC6194].
6. Added SHA-3 / Keccak placeholder section including #sha3-224, #sha3-256, #sha3-384, and #sha3-512.
7. Added RSASSA-PSS sections including #sha3-224-MGF1, #sha3-256-MGF1, #sha3-384-MGF1, #sha3-512-MGF1, #md2-rsa-MGF1, #md5-rsa-MGF1, #sha1-rsa-MGF1, #sha224-rsa-MGF1, #sha256-rsa-MGF1, #sha384-rsa-MGF1, #sha512-rsa-MGF1, #ripemd128-rsa-MGF1, #ripemd160-rsa-MGF1, and #whirlpool-rsa-MGF1.
8. Added new URIs from Canonical XML 1.1 and XML Encryption 1.1 including: #aes128-gcm, #aes192-gcm, #aes256-gcm, #ConcatKDF, #pbkdf, #rsa-oaep, #ECDH-ES, and #dh-es.
9. Added numerous URIs that are specified in W3C XML Security documents to the Indexes. These do not have sections in the body of this document -- for example, those for dsa-sha256, mgf1sha*, decrypt#XML, and xmldsig-filter2.
10. Requested establishment of an IANA registry.
11. Made various editorial changes.
Normative References


Informative References


Author’s Address

Donald E. Eastlake, 3rd
Huawei Technologies
155 Beaver Street
Milford, MA 01757
USA

Phone: +1-508-333-2270
EMail: d3e3e3@gmail.com