AlgorithmIdentification18

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lvl | AlgorithmIdentification18 | Mult | Constraint | Rule | Usage |
| 1 | Algorithm | [1..1] |  |  | <Mask generator functions of the RSAES-OAEP encryption algorithm (RSA Encryption Scheme: Optimal Asymmetric Encryption Padding).- **MGF1: MGF1** : *Generator Function, used for RSA encryption and RSA igital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).::Algorithm8Code*<br/>Mask generator functions of the RSAES-OAEP encryption algorithm (RSA Encryption Scheme: Optimal Asymmetric Encryption Padding).<br/>- <b>MGF1: MGF1</b> : <i>Generator Function, used for RSA encryption and RSA igital signature (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-mgf1).</i><br/>*<Algo>::Algorithm8Code* |
| 1 | Parameter | [0..1] |  |  | <*::Parameter9<Param>::Parameter9* |
| 2 | DigestAlgorithm | [0..1] |  |  | <Identification of a digest algorithm.- **HS25: SHA256** : *Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).*- **HS38: SHA384** : *Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).*- **HS51: SHA512** : *Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).*- **HS01: SHA1** : *The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).*- **SH31: SHA3-224** : *Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).*- **SH32: SHA3-256** : *Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).*- **SH33: SHA3-384** : *Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).*- **SH35: SHA3-512** : *Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).*- **SHK1: SHAKE128** : *Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).*- **SHK2: SHAKE256** : *Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).::Algorithm16Code*<br/>Identification of a digest algorithm.<br/>- <b>HS25: SHA256</b> : <i>Message digest algorithm SHA-256 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha256).</i><br/>- <b>HS38: SHA384</b> : <i>Message digest algorithm SHA-384 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha384).</i><br/>- <b>HS51: SHA512</b> : <i>Message digest algorithm SHA-512 as defined in FIPS 180-1 and 2 - (ASN.1 Object Identifier: id-sha512).</i><br/>- <b>HS01: SHA1</b> : <i>The DEPRECATED Message digest algorithm SHA-1 as defined in FIPS 180-1 - (ASN.1 Object Identifier: id-sha1).</i><br/>- <b>SH31: SHA3-224</b> : <i>Message digest algorithm SHA3-224 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-224).</i><br/>- <b>SH32: SHA3-256</b> : <i>Message digest algorithm SHA3-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-256).</i><br/>- <b>SH33: SHA3-384</b> : <i>Message digest algorithm SHA3-384 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-384).</i><br/>- <b>SH35: SHA3-512</b> : <i>Message digest algorithm SHA3-512 as defined in FIPS 202 - (ASN.1 Object Identifier: id-sha3-512).</i><br/>- <b>SHK1: SHAKE128</b> : <i>Message digest algorithm SHAKE-128 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake128).</i><br/>- <b>SHK2: SHAKE256</b> : <i>Message digest algorithm SHAKE-256 as defined in FIPS 202 - (ASN.1 Object Identifier: id-shake256).</i><br/>*<DgstAlgo>::Algorithm16Code* |