SCTS-SC

Appendix A

Technical Overview

Version 1.0.0

2010-11-22

Index

Appendix:
Appendix A - Technical overview (this appendix)
Appendix C - Codelists
Appendix G - Branching diagram
Appendix H - EDIFACT segment descriptions
Appendix Q - Data model

1 Introduction

1.1 General for the framework

1.2 Digital Signature and AUTACK message

1.2.1 Some general points

- For each message a cryptographic checksum (hash value) and an encrypted cryptographic checksum (digital signature) is created. A signed checksum provide the possibility to verify that the message has not been changed. The digital signature ensures the identification of the sender and that the sender can not deny that he sent the message. The whole EDIFACT message is used in the calculations of checksum and digital signature, refer to figure in the next section.

- The checksums and digital signatures in an interchange are located in an AUTACK message.

- The AUTACK message clearly identifies the CUSDEC / CUSRES message a specific checksum and digital signature belongs to.

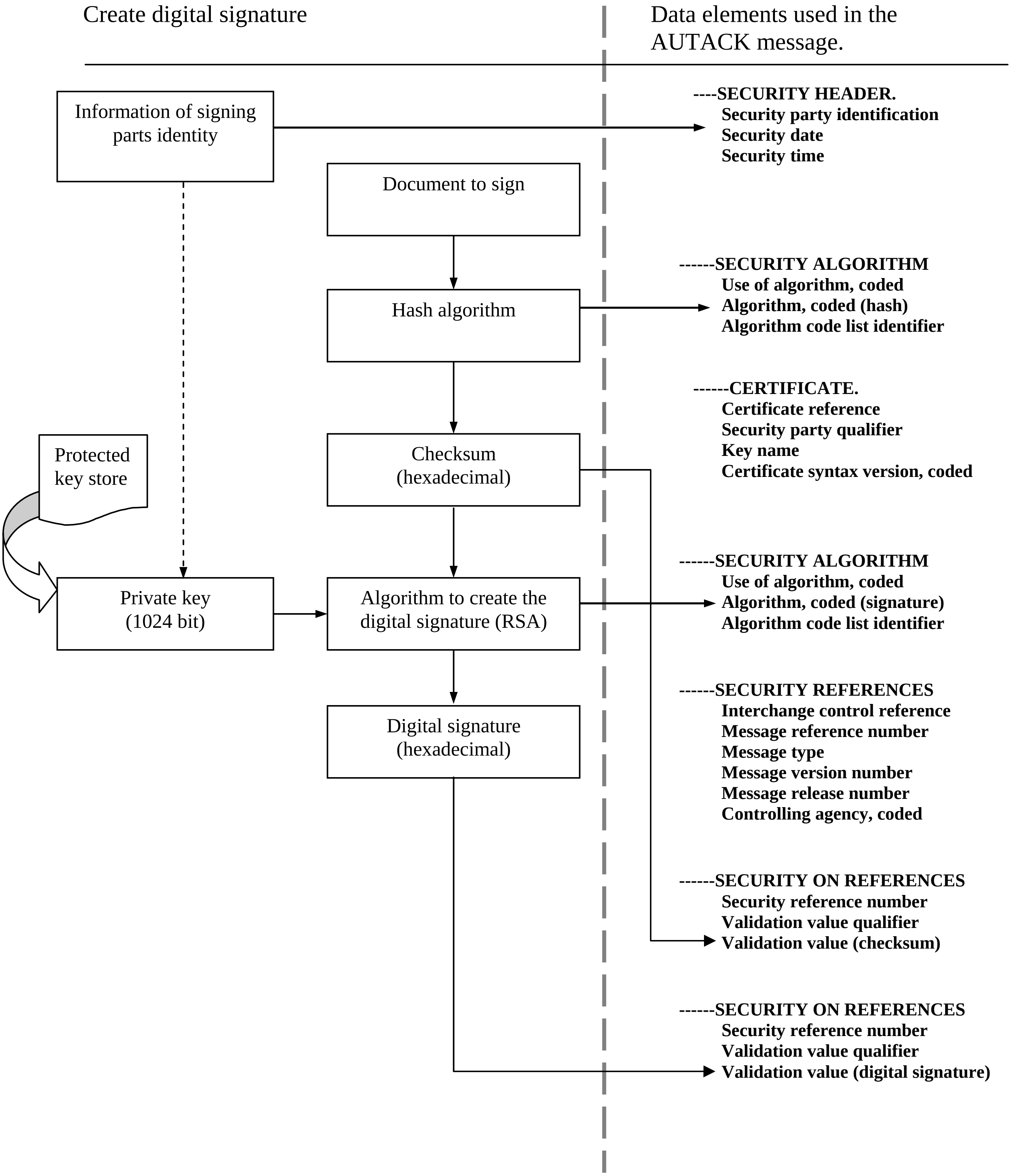
- All interchanges containing one or more CUSDEC or CUSRES *must* contain *one* AUTACK.
  An interchange can not contain more than *one* AUTACK message (more than one AUTACK results in EDIFACT error).

- For transfers in direction “Trader --> Swedish Customs”, the content of a transfer will always be one of the following:
  - One or more CUSDEC + one AUTACK
  - A CONTRL type 2

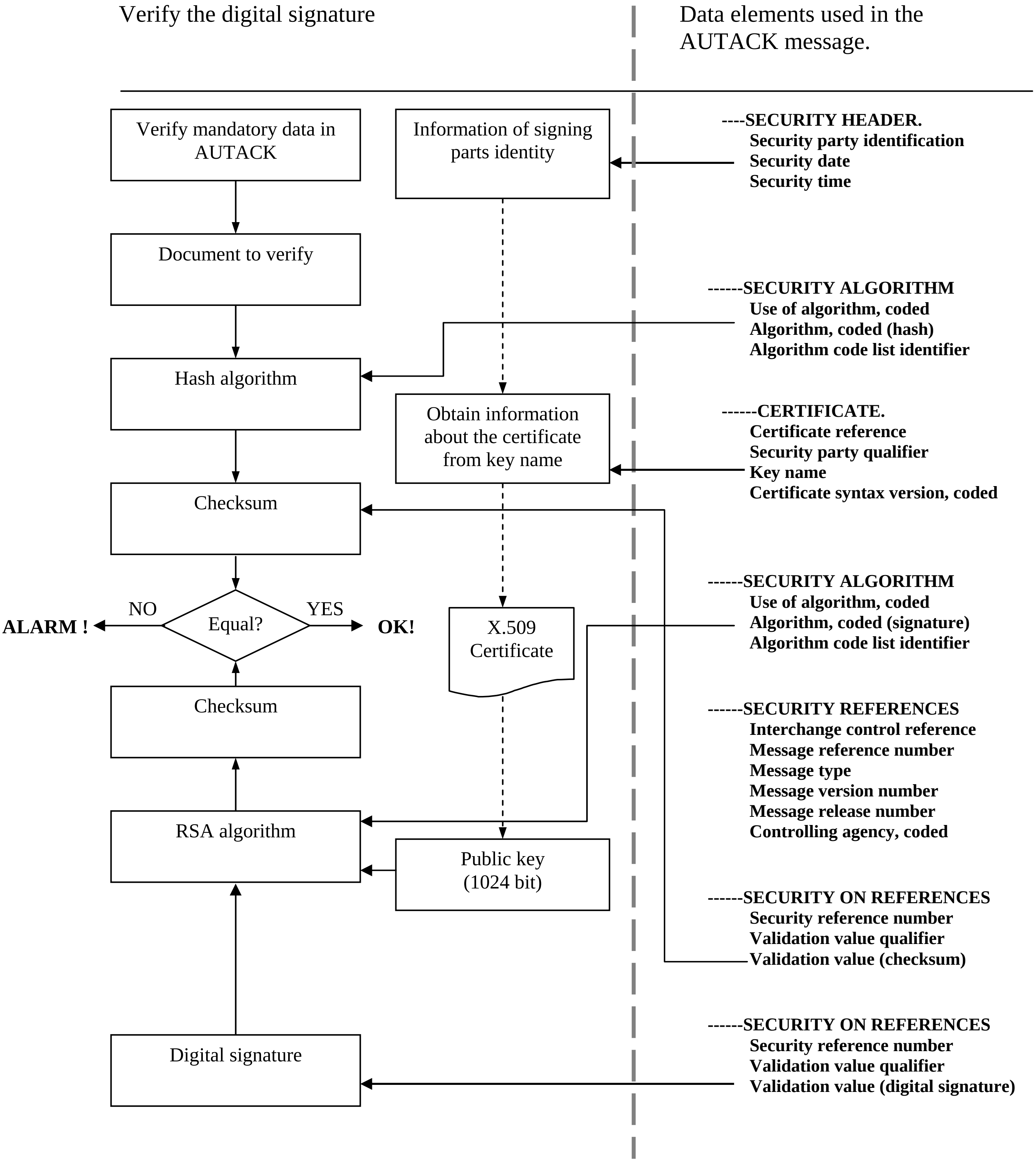
- For transfers in direction “Swedish Customs --> Trader”, the content of a transfer will always be one of the following:
  - One or more CUSRES + one AUTACK
  - One CUSDEC + one AUTACK
  - One CONTRL type 1
  - One CONTRL type 2

- More detailed information regarding the AUTACK message is described in Appendix G (structure), H (mapping), C (code lists) and Q (data model).

1.2.2 Creating an AUTACK message


Create digital signature
Data elements used in the AUTACK message.
Information of signing parts identity
----SECURITY HEADER.
Security party identification
Security date
Security time
Document to sign
------SECURITY ALGORITHM
Use of algorithm, coded
Algorithm, coded (hash)
Algorithm code list identifier
Hash algorithm
------CERTIFICATE.
Certificate reference
Security party qualifier
Key name
Certificate syntax version, coded
Protected key store
Checksum (hexadecimal)
------SECURITY ALGORITHM
Use of algorithm, coded
Algorithm, coded (signature)
Algorithm code list identifier
Private key (1024 bit)
Algorithm to create the digital signature (RSA)
------SECURITY REFERENCES
Interchange control reference
Message reference number
Message type
Message version number
Message release number
Controlling agency, coded
Digital signature (hexadecimal)
------SECURITY ON REFERENCES
Security reference number
Validation value qualifier
Validation value (checksum)
------SECURITY ON REFERENCES
Security reference number
Validation value qualifier
Validation value (digital signature)

1.2.3 Verifying an AUTACK message


Verify the digital signature
Data elements used in the AUTACK message.
Verify mandatory data in AUTACK
Information of signing parts identity
Document to verify
Hash algorithm
Obtain information about the certificate from key name
Checksum
NO
YES
ALARM !
Equal?
OK!
X.509 Certificate
Checksum
RSA algorithm
Public key (1024 bit)
Digital signature
----SECURITY HEADER.
Security party identification
Security date
Security time
------SECURITY ALGORITHM
Use of algorithm, coded
Algorithm, coded (hash)
Algorithm code list identifier
------CERTIFICATE.
Certificate reference
Security party qualifier
Key name
Certificate syntax version, coded
------SECURITY ALGORITHM
Use of algorithm, coded
Algorithm, coded (signature)
Algorithm code list identifier
------SECURITY REFERENCES
Interchange control reference
Message reference number
Message type
Message version number
Message release number
Controlling agency, coded
------SECURITY ON REFERENCES
Security reference number
Validation value qualifier
Validation value (checksum)
------SECURITY ON REFERENCES
Security reference number
Validation value qualifier
Validation value (digital signature)