AlgorithmIdentification19

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lvl | AlgorithmIdentification19 | Mult | Constraint | Rule | Usage |
| 1 | Algorithm | [1..1] |  |  | <Asymmetric encryption algorithm of a transport key.- **ERSA: RSAEncryption** : *RSA encryption algorithm - (ASN.1 Object Identifier: rsaEncryption).*- **RSAO: RSAES-OAEP** : *RSA encryption scheme based on Optimal Asymmetric Encryption scheme (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-RSAES-OAEP).::Algorithm7Code*<br/>Asymmetric encryption algorithm of a transport key.<br/>- <b>ERSA: RSAEncryption</b> : <i>RSA encryption algorithm - (ASN.1 Object Identifier: rsaEncryption).</i><br/>- <b>RSAO: RSAES-OAEP</b> : <i>RSA encryption scheme based on Optimal Asymmetric Encryption scheme (PKCS #1 version 2.1) - (ASN.1 Object Identifier: id-RSAES-OAEP).</i><br/>*<Algo>::Algorithm7Code* |
| 1 | Parameter | [0..1] |  |  | <*::Parameter10<Param>::Parameter10* |
| 2 | EncryptionFormat | [0..1] |  |  | <Format of data before encryption, if the format is not plaintext or implicit.- **TR31: TR31** : *Format of a cryptographic key specified by the ANSI X9 TR-31 standard.*- **TR34: TR34** : *Format of a cryptographic key specified by the ANSI X9 TR-34 standard.*- **I238: ISO20038KeyWrap** : *Format of a cryptographic key specified by the ISO20038 standard.::EncryptionFormat2Code*<br/>Format of data before encryption, if the format is not plaintext or implicit.<br/>- <b>TR31: TR31</b> : <i>Format of a cryptographic key specified by the ANSI X9 TR-31 standard.</i><br/>- <b>TR34: TR34</b> : <i>Format of a cryptographic key specified by the ANSI X9 TR-34 standard.</i><br/>- <b>I238: ISO20038KeyWrap</b> : <i>Format of a cryptographic key specified by the ISO20038 standard.</i><br/>*<NcrptnFrmt>::EncryptionFormat2Code* |
| 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] |  |  | FSee MDR for sub elements and [AlgorithmIdentification18](#AlgorithmIdentification18)*::AlgorithmIdentification18*For sub elements see AlgorithmIdentification18 <br>See MDR for sub elements and <a href="#AlgorithmIdentification18">AlgorithmIdentification18</a><br/>*<MskGnrtrAlgo>::AlgorithmIdentification18* |