AuthenticatedData9

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lvl | AuthenticatedData9 | Mult | Constraint | Rule | Usage |
| 1 | Version | [0..1] |  |  | <*::Number<Vrsn>::Number* |
| 1 | Recipient | [1..\*] |  |  | <*::Recipient14Choice<Rcpt>::Recipient14Choice* |
| 2 | KeyTransport | [1..1] |  |  | <*::KeyTransport9<KeyTrnsprt>::KeyTransport9* |
| 3 | Version | [0..1] |  |  | <*::Number<Vrsn>::Number* |
| 3 | RecipientIdentification | [1..1] |  |  | <*::Recipient13Choice<RcptId>::Recipient13Choice* |
| 4 | IssuerAndSerialNumber | [1..1] |  |  | <*::IssuerAndSerialNumber2<IssrAndSrlNb>::IssuerAndSerialNumber2* |
| 5 | Issuer | [1..1] |  |  | <*::CertificateIssuer1<Issr>::CertificateIssuer1* |
| 6 | RelativeDistinguishedName | [1..\*] |  |  | <*::RelativeDistinguishedName1<RltvDstngshdNm>::RelativeDistinguishedName1* |
| 7 | AttributeType | [1..1] |  |  | <Type of attribute of a distinguished name (DN).- **CNAT: CommonName** : *Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).*- **LATT: Locality** : *Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).*- **OATT: OrganisationName** : *Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).*- **OUAT: OrganisationUnitName** : *Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).*- **CATT: CountryName** : *Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).::AttributeType1Code*<br/>Type of attribute of a distinguished name (DN).<br/>- <b>CNAT: CommonName</b> : <i>Common name of the attribute (ASN.1 Object Identifier: id-at-commonName).</i><br/>- <b>LATT: Locality</b> : <i>Locality of the attribute (ASN.1 Object Identifier: id-at-localityName).</i><br/>- <b>OATT: OrganisationName</b> : <i>Organization name of the attribute (ASN.1 Object Identifier: id-at-organizationName).</i><br/>- <b>OUAT: OrganisationUnitName</b> : <i>Organization unit name of the attribute (ASN.1 Object Identifier: id-at-organizationalUnitName).</i><br/>- <b>CATT: CountryName</b> : <i>Country name of the attribute (ASN.1 Object Identifier: id-at-countryName).</i><br/>*<AttrTp>::AttributeType1Code* |
| 7 | AttributeValue | [1..1] |  |  | <*::Max140Text<AttrVal>::Max140Text* |
| 5 | SerialNumber | [1..1] |  |  | <*::Max500Binary<SrlNb>::Max500Binary* |
| 4 | SubjectKeyIdentifier | [1..1] |  |  | <*::Max140Binary<SbjtKeyIdr>::Max140Binary* |
| 3 | KeyEncryptionAlgorithm | [1..1] |  |  | FSee MDR for sub elements and [AlgorithmIdentification19](#AlgorithmIdentification19)*::AlgorithmIdentification19*For sub elements see AlgorithmIdentification19 <br>See MDR for sub elements and <a href="#AlgorithmIdentification19">AlgorithmIdentification19</a><br/>*<KeyNcrptnAlgo>::AlgorithmIdentification19* |
| 3 | EncryptedKey | [1..1] |  |  | <*::Max5000Binary<NcrptdKey>::Max5000Binary* |
| 2 | KEK | [1..1] |  |  | <*::KEK8<KEK>::KEK8* |
| 3 | Version | [0..1] |  |  | <*::Number<Vrsn>::Number* |
| 3 | KEKIdentification | [1..1] |  |  | FSee MDR for sub elements and [KEKIdentifier7](#KEKIdentifier7)*::KEKIdentifier7*For sub elements see KEKIdentifier7 <br>See MDR for sub elements and <a href="#KEKIdentifier7">KEKIdentifier7</a><br/>*<KEKId>::KEKIdentifier7* |
| 3 | KeyEncryptionAlgorithm | [1..1] |  |  | <*::AlgorithmIdentification29<KeyNcrptnAlgo>::AlgorithmIdentification29* |
| 4 | Algorithm | [1..1] |  |  | <Cryptographic algorithms for the protection of transported keys.- **EA2C: AES128CBC** : *AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **E3DC: DES112CBC** : *Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with double length key (112 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).*- **DKP9: DUKPT2009** : *DUKPT (Derived Unique Key Per Transaction) algorithm, as specified in ANSI X9.24-2009 Annex A.*- **UKPT: UKPT** : *UKPT (Unique Key Per Transaction) or Master Session Key key encryption - (ASN.1 Object Identifier: id-ukpt-wrap).*- **UKA2: UKPTwithAES192** : *UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 192 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **EA9C: AES192CBC** : *AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 – November 6, 2001 - Advanced Encryption Standard).*- **EA5C: AES256CBC** : *AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 – November 6, 2001 - Advanced Encryption Standard).*- **DA12: AESDUKPT128ECB** : *AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A, With key length of 128 bits.*- **DA19: AESDUKPT192ECB** : *AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 192 bits.*- **DA25: AESDUKPT256ECB** : *AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 256 bits.*- **N108: Nist800-108KeyDerivation** : *Key Derivation according to the Special Publication from the NIST entitled 800-108.*- **EA5R: AES256CTR** : *AES (Advanced Encryption Standard) CTR (Counter) encryption with a 256 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **EA9R: AES192CTR** : *AES (Advanced Encryption Standard) CTR (Counter) encryption with a 192 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **EA2R: AES128CTR** : *AES (Advanced Encryption Standard) CTR (Counter) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **E3DR: DES112CTR** : *Triple DES (Data Encryption Standard) CTR (Counter) encryption with double length key (112 Bit) as defined in FIPS SP 800-38a.*- **E36C: DES168CBC** : *Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with triple length key (168 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).*- **E36R: DES168CTR** : *Triple DES (Data Encryption Standard) CTR (Counter) encryption with triple length key (168 Bit) as defined in FIPS SP 800-38a.*- **SD5C: SDE056CBC** : *The DEPRECATED Simple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with simple length key (56 Bit) as defined in FIPS PUB 81 - (ASN.1 Object Identifier: des-cbc).*- **UKA1: UKPTwithAES128** : *UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 128 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).*- **UKA3: UKPTwithAES256** : *UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using Advanced Encryption Standard with a 256 bits cryptographic key, approved by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).::Algorithm24Code*<br/>Cryptographic algorithms for the protection of transported keys.<br/>- <b>EA2C: AES128CBC</b> : <i>AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>E3DC: DES112CBC</b> : <i>Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with double length key (112 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).</i><br/>- <b>DKP9: DUKPT2009</b> : <i>DUKPT (Derived Unique Key Per Transaction) algorithm, as specified in ANSI X9.24-2009 Annex A.</i><br/>- <b>UKPT: UKPT</b> : <i>UKPT (Unique Key Per Transaction) or Master Session Key key encryption - (ASN.1 Object Identifier: id-ukpt-wrap).</i><br/>- <b>UKA2: UKPTwithAES192</b> : <i>UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using 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>EA9C: AES192CBC</b> : <i>AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) 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>EA5C: AES256CBC</b> : <i>AES (Advanced Encryption Standard) CBC (Chaining Block Cypher) 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>DA12: AESDUKPT128ECB</b> : <i>AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A, With key length of 128 bits.</i><br/>- <b>DA19: AESDUKPT192ECB</b> : <i>AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 192 bits.</i><br/>- <b>DA25: AESDUKPT256ECB</b> : <i>AES DUKPT (Derived Unique Key Per Transaction) ECB algorithm, as specified in ANSI X9.24-3-2017 Annex A.With key length of 256 bits.</i><br/>- <b>N108: Nist800-108KeyDerivation</b> : <i>Key Derivation according to the Special Publication from the NIST entitled 800-108.</i><br/>- <b>EA5R: AES256CTR</b> : <i>AES (Advanced Encryption Standard) CTR (Counter) 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>EA9R: AES192CTR</b> : <i>AES (Advanced Encryption Standard) CTR (Counter) 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>EA2R: AES128CTR</b> : <i>AES (Advanced Encryption Standard) CTR (Counter) encryption with a 128 bits cryptographic key as defined by the Federal Information Processing Standards (FIPS 197 - November 6, 2001 - Advanced Encryption Standard).</i><br/>- <b>E3DR: DES112CTR</b> : <i>Triple DES (Data Encryption Standard) CTR (Counter) encryption with double length key (112 Bit) as defined in FIPS SP 800-38a.</i><br/>- <b>E36C: DES168CBC</b> : <i>Triple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with triple length key (168 Bit) as defined in FIPS PUB 46-3 - (ASN.1 Object Identifier: des-ede3-cbc).</i><br/>- <b>E36R: DES168CTR</b> : <i>Triple DES (Data Encryption Standard) CTR (Counter) encryption with triple length key (168 Bit) as defined in FIPS SP 800-38a.</i><br/>- <b>SD5C: SDE056CBC</b> : <i>The DEPRECATED Simple DES (Data Encryption Standard) CBC (Chaining Block Cypher) encryption with simple length key (56 Bit) as defined in FIPS PUB 81 - (ASN.1 Object Identifier: des-cbc).</i><br/>- <b>UKA1: UKPTwithAES128</b> : <i>UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using 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>UKA3: UKPTwithAES256</b> : <i>UKPT (Unique Key Per Transaction) or Master Session Key key encryption, using 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>::Algorithm24Code* |
| 4 | Parameter | [0..1] |  |  | <*::Parameter12<Param>::Parameter12* |
| 5 | 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* |
| 5 | InitialisationVector | [0..1] |  |  | <*::Max500Binary<InitlstnVctr>::Max500Binary* |
| 5 | 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* |
| 3 | EncryptedKey | [0..1] |  |  | <*::Max500Binary<NcrptdKey>::Max500Binary* |
| 2 | KeyIdentifier | [1..1] |  |  | FSee MDR for sub elements and [KEKIdentifier7](#KEKIdentifier7)*::KEKIdentifier7*For sub elements see KEKIdentifier7 <br>See MDR for sub elements and <a href="#KEKIdentifier7">KEKIdentifier7</a><br/>*<KeyIdr>::KEKIdentifier7* |
| 1 | MACAlgorithm | [1..1] |  |  | FSee MDR for sub elements and [AlgorithmIdentification22](#AlgorithmIdentification22)*::AlgorithmIdentification22*For sub elements see AlgorithmIdentification22 <br>See MDR for sub elements and <a href="#AlgorithmIdentification22">AlgorithmIdentification22</a><br/>*<MACAlgo>::AlgorithmIdentification22* |
| 1 | EncapsulatedContent | [1..1] |  |  | <See MDR for sub elements and [EncapsulatedContent3](#EncapsulatedContent3)*::EncapsulatedContent3*<br>See MDR for sub elements and <a href="#EncapsulatedContent3">EncapsulatedContent3</a><br/>*<NcpsltdCntt>::EncapsulatedContent3* |
| 1 | MAC | [1..1] |  |  | <*::Max140Binary<MAC>::Max140Binary* |