|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **itu-old** | INTERNATIONAL TELECOMMUNICATION UNION | | | | COM 17 – C 230 – E |
| **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2013-2016 | | | **September 2014** | |
| **English only**  **Original: English** | |
| **Question(s):** | | 11/17 |  | | |
| **STUDY GROUP 17 – CONTRIBUTION 230** | | | | | |
| **Source:** | | **Denmark** | | | |
| **Title:** | | Proposal for including relevant cryptographic algorithm information into Annex B of Rec. ITU-T X.509 | ISO/IEC 9594-8. | | | |

Justification

Several specifications, such as Smart Grid specifications, have a requirement to specify the use of a specific repertoire of cryptographic algorithms. Relevant cryptographic algorithm specifications should be collected and included in a specific module to allow for easy reference. It is suggested that Annex B of Rec. ITU-T X.509 | ISO/IEC 9594-8 could contain such specifications.

The actual proposal

Replace Annex B with the following

Annex B  
  
Reference definition of algorithm object identifiers

(This annex forms an integral part of this Recommendation | International Standard.)

This annex defines object identifiers assigned to authentication and encryption algorithms, in the absence of a formal register. It is intended to make use of such a register as it becomes available. The definitions take the form of the ASN.1 module, AlgorithmObjectIdentifiers.

AlgorithmObjectIdentifiers {joint-iso-itu-t ds(5) module(1)

algorithmObjectIdentifiers(8) 8}

DEFINITIONS ::=

BEGIN

-- EXPORTS All

/\*

The values defined in this module are primarily taking from various specifications and

collected here for easy reference by other specifcations.

Wen values are copied form an IETF RFC, the IETF RFC number is shown.

When values are copied from the NIST Computer Security Objects Register (CSOR),

the label CSOR is used.

\*/

IMPORTS

algorithm, authenticationFramework

FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 8}

ALGORITHM

FROM AuthenticationFramework authenticationFramework;

-- Object identifier allocations

-- Object identifiers allocated by this Specification

nullAlgorithm OBJECT IDENTIFIER ::= {algorithm 0}

encryptionAlgorithm OBJECT IDENTIFIER ::= {algorithm 1}

hashAlgorithm OBJECT IDENTIFIER ::= {algorithm 2}

signatureAlgorithm OBJECT IDENTIFIER ::= {algorithm 3}

-- synonyms

id-ea OBJECT IDENTIFIER ::= encryptionAlgorithm

id-ha OBJECT IDENTIFIER ::= hashAlgorithm

id-sa OBJECT IDENTIFIER ::= signatureAlgorithm

-- the following object identifier assignments reserve values assigned to deprecated functions

id-ea-rsa OBJECT IDENTIFIER ::= {id-ea 1}

id-ha-sqMod-n OBJECT IDENTIFIER ::= {id-ha 1}

id-sa-sqMod-nWithRSA OBJECT IDENTIFIER ::= {id-sa 1}

-- object identifiers allocated by other organization

us-iso OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) }

ansi-x962 OBJECT IDENTIFIER ::= { us-iso ansi-x962(10045 }

us-joint OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840) }

usgov OBJECT IDENTIFIER ::= { us-joint organization(1) gov(101) }

dodAlgorithms OBJECT IDENTIFIER ::= { usgov dod(2) infosec(1) algorithms(1) }

csor OBJECT IDENTIFIER ::= { usgov csor(3) }

nistAlgorithms OBJECT IDENTIFIER ::= { csor nistAlgorithm(4) } -- CSOR

aes OBJECT IDENTIFIER ::= { nistAlgorithms 1 } -- CSOR

hashAlgs OBJECT IDENTIFIER ::= { nistAlgorithms 2 } -- CSOR

sigAlgs OBJECT IDENTIFIER ::= { nistAlgorithms 3 } -- CSOR

rsadsi OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)

rsadsi(113549) }

pkcs-1 OBJECT IDENTIFIER ::= { rsadsi pkcs(1) pkcs-1(1) }

-- Symmetric key algorithm object identifiers

id-aes128-CBC OBJECT IDENTIFIER ::= { aes 2 } -- CSOR

id-aes192-CBC OBJECT IDENTIFIER ::= { aes 22 } -- CSOR

id-aes256-CBC OBJECT IDENTIFIER ::= { aes 42 } -- CSOR

-- Asymmetric key algorithm object identifiers

rsaEncryption OBJECT IDENTIFIER ::= {pkcs-1 rsaEncryption(1)} -- IETF RFC 4055

id-RSASSA-PSS OBJECT IDENTIFIER ::= {pkcs-1 rsassa-pss(10) } -- IETF RFC 4055

id-keyExchangeAlgorithm OBJECT IDENTIFIER ::= {dodAlgorithms id-keyExchangeAlgorithm(22)}

--IETF RFC 3279

-- Hash algorithms object identifiers

-- The OID for SHA hash algorithms are specified in NIST FIPS PUB 180-4

id-sha1 OBJECT IDENTIFIER ::=

{iso(1) identified-organization(3) oiw(14) secsig(3)

algorithms(2) 26} -- IETF RFC 3279

id-sha256 OBJECT IDENTIFIER ::= { hashAlgs 1 } -- CSOR

id-sha384 OBJECT IDENTIFIER ::= { hashAlgs 2 } -- CSOR

id-sha512 OBJECT IDENTIFIER ::= { hashAlgs 3 } -- CSOR

id-sha224 OBJECT IDENTIFIER ::= { hashAlgs 4 } -- CSOR

id-sha512-224 OBJECT IDENTIFIER ::= { hashAlgs 5 } -- CSOR

id-sha512-256 OBJECT IDENTIFIER ::= { hashAlgs 6 } -- CSOR

-- Signature algorithm object identifiers

-- DSA algorithms

id-dsa-with-sha1 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) x9-57(10040)

x9algorithm(4) dsa-with-sha1(3)}

id-dsa-with-sha224 OBJECT IDENTIFIER ::= { sigAlgs 1 } -- CSOR

id-dsa-with-sha256 OBJECT IDENTIFIER ::= { sigAlgs 2 } -- CSOR

-- From IETF RFC 3447

sha1-with-rsa-signature OBJECT IDENTIFIER ::= { pkcs-1 sha1-with-rsa-signature(5) }

sha256WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 sha256WithRSAEncryption(11) }

sha384WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 sha384WithRSAEncryption(12) }

sha512WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 sha512WithRSAEncryption(13) }

sha224WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 sha224WithRSAEncryption(14) }

-- From IETF RFC 5758

ecdsa-with-SHA224 OBJECT IDENTIFIER ::= {ansi-x962 signatures(4) ecdsa-with-SHA2(3) 1 }

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {ansi-x962 signatures(4) ecdsa-with-SHA2(3) 2 }

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {ansi-x962 signatures(4) ecdsa-with-SHA2(3) 3 }

ecdsa-with-SHA512 OBJECT IDENTIFIER ::= {ansi-x962 signatures(4) ecdsa-with-SHA2(3) 4 }

-- Hashing alogorithms

mD5Algorithm ALGORITHM ::= {

PARMS NULL

IDENTIFIED BY {iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) md5(5)}}

-- Note that the MD5 algorithm is not considered secure

sha1Algorithm ALGORITHM ::= {

PARMS NULL

IDENTIFIED BY id-sha1 }

-- Note that the SHA1 algorithm may not be considered secure

sha256 ALGORITHM ::= { -- IETF RFC 5754

IDENTIFIED BY id-sha256 }

sha384 ALGORITHM ::= { -- IETF RFC 5754

IDENTIFIED BY id-sha384 }

sha512 ALGORITHM ::= { -- IETF RFC 5754

IDENTIFIED BY id-sha512 }

sha224 ALGORITHM ::= { -- IETF RFC 5754

IDENTIFIED BY id-sha224 }

-- Symmetric encryption algorithms

aes128-CBC ALGORITHM ::= { -- CSOR

PARMS AES-InitializationVector

IDENTIFIED BY id-aes128-CBC }

aes192-CBC ALGORITHM ::= { -- CSOR

PARMS AES-InitializationVector

IDENTIFIED BY id-aes192-CBC }

aes256-CBC ALGORITHM ::= { -- CSOR

PARMS AES-InitializationVector

IDENTIFIED BY id-aes256-CBC }

AES-InitializationVector ::= OCTET STRING (SIZE (16))

-- Asymmetric encryption algorithm

rsaEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 4055

PARMS NULL

IDENTIFIED BY rsaEncryption }

keyExchangeAlgorithm ALGORITHM ::= { -- IETF RFC 3279

PARMS KEA-Parms-Id

IDENTIFIED BY id-keyExchangeAlgorithm }

KEA-Parms-Id ::= OCTET STRING (SIZE (10))

-- Signature algorithms

sha224WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 5754

PARMS NULL

IDENTIFIED BY sha224WithRSAEncryption }

sha256WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 5754

PARMS NULL

IDENTIFIED BY sha256WithRSAEncryption }

sha384WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 5754

PARMS NULL

IDENTIFIED BY sha384WithRSAEncryption }

sha512WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 5754

PARMS NULL

IDENTIFIED BY sha512WithRSAEncryption }

dsa-with-sha224 ALGORITHM ::= { -- IETF RFC 5754

IDENTIFIED BY id-dsa-with-sha224 }

dsa-with-sha256 ALGORITHM ::= { -- IETF RFC 5754

IDENTIFIED BY id-dsa-with-sha256 }

END -- AlgorithmObjectIdentifiers