SCTS-SC

Appendix C

Codelists

Version 1.0.0

2010-11-22

Innehållsförteckning

1 Koder i AUTACK

K301 Security service

Description: Specification of the security service applied.

Used in EDIFACT element USH[2].0501

Code	Description:
7	Referenced EDIFACT structure non-repudiation of origin The referenced EDIFACT structure is secured by a digital signature protecting the receiver of the message from the sender's denial of having sent the message

K302 Scope of security application

Description: Specification of the scope of application of the security service defined in the security header.

Used in EDIFACT element USH[2].0541

Code	Description:
3	Whole related message, group or interchange From the first character of the message, group or interchange to the last character of the message, group or interchange

K303 Role of security provider

Description: Identification of the function of the security provider in relation to the secured item.

Used in EDIFACT element USH[2].0509

Code	Description:
1	Issuer The security provider is the rightful issuer of the signed document

K304 Security party qualifier

Description: Specification of the role of the security party.

Used in EDIFACT element USH[2].S500.0577

Code	Description:
ZH1	Mutually agreed Identifies the party which generates the security parameters of the message (i.e. security originator). The identification details are: 1. S500.0511 (Security party identification) carries the registration number (*organisationsnummer*)

K305 Use of algorithm

Description: Specification of the usage made of the algorithm.

Used in EDIFACT elements USA[3].S502.0523 & USA[5].S502.0523

Code	Description:
1	Owner hashing Specifies that the algorithm is used by the message sender to compute the hash function on the message
6	Owner signing Specifies that the algorithm is used by the message sender to sign either the hash result computed on the message or the symmetric keys

K308 Validation value qualifier

Description: Identification of the type validation value.

Used in EDIFACT element USY[9].S508.0563

Code	Description:
ZS3	Cryptographic checksum (hash value) Calculated with algorithm defined in USA[3].0527
ZS4	Encrypted cryptographic checksum (digital signature) Calculated with algorithm defined in USA[5].0527

K309 Security party qualifier

Description: Specification of the role of the security party.

Used in EDIFACT element USC[4].S500.0577

Code	Description:
4	Authenticating party Party which certifies that the document (i.e. the certificate) is authentic

Comment: USC[4].0538 (Key name) carries a unique identifier of the Certificate Authority.

K310 Certificate syntax and version

Description: Specification of Coded identification of the syntax version used to create the certificate.

Used in EDIFACT element USC[4].0545

Code	Description:
3	X.509 ISO/IEC 9594-8, ITU X.509 key/certificate reference

K311 Filter function, coded

Description: Identification of the filtering function used to reversibly map any bit pattern on to a restricted character set.

Used in EDIFACT element USH[2].0505

Code	Description:
2	Hexadecimal filter

Comment: Conversion of hexadecimal data (digital signature) to a readable character format.

K312 Algorithm, coded

Description: Identification of the algorithm.

Used in EDIFACT element USA[3].0527

Code	Description:
48	SHA-256 Secure Hash Algorithm, dedicated Hash-Function #4; ISO 10118-3.

K313 Algorithm, coded

Description: Identification of the algorithm.

Used in EDIFACT element USA[5].0527

Code	Description:
10	RSA Rivest, Shamir, Adleman: A Method for obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, Vol.21(2), pp 120-126 (1978).