CryptographicKey17

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lvl | CryptographicKey17 | Mult | Constraint | Rule | Usage |
| 1 | Identification | [1..1] |  |  | <*::Max350Text<Id>::Max350Text* |
| 1 | AdditionalIdentification | [0..1] |  |  | <*::Max35Binary<AddtlId>::Max35Binary* |
| 1 | Name | [0..1] |  |  | <*::Max256Text<Nm>::Max256Text* |
| 1 | SecurityProfile | [0..1] |  |  | <*::Max35Text<SctyPrfl>::Max35Text* |
| 1 | ItemNumber | [0..1] |  |  | <*::Max35Text<ItmNb>::Max35Text* |
| 1 | Version | [1..1] |  |  | <*::Max256Text<Vrsn>::Max256Text* |
| 1 | Type | [0..1] |  |  | <Codes for qualifying the type of cryptographic keys.- **AES2: AES128** : *AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **EDE3: DES112** : *Data encryption standard key of 112 bits (without the parity bits).*- **DKP9: DUKPT2009** : *DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.*- **AES9: AES192** : *AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 – November 6, 2001 - Advanced Encryption Standard).*- **AES5: AES256** : *AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 – November 6, 2001 - Advanced Encryption Standard).*- **EDE4: DES168** : *Data encryption standard key of 168 bits (without the parity bits).::CryptographicKeyType3Code*<br/>Codes for qualifying the type of cryptographic keys.<br/>- <b>AES2: AES128</b> : <i>AES (Advanced Encryption Standard) 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>EDE3: DES112</b> : <i>Data encryption standard key of 112 bits (without the parity bits).</i><br/>- <b>DKP9: DUKPT2009</b> : <i>DUKPT (Derived Unique Key Per Transaction) key, as specified in ANSI X9.24-2009 Annex A.</i><br/>- <b>AES9: AES192</b> : <i>AES (Advanced Encryption Standard) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 – November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>AES5: AES256</b> : <i>AES (Advanced Encryption Standard) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 – November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>EDE4: DES168</b> : <i>Data encryption standard key of 168 bits (without the parity bits).</i><br/>*<Tp>::CryptographicKeyType3Code* |
| 1 | Function | [0..\*] |  |  | <Allowed usages of the key.- **ENCR: Encryption** : *Key may encrypt.*- **DCPT: Decryption** : *Key may decrypt.*- **DENC: DataEncryption** : *Key may encrypt data.*- **DDEC: DataDecryption** : *Key may decrypt data.*- **TRNI: TranslateInput** : *Key may encrypt information before translation.*- **TRNX: TranslateOutput** : *Key may encrypt information after translation.*- **MACG: MessageAuthenticationCodeGeneration** : *Key may generate message authentication codes (MAC).*- **MACV: MessageAuthenticationCodeVerification** : *Key may verify message authentication codes (MAC).*- **SIGG: SignatureGeneration** : *Key may generate digital signatures.*- **SUGV: SignatureVerification** : *Key may verify digital signatures.*- **PINE: PINEncryption** : *Key may encrypt personal identification numbers (PIN).*- **PIND: PINDecryption** : *Key may decrypt personal identification numbers (PIN).*- **PINV: PINVerification** : *Key may verify personal identification numbers (PIN).*- **KEYG: KeyGeneration** : *Key may generate keys.*- **KEYI: KeyImport** : *Key may import keys.*- **KEYX: KeyExport** : *Key may export keys.*- **KEYD: KeyDerivation** : *Key may derive keys.::KeyUsage1Code*<br/>Allowed usages of the key.<br/>- <b>ENCR: Encryption</b> : <i>Key may encrypt.</i><br/>- <b>DCPT: Decryption</b> : <i>Key may decrypt.</i><br/>- <b>DENC: DataEncryption</b> : <i>Key may encrypt data.</i><br/>- <b>DDEC: DataDecryption</b> : <i>Key may decrypt data.</i><br/>- <b>TRNI: TranslateInput</b> : <i>Key may encrypt information before translation.</i><br/>- <b>TRNX: TranslateOutput</b> : <i>Key may encrypt information after translation.</i><br/>- <b>MACG: MessageAuthenticationCodeGeneration</b> : <i>Key may generate message authentication codes (MAC).</i><br/>- <b>MACV: MessageAuthenticationCodeVerification</b> : <i>Key may verify message authentication codes (MAC).</i><br/>- <b>SIGG: SignatureGeneration</b> : <i>Key may generate digital signatures.</i><br/>- <b>SUGV: SignatureVerification</b> : <i>Key may verify digital signatures.</i><br/>- <b>PINE: PINEncryption</b> : <i>Key may encrypt personal identification numbers (PIN).</i><br/>- <b>PIND: PINDecryption</b> : <i>Key may decrypt personal identification numbers (PIN).</i><br/>- <b>PINV: PINVerification</b> : <i>Key may verify personal identification numbers (PIN).</i><br/>- <b>KEYG: KeyGeneration</b> : <i>Key may generate keys.</i><br/>- <b>KEYI: KeyImport</b> : <i>Key may import keys.</i><br/>- <b>KEYX: KeyExport</b> : <i>Key may export keys.</i><br/>- <b>KEYD: KeyDerivation</b> : <i>Key may derive keys.</i><br/>*<Fctn>::KeyUsage1Code* |
| 1 | ActivationDate | [0..1] |  |  | <*::ISODateTime<ActvtnDt>::ISODateTime* |
| 1 | DeactivationDate | [0..1] |  |  | <*::ISODateTime<DeactvtnDt>::ISODateTime* |
| 1 | KeyValue | [0..1] |  |  | ISee MDR for sub elements and [ContentInformationType34](#ContentInformationType34)*::ContentInformationType34*If necessary, CMS structure used to exchange sensitive information related to this SecurityElement. <br>See MDR for sub elements and <a href="#ContentInformationType34">ContentInformationType34</a><br/>*<KeyVal>::ContentInformationType34* |
| 1 | KeyCheckValue | [0..1] |  |  | <*::Max35Binary<KeyChckVal>::Max35Binary* |
| 1 | AdditionalManagementInformation | [0..\*] |  |  | <*::GenericInformation1<AddtlMgmtInf>::GenericInformation1* |
| 2 | Name | [1..1] |  |  | <*::Max70Text<Nm>::Max70Text* |
| 2 | Value | [0..1] |  |  | <*::Max140Text<Val>::Max140Text* |