AlgorithmIdentification22

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lvl | AlgorithmIdentification22 | Mult | Constraint | Rule | Usage |
| 1 | Algorithm | [1..1] |  |  | <Cryptographic algorithms for the MAC (Message Authentication Code).- **MACC: RetailCBCMAC** : *Retail CBC (Chaining Block Cypher) MAC (Message Authentication Code) (cf. ISO 9807, ANSI X9.19) - (ASN.1 Object Identifier: id-retail-cbc-mac).*- **MCCS: RetailSHA256MAC** : *Retail-CBC-MAC with SHA-256 (Secure HAsh standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-256).*- **CMA1: SHA256CMACwithAES128** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.*- **MCC1: RetailSHA1MAC** : *The DEPRECATED Retail-CBC-MAC with SHA-1 (Secure Hash standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-1).*- **CMA9: SHA384CMACwithAES192** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-384 digest of the message.*- **CMA5: SHA512CMACwithAES256** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-512 digest of the message.*- **CMA2: SHA256CMACWithAES256** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.*- **CM31: SHA3-256CMACWithAES128** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-256 digest of the message.*- **CM32: SHA3-384CMACWithAES192** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-384 digest of the message.*- **CM33: SHA3-512CMACWithAES256** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-512 digest of the message.*- **MCS3: SHA3-256-3DESMAC** : *3DES CBC-MAC with SHA3-256 (SecureHAsh standard) and ISO/IEC9797-1 method 2 padding.*- **CCA1: CMACAES128** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **CCA2: CMACAES192** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **CCA3: CMACAES256** : *CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).::Algorithm17Code*<br/>Cryptographic algorithms for the MAC (Message Authentication Code).<br/>- <b>MACC: RetailCBCMAC</b> : <i>Retail CBC (Chaining Block Cypher) MAC (Message Authentication Code) (cf. ISO 9807, ANSI X9.19) - (ASN.1 Object Identifier: id-retail-cbc-mac).</i><br/>- <b>MCCS: RetailSHA256MAC</b> : <i>Retail-CBC-MAC with SHA-256 (Secure HAsh standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-256).</i><br/>- <b>CMA1: SHA256CMACwithAES128</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.</i><br/>- <b>MCC1: RetailSHA1MAC</b> : <i>The DEPRECATED Retail-CBC-MAC with SHA-1 (Secure Hash standard) - (ASN.1 Object Identifier: id-retail-cbc-mac-sha-1).</i><br/>- <b>CMA9: SHA384CMACwithAES192</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-384 digest of the message.</i><br/>- <b>CMA5: SHA512CMACwithAES256</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-512 digest of the message.</i><br/>- <b>CMA2: SHA256CMACWithAES256</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA-256 digest of the message.</i><br/>- <b>CM31: SHA3-256CMACWithAES128</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-256 digest of the message.</i><br/>- <b>CM32: SHA3-384CMACWithAES192</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-384 digest of the message.</i><br/>- <b>CM33: SHA3-512CMACWithAES256</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard). The CMAC algorithm is computed on the SHA3-512 digest of the message.</i><br/>- <b>MCS3: SHA3-256-3DESMAC</b> : <i>3DES CBC-MAC with SHA3-256 (SecureHAsh standard) and ISO/IEC9797-1 method 2 padding.</i><br/>- <b>CCA1: CMACAES128</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>CCA2: CMACAES192</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>CCA3: CMACAES256</b> : <i>CMAC (Cipher based Message Authentication Code) defined by the National Institute of Standards and Technology (NIST 800-38B - May 2005), using the block cipher Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).</i><br/>*<Algo>::Algorithm17Code* |
| 1 | Parameter | [0..1] |  |  | <*::Parameter7<Param>::Parameter7* |
| 2 | InitialisationVector | [0..1] |  |  | <*::Max500Binary<InitlstnVctr>::Max500Binary* |
| 2 | BytePadding | [0..1] |  |  | <Byte padding for a cypher block chaining mode encryption, if the padding is not implicit.- **LNGT: LengthPadding** : *Message to encrypt is completed by a byte value containing the total number of added bytes.*- **NUL8: Null80Padding** : *Message to encrypt is completed by one bit of value 1, followed by null bits until the encryption block length is reached.*- **NULG: NullLengthPadding** : *Message to encrypt is completed by null byte values, the last byte containing the total number of added bytes.*- **NULL: NullPadding** : *Message to encrypt is completed by null bytes.*- **RAND: RandomPadding** : *Message to encrypt is completed by random value, the last byte containing the total number of added bytes.::BytePadding1Code*<br/>Byte padding for a cypher block chaining mode encryption, if the padding is not implicit.<br/>- <b>LNGT: LengthPadding</b> : <i>Message to encrypt is completed by a byte value containing the total number of added bytes.</i><br/>- <b>NUL8: Null80Padding</b> : <i>Message to encrypt is completed by one bit of value 1, followed by null bits until the encryption block length is reached.</i><br/>- <b>NULG: NullLengthPadding</b> : <i>Message to encrypt is completed by null byte values, the last byte containing the total number of added bytes.</i><br/>- <b>NULL: NullPadding</b> : <i>Message to encrypt is completed by null bytes.</i><br/>- <b>RAND: RandomPadding</b> : <i>Message to encrypt is completed by random value, the last byte containing the total number of added bytes.</i><br/>*<BPddg>::BytePadding1Code* |