SCTS-SC

Appendix Q

Data model

Version 1.0.1

2012-02-17

1 Introduction

This appendix describes the detailed structure of Functional Message Structure (FMS) for SEA02.

FMS's are organised into data groups that contain data items. A data group is not necessarily the equivalent of a database entity. The data items are grouped together in such a way that they build up coherent logical blocks within the scope of each FMS.

The detailed structures comprising:

- The characteristics of the data groups belonging to the FMS: sequence, number of repetitions, status value to indicate if the data group is mandatory (R: Required), optional (O: Optional) or conditional (D: Dependent).

- The characteristics of the data items belonging to a data group : sequence, number of repetitions, type, length and a value to indicate if a data item is mandatory (R:Required), optional (O: Optional) or conditional (D: Dependent).

- Data group indentation to indicate that the data group may contain not only data items but also other groups of data.

- Rules and Conditions applying.

2 Representation of FMS's

A

(1) **SEA02A** (2) **AUTACK**

B

(3)	(4)	(5)	(6)
MESSAGE	1x	R	
----SECURITY HEADER	99x	R	
------SECURITY ALGORITHM(hash algorithm), (7)	1x	R	NXXX
------CERTIFICATE	1x	R	
--------SECURITY ALGORITHM(signature algorithm),	1x	R	

C

(8)	(11)	(10)	(12)	(13)
--MESSAGE				
Message reference (9)	an..14	R		N004
Message type	an..6	R		
Message version number	an..3	R		
Message release number	an..3	R		
Controlling agency	an..2	R		
Association assigned code	an6	R		
Number of segments in the message	n..6	R		
----SECURITY HEADER				
Security service	n1	R	K301	
Security reference number	an..14	R		N007
Scope of security application	n1	R	K302	
Filter function	an..3	R	K311	
Role of security provider	n1	R	K303	
Security party qualifier	n1	R	K304	
Security party identification	an..17	R		N009
Security date and time qualifier	n1	R		
Security date (CCYYMMDD)	n8	R		
Security time (HHMMSS)	n6	R		

The model is divided into three parts:

A The identification part, each message is identified by:

- a unique number that consists of the two characters 'SE' followed by (1) message identification (an3) and version (a1)
- the title of the message. (2)

B The structure part provides the following:

- the sequence of the data groups in the message;
- a data group name; (3)
- a number followed by the character 'x' (4) indicating how many times the data group is repeated in the message;
- a value (5) indicating whether the data group is (R)equired, (O)ptional or conditional (D)ependent;
- when any Rules, Conditions or Notifications apply, a reference (6) is provided;
- data group indentation (7) indicates that the data group depends on lower indent data group.

C The 'data group' detail part provides for each attribute the following:

- the sequence of attributes within a data group;
- a data group name (8), as in the structure part;
- the attribute name (9) within the data group;
- a value (10) indicating whether an attribute is (R)equired, (O)ptional or conditional (D)ependent;

- 11 the data type of a data item: (a)lphabetic and/or (n)umeric and the attribute length (the optional 2 dots before the length indicator mean that a data item has no fixed length, but it can have up to a number of digits, as specified by the length indicator); it must be noted that the data type / attribute length of fields representing a date is always ‘n8’ in order to be year 2000 compliant (e.g. 19980220); also, a comma in the data item length (e.g. 11,3), means that a data item can hold decimals, the digit before the comma indicates the maximum total length of an data item, the digit after the comma indicates the maximum number of digits after the decimal point;

- when there is a relevant codelist, a reference 12 (to appendix C) is provided;

- when any Rules or Conditions apply, a reference 13 is provided.

3 Data model for CUSDEC/CUSRES messages in the direction to and from Swedish Customs

3.1 Common for all messages in TDR050

3.1.1 Common for all CUSDEC messages

Data groups *(CUSDEC in direction to Swedish Customs)*

SERVICE STRING ADVICE	R	1x
INTERCHANGE	R	1x
--MESSAGE	R	998x

Data groups *(CUSDEC in direction from Swedish Customs)*

SERVICE STRING ADVICE	R	1x
INTERCHANGE	R	1x
--MESSAGE	R	1x

3.1.2 Common for all CUSRES messages

Data groups *(CUSRES in direction from Swedish Customs)*

SERVICE STRING ADVICE	R	1x
INTERCHANGE	R	1x
--MESSAGE	R	998x

3.2 Common for all messages in SCTS-AIS and TDR310.

3.2.1 Common for all CUSDEC/CUSRES messages

Data groups *(in direction to Swedish Customs)*

SERVICE STRING ADVICE	R	1x
INTERCHANGE	R	1x
--MESSAGE	R	1x

Data groups *(in direction from Swedish Customs)*

SERVICE STRING ADVICE	R	1x
INTERCHANGE	R	1x
--MESSAGE	R	1x

4 Data model for security message

4.1 SEA02A (AUTACK)

Since the message AUTACK always exists together with one or more CUSDEC/CUSRES messages in an interchange, SERVICE STRING ADVICE and INTERCHANGE are not specified here.

SERVICE STRING ADVICE	R	1x
INTERCHANGE	R	1x
--MESSAGE	R	1x
----SECURITY HEADER	R	99x
------SECURITY ALGORITHM(hash algorithm),	R	1x
------CERTIFICATE	R	1x
--------SECURITY ALGORITHM(signature algorithm),	R	1x
--------SECURITY RESULT		-
----SECURED DATA IDENTIFICATION		-
----SECURITY REFERENCES	R	998x
------SECURITY ON REFERENCES(hash value)	R	1x
------SECURITY ON REFERENCES(digital signature)	R	1x
----SECURITY TRAILER		-
------SECURITY RESULT		-

--MESSAGE				
Message reference	an..14	R		N004
Message type	an..6	R		
Message version number	an..3	R		
Message release number	an..3	R		
Controlling agency	an..2	R		
Association assigned code	an6	R		
Number of segments in the message	n..6	R		
----SECURITY HEADER				
Security service	n1	R	K301	
Security reference number	an..14	R		N007
Scope of security application	n1	R	K302	
Filter function	an..3	R	K311	
Role of security provider	n1	R	K303	
Security party qualifier	an..3	R	K304	
Security party identification	an..17	R		N009
Security date and time qualifier	n1	R		
Security date (CCYYMMDD)	n8	R		
Security time (HHMMSS)	n6	R		
------SECURITY ALGORITHM, hash algorithm				
Use of algorithm	n1	R	K305	
Algorithm, coded	n2	R	K312	
------CERTIFICATE				
Certificate reference	an..35	R		N010
Security party qualifier	n1	R	K309	
Key name	an..35	R		N011
Certificate syntax version, coded	n1	R	K310	
--------SECURITY ALGORITHM, digital signature				
Use of algorithm, coded	n1	R	K305	
Algorithm, coded	n2	R	K313	
----SECURITY REFERENCES				
Interchange control reference	an..14	R		N005, N012
Message reference number	an..14	R		N004, N012
Message type	an..6	R		N012
Message version number	an..3	R		N012
Message release number	an..3	R		N012
Controlling agency, coded	an..3	R		N012
------SECURITY ON REFERENCES, hash value				
Security reference number	an..14	R		N007
Validation value qualifier	an3	R	K308	
Validation value (hash value)	an..1024	R		
------SECURITY ON REFERENCES, digital signature				
Security reference number	an..14	R		N007
Validation value qualifier	an3	R	K308	
Validation value(digital signature)	an..1024	R		

5 Notifications

N001	-
N002	-
N003	-
N004	A unique identification of a message within an interchange.
N005	Unique reference assigned by the sender to an interchange.
N006	-
N007	Unique reference number assigned by the security originator to a pair of security header and security trailer groups. Connects SECURITY HEADER with SECURITY ON REFERENCES(hash value) and SECURITY ON REFERENCES(digital signature).
N008	-
N009	Identifies signing part's EORI number.
N010	Serial number of signing part's certificate, unique within a given Certificate Authority
N011	A unique identifier of the Certificate Authority, i.e. *authorityKeyIdentifier* in the certificate.
N012	Identifies the referred message.