AlgorithmIdentification30

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lvl | AlgorithmIdentification30 | Mult | Constraint | Rule | Usage |
| 1 | Algorithm | [1..1] |  |  | <Cryptographic algorithms for digital signatures.- **ERS2: SHA256WithRSA** : *Signature algorithms with RSA, using SHA-256 digest algorithm - (ASN.1 Object Identifier: sha256WithRSAEncryption).*- **ERS1: SHA1WithRSA** : *The DEPRECATED Signature algorithms with RSA (PKCS #1 version 2.1), using SHA-1 digest algorithm - (ASN.1 Object Identifier: sha1WithRSAEncryption).*- **RPSS: RSASSA-PSS** : *Signature algorithm with Appendix, Probabilistic Signature Scheme (PKCS #1 version 2.1), - (ASN.1 Object Identifier: id-RSASSA-PSS).*- **ERS3: SHA3-256WithRSA** : *Signature algorithms with RSA, using SHA3-256 digest algorithm. (ASN.1 Object Identifier: id-rsassa-pkcs1-v1-5-with-sha3-256).*- **ED32: EcdsaSha3-256** : *Elliptic Curve Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.*- **ED33: EcdsaSha3-384** : *Elliptic Curve Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.*- **ED35: EcdsaSha3-512** : *Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.*- **ED23: EcdsaSha384** : *Elliptic Curve Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.*- **ED25: EcdsaSha512** : *Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.*- **ES22: EcsdsaSha256** : *Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.*- **ES32: EcsdaSha3-256** : *Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.*- **ES33: EcsdsaSha3-384** : *Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.*- **ES35: EcsdsaSha3-512** : *Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.*- **ES23: EcsdsaSha384** : *Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.*- **ES25: EcsdsaSha512** : *Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.*- **ED22: EcdsaSha256** : *Elliptic Curve Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.::Algorithm25Code*<br/>Cryptographic algorithms for digital signatures.<br/>- <b>ERS2: SHA256WithRSA</b> : <i>Signature algorithms with RSA, using SHA-256 digest algorithm - (ASN.1 Object Identifier: sha256WithRSAEncryption).</i><br/>- <b>ERS1: SHA1WithRSA</b> : <i>The DEPRECATED Signature algorithms with RSA (PKCS #1 version 2.1), using SHA-1 digest algorithm - (ASN.1 Object Identifier: sha1WithRSAEncryption).</i><br/>- <b>RPSS: RSASSA-PSS</b> : <i>Signature algorithm with Appendix, Probabilistic Signature Scheme (PKCS #1 version 2.1), - (ASN.1 Object Identifier: id-RSASSA-PSS).</i><br/>- <b>ERS3: SHA3-256WithRSA</b> : <i>Signature algorithms with RSA, using SHA3-256 digest algorithm. (ASN.1 Object Identifier: id-rsassa-pkcs1-v1-5-with-sha3-256).</i><br/>- <b>ED32: EcdsaSha3-256</b> : <i>Elliptic Curve Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.</i><br/>- <b>ED33: EcdsaSha3-384</b> : <i>Elliptic Curve Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.</i><br/>- <b>ED35: EcdsaSha3-512</b> : <i>Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.</i><br/>- <b>ED23: EcdsaSha384</b> : <i>Elliptic Curve Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.</i><br/>- <b>ED25: EcdsaSha512</b> : <i>Elliptic Curve Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.</i><br/>- <b>ES22: EcsdsaSha256</b> : <i>Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.</i><br/>- <b>ES32: EcsdaSha3-256</b> : <i>Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-256 Digest Algorithm.</i><br/>- <b>ES33: EcsdsaSha3-384</b> : <i>Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA3-384 Digest Algorithm.</i><br/>- <b>ES35: EcsdsaSha3-512</b> : <i>Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.</i><br/>- <b>ES23: EcsdsaSha384</b> : <i>Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-384 Digest Algorithm.</i><br/>- <b>ES25: EcsdsaSha512</b> : <i>Elliptic Curve Schnorr Digital Signature Algorithm coupled with SHA2-512 Digest Algorithm.</i><br/>- <b>ED22: EcdsaSha256</b> : <i>Elliptic Curve Digital Signature Algorithm coupled with SHA2-256 Digest Algorithm.</i><br/>*<Algo>::Algorithm25Code* |
| 1 | Parameter | [0..1] |  |  | <*::Parameter15<Param>::Parameter15* |
| 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* |
| 2 | MaskGeneratorAlgorithm | [0..1] |  |  | <*::AlgorithmIdentification12<MskGnrtrAlgo>::AlgorithmIdentification12* |
| 3 | 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* |
| 3 | Parameter | [0..1] |  |  | <*::Parameter5<Param>::Parameter5* |
| 4 | 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).::Algorithm11Code*<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/>*<DgstAlgo>::Algorithm11Code* |
| 2 | SaltLength | [0..1] |  |  | <*::Number<SaltLngth>::Number* |
| 2 | TrailerField | [0..1] |  |  | <*::Number<TrlrFld>::Number* |
| 2 | OIDCurveName | [0..1] |  |  | <*::Max140Text<OIDCrvNm>::Max140Text* |