ETS
1997-12-13
12:30:23 Z
PKITS

PKITS
Public Key Infrastructure with Time-Stamping Authority

(a.k.a. PITA)

ETS PROJECT: 23.192

Deliverable D5
Time-Stamping Service
Functional Specification and Protocols
for Structured Data: EDI Documents

Produced by: ***UPC***
Date of issue: 2nd ***August 1998***
Revision Number: 5

TABLE OF CONTENTS

HISTORY

version	date	author	comment
1	1998-august-1	Manel Medina, Eduard Bel Serra	1st index proposal
2	1998-august-20	Manel Medina, Eduard Bel Serra, Juan Carlos Cruellas, Montserrat Rubia	Executive summary and protocols
3	1998-september-2	Manel Medina, Eduard Bel Serra, Juan Carlos Cruellas, Montserrat Rubia	Protocols, appendixes, scenarios of use, requirements, access means
4	1998-september-4	Manel Medina, Eduard Bel Serra, Juan Carlos Cruellas, Montserrat Rubia	Protocols, appendixes, scenarios of use, requirements, access means
5	1998-september-8	Manel Medina, Eduard Bel Serra, Juan Carlos Cruellas, Montserrat Rubia	Scenarios of use, requirements, access means

GLOSSARY OF TERMS

Specifications:	
SHALL	Essential requirement. A requirement must be fulfilled or a feature implemented wherever this term occurs. The designer is requested, however, to indicate if one or more “shall requirements” would increase the cost or time unreasonably in relation to the total cost or design cost, in which case the specification may have to be revised.
SHOULD	Important requirement. Shall be implemented without or with minimum extra cost. Valid reasons in particular circumstances may allow ignoring such requirements.
MAY	Optional requirement. From case to case, it should be decided whether implementing it or not, in any case without exceeding the budget planned for the related activity.

Technical:	
CA	Certification Authority
DS	Digital Signature
EDI	Electronic data Interchange
EDIFACT	Electronic data Interchange for administration, commerce and transport
ETS	European Trusted Systems
MTBF	Mean Time Between Fails
MTTF	Mean Time to Fail
NA	Notary Authority
PKI	Public Key Infrastructure
SJWG	Security Joint Working Group
TS	Time-Stamping
TSA	Time-Stamping Authority
TSS	Time-Stamping Service
TTP	Trusted Third Party
UNA	Service string advice
UNB	Interchange header
UNH	Message header segment
UNT	Message trailer segment
USA	Security algorithm segment
USH	Security header segment
USR	Security result segment
UST	Security trailer segment

1 EXECUTIVE SUMMARY

This document covers the provision of a time-stamping service when the time-stamping authority has knowledge of the internal structure of the documents to be time-stamped, specially when these documents comply with UN/EDIFACT syntax rules (Electronic Data Interchange for Administration, Commerce and Transport) in a batch environment processing. This time stamp service specification proposal follows the guidelines developed by "Security Joint Working Group" UN/EDIFACT (SJWG)

The document is organised as follows. Section 3 covers service requirements from the points of view of the service users (requester and verifier). Section 4 formalises the protocols described in Deliverable D3 [PKITS D3] which are applicable to these kind of documents, going into syntax rules version 4 defined in ISO 9735-1 [SJWG 1], ISO 9735-2 [SJWG 2] and ISO 9735-5 [SJWG 3] and details of formats and encoding. Section 5 presents four implementations of the service over Internet. Lastly, section 6 briefly describes real scenarios of use.

1.1 WHAT ARE “EDI STRUCTURED DOCUMENTS”?

The term “structured documents”, which is used frequently in this document refers to those messages complying with the UN/EDIFACT syntax rules in a batch environment processing defined by ISO. An UN/EDIFACT message has an internal structure known by the TSS context, so the TSA embed a trusted time reference into some specific data fields from the original EDI document (EDI interchange) the requester submitted. Finally, the whole EDI document (EDI interchange) is returned to the requester in a secure manner.

This procedure differs with those specified in previous Deliverable D4 [PKITS D4] where unstructured documents where involved and only a representation of the original documents (document digest) were time-stamped. This kind of documents were handled as raw data.

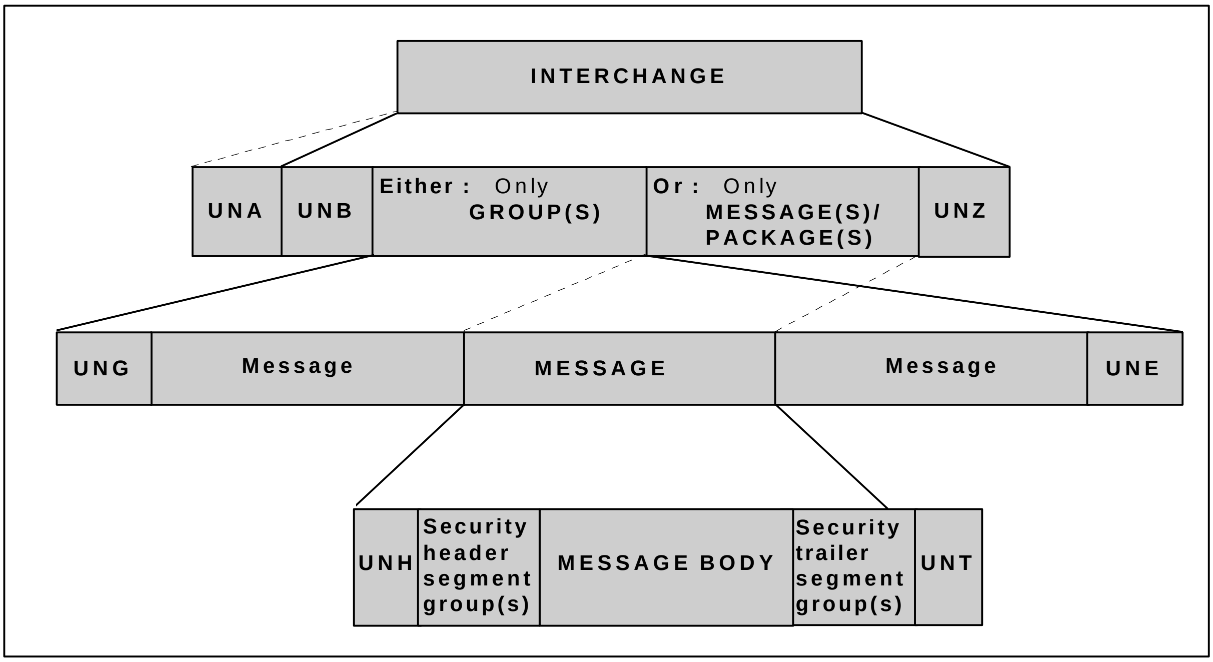
It is also important to notice that the distinction made between structured and unstructured documents is forced by completely different functional specifications of TSS.

1.2 SECURITY MECHANISMS FOR BATCH EDI AND TIME STAMP SERVICE

An UN/EDIFACT complaint message following ISO 9735-1 [SJWG 1] and ISO 9735-2 [SJWG 2] syntax rules does not offer any security mechanism in front of authenticity, integrity and no repudiation attacks. This lack was solved by years using private infrastructures and communication networks as VAN (Value Added Networks).

However, today Internet is a cheaper infrastructure and an easier way to interchange messages and the security problem related to EDI messages has been solved by syntax rules extensions. These syntax rules extensions for batch processing environment EDI messages are specified in OSI 9735-5 [SJWG 3] for authenticity, integrity and no repudiation of origin. These syntax rules specify a new security header and trailer pair, which embeds cryptographic information to protect messages involved in an EDI interchange.

The following illustration shows where this new security header and trailer pair shall be embedded in an EDI interchange:


INTERCHANGE
UNA
UNB
Either : Only GROUP(S)
Or : Only MESSAGE(S)/ PACKAGE(S)
UNZ
UNG
Message
MESSAGE
Message
UNE
UNH
Security header segment group(s)
MESSAGE BODY
Security trailer segment group(s)
UNT

As it was defined in the previous deliverable Deliverable D3 [PKITS D3], the data structures the requester of the time stamp service and the TSA interchanges shall be protected against authenticity, integrity and no repudiation of origin attacks by using digital signatures. These digital signatures will be embedded into the EDI interchange through the security header and trailer mentioned above.

Moreover, in order to provide Time Stamp Service over secure EDI compliant messages, additional security information, which specifies some details related to time stamp quality service is mandatory. This additional security information will be added through additional headers and trailers embedded into the EDI interchange, but instead of defining a new time stamp header and trailer pair, we use additional instances of the security header and trailer structures mentioned above and standardised by ISO.

This solution is described in detail in chapter 4 Protocols.

2 REFERENCES

[SJWG 1] SJWG: “EDIFACT CD-9735-1: Application level syntax rules. Part 1: Syntax rules common to all parts, together with syntax service directories for each of the parts.” 1997.

[SJWG 2] SJWG: “EDIFACT CD-9735-2: Application level syntax rules. Part2: Syntax rules specific to batch EDI security rules for batch EDI.” 1997.

[SJWG 3] SJWG: “EDIFACT CD-9735-5: Application level syntax rules: Security rules for batch EDI. Part 5: (authenticity, integrity and non-repudiation of origin)”. 1997.

[SJWG 4] SJWG: “Recommendations for UN/EDIFACT message level security from the UN/EDIFACT Security JWG” 1993.

[SJWG 5] SJWG: “TRADE/WP4/R1026: EDIFACT SECURITY IMPLEMENTATION GUIDELINES”. 1994.

[SJWG 6] SJWG: “EDIFACT CD-9735-9. Application level syntax rules: Part 9: Security key and certificate management message (message type KEYMAN).

[PKITS D3] Architecture of Time-Stamping Service and Scenarios of Use: Service and Features, Deliverable D3 of ETS Project 23.192 Public Key Infrastructure with Time-Stamping Authority, May, 1998.

[PKITS D4] Time-Stamping Service Functional Specification and Protocols for Unstructured Data, Deliverable D4 of ETS Project 23.192 Public Key Infrastructure with Time-Stamping Authority, July, 1998.

[RFC 1767] D.Crocker. “MIME Encapsulation of EDI Objects”, March 1995. Ftp:://ds.internic.net/rfc/rfc1767.txt

[RFC 1847] Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. J. Galvin, S. Murphy, S. Crocker & N. Freed. October 1995.

[RFC 2311] S/MIME Version 2 Message Specification. S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka. March 1998.

[RFC 2312] S/MIME Version 2 Certificate Handling:. S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein. March 1998.

[RFC 2313] RSA Laboratories, “PKCS #1 - RSA Encryption Standard”, version 1.5, Nov. 1993.
http://www.rsa.com/rsalabs/pubs/PKCS

[X.509 v3] ITU Recommendation X.509, “The Directory – Authentication Framework”, version 3, Geneve 1996.
http://www.itu.ch/itudoc/itu-t/rec/x/x500up.html

3 REQUIREMENTS

3.1 USERS' REQUIREMENTS

3.1.1 The requester

The requester imposes the following requirements over TSS provision that have to be met in order to satisfy his needs:

1 The requester should be able to use standard EDIFACT version 4 syntax interpreters

2 The requester should be allowed to embed the complete document to be time stamped

3 The requester wants that the application embeds and retrieves time stamp service-related information from USH (Security message header). This is an extension of EDIFACT version 4 syntax interpreters

3.1.2 The verifier

1 The verifier should be able to verify the response issued by the TSA and retrieve time stamp-related information from USH.

2 The verifier should be able to forward the complete EDI interchange received from the TSA

4 PROTOCOLS

As described in previous deliverables Deliverable D3 [PKITS D3] and Deliverable D4 [PKITS D4], the time stamp service proposed distinct between three time-stamping certificate generation schemes. These three schemes are: a basic protocol, that time-stamps documents independently, a linking protocol, that links every time-stamped document in an unforgeable chain, and a distributed protocol, that does not require a central time-stamping authority.

Four service elements (and protocols) were studied for unstructured documents:

- ❑ Time-stamping, describes the process the user shall apply to get a new time certificate from the TSA and the data structures involved in simple, linking or distributed schemes
- ❑ Renewal, that extends the validity of an existing certificate
- ❑ Verification, that can be used to check the validity of an existing time certificate and its consistency with other time certificates stored in the TSA storage subsystem.
- ❑ Synchronisation between TSAs. All TSAs involved in a public key infrastructure shall synchronise each other to increase the security of the service. This service element is an internal TSA management procedure, and not related to the kind of (un/structured) documents being processed by TSA involved.

So, for unstructured documents we consider the following service elements: Time-stamping, renewal and verification.

4.1 INTERCHANGES IN A SECURE ENVIRONMENT

As mentioned above, a mandatory requirement in the time stamping service scheme we are proposing, is to protect the data structures involved in time stamping transactions between end-users and TSA against authenticity, integrity and no repudiation of origin attacks. We propose to use digital signatures in the interchanged messages through the syntax rules extensions for the EDI batch environment OSI 9735-5 proposed by SJWG.

The following table shows the segment groups that define the security header and trailer in syntax rules version 4:

S: Status of the service string character (M: Mandatory)
R: Maximum number of occurrences of the stand-alone data element or composite-data element in the segment

```
TAG    Name                             S  R

UNH    Message Header                   M  1
-----  Segment Group 1 ---------------- C  99  --------+
USH    Security Header                  M  1          I
USA    Security Algorithm               C  3          I
-----  Segment Group 2 ---------------- C  2   ----+  I
USC    Certificate                      M  1       I  I
USA    Security Algorithm               C  3       I  I
USR    Security Result                  C  1   --------+

       Message body

-----  Segment Group n ---------------- C  99  ----+
UST    Security Trailer                 M  1       I
USR    Security Result                  C  1   ----+
UNT    Message Trailer                  M  1
```

In order to perform a digital signature over the message body, the following shadowed segments and simple data element shall be used:

Segment Group 1

USH SECURITY HEADER

POS	TAG	Name	S	R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M	1	an..3	“1”
020	0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
030	0541	SCOPE OF SECURITY APPLICATION, CODED	C	1	an..3	
040	0503	RESPONSE TYPE, CODED	C	1	an..3	DEP
050	0505	FILTER FUNCTION, CODED	C	1	an..3	“2”
060	0507	ORIGINAL CHARACTER SET ENCODING, CODED	C	1	an..3	“2”
070	0509	ROLE OF SECURITY PROVIDER, CODED	C	1	an..3	
080	S500	SECURITY IDENTIFICATION DETAILS	C	2		
	0577	Security party qualifier	M		an	“1”
	0538	Key name	C		an..35	
	0511	Security party identification	C		an..17	AD
	0513	Security party code list qualifier	C		an..3	
	0515	Security party code list responsible agency, coded	C		an..3	
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
090	0520	SECURITY SEQUENCE NUMBER	C	1	an..35	
100	S501	SECURITY DATE AND TIME	C	1		
	0517	Date and time qualifier	M		an..3	
	0338	Event date	C		n..8	
	0314	Event time	C		an..15	
	0336	Time offset	C		n4	

The Value column shows the values that are proposed for the related fields.
Value AP: Value calculated by the application
Value DEP: The related field will be present depending on the circumstances.

The profiles and proposed values are as following:

- 0501: Mandatory. Describes the security service applied. In order to provide no repudiation of origin, it shall have value "1"
- 0534: Mandatory. Reference number that links a USH segment with the related UST segment. Its value will be generated automatically by the application
- 0503: Optional. It allows requesting to the recipient of the message a no repudiation of recipient receipt.
- 0505: Optional. Identifies the filter function used for binary fields of theUSA segments and USR segments within segment group 2. An hexadecimal filter function shoud be enough, so the value should be "2"
- 0507: Optional. The original character set encoding. It should be 8 bit ASCII, so it should have value "2"
- S500.0577: Mandatory. Identification of the role of the security party. This shall have value message sender "1".
- S500.0511: Optional. Identification of a party involved in the security process, according to a defined registry of security parties

- S500.0586: Optional. Name of the security party

The following elements should not be used:

- 0541: Defines the security scope. If not present (value "1"), the default scope is the current "Security Header Group" and the message body or object itself.
- 0509: Identification of the role of the security provider in relation ti the secured item. The default value is the owner of the secured item role
- S500: Elements not included. All of them provide additional mechanisms to identify organisations and requesters of the service through codes
- 05020: Sequence number assigned to EDIFACT structure to which security is applied.
- S501: May be used as a security timestamp to provide integrity. As we detail later, these fields will be used to embed the time certified.

USA SECURITY ALGORITHM

POS	TAG	Name	S	R	Repr.	Value
010	S502	SECURITY ALGORITHM	M	1		
	0523	Use of algorithm, coded	M		an..3	“1”
	0525	Cryptographic mode of operation, coded	C		an..3	
	0533	Mode of operation code list identifier	C		an..3	
	0527	Algorithm, coded	C		an..3	“16”
	0529	Algorithm code list identifier	C		an..3	
020	S503	ALGORITHM PARAMETER	C	9		
	0531	Algorithm parameter qualifier	M		an..3	
	0554	Algorithm parameter value	M		an..512	

The profiles and proposed values are as following:

- S502.0523: Mandatory. Specification of the usage made of the algorithm. It shall have value "1" in order to indicate that the algorithm is used as a hash function by the sender of the message
- S502.0527: Optional. It is the coded identifier of the algorithm used. It should have value "16" if SHA1 algorithm is used.

Segment Group 2

The second segment group of the security headers encapsulates an EDIFACT certificate, which should be sent in the first message in an interchange to allow de recipient to access to the sender public key.

Segment Group n

UST	SECURITY TRAILER				
TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	

USR	SECURITY RESULT				
TAG	Name	S	R	Repr.	Value
S508	VALIDATION RESULT	M	2		
0563	Validation value, qualifier	M		an..3	“1”
0560	Validation value	C		an..512	AP

The profiles and proposed values are as following:

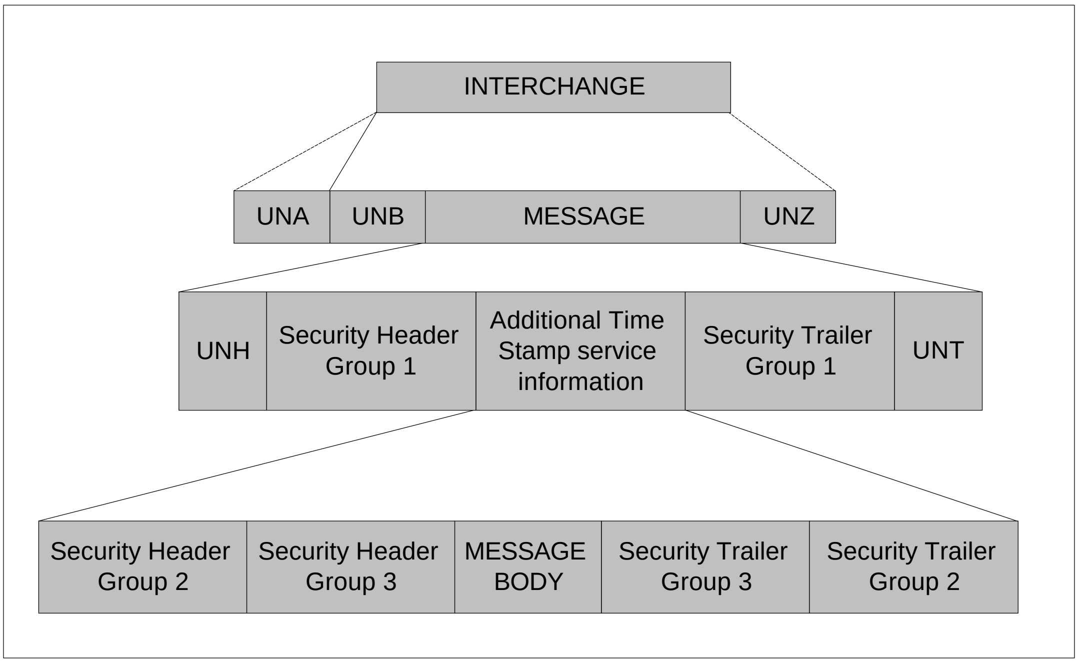
- UST.0534: Mandatory. Reference number that links a UST segment with the related USH segment. Its value will be generated automatically by the application
- UST.0588: Mandatory. The number of the security segments in a security header/trailer group pair
- USR.S508.0563: Identification of the type of validation value. It should have value RSA digital signature
- USR.S508.0560: Security result corresponding to the security function specified.

4.2 TIME STAMPING SERVICE ELEMENTS

We can consider three time stamping service elements and their related protocols in an EDI batch-processing environment: time stamping, time certificate renewal and time certificate verification.

Time stamping, renewal and verification protocols are based on the same header and trailer segment groups structure. One security header and trailer pair is used as described above to protect time-stamping transactions from security attacks and to include the stamped time. Then, one or more additional security header and trailer pairs provide additional service element information the user requested to the TSA over a single message.

The following illustration shows schematically this header and trailers basic structure:



The "Security Header Group 1" and the "Security Trailer Group 1" represents the security header and trailer pair that protect the time stamp service element from security attacks and also embeds the stamped time. "Security Header and Trailer Group 2" (mandatory) and "Security Header and Trailer Group 3" (optional) are time stamp service related information and depend on the service element and quality of service the end user requested to the TSA. They will be explained in detail in the following chapters.

4.2.1 Time-Stamping

Using this service element, a requester will get a new time certificate in a basic protocol, linking protocol or distributed protocol schemes. In all these schemes the protocol the requester and the TSA shall establish is a two-way handshake protocol: the requester is supposed to send a batch secure EDI single message within an interchange which is considered the message to timestamp. This time stamp request EDI interchange shall encapsulate the following information:

The message body the requester wants to time-stamp. It shall be a single message. Neither groups nor multiple messages are supported.

Some time stamp service-related information specifying the time stamping scheme the requester wants to be applied by the TSA (simple or linking protocol) and the security policy under the TSA issues the time certificate. This information is embedded as a security header and trailer pair.

Security related information to identify the requester and to provide protection against security attacks (digital signature). This information is embedded as a security header and trailer pair.

As a response, the TSA will issue a new EDI interchange with the following information:

The message body the requester sent to be time stamped

Some time stamp service-related information that encapsulates the resulting time stamp procedure done by the TSA. This information is embedded as one or more security header and trailer pairs.

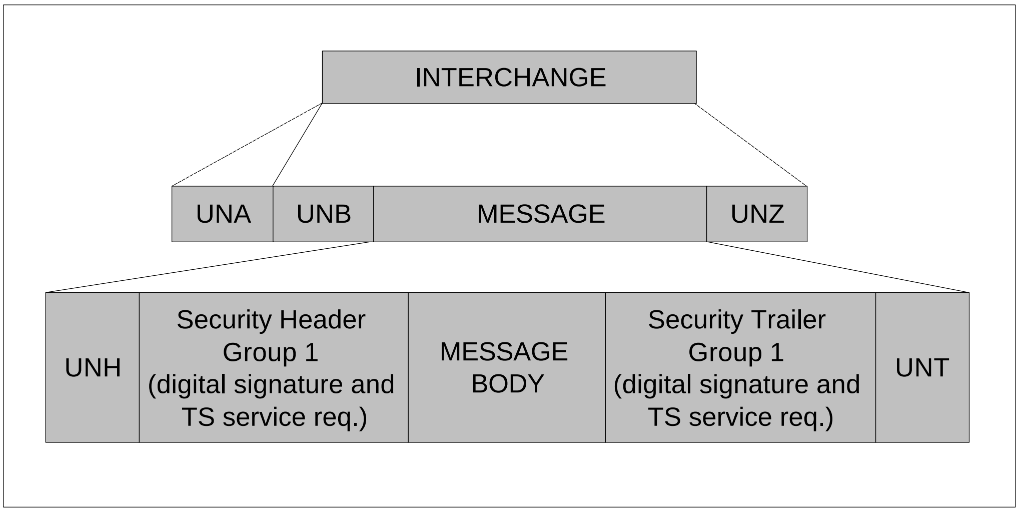
Security related information to identify the TSA and to provide protection against cryptographic attacks (digital signature). This information is embedded as a security header and trailer pair.

Distributed protocol is applicable upon both simple and linking protocol. The requester sends a time stamp request EDI interchange to n different TSA (as described in [PKITS D3]) and as a result it receives *n* time certificates (into simple or linking protocol scheme) that the requester shall encapsulate in a single EDI interchange structure. This process will be detailed later in chapter 4.2.1.4

If the TSA detects any error in the request or during the time stamping process, it shall notify to the requester in an AUTACK message. This AUTACK message is described in appendix C.

4.2.1.1 Time Stamp Request EDI Interchange

The following illustration describes schematically the segments encapsulated in a time stamp request EDI interchange when simple protocol or linking protocol scheme is requested:


INTERCHANGE
UNA
UNB
MESSAGE
UNZ
UNH
Security Header Group 1 (digital signature and TS service req.)
MESSAGE BODY
Security Trailer Group 1 (digital signature and TS service req.)
UNT

"Security Header Group 1" and "Security Trailer Group 1": A security header and trailer pair that identifies the requester of the time-stamp, protects the interchange against security attacks and embed the information to request a new time certificate to the TSA. This header and trailer pair is an extension of the header and trailer pair described above in chapter 4 that encapsulates a digital signature. In order to implement a digital signature and to provide time stamp service request related information, it shall encapsulate the following segments and data elements.

```
TAG    Name                              S   R

UNH    Message Header                    M   1
-----  Segment Group 1 ---------------   C   99  --------+
USH    Security Header                   M   1          I
USA    Security Algorithm                C   3          I
-----  Segment Group 2 ---------------   C   2   ----+   I
USC    Certificate                       M   1       I   I
USA    Security Algorithm                C   3       I   I
USR    Security Result                   C   1   --------+

       Message body

-----  Segment Group n ---------------   C   99  ----+
UST    Security Trailer                  M   1      I
USR    Security Result                   C   1   ----+
UNT    Message Trailer                   M   1
```

Segment Group 1

USH	SECURITY HEADER					
POS	TAG	Name	S	R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M	1	an..3	DEP
020	0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
030	0541	SCOPE OF SECURITY APPLICATION, CODED	C	1	an..3	
040	0503	RESPONSE TYPE, CODED	C	1	an..3	DEP
050	0505	FILTER FUNCTION, CODED	C	1	an..3	
060	0507	ORIGINAL CHARACTER SET ENCODING, CODED	C	1	an..3	“2”
070	0509	ROLE OF SECURITY PROVIDER, CODED	C	1	an..3	
080	S500	SECURITY IDENTIFICATION DETAILS	C	2		
	0577	Security party qualifier	M		an	“1”
	0538	Key name	C		an..35	
	0511	Security party identification	C		an..17	AD
	0513	Security party code list qualifier	C		an..3	
	0515	Security party code list responsible agency, coded	C		an..3	
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
090	0520	SECURITY SEQUENCE NUMBER	C	1	an..35	
100	S501	SECURITY DATE AND TIME	C	1		
	0517	Date and time qualifier	M		an..3	
	0338	Event date	C		n..8	
	0314	Event time	C		an..15	
	0336	Time offset	C		n4	

The profiles and proposed values are as following:

- 0501: Mandatory. Describes the time stamp service element request and the security policy the TSA shall apply. In this case, the service element requested is TimeStamping, so the coded related value shall be "10". Because the policy requested to the TSA shall also be indicated, an additional character is mandatory. When time stamping service element is requested, it also implies that these headers implement a digital signature.
- 0534: Mandatory. Reference number that links a USH segment with the related UST segment. Its value will be generated automatically by the application
- 0503: Optional. This field shall be used to distinct between simple and linking protocol schemes: If value "1" is indicated, the TSA shall apply the Simple protocol scheme. If value "2" is requested, the TSA shall apply Linking protocol scheme. If this data element is omitted, the TSA shall apply time stamp element service in a simple protocol scheme.
- 0507: Optional. The original character set encoding. It should be 8 bit ASCII, so it should have value "2"
- S500.0577: Mandatory. Identification of the role of the security party. This shall have value message sender "1".
- S500.0511: Optional. Identification of a party involved in the security process, according to a defined registry of security parties
- S500.0586: Optional. Name of the security party

Because the time stamp service element also implies that the request and the response shall be digitally signed, the segment USA in group 1 is mandatory. It indicates the hash function used in digital signature.

The following profile is proposed:

USA SECURITY ALGORITHM

POS	TAG	Name	S	R	Repr.	Valor
010	S502	SECURITY ALGORITHM	M	1		
	0523	Use of algorithm, coded	M		an..3	“1”
	0525	Cryptographic mode of operation, coded	C		an..3	
	0533	Mode of operation code list identifier	C		an..3	
	0527	Algorithm, coded	C		an..3	“16”
	0529	Algorithm code list identifier	C		an..3	
020	S503	ALGORITHM PARAMETER	C	9		1
	0531	Algorithm parameter qualifier	M		an..3	
	0554	Algorithm parameter value	M		an..512	

- S502.0523: Mandatory. Specification of the usage made of the algorithm. It shall have value "1" in order to indicate hash function used by the sender.
- S502.0527: Optional. Identification of the algorithm. The proposed value is "16" SHA1 algorithm.

Segment Group 2

The segment group 2 shall embed an EDIFACT certificate, because the TSA shall access to the public key in order to verify the digital signature.

Segment Group n

A group of segments containing a link with Security Header Group 1 and the result of the security functions applied to the message. In this case, it shall encapsulate the result of the digital signature process.

UST SECURITY TRAILER

TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	

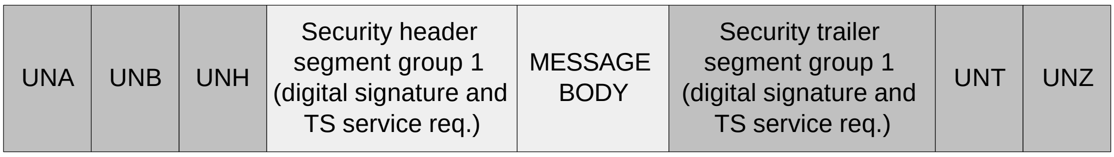
USR SECURITY RESULT

TAG	Name	S	R	Repr.	Value
S508	VALIDATION RESULT	M	2		
0563	Validation value, qualifier	M		an..3	“1”
0560	Validation value	C		an..512	AP

The profiles and proposed values are as following:

- UST.0534: Mandatory. Reference number that links a UST segment with the related USH segment. Its value will be generated automatically by the application
- UST.0588: Mandatory. The number of the security segments in a security header/trailer group pair
- USR.S508.0563: Identification of the type of validation value. It shall have value "1" RSA digital signature
- USR.S508.0560: Security result corresponding to the security function specified. It shall encapsulate the result of the digital signature process.

This digital signature will protect the following unshadowed segments as specifies the default digital signature scope:

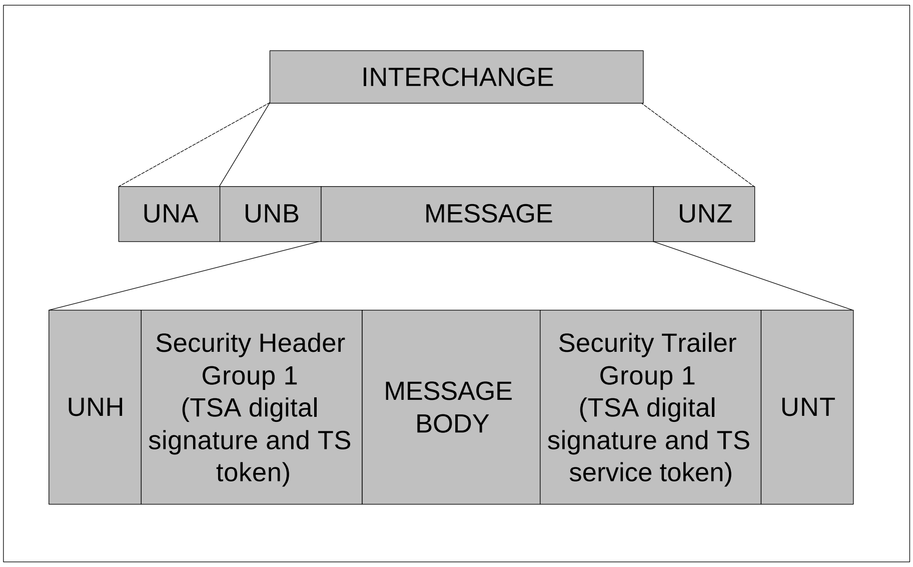


UNA	UNB	UNH	Security header segment group 1 (digital signature and TS service req.)	MESSAGE BODY	Security trailer segment group 1 (digital signature and TS service req.)	UNT	UNZ

4.2.1.2 Time Stamp Token EDI Interchange (Simple Protocol scheme)

When the user requests a time certificate in a simple protocol scheme, he will receive a single time stamp token as a response from the TSA. In case an error occurs during the time stamping process, the TSA shall indicate it to the requester and the received token shall be considered as an invalid time certificate.

The following illustration describes schematically the segments encapsulated in a time stamp token EDI interchange when the user requested simple protocol scheme:


INTERCHANGE
UNA
UNB
MESSAGE
UNZ
UNH
Security Header Group 1 (TSA digital signature and TS token)
MESSAGE BODY
Security Trailer Group 1 (TSA digital signature and TS service token)
UNT

"Security Header Group 1" and "Security Trailer Group 1": A security header and trailer pair that identifies the TSA that issues the time-stamp, protects the interchange against security attacks and also encapsulates the time stamped by the TSA. This header and trailer pair is an extension of the header and trailer pair described above in chapter 4 that encapsulates a digital signature. In order to implement a digital signature and to provide time stamp service token in Simple protocol scheme, it shall encapsulate the following segments and data elements.

```
TAG    Name                              S   R

UNH    Message Header                    M   1
-----  Segment Group 1 ---------------   C   99  --------+
USH    Security Header                   M   1           I
USA    Security Algorithm                C   3           I
-----  Segment Group 2 ---------------   C   2   ----+   I
USC    Certificate                       M   1       I   I
USA    Security Algorithm                C   3       I   I
USR    Security Result                   C   1   --------+

       Message body

-----  Segment Group n ---------------   C   99  ----+
UST    Security Trailer                  M   1       I
USR    Security Result                   C   1   ----+
UNT    Message Trailer                   M   1
```

Segment Group 1

USH SECURITY HEADER

POS	TAG	Name	S	R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M	1	an..3	DEP
020	0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
030	0541	SCOPE OF SECURITY APPLICATION, CODED	C	1	an..3	
040	0503	RESPONSE TYPE, CODED	C	1	an..3	"1"
050	0505	FILTER FUNCTION, CODED	C	1	an..3	
060	0507	ORIGINAL CHARACTER SET ENCODING, CODED	C	1	an..3	“2”
070	0509	ROLE OF THE SECURITY PROVIDEE, CODED	C	1	an..3	
080	S500	SECURITY IDENTIFICATION DETAILS	C	2		
	0577	Security party qualifier	M		an	“3”
	0538	Key name	C		an..35	
	0511	Security party identification	C		an..17	AD
	0513	Security party code list qualifier	C		an..3	
	0515	Security party code list responsible agency, coded	C		an..3	
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
090	0520	SECURITY SEQUENCE NUMBER	C	1	an..35	
100	S501	SECURITY DATE AND TIME	C	1		
	0517	Date and time qualifier	M		an..3	"1"
	0338	Event date	C		n..8	AD
	0314	Event time	C		an..15	AD
	0336	Time offset	C		n4	AD

The profiles and proposed values are as following:

- 0501: Mandatory. Describes the time stamp service element and the security policy under the TSA issues the time certificate. It shall have value "10" to indicate TimeStamping security service plus a character to indicate the policy applied by the TSA. It also indicates that a digital signature is also applied.
- 0534: Mandatory. Reference number that links a USH segment with the related UST segment. Its value will be generated automatically by the application
- 0503: Optional. This field shall be used to distinct between simple and linking protocol schemes: In this case, it shall have value Simple Protocol "1". If it is omitted, the TSA shall also applied time stamp element service in a simple protocol scheme.
- 0507: Optional. The original character set encoding. It should be 8 bit ASCII, so it should have value "2"

- S500: This composite data element shall refer to the recipient of the time certificate, this is the owner who requested the time stamp service. The TSA that issues the current time certificate shall retrieve this information from the request received from the user.
- S500.0577: Mandatory. Identification of the role of the security party. This shall have value "Certificate Owner", so it should be value "3".
- S500.0511: Optional. Identification of a party involved in the security process, according to a defined registry of security parties
- S500.0586: Optional. Name of the security party
- 0520: Sequence number assigned to EDIFACT structure to which security is applied. This sequence number is the time certificate serial number and uniquely identifies a time certificate issued by one TSA. This serial number shall be used in time stamp renovation and time stamp verification to link these service elements to an existing previous time certificate.
- S501: This composite data element encapsulates the time stamped by the TSA.S501.0517 shall have value Security Timestamp "1"

Because the time stamp service element also implies that the request and the response shall be digitally signed, the segment USA in group 1 is mandatory. It indicates the hash function used in digital signature performed by the TSA.

The following profile is proposed:

USA SECURITY ALGORITHM

POS	TAG	Name	S	R	Repr.	Valor
010	S502	SECURITY ALGORITHM	M	1		
	0523	Use of algorithm, coded	M		an..3	“1”
	0525	Cryptographic mode of operation, coded	C		an..3	
	0533	Mode of operation code list identifier	C		an..3	
	0527	Algorithm, coded	C		an..3	“16”
	0529	Algorithm code list identifier	C		an..3	
020	S503	ALGORITHM PARAMETER	C	9		1
	0531	Algorithm parameter qualifier	M		an..3	
	0554	Algorithm parameter value	M		an..512	

- S502.0523: Mandatory. Specification of the usage made of the algorithm. It shall have value "1" in order to indicate hash function used by the sender.
- S502.0527: Optional. Identification of the algorithm. The proposed value is "16" SHA1 algorithm.

Segment Group 2

The segment group 2 shall embed the TSA EDIFACT certificate, in order to identify the TSA that issued and signed the response and because the requester shall access to the public key in order to verify the digital signature.

Segment Group n

A group of segments containing a link with Security Header Group 1 and the result of the security functions applied to the message. In this case, it shall encapsulate the result of the digital signature process done by the TSA.

UST SECURITY TRAILER

TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	

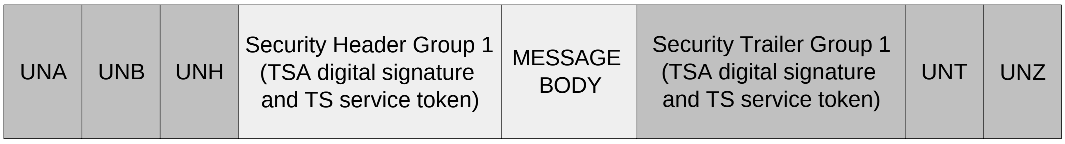
USR SECURITY RESULT

TAG	Name	S	R	Repr.	Value
S508	VALIDATION RESULT	M	2		
0563	Validation value, qualifier	M		an..3	“1”
0560	Validation value	C		an..512	AP

The profiles and proposed values are as following:

- UST.0534: Mandatory. Reference number that links a UST segment with the related USH segment. Its value will be generated automatically by the application
- UST.0588: Mandatory. The number of the security segments in a security header/trailer group pair
- USR.S508.0563: Identification of the type of validation value. It shall have value "1" RSA digital signature
- USR.S508.0560: Security result corresponding to the security function specified. It shall encapsulate the result of the digital signature process.

This digital signature will protect the following unshadowed segments as specifies the default digital signature scope:

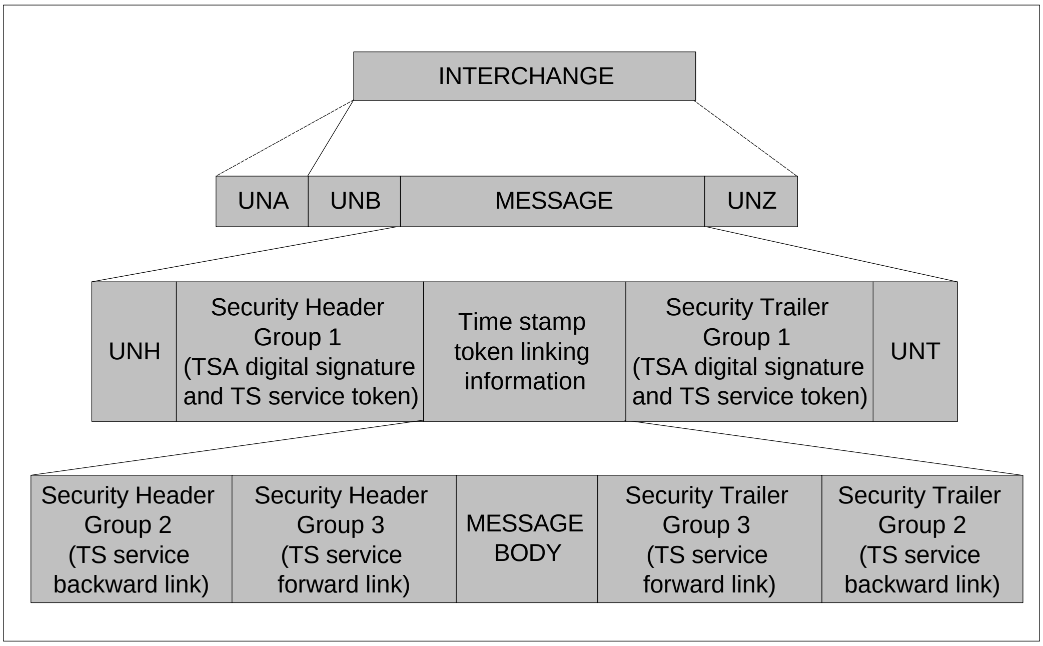

UNA
UNB
UNH
Security Header Group 1 (TSA digital signature and TS service token)
MESSAGE BODY
Security Trailer Group 1 (TSA digital signature and TS service token)
UNT
UNZ

4.2.1.3 Time Stamp Token EDI Interchange (Linking Protocol scheme)

The protocol to be used in linking protocol time-stamping service scheme is also a two-way handshake protocol. As we described in previous deliverables (PKITS D3), when the user requests the time stamping service element in linking protocol scheme, he will receive a time certificate from the TSA that is linked with the previous and the following time certificates issued (or that will be issued) by the time stamping authority. We will refer to previous time certificates as backward links, and following time certificates as forward links.

In case an error occurs during the time stamping process, the TSA shall indicate it to the requester and the received token shall be considered as an invalid time certificate.

The following illustration describes schematically the segments encapsulated in a time stamp token EDI interchange when the user requested linking protocol scheme:


INTERCHANGE
UNA
UNB
MESSAGE
UNZ
UNH
Security Header Group 1 (TSA digital signature and TS service token)
Time stamp token linking information
Security Trailer Group 1 (TSA digital signature and TS service token)
UNT
Security Header Group 2 (TS service backward link)
Security Header Group 3 (TS service forward link)
MESSAGE BODY
Security Trailer Group 3 (TS service forward link)
Security Trailer Group 2 (TS service backward link)

The main difference between time stamp token EDI interchanges in simple protocol scheme and linking protocol scheme, at segment level, is two additional security header and trailer pair that embeds the necessary information to link the time certificate in an unforgeable chain as described in deliverable [PKITS D3].

"Security Header Group 1" and "Security Trailer Group 1": As for the simple protocol scheme, it is security header and trailer pair that identifies the TSA that issues the time-stamp, protects the interchange against security attacks and embed the information to request a new time certificate to the TSA. This header and trailer pair is an extension of the header and trailer pair described above in chapter 4 that encapsulates the digital signature.

In order to implement a digital signature and to provide time stamp service token in Linking protocol scheme related information, it shall encapsulate the same information as in Simple protocol scheme in previous chapter. This is, it contains information related to the owner of the time certificate, the time stamped, the policy used by the TSA to time-stamp the interchange , the TSA EDIFACT certificate and the digital signature made by the TSA.

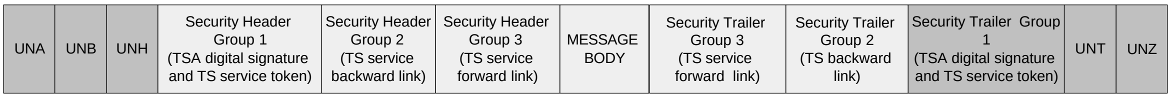
However, there is a difference in segment USH (Security Header) (segment group 1) because linking protocol scheme is used instead of simple protocol scheme.

USH SECURITY HEADER

POS	TAG	Name	S	R	Repr.	Value
.						
.						
.						
040	0503	RESPONSE TYPE, CODED	C	1	an..3	"2"
.						
.						
.						

The simple data element 0503 RESPONSE TYPE, CODED shall have value Linking protocol instead of Simple protocol "2".

This digital signature will protect the following unshadowed segments as specifies the default digital signature scope:



UNA	UNB	UNH	Security Header Group 1 (TSA digital signature and TS service token)	Security Header Group 2 (TS service backward link)	Security Header Group 3 (TS service forward link)	MESSAGE BODY	Security Trailer Group 3 (TS service forward link)	Security Trailer Group 2 (TS backward link)	Security Trailer Group 1 (TSA digital signature and TS service token)	UNT	UNZ

"Security Header Group 2" and "Security Trailer Group 2": This is a security header and trailer pair that not appears in simple protocol scheme and embeds information of the backward link of the current time certificate.

In order to indicate the owner, the stamped time, the serial number and the policy of the previous certificate issued by the TSA, it shall encapsulate the following segments and data elements:

```
TAG    Name                             S   R

UNH    Message Header                   M   1
-----  Segment Group 1 ---------------  C   99  --------+
USH    Security Header                  M   1           I
USA    Security Algorithm               C   3           I
-----  Segment Group 2 ---------------  C   2   ----+   I
USC    Certificate                      M   1       I   I
USA    Security Algorithm               C   3       I   I
USR    Security Result                  C   1   --------+

       Message body

-----  Segment Group n ---------------  C   99  ----+
UST    Security Trailer                 M   1       I
USR    Security Result                  C   1   ----+
UNT    Message Trailer                  M   1
```

Segment Group 1

It shall encapsulate information about the time certificate the TSA issued before the current one. Because of this, this segment group 1 in "Security Header Group 2 (TS Service Backward Link)" of the current time certificate shall be a copy of the segment group 1 related to the "Security Header Group1 (TSA digital signature and TS service token)" of the previous time certificate issued by the TSA.

Retrieving this segment group 1 of the "Security Header Group 2 " from the time certificate received, the user who requested the token will get the following information about the previous time certificate issued by the TSA:

- The requester of the previous time certificate. This information is encapsulated in the composite data element S500
- The protocol and the policy requested to the TSA by the owner of the previous certificate. This information is encapsulated in 0501 and 0503.
- The time certificate serial number of the previous time certificate. This information is encapsulated in the simple data element 0520

- The time the TSA stamped in the previous time certificate. This information is embedded in the composite data element S501

Segment group 2

As it was in the segment group 2 related to the "Security Header Group 1 (TSA digital signature and TS service token)" of the previous time certificate issued by the TSA, it shall encapsulate the TSA EDIFACT certificate the TSA used to sign the previous token.

Segment Group n

This segment group n in "Security Trailer Group 2 (TS backward linking) shall be a copy of the segment group n in the "Security Trailer Group 1 (TSA digital signature and TS service token) of the previous time certificate issued by the TSA as an additional linking information.

"Security Header Group 3" and "Security Trailer Group 3": This is a security header and trailer pair that not appears in simple protocol scheme and embeds information of the forward link of the current time certificate.

The forward link shall indicate the time certificate serial number of the time certificate the TSA will issue after the current one. Because of this, the following segments and data elements are proposed:

```
TAG    Name                              S   R

UNH    Message Header                    M   1
-----  Segment Group 1 ----------------  C   99  --------+
USH    Security Header                   M   1           I
USA    Security Algorithm                C   3           I
-----  Segment Group 2 ----------------  C   2   ----+   I
USC    Certificate                       M   1       I   I
USA    Security Algorithm                C   3       I   I
USR    Security Result                   C   1   --------+

       Message body

-----  Segment Group n ----------------  C   99  ----+
UST    Security Trailer                  M   1       I
USR    Security Result                   C   1   ----+
UNT    Message Trailer                   M   1
```

Segment Group 1

It shall encapsulate the serial number of the time certificate the TSA will issue after the current one.

USH SECURITY HEADER

POS	TAG	Name	S	R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M	1	an..3	DEP
020	0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
030	0541	SCOPE OF SECURITY APPLICATION, CODED	C	1	an..3	
040	0503	RESPONSE TYPE, CODED	C	1	an..3	
050	0505	FILTER FUNCTION, CODED	C	1	an..3	
060	0507	ORIGINAL CHARACTER SET ENCODING, CODED	C	1	an..3	“2”
070	0509	ROLE OF SECURITY PROVIDER, CODED	C	1	an..3	
080	S500	SECURITY IDENTIFICATION DETAILS	C	2		

	0577	Security party qualifier	M		an	
	0538	Key name	C		an..35	
	0511	Security party identification	C		an..17	
	0513	Security party code list qualifier	C		an..3	
	0515	Security party code list responsible agency, coded	C		an..3	
	0586	Security party name	C		an..35	
	0586	Security party name	C		an..35	
	0586	Security party name	C		an..35	
090	0520	SECURITY SEQUENCE NUMBER	C	1	an..35	DEP
100	S501	SECURITY DATE AND TIME	C	1		
	0517	Date and time qualifier	M		an..3	
	0338	Event date	C		n..8	
	0314	Event time	C		an..15	
	0336	Time offset	C		n4	

The profiles and proposed values are as following:

- 0501: Mandatory. Describes the time stamp service element requested and the security policy the TSA shall apply. In this case, the service element requested is TimeStamping, so the coded related value shall be "10".
- 0534: Mandatory. Reference number that links a USH segment with the related UST segment. Its value will be generated automatically by the application
- 0507: Optional. The original character set encoding. It should be 8 bit ASCII, so it should have value "2"
- 0520: It shall be mandatory. It encapsulates the certificate serial number of the following time certificate issued by the TSA.

USA SECURITY ALGORITHM

The USA segment shall be omitted because there is no security operation related to this "Security Header and Trailer Group 3"

Segment group 2

The segment group 2 shall be also omitted because there is no need to encapsulate an additional EDIFACT certificate. There is no security operation related to this "Security Header and Trailer Group 3"

Segment Group n

Because there is no security operation in "Security Header and Trailer Group 3", USR shall be omitted.

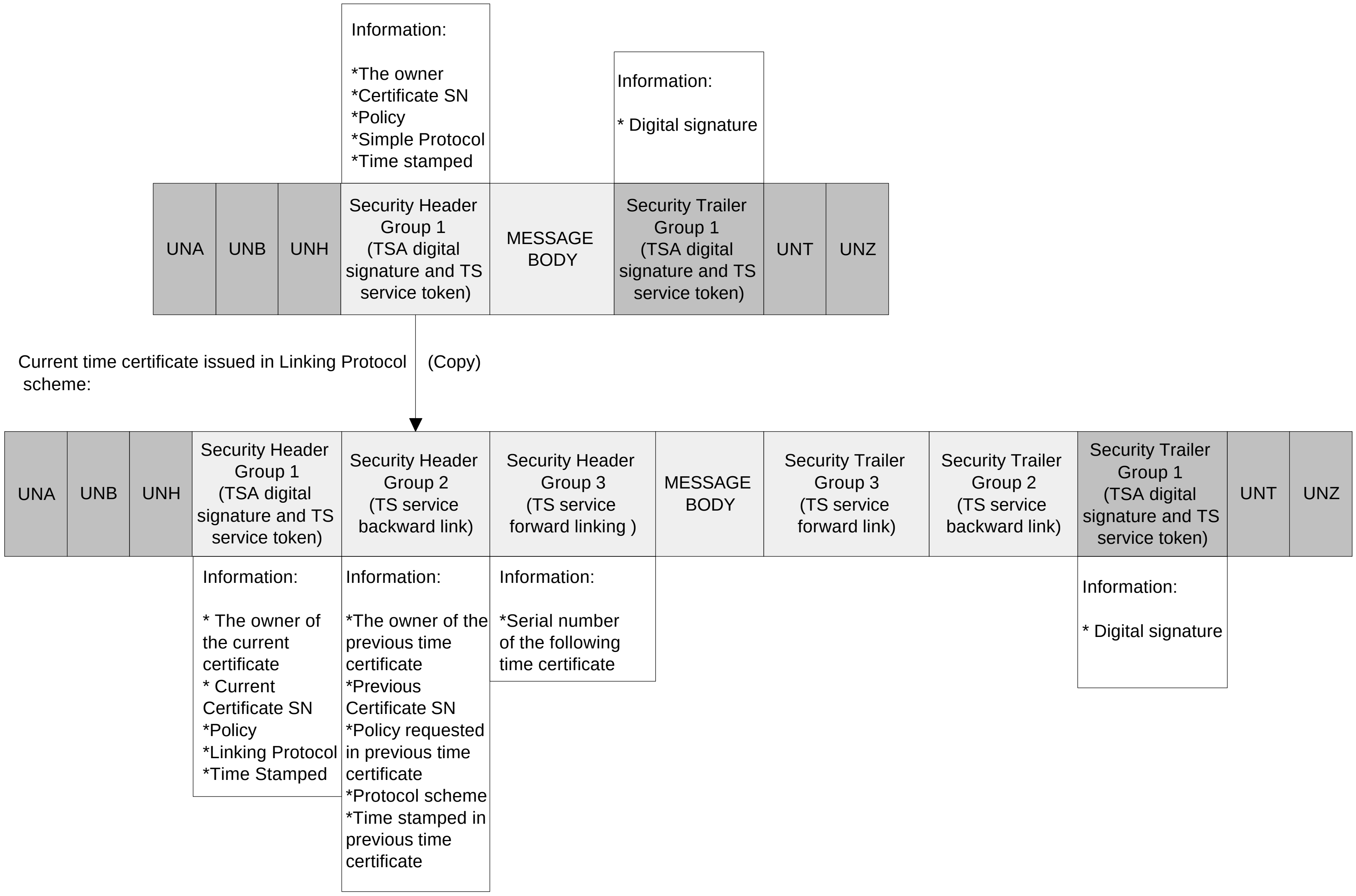
UST SECURITY TRAILER

TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	

- UST.0534: Mandatory. Reference number that links a UST segment with the related USH segment. Its value will be generated automatically by the application
- UST.0588: Mandatory. The number of the security segments in a security header/trailer group pair

The following illustration is a schematic example of the linking information a time certificate shall encapsulate in case a previous simple protocol scheme time certificate was issued:

Previous time certificate issued in Simple Protocol scheme:


Information:
*The owner
*Certificate SN
*Policy
*Simple Protocol
*Time stamped
Information:
* Digital signature
UNA
UNB
UNH
Security Header Group 1 (TSA digital signature and TS service token)
MESSAGE BODY
Security Trailer Group 1 (TSA digital signature and TS service token)
UNT
UNZ
Current time certificate issued in Linking Protocol scheme:
(Copy)
UNA
UNB
UNH
Security Header Group 1 (TSA digital signature and TS service token)
Security Header Group 2 (TS service backward link)
Security Header Group 3 (TS service forward linking)
MESSAGE BODY
Security Trailer Group 3 (TS service forward link)
Security Trailer Group 2 (TS service backward link)
Security Trailer Group 1 (TSA digital signature and TS service token)
UNT
UNZ
Information:
* The owner of the current certificate
* Current Certificate SN
*Policy
*Linking Protocol
*Time Stamped
Information:
*The owner of the previous time certificate
*Previous Certificate SN
*Policy requested in previous time certificate
*Protocol scheme
*Time stamped in previous time certificate
Information:
*Serial number of the following time certificate
Information:
* Digital signature

4.2.1.4 Time Stamp Token EDI Interchange (Distributed Protocol scheme)

The distributed protocol scheme shall be considered as a higher-level protocol than simple and linking protocol schemes.

Distributed time stamping makes sense when there is no clear central authority to provide the service. When a user wants to time stamp a document with the distributed protocol scheme he shall issue a time stamp request EDI interchange to the *n* TSAs selected as described in [PKITS D3]. As a result, the requester will receive *n* time stamp token EDI interchanges in simple or linking protocol schemes (depending on the user's request) form the TSAs and he shall encapsulate as a single time certificate.

Because the requester-TSA interaction is independent from the interactions the requester do with the others *n-1* TSAs, the *n* time stamp request EDI interchanges submitted to the *n* TSAs can be different on the protocol scheme requested. In this case, the user will receive some time stamp token EDI interchange in Simple Protocol scheme and some others in Linking Protocol scheme. The same time stamp request and tokens EDI interchanges defined in previous chapters 4.2.1.1, 4.2.1.2 and 4.2.1.3 shall be used in user-TSA interactions in Distributed Protocol scheme.

Upon receiving the *n* time stamp token EDI interchanges, the requester shall embed them into a time stamp distributed token EDI interchange that shall be considered as the time certificate. This new EDI interchange shall embed the original message body encapsulated in the time stamp request EDI interchange the requester submitted to the TSA, and the security header and trailer groups from all the time stamp token EDI interchange the *n* TSA sent to the requester.

The following illustration is a schematic example of a resulting time stamp distributed token EDI interchange when two TSAs are involved, one in Simple Protocol scheme and the other in Linking Protocol scheme:

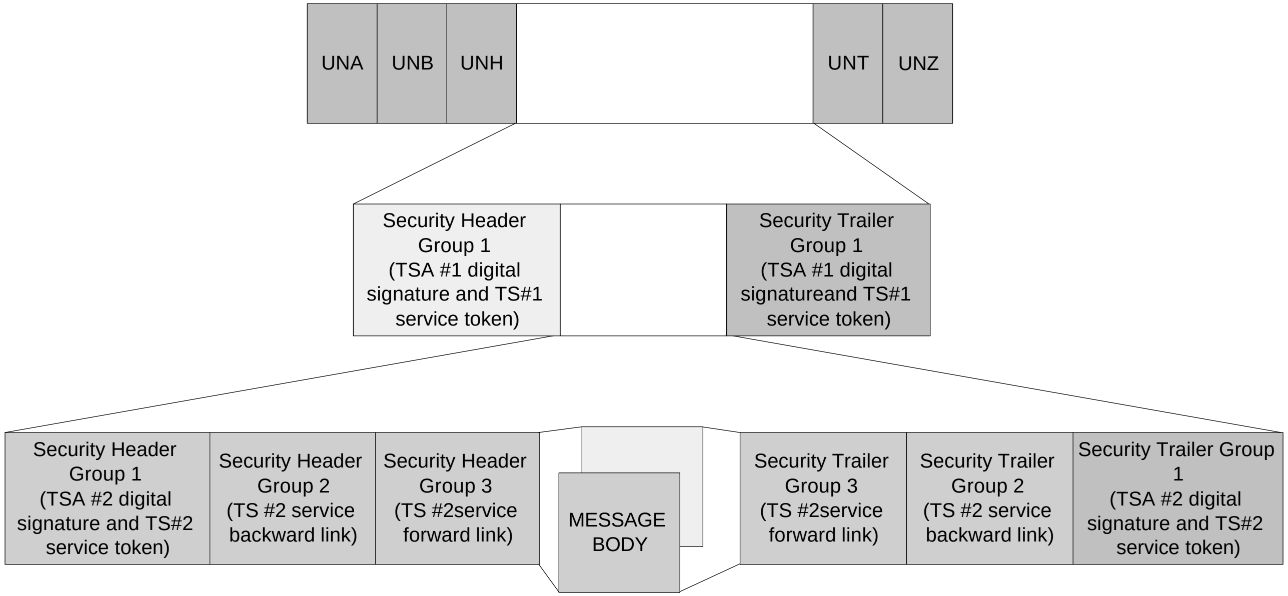
Time stamp token EDI interchange issued by TSA #1 in Simple Protocol scheme:

UNA	UNB	UNH	Security Header Group 1 (TSA #1 digital signature and TS#1 service token)	MESSAGE BODY	Security Trailer Group 1 (TSA #1 digital signature and TS#1 service token)	UNT	UNZ

Time stamp token EDI interchange issued by TSA #2 in Linking Protocol scheme:

UNA	UNB	UNH	Security Header Group 1 (TSA #2 digital signature and TS service token)	Security Header Group 2 (TS #2 service backward link)	Security Header Group 3 (TS #2service forward link)	MESSAGE BODY	Security Trailer Group 3 (TS #2service forward link)	SecurityTrailer Group 2 (TS #2 service backward link)	Security Trailer Group 1 (TSA #2 digital signature and TS service token)	UNT	UNZ

Resulting time stamp token EDI interchange assembled by the requester in Distributed Protocol scheme:


UNA
UNB
UNH
UNT
UNZ
Security Header Group 1 (TSA #1 digital signature and TS#1 service token)
Security Trailer Group 1 (TSA #1 digital signatureand TS#1 service token)
Security Header Group 1 (TSA #2 digital signature and TS#2 service token)
Security Header Group 2 (TS #2 service backward link)
Security Header Group 3 (TS #2service forward link)
MESSAGE BODY
Security Trailer Group 3 (TS #2service forward link)
Security Trailer Group 2 (TS #2 service backward link)
Security Trailer Group 1 (TSA #2 digital signature and TS#2 service token)

Only a single message body occurence. It is protected by both digital signatures (TSA#1 and TSA#2)

In order to store safety the resulting time certificate, the user should digitally sign the resulting token by embedding an additional header and trailer pair after the UNH header and before UNT trailer.

Because TSA's signatures were calculated over "Security Header Groups 1, 2 and 3 (2 and 3 only if Linking Protocol scheme was requested), message body and "Security Trailer Groups" 2 and 3 (only if Linking Protocol scheme was requested), the user's application will also be able to check these digital signatures in the future reassembling the original interchanges.

4.2.2 Renewal

Time stamps may be valid for a limited period of time, that may be explicit in the policy statement, or in the certificates that supports the signing key of the TSA, or implicit if cryptography advances introduce reasonable doubts about the soundness of the elements (either the signing protocol, or the keys, or …). For one or other reason, a time-stamp certificate may become void, and need to go under a renewal process to extend the non-repudiation period.

We describe how simple, linking and distributed time certificates can be renewed and the protocols to be used for this purpose. During the renewal process the TSA shall validate that the time certificate to be renewed is a valid one, and it shall indicate in the response any error occurred during the renewal in an AUTACK message to the requester. This AUTACK message is described in appendix C.

4.2.2.1 Simple Protocol scheme Time Stamp Token renewal

When a user request a time certificate using the Simple Protocol scheme he gets a time stamp token EDI interchange as described in chapter 4.2.1.2

Time-stamp certificate renewal shall be performed as a normal new time stamping process by submitting to the TSA the complete time certificate to be renewed. This shall be embedded in a new time stamp request EDI interchange. However, it is necessary to specify that the renewal process is requested, as we detail later in this chapter.

Because the renewal process is a normal document time stamp process as described in [PKITS D3], the same protocols described for Simple, Linking and Distributed time stamping protocols scheme can be used to renewal a time stamp token that was obtained through a simple time stamp protocol scheme. This is, a Simple protocol scheme time certificate can be renewed throw the Simple, Linking or Distributed protocol scheme, and the receipt issued by the TSA(s) will be a new time stamp token EDI interchange (if simple or linking protocol is requested) or a new time stamp distributed token EDI interchange (if distributed protocol is requested). This new time certificate shall encapsulate the original message body and the certificate serial number of the renewed time certificate.

In case distributed protocol scheme is requested, the user shall encapsulated the *n*-time stamp token EDI interchange received from TSAs as a single time certificate EDI interchange as described in the distributed protocol scheme chapter 4.2.1.4

4.2.2.2 Linking Protocol scheme Time Stamp Token renewal

The same process as in Simple protocol scheme time stamp token renewal shall be applied. When a user requests a time certificate using the Linking Protocol scheme, he gets a time stamp EDI interchange from the TSA that encapsulates the same time stamp service-related information plus additional linking information.

The same information as in Simple Protocol scheme time stamp token renewal shall be submitted to the TSA in a Linking Protocol scheme time stamp token renewal, this is, the complete time certificate embedded in a new time stamp request EDI interchange. The renewal process can be also requested either in Simple, Linking or Distributed protocol schemes

As a result, and depending on the time stamp protocol scheme requested, the response issued by the TSA(s) will be a new time stamp token EDI interchange (if simple or linking protocol is requested) or a new time stamp distributed token EDI interchange (if distributed protocol is requested in this renewal process). This new time certificate shall also encapsulate the original message body and the certificate serial number of the renewed time certificate.

Again, in case Distributed Protocol scheme is requested, the user shall encapsulated the *n*-time stamp token EDI interchange received from TSAs as a single time certificate as described in the distributed protocol chapter 4.2.1.4

4.2.2.3 Distributed Protocol TimeStampToken renewal

When a user requests a time certificate using the Distributed protocol scheme, he shall to encapsulate the *n*-time stamp token EDI interchange received from TSAs as a single time certificate as described above in order to obtain a time stamp distributed token EDI interchange.

This time stamp distributed token EDI interchange shall be considered as the time certificate, and the same processes described for Simple and Linking protocol schemes time stamp token renewal shall be applied in order to extend its validity. This is, the user shall submit the complete "distributed" time certificate to the TSAs requesting Simple, Linking or Distributed protocol schemes in a new time stamp request EDI interchange.

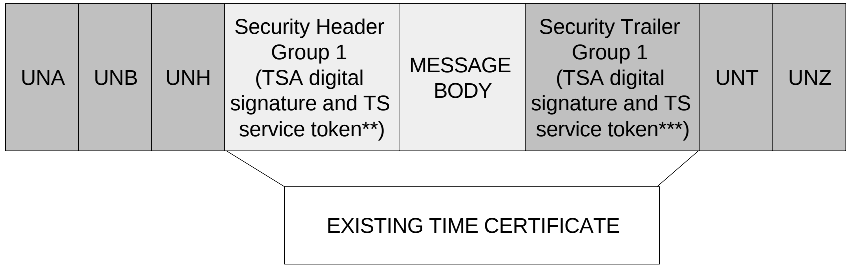
Again, the requester will receive from TSA(s) a new time stamp token EDI interchange(s) or a new time stamp distributed token EDI interchange, depending on the time stamp protocol scheme requested to the TSA(s). Again, the time certificate shall encapsulate the original message body of the "distributed" tine certificate that is being renewed.

In case Distributed Protocol scheme is requested, the user shall encapsulated the *n*-time stamp token EDI interchange received from TSAs as a single time certificate as described in the distributed protocol chapter 4.2.1.4

4.2.2.4 Time certificate renewal EDI interchange example

The following illustration is a schematic example of the renewal process when a user request to renew an existing Simple protocol scheme time certificate with Linking protocol scheme:

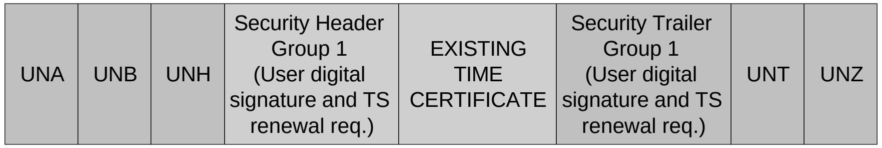
Existing Simple Protocol scheme time stamp token EDI interchange to be renewed. We will refer to it as EXISTING TIME CERTIFICATE



UNA	UNB	UNH	Security Header Group 1 (TSA digital signature and TS service token**)	MESSAGE BODY	Security Trailer Group 1 (TSA digital signature and TS service token***)	UNT	UNZ

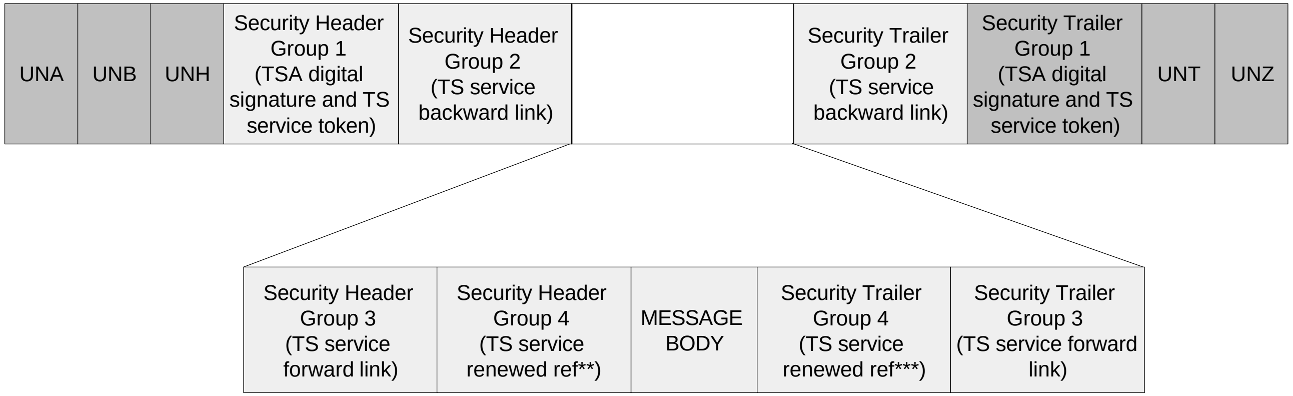
EXISTING TIME CERTIFICATE

The requester shall issue the following time stamp request EDI interchange in order to renewal the existing time certificate:



UNA	UNB	UNH	Security Header Group 1 (User digital signature and TS renewal req.)	EXISTING TIME CERTIFICATE	Security Trailer Group 1 (User digital signature and TS renewal req.)	UNT	UNZ

The TSA will send as a renewal service response the following new Linking Protocol scheme time stamp token EDI interchange :



UNA	UNB	UNH	Security Header Group 1 (TSA digital signature and TS service token)	Security Header Group 2 (TS service backward link)		Security Trailer Group 2 (TS service backward link)	Security Trailer Group 1 (TSA digital signature and TS service token)	UNT	UNZ

Security Header Group 3 (TS service forward link)	Security Header Group 4 (TS service renewed ref**)	MESSAGE BODY	Security Trailer Group 4 (TS service renewed ref***)	Security Trailer Group 3 (TS service forward link)

** Copy of the Security Header Group 1 of the renewed time certificate
*** Copy of the Security Trailer Group 1 of the renewed time certificate

As we have mentioned above, it is necessary that the user indicate in the time stamp renewal request that the TSA has to apply the renewal element service to the EDI interchange he received. This will allow the TSA to extract the message body from the request and embed it into the response. In order to indicate this renewal service element, the user shall use two simple data elements in the USH of the "Security Header Group 1" of the request EDI interchange (which also specifies the time stamp protocol scheme, the policy and the requester of the service element, as we specified in this proposal)

This additional simple data element and the modified USH of the renewal request EDI interchange are:

USH SECURITY HEADER

POS	TAG	Name	S	R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M	1	an..3	DEP
.						
.						
.						
090	0520	SECURITY SEQUENCE NUMBER	C	1	an..35	"DEP"
.						
.						
.						

- 0501: Mandatory. Describes the time stamp service element requested and the security policy the TSA shall apply. In this case, the service element requested is Time Stamping Renewal. This value is not supported in syntax rules version 4, so we propose an additional value "13" Time Stamping Renewal". Moreover, an additional character is mandatory in order to indicate the policy the TSA shall apply. The same value shall be present on the 0501 data element in the time stamp service-related security header of the resulting response issued by the TSA. When Time Stamping Renewal is specified, this header also implements a digital signature
- The simple data element 0520 SECURITY SEQUENCE NUMBER shall be used by the requester to indicate the serial number of the time certificate embedded in the EDI interchange message body when Simple or Linking protocol schemes are used. However, when Distributed protocol scheme is requested, it shall be omitted. (Note: this simple data element field is also used in all the time stamp token EDI interchange the TSA issues in order to indicate the certificate serial number of the time certificate issued).

Others simple and composite data elements shall have the values as described in previous chapters in Simple, Linking and distributed protocols scheme time stamping element service requests.

The time certificate the TSA issued as a renewal is a time certificate in Simple or Linking protocol scheme as defined in previous chapters, but also has additional Security Header and Trailer Groups, in order to encapsulate information about the time certificate that is renewed by the current one. Because of this, two cases have to be considered:

1. If the user wants to renew a non-distributed token, this new Security Header and Trailer Groups are a copy of the Security Header Group 1 and Security Trailer Group 1 of the renewed time certificate.

2. If the user is renewing a distributed token, there shall be as additional Security Header and Trailer Groups as time certificates encapsulated in the distributed one, and everyone of them shall be a copy of the Security Header Group 1 and Security Trailer Group 1 of one time certificate encapsulated in the distributed token.

This(ese) additional(s) Security Groups can appears as Security Header and Trailer Group 2 or 4 (and following in distributed token renewal) in the EDI interchange response issued by the TSA depending on if Simple or Linking renewal scheme is requested by the user.

As shown in the last example, the message body of the renewal request shall encapsulate the message body of the original time certificate and the time stamp service-related segments if Simple or Linking protocol scheme existing time certificate is being renewed. Moreover, if a Distributed protocol scheme time certificate is being renewed, the renewal request shall encapsulate the original message body, and all the time stamp service-related segments that are encapsulated by the original "distributed" time certificate. The TSA shall retrieve this information from the request in order to embed the additional "Security Groups" in the EDI interchange it issues as a new time certificate

The presence of these security-related and time stamp service-related segments into the renewal request is also because the TSA shall check the validity of the time certificates sent by the user before the TSA applies the renewal procedure on them.

4.2.3 Verification

Verification phase covers the activities related to the assurance that the time certificate is valid. It may be requested by the owner of the certificate to assure himself of the correctness of its object. It may be requested by another party that is concerned, either to prove it is a correct certificate, or looking after proving it is not a valid one. Verification may lastly be carried out by a third party on behalf of the disputing parties.

Verification is not a simple task, not even an easy to formalise one. It may be as simple as verifying the signature of the TSA (contents, dates, rights to sign, liabilities, etc.) or may go through the chain of links (in the linked protocol) or explore the collection of singular certificates (in the distributed protocol), or a mixture of each the previous ones.

Verification may include the analysis of synchronisation stages between different TSA to prevent some operation risks and collusion attacks (see [PKITS D3] for further details).

When the linking protocol is used, the verifier traverses the chain of links, performing singular verification checks on every link, or on a selected subset of links. A verifier may prefer to check thoroughly the immediate previous and posteriors time-certificates, or may prefer a random selection, either close or remote. The only objective is to assure that the chain of links is genuine, and that the TSA behaves correctly.

Lastly, verification may imply auditing the TSA operation: installation, procedures, stored data, and so on, as well as extend the analysis to those TSA used for mutual synchronisation.

In this complicated scenario, three coarse procedures may be foreseen:

1. verify the correctness of a single certificate
2. ask the TSA, that is trusted, to emit a verdict according to some procedure previously agreed and published
3. retrieve evidence (collections of certificates direct or indirectly related) to carry out a specific verification analysis

First procedure is a traditional service provided by a notary authority that checks the formal correctness of the signed data, and certifies that the identity certificates are valid, and each entity is duly entitled for its work.

The second procedure asks the TSA to play a role closed to that of a notary, being specialised on time-stamping. The benefit for users is that standardised procedures help to resolve disputes, and the TSA has the needed machinery to perform a verification in house, and to contact synchronising TSA for needed evidence.

The third procedure may be expected from a notary authority applying its own criteria to issue a verdict based on enough evidence. Involved parties are requested to provide needed evidence (that is, stored time-certificates).

Two protocols are identified to support these foreseen scenarios:
TSA Verification protocol: It is a two-way handshake protocol between a user and a TSA where the user asks the TSA to issue a verdict for a time-certificate, according to some procedure stated in its TSPS. The TSA responds with a verdict.

TSA Retrieval protocol: It is a retrieval protocol between a user and a TSA where the user requests one or more certificates. Certificates are identified by their unique serial number. If the TSA is using a linking protocol, a collection of certificates (e.g. N before, N after) may be requested simultaneously. The TSA response is the requested collection of time-certificates, if available, or a reason to explain why a certificate cannot be retrieved.

As time stamping and renewal element services, the verification and retrieval protocols shall be protected against authenticity, integrity and no repudiation of origin attacks. Because of this, the same security header and trailer pair solution shall be applied.

4.2.3.1 Time Stamp Verification Protocol

When verifying an existing Simple or Linking protocol scheme time certificate, the requester shall submit to the TSA an EDI interchange with the following information:

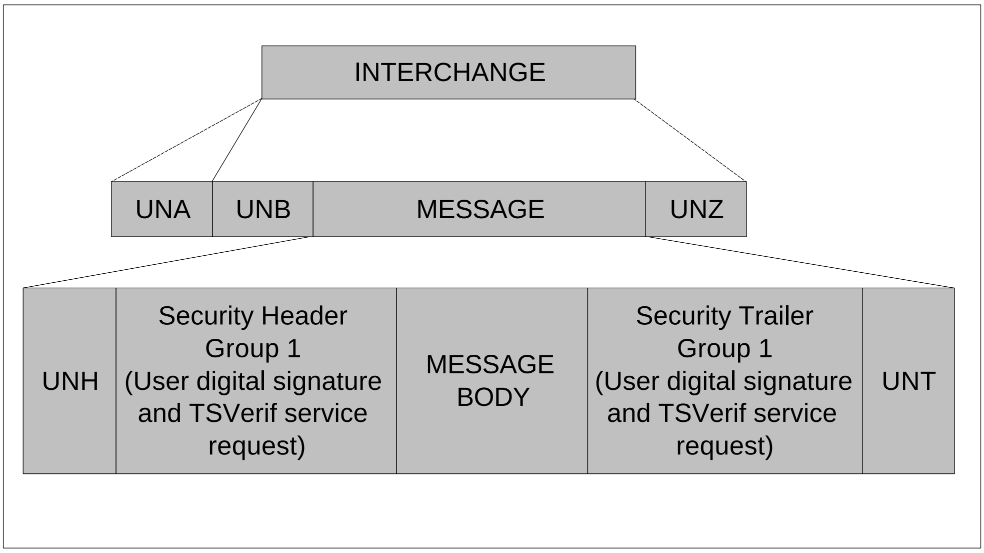
- ❑ Time certificate verification is requested
- ❑ The policy under the TSA shall verify the existing certificate
- ❑ The complete time certificate to be verified. It shall be embedded in the message body of the new EDI interchange
- ❑ The serial number of the time certificate to be verified. It shall be indicated in the USH related to time stamp service as it was in a time certificate renewal request.
- ❑ The identity of the requester of the verification service element

As a response, the requester will receive an AUTACK message that indicates the verification status with the submitted time certificate.

In case the user wants to verify a "distributed" time stamp token, he shall extract the *n* time certificates encapsulated in the "distributed" token and then request *n* individual time certificate verification to the related TSAs.

4.2.3.1.1 Time Stamp Verification request EDI interchange

The following illustration describes schematically the segments encapsulated in a time stamp verification request EDI interchange:


INTERCHANGE
UNA
UNB
MESSAGE
UNZ
UNH
Security Header Group 1 (User digital signature and TSVerif service request)
MESSAGE BODY
Security Trailer Group 1 (User digital signature and TSVerif service request)
UNT

"Security Header Group 1" and "Security Trailer Group 1": A security header and trailer pair that identifies the requester of the time-stamp, protects the interchange against security attacks and embed the information to request a new time certificate to the TSA. This header and trailer is an extension of the header and trailer pair described above in chapter 4 that encapsulates a digital signature. In order to implement a digital signature and to provide time verification request related information, it shall encapsulate the following segments and data elements:

```
TAG    Name                              S   R

UNH    Message Header                    M   1
-----  Segment Group 1 ---------------   C   99  --------+
USH    Security Header                   M   1           I
USA    Security Algorithm                C   3           I
-----  Segment Group 2 ---------------   C   2   ----+   I
USC    Certificate                       M   1       I   I
USA    Security Algorithm                C   3       I   I
USR    Security Result                   C   1   --------+

       Message body

-----  Segment Group n ---------------   C   99  ----+
UST    Security Trailer                  M   1       I
USR    Security Result                   C   1   ----+
UNT    Message Trailer                   M   1
```

Segment Group 1

USH   SECURITY HEADER

POS	TAG	Name	S	R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M	1	an..3	DEP
020	0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
030	0541	SCOPE OF SECURITY APPLICATION, CODED	C	1	an..3	
040	0503	RESPONSE TYPE, CODED	C	1	an..3	DEP
050	0505	FILTER FUNCTION, CODED	C	1	an..3	
060	0507	ORIGINAL CHARACTER SET ENCODING, CODED	C	1	an..3	“2”
070	0509	ROLE OF SECURITY PROVIDER, CODED	C	1	an..3	
080	S500	SECURITY IDENTIFICATION DETAILS	C	2		
	0577	Security party qualifier	M		an	“1”
	0538	Key name	C		an..35	
	0511	Security party identification	C		an..17	AD
	0513	Security party code list qualifier	C		an..3	
	0515	Security party code list responsible agency, coded	C		an..3	
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
	0586	Security party name	C		an..35	AD
090	0520	SECURITY SEQUENCE NUMBER	C	1	an..35	
100	S501	SECURITY DATE AND TIME	C	1		
	0517	Date and time qualifier	M		an..3	
	0338	Event date	C		n..8	
	0314	Event time	C		an..15	
	0336	Time offset	C		n4	

The profiles and proposed values are as following:

- 0501: Mandatory. Describes the time stamp service element requested and the security policy (which should identify the verification method) the TSA shall apply. In this case, the service element requested is TimeStampingVerification. Because this value is not supported by 0501 available data values, we propose value "14" "Time Stamping Verification". When time stamping verification service element is requested, it also implies that these headers implement a digital signature.
- 0534: Mandatory. Reference number that links a USH segment with the related UST segment. Its value will be generated automatically by the application
- 0507: Optional. The original character set encoding. It should be 8 bit ASCII, so it should have value "2"
- S500.0577: Mandatory. Identification of the role of the security party. This shall have value message sender "1".
- S500.0511: Optional. Identification of a party involved in the security process, according to a defined registry of security parties
- S500.0586: Optional. Name of the security party
- 0520: It shall indicate, as in time stamping renewal request EDI interchange, the serial number of the time certificate that is embedded in the message body in the current EDI interchange, which is the time certificate to be verified.

Because the time stamp service element also implies that the request and the response shall be digitally signed, the segment USA in group 1 is mandatory. It indicates the hash function used in digital signature.

The following profile is proposed:

USA SECURITY ALGORITHM

POS	TAG	Name	S	R	Repr.	Valor
010	S502	SECURITY ALGORITHM	M	1		
	0523	Use of algorithm, coded	M		an..3	“1”
	0525	Cryptographic mode of operation, coded	C		an..3	
	0533	Mode of operation code list identifier	C		an..3	
	0527	Algorithm, coded	C		an..3	“16”
	0529	Algorithm code list identifier	C		an..3	
020	S503	ALGORITHM PARAMETER	C	9		1
	0531	Algorithm parameter qualifier	M		an..3	
	0554	Algorithm parameter value	M		an..512	

- S502.0523: Mandatory. Specification of the usage made of the algorithm. It shall have value "1" in order to indicate hash function used by the sender.
- S502.0527: Optional. Identification of the algorithm. The proposed value is "16" SHA1 algorithm.

Segment Group 2

The segment group 2 shall embed an EDIFACT certificate, because the TSA shall access to the public key in order to verify the digital signature.

Segment Group n

A group of segments containing a link with Security Header Group 1 and the result of the security functions applied to the message. In this case, it shall encapsulate the result of the digital signature process.

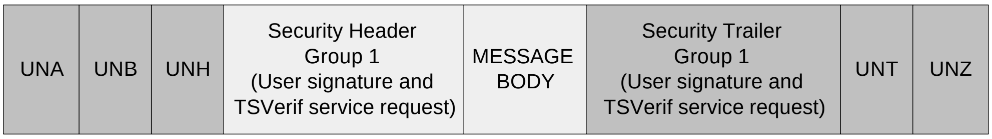
UST	SECURITY TRAILER				
TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	

USR	SECURITY RESULT				
TAG	Name	S	R	Repr.	Value
S508	VALIDATION RESULT	M	2		
0563	Validation value, qualifier	M		an..3	“1”
0560	Validation value	C		an..512	AP

The profiles and proposed values are as following:

- UST.0534: Mandatory. Reference number that links a UST segment with the related USH segment. Its value will be generated automatically by the application
- UST.0588: Mandatory. The number of the security segments in a security header/trailer group pair
- USR.S508.0563: Identification of the type of validation value. It shall have value "1" RSA digital signature
- USR.S508.0560: Security result corresponding to the security function specified. It shall encapsulate the result of the digital signature process.

This digital signature will protect the following unshadowed segments as specifies the default digital signature scope:



UNA	UNB	UNH	Security Header Group 1 (User signature and TSVerif service request)	MESSAGE BODY	Security Trailer Group 1 (User signature and TSVerif service request)	UNT	UNZ

4.2.3.1.2 Time Stamp Verification token EDI interchange

As a response of the time stamp verification request EDI interchange, the TSA shall issue an AUTACK message in order to indicate the result of the verification process. See appendix C.

Depending on the verification procedure the TSA will apply (indicated in the request in the 0501 USH data element of "Security Header Group 1") over the time certificate specified in the same segment, additional information shall be included in the request. Because of this, the message body of the verification request and the resulting verification token shall embed the same information as in renewal request and token. This is, the message body shall include the time stamp service-related segments and the message body of the original time certificate that is being verified.

4.2.3.2 Time Stamp Retrieval Protocol

In order to retrieve time certificates from the TSA the user shall submit a KEYMAN message that shall encapsulate the serial numbers of the certificates to be retrieved. As a response, the TSA shall issue a KEYMAN message with the information related to the requested time stamps and it shall indicate which time certificates are encapsulated in the response and which ones not.

The KEYMAN messages the user and the TSA interchange shall be digitally signed in order to protect them from security attacks. The following illustration schematically exemplifies a secured KEYMAN message using a security header and trailer pair as described in chapter 4.1 Interchanges in a secure environment:

UNA	UNB	UNH	Security Header Group 1 (Digital signature algorithms)	KEYMAN MESSAGE	Security Trailer Group 1 (Digital signature)	UNT	UNZ

4.2.3.2.1 Time Stamp Retrieval request EDI interchange

The user shall submit to the TSA a secured KEYMAN message with the serial numbers of the time stamps to be retrieved.

The syntax rules for the KEYMAN message are as follows:

POS	TAG	Name	S	R	
0010	UNH	Message header	M	1	
0020	-----	Segment group 1 -----------	C	999	--------+
0030	USE	Security message relation	M	1	I
0040	USX	Security references	C	1	I
0050	-----	Segment group 2 -----------	M	9	----+ I
0060	USF	Key management function	M	1	I I
0070	USA	Security algorithm	C	1	I I
0080	-----	Segment group 3 -----------	C	1	-+ I I
0090	USC	Certificate	M	1	I I I
0100	USA	Security algorithm	C	3	I I I
0110	USR	Security result	C	1	--------+
0120	-----	Segment group 4 -----------	C	99	--------+
0130	USL	Security list status	M	1	I
0140	-----	Segment group 5 -----------	M	9999	----+ I
0150	USC	Certificate	M	1	I I
0160	USA	Security algorithm	C	3	I I
0170	USR	Security result	C	1	--------+
0180	UNT	Message trailer	M	1	

The data segments and data elements proposed to be used in order to request time stamp retrieval element service to the TSA are as follows:

Segment group 1

USE   SECURITY MESSAGE RELATION

This segment is mandatory and specifies the relation to earlier or future security messages. Because this is a time stamp retrieval request, there is a relation with the response the TSA shall issue.

POS	TAG	Name	S	R	Repr.	Value
010	0565	MESSAGE RELATION, CODED	M	1	an..3	“3”

- 0565: Mandatory. To specify the relation to earlier or future security messages. It shall be value "3" because this is a message requesting for a response. Response requested

USX   SECURITY REFERENCES

A segment identifying a to an earlier message such as a request. Because there is no relation with previous messages, it shall be omitted

Segment group 2

USF   KEY MANAGEMENT FUNCTION

This segment identifies the function of the group it triggers. In our proposal, this segment shall encapsulate the list of serial number of the time stamps to be retrieved.

POS	TAG	Name	S	R	Repr.	Valor
010	0579	KEY MANAGEMENT FUNCTION QUALIFIER	M	1	an..3	“300”
020	S504	LIST PARAMETER	C	9		
	0575	List parameter qualifier	M		an..3	
	0558	List parameter	M		an..70	
030	0567	SECURITY STATUS, CODED	C	1	an..3	
040	0572	CERTIFICATE SEQUENCE NUMBER	C	1	an..4	
050	0505	FILTER FUNCTION, CODED	C	1	an..3	

- 0579: Mandatory. Specification of the type of key management function. It shall indicate that time stamp retrieval element service is requested. The proposed value is 300 "Time Stamp retrieval"
- S504.0575: Mandatory. Specification of the type of list parameter. In this proposal, this code shall have value "TSN" in order to indicate that the list parameter encapsulates time stamp serial number. In case the length of the list parameter data element was not enough to encapsulate all the serial numbers the user wants to retrieve, additional instances of S504 composite data element should be inserted.
- S504.0558:Mandatory. This is the serial numbers list of time stamp to retrieve from the TSA.

USA SECURITY ALGORITHM

This segment in this segment group shall be omitted because there is no key operation in this proposal of time stamp retrieval protocol.

Segment group 3

This group is normally used to encapsulate the data necessary to validate the security methods applied to the message when asymmetric algorithms are used. However, in this retrieval request proposal there are no cryptographic operations related to previous messages, so this filed shall also be omitted.

Segment group 4 and segment group 5

These segments shall also be omitted. The TSA will use it in the response in order to return the lists of retrieved time stamps and non-retrieved time stamps.

4.2.3.2.2 Time Stamp Retrieval token EDI interchange

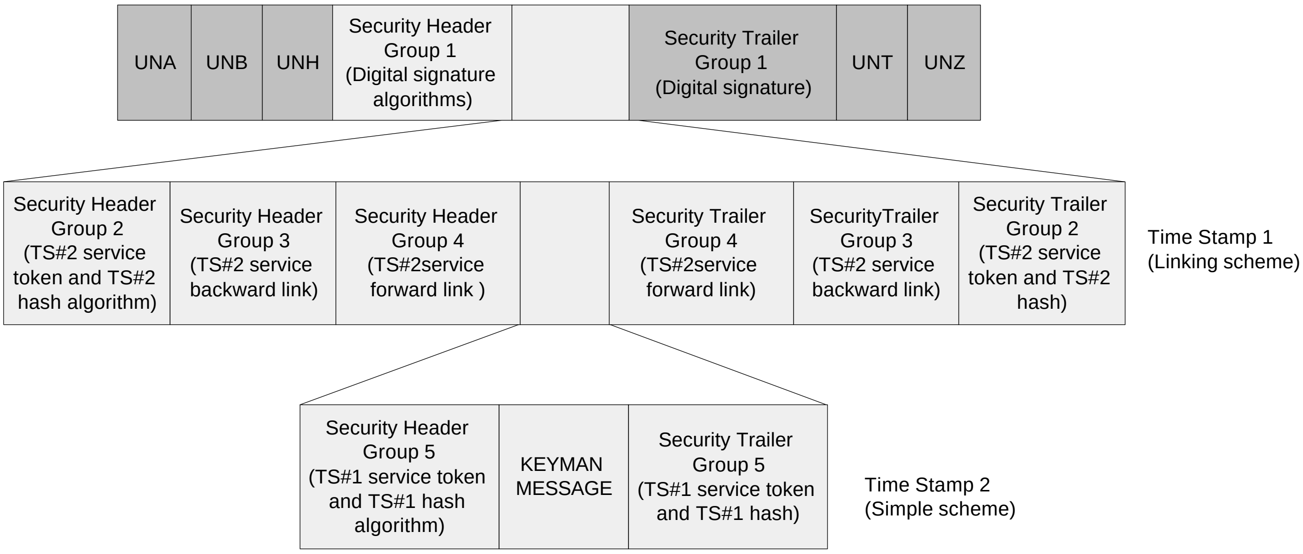
The TSA shall respond to a verification request with a secured KEYMAN message. This token EDI interchange that embeds a secured KEYMAN message shall encapsulate the following information:

- ❑ A list containing the serial number of the time stamps that are encapsulated in the response issued by the TSA. This information is embedded inside the KEYMAN message.

- ❑ A list containing the serial number of the time stamps that the TSA encountered problems trying to retrieve from its storage (for instance, time stamps that expired). This information is embedded inside the KEYMAN message.

- ❑ The information related to the retrieved time stamps. It is embedded outside the KEYMAN message, but also protected by the security header and trailer pair the TSA uses for digitally sign the response interchange. This information is encapsulated in additional security header and trailer pairs as in the response the TSA issues as a new time stamp or a renewal. This is, it encapsulates the owner of the time stamp, the stamped time, the security policy, the forward and backward links (if the time stamp was requested in Linking protocol scheme), but also a hash value of the original time stamp token issued to its requester.

The following illustration schematically exemplifies a time stamp retrieval token EDI interchange when two time stamps are retrieved (one of them was issued in Simple protocol scheme and the other in a Linking protocol scheme):


UNA
UNB
UNH
Security Header Group 1 (Digital signature algorithms)
Security Trailer Group 1 (Digital signature)
UNT
UNZ
Security Header Group 2 (TS#2 service token and TS#2 hash algorithm)
Security Header Group 3 (TS#2 service backward link)
Security Header Group 4 (TS#2service forward link)
Security Trailer Group 4 (TS#2service forward link)
SecurityTrailer Group 3 (TS#2 service backward link)
Security Trailer Group 2 (TS#2 service token and TS#2 hash)
Time Stamp 1 (Linking scheme)
Security Header Group 5 (TS#1 service token and TS#1 hash algorithm)
KEYMAN MESSAGE
Security Trailer Group 5 (TS#1 service token and TS#1 hash)
Time Stamp 2 (Simple scheme)

Security header and trailer pairs that encapsulates the backward and the forward links are exactly the same as in the time stamp EDI interchange the TSA issued to the requester when this submits the time stamp request or time stamp renewal. However, the security header and trailer pair that encapsulates the other information related to the timestamp (Security Header and Trailer groups 2 and 5 in the previous illustration), differs from Security Header and Trailer Groups 1 of individuals time stamps. They encapsulates the same service-related information but now it implements a hash result instead of the signature the TSA made on the existing time stamp when it was issued. The TSA shall calculate this hash value over the complete EDI interchange it issued to the user when he submits a time stamp request or time stamp renewal.

These modifications on the security header-trailer pair will be detailed later in this chapter.

The syntax rules for the KEYMAN message returned by the TSA are as follows:

POS	TAG	Name	S	R	
0010	UNH	Message header	M	1	
0020	-----	Segment group 1 -----------	C	999	--------+
0030	USE	Security message relation	M	1	I
0040	USX	Security references	C	1	I
0050	-----	Segment group 2 -----------	M	9	----+ I
0060	USF	Key management function	M	1	I I
0070	USA	Security algorithm	C	1	I I
0080	-----	Segment group 3 -----------	C	1	-+ I I
0090	USC	Certificate	M	1	I I I
0100	USA	Security algorithm	C	3	I I I
0110	USR	Security result	C	1	--------+
0120	-----	Segment group 4 -----------	C	99	--------+
0130	USL	Security list status	M	1	I
0140	-----	Segment group 5 -----------	M	9999	----+ I
0150	USC	Certificate	M	1	I I
0160	USA	Security algorithm	C	3	I I
0170	USR	Security result	C	1	--------+
0180	UNT	Message trailer	M	1	

The data segments and data elements proposed to be used by the TSA in order to response time stamp retrieval requests are as follows:

Segment group 1

USE SECURITY MESSAGE RELATION

This segment is mandatory and specifies the relation to earlier or future security messages. Because this is a time stamp retrieval token, this is a response to a previous time stamp retrieval request.

POS	TAG	Name	S	R	Repr.	Valor
010	0565	MESSAGE RELATION, CODED	M	1	an..3	“2”

- 0565: Mandatory. It shall be value "2" because this is a response message. Response

USX SECURITY REFERENCES

A segment identifying a to an earlier message such as a request. Because there is a relation with a previous request message, it shall refer to it.USX encapsulate reference to the secured request EDI interchange the requester submitted to the TSA.

TAG	Name	S	R	Repr.	Value
0020	INTERCHANGE CONTROL REFERENCE	M	1	an..14	AD
S002	INTERCHANGE SENDER	C	1		
0004	Interchange sender identification	C		an..35	AD
0007	Identification code qualifier	C		an..4	AD
0008	Interchange sender internal identification	C		an..35	
0042	Interchange sender internal sub-identification	C		an..35	
S003	INTERCHANGE RECIPIENT	C	1		
0010	Interchange recipient identification	C		an..35	AD
0007	Identification code qualifier	C		an..4	AD
0008	Interchange recipient internal identification	C		an..35	
0042	Interchange recipient internal sub-identification	C		an..35	
0048	GROUP REFERENCE NUMBER	C	1	an..14	
S006	APLICATION SENDER IDENTIFICATION	C	1		
0040	Aplication sender identification	M		an..35	
0007	Identification code qualifier	C		an..4	
S007	APLICATION RECIPIENT IDENTIFICATION	C	1		
0044	Aplication recipient identification	M		an..35	
0007	Identification code qualifier	C		an..4	
0062	MESSAGE REFERENCE NUMBER	C	1	an..14	AD
S009	MESSAGE IDENTIFIER	C	1		
0065	Message type	M		an..6	
0052	Message version number	M		an..3	
0054	Message release number	M		an..3	
0051	Controlling agency, coded	M		an..3	
0057	Association assigned code	C		an..6	
0110	Code list directory version number	C		an..6	
0113	Message type sub-function identification	C		an..6	

```
0800  PACKAGE REFERENCE NUMBER                      C  1   an..14

S501  SECURITY DATE AND TIME                        C  1
0517   Date and time qualifier, coded               M      an..3
0338   Event date                                   C      n8
0314   Event time                                   C      an..15
0336   Time offset                                  C      n4
```

- 0020: Mandatory. It is a reference to the time stamp retrieval EDI interchange the requester submit to the TSA
- S002: Optional. The identification of the sender of the request EDI interchange, this is the user.
- S003: Optional. The identification of the recipient of the time stamp retrieval EDI interchange request, this is the TSA.
- 0062: Optional. A reference to the message embedded in the message body of the time stamp retrieval request EDI interchange the user sent to the TSA

Segment group 2

USF   KEY MANAGEMENT FUNCTION

This segment identifies the function of the group it triggers. In our proposal, the TSA shall only indicate that this KEYMAN message is a result of a time stamp retrieval process.

POS	TAG	Name	S	R	Repr.	Valor
010	0579	KEY MANAGEMENT FUNCTION QUALIFIER	M	1	an..3	“300”
020	S504	LIST PARAMETER	C	9		
	0575	List parameter qualifier	M		an..3	
	0558	List parameter	M		an..70	
030	0567	SECURITY STATUS, CODED	C	1	an..3	
040	0572	CERTIFICATE SEQUENCE NUMBER	C	1	an..4	
050	0505	FILTER FUNCTION, CODED	C	1	an..3	

- 0579: Mandatory. Specification of the type of key management function. It shall indicate that time stamp retrieval element service is requested. The proposed value is 300 "Time Stamp retrieval"

USA SECURITY ALGORITHM

This segment in this segment group shall be omitted because there is no key operation in this proposal of time stamp retrieval protocol.

Segment group 3

This group is normally used to encapsulate the data necessary to validate the security methods applied to the message when asymmetric algorithms are used. However, in this retrieval request proposal there are no cryptographic operations related to previous messages, so this filed shall also be omitted.

Segment group 4

Two instances of this segment shall be used by the TSA to encapsulate in two different kind of lists the serial number of the time stamps that could be retrieved or not from the TSA storage. One of these instances shall encapsulate the serial number of the certificates correctly retrieved from the TSA. The other shall encapsulate the serial number of the certificates that could not be retrieved from the TSA.

USL SECURITY LIST STATUS

POS	TAG	Name	S	R	Repr.	Valor
010	0567	SECURITY STATUS,CODED	M	1	an..3	“TSR” or “TRE”
020	S504	LIST PARAMETER	C	9		
	0575	List parameter qualifier	M		an..3	
	0558	List parameter	M		an..70	

- 0567:Mandatory. Identification of the security element (key,certificate, or time stamp for instance) status. In this proposal, it shall have two possible values: "TSR" (Time Stamp Retrieved) or "TRE" (Time Stamp Retrieval Error) which identifies if the serial numbers encapsulated on each list are encapsulated in the response or not, this is they could be retrieved correctly or not from the TSA storage.
- S504.0575: Mandatory. Specification of the type of list parameter. In this proposal, this code shall have value "TSN" in order to indicate that the list parameter encapsulates time stamp serial number. In case the length of the list parameter data element was not enough to encapsulate all the serial numbers the user wants to retrieve, additional instances of S504 composite data element should be inserted.
- S504.0558: Mandatory. This is the serial numbers list of time stamp retrieved (or not) from the TSA.

Segment group 5

These segments might be omitted. However, to conform to the v4-syntax standard it shall be fulfilled with the TSA EDIFACT certificate.

As we said above, there are some differences in the security header and trailer pair that encapsulates time stamp service-related information in a time stamp retrieval token with the security header and trailer pair described in time stamp request and renewal service elements.

The main difference is that, in this case, these security header and trailer pair do not implement a digital signature of the whole EDI interchange (it is done by the most external USH in fact, Security Header and Trailer Group 1 in the above illustration). In this case, these security header and trailer pair is also used to encapsulate the hash value computed by the TSA over the complete original timestamp. This is the way the TSA shall use to link the original document time stamped with the stamped time returned in a time stamp retrieval token, because the TSA shall not examine or storage the message to be time stamped. This is the reason why the original message body shall not be returned by the TSA.

The following segments and data elements shall be used by the TSA in this type of security header and trailer pair:

```
TAG    Name                            S   R

UNH    Message Header                  M   1
-----  Segment Group 1 --------------- C   99  --------+
USH    Security Header                 M   1           I
USA    Security Algorithm              C   3           I
-----  Segment Group 2 --------------- C   2   ----+   I
USC    Certificate                     M   1       I   I
USA    Security Algorithm              C   3       I   I
```

```
USR    Security Result                 C  1   --------+

       Message body

-----  Segment Group n --------------- C  99  ----+
UST    Security Trailer                M  1       I
USR    Security Result                 C  1   ----+
UNT    Message Trailer                 M  1
```

Segment Group 1

USH	SECURITY HEADER				
POS	TAG	Name	S R	Repr.	Value
010	0501	SECURITY SERVICE, CODED	M 1	an..3	DEP
020	0534	SECURITY REFERENCE NUMBER	M 1	an..14	AP
030	0541	SCOPE OF SECURITY APPLICATION, CODED	C 1	an..3	
040	0503	RESPONSE TYPE, CODED	C 1	an..3	DEP
050	0505	FILTER FUNCTION, CODED	C 1	an..3	
060	0507	ORIGINAL CHARACTER SET ENCODING, CODED	C 1	an..3	“2”
070	0509	ROLE OF THE SECURITY PROVIDEE, CODED	C 1	an..3	
080	S500	SECURITY IDENTIFICATION DETAILS	C 2		
	0577	Security party qualifier	M	an	“3”
	0538	Key name	C	an..35	
	0511	Security party identification	C	an..17	AD
	0513	Security party code list qualifier	C	an..3	
	0515	Security party code list responsible agency, coded	C	an..3	
	0586	Security party name	C	an..35	AD
	0586	Security party name	C	an..35	AD
	0586	Security party name	C	an..35	AD
090	0520	SECURITY SEQUENCE NUMBER	C 1	an..35	
100	S501	SECURITY DATE AND TIME	C 1		
	0517	Date and time qualifier	M	an..3	"1"
	0338	Event date	C	n..8	AD
	0314	Event time	C	an..15	AD
	0336	Time offset	C	n4	AD

The profiles and proposed values are as following:

- 0501: Mandatory. Describes the time stamp retrieval service element and the security policy under the TSA issues the original time certificate. It shall have value "15" to indicate TimeStamping retrieval security service plus a character to indicate the policy applied by the TSA. It also indicates that a hash algorithm of the original time stamp is also encapsulated.
- 0534: Mandatory. Reference number that links a USH segment with the related UST segment. Its value will be generated automatically by the application
- 0503: Optional. This field shall be used to distinct between simple and linking protocol schemes of the original time certificate. If it is omitted, the TSA applied time stamp element service in a simple protocol scheme when the original time certificate was issued.
- 0507: Optional. The original character set encoding. It should be 8 bit ASCII, so it should have value "2"
- S500: This composite data element shall refer to the recipient of the time certificate, this is the owner who requested the time-stamp service and got the corresponding certificate.
- S500.0577: Mandatory. Identification of the role of the security party. This shall have value "Certificate Owner", so it should be value "3".
- S500.0511: Optional. Identification of a party involved in the security process, according to a defined registry of security parties
- S500.0586: Optional. Name of the security party

- 0520: Sequence number assigned to EDIFACT structure to which security is applied. This sequence number is the time certificate serial number and uniquely identifies a time certificate issued by one TSA.
- S501: This composite data element encapsulates the time stamped by the TSA.S501.0517 shall have value Security Timestamp "1"

USA SECURITY ALGORITHM

The USA segment in segment group 1 shall indicates the hash function the TSA used to get a digest of the original time stamp, that will appear in the USR segment.

The following profile is proposed:

POS	TAG	Name	S	R	Repr.	Valor
010	S502	SECURITY ALGORITHM	M	1		
	0523	Use of algorithm, coded	M		an..3	“1”
	0525	Cryptographic mode of operation, coded	C		an..3	
	0533	Mode of operation code list identifier	C		an..3	
	0527	Algorithm, coded	C		an..3	“16”
	0529	Algorithm code list identifier	C		an..3	
020	S503	ALGORITHM PARAMETER	C	9		1
	0531	Algorithm parameter qualifier	M		an..3	
	0554	Algorithm parameter value	M		an..512	

- S502.0523: Mandatory. Specification of the usage made of the algorithm. It shall have value "1" in order to indicate hash function used by the sender.
- S502.0527: Optional. Identification of the algorithm. The proposed value is "16" SHA1 algorithm.

Segment Group 2

This segment shall be omitted because the USR will only encapsulate a digest value of the original time stamp calculated with the algorithm specified in the USH segment.

Segment Group n

A group of segments containing a link with Security Header Group 1 and the result of the security functions applied to the original time stamp. In this case, it shall encapsulate the result of the hash of the original time stamp calculated by the TSA.

UST SECURITY TRAILER

TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AP
0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	

USR SECURITY RESULT

TAG	Name	S	R	Repr.	Value
S508	VALIDATION RESULT	M	2		
0563	Validation value, qualifier	M		an..3	“1”
0560	Validation value	C		an..512	AP

The profiles and proposed values are as following:

- UST.0534: Mandatory. Reference number that links a UST segment with the related USH segment. Its value will be generated automatically by the application

- UST.0588: Mandatory. The number of the security segments in a security header/trailer group pair
- USR.S508.0563: Identification of the type of validation value. It shall have value "1" SHA1 digest
- USR.S508.0560: Security result corresponding to the security function specified. It shall encapsulate the result of the digital signature process.

5 ACCESS MEANS

The previously described formats for provision of the time-stamping service are specific for a batch environment processing. Two basic means are identified below:

	E-mail	**TCP/IP**
Frequency of use	Low	High
User	Human and application	Application
Interactive	Batch	Batch
Volume	Heavy	Heavy
Number of certificates	One or more	One or more

Whatever the access means is, the client is expected to submit properly packaged requests, and to be able to understand properly formatted responses, as well as to provide the means to store evidence as needed for future use. This statement has a serious impact on the need to provide adequate client user interfaces to

- collect needed information
- pack the information and sign it
- request the service and interpret the response
- store evidence locally

5.1 BATCH TCP/IP BASED SERVICE

The following simple socket-based protocol is suitable for cases where the time-stamping service is initiated by an application: the service request and response analysis is embedded within a bigger application.

The protocol basically assumes a listener process on a TSA which can accept time-stamping requests on a well-defined port. The transport socket is established upon client request, establishing a two-way reliable transmission channel that, once established may be used for more than one transaction. This architecture permits batch operation: the client application prepares a bunch of requests, and processes them in a row. The architecture is oriented towards unattended services without human intervention.

This architecture was described in previous deliverable [PKITS D4]

5.2 E-MAIL BASED SERVICE

This format is intended for batch transactions. S/MIME will be used to make a pack of requests that is transferred to the TSA for certification. The TSA responds with another pack of responses.

The client shall have tools to generate EDI interchanges requests, to pack bunches of requests with a single certificate, to analyse responses, and to keep track of requests and responses to keep final users informed of the state of the time-stamping service.

E-mail may be used to time-stamp a single document, or a larger number of them. The mail agent may be exercised by another application as transport mechanism.

The core idea is to provide a MIME envelope to EDI interchanges as identified above. The rules to produce secure MIME objects [RFC 1847] will follow S/MIME [RFC 2311, RFC 2312, RFC 1767] recommendations. According to RFC 1767, the MIME content-type specified when using the e-mail based service shall be "APPLICATION/EDI-CONSENT SPECIFICATION".

Notice that E-mail is used as a transport agent, and therefore S/MIME is not interfering with the inners of EDI interchange objects exchanged.

RFC 1767 "MIME Encapsulation of EDI Objects" can be found on appendix D.

6 SCENARIOS OF USE

The protocols and means described in this document will be used in a large number of situations to provide time-stamping services to users over the EDIFACT standard. These situations were described in details for a generic Time Stamp Service in previous deliverable [PKITS D3].

6.1 TIME STAMP SERVICE APPLICATIONS

We present a list of the possible applications of the Time Stamp Service over EDIFACT standard. In order to follow a systematic approach to analyse possible scenarios of use, we must group examples of use so that we can identify usage patterns representing homogeneous user groups. Let us consider the point of view of where is the TSA located: either in the public sector or in the private sector:

- TSS users from Public Sector.
- TSS users from Private Sector.

6.1.1 Application in Public Sector

The following are the common applications to the Time Stamp Service over EDIFACT interchanges:

Administrative registry
Every official organism, regardless its domain, provides a registry service whose aim is to admit and register documents that citizens submit to public administration. It is also in charge of registering the outcome of official documents. Modernisation of public service provision will introduce electronic registers that would use security services provided and specially would require Time stamping services to operate in a secure way. One of the main purposes of EDIFACT is to standardise electronic data for administration purposes, and Time Stamp Service is mandatory in these situations

Notary & property registry
The use of digital signature schemes in notary tasks will allow remote signing introducing a new electronic notary scheme where the notary digitally signs the documents once their contents have been verified. This new scheme needs the existence of a TSA to time stamp documents setting their creation, modification and/or signing date and time. This scenario was solved by years using private infrastructures and communication networks as VAN (Value Added Networks).

Copyright & intellectual property
Nowadays there are some different groups working on EDIFACT standards to standardise EDI interchanges about copyright and intellectual property, and because of this the Time Stamp Service over EDIFACT standard becomes of mandatory importance since it will provide trustful evidence on the date of protected work delivery.

Stock exchange
This is one of the most important EDIFACT standard appliances. Buy/sell orders supplied in electronic format must be time stamped independently from parties involved in transactions.

Justice administration/procurement

Since communication among courts and judicial agents are subject to strict terms that must be accomplished in its execution, EDIFACT interchanges containing this information demand time stamps that assure their validity and integrity within the given terms.

Public health care

EDIFACT interchanges are nowadays widely used as a stock exchange in public health care, and the expected increase on the number of medical interventions made through telematics will force public and private health systems to be main users of TSS. In this sector, time stamping will provide security and coherence in diagnosis and images that would be inserted in historic records for each patient.

6.1.2 Application in Private Sector

Electronic commerce

There are a large number of scenarios of use of electronic commerce and it is one of the main targets of the EDIFACT world. Time-stamping services are mandatory in order to reach an adequate level of security, and evidence to face potential disputes.

Transport

It is rather usual that contractual terms are referenced to delivery times, and to the satisfaction of time constraints along intermediate stages along the logistic chain, specially when different means of transport are involved. Another purpose of the EDIFACT standard is to accelerate as much as possible this logistic chain and Time-stamping may be used to certify the pass across intermediate and extreme points.

Finances (banking and assurance)

Finances was one of the sector that uses VAN and EDIFACT standard in order to offer secure transactions, and because of this presents opportunities for time-stamping services. In the assurance sector, there is another large amount of opportunities for TSA activities, as referred to on-line contracts, and assurance in general.

Broadcasting

There are many applications of time-stamping services in radio, TV, cable, satellite, and so on. Let’s mention those related to emission control, that has an impact on publicity costs and revenues, since the instant of emission makes a deep difference in its impact. EDIFACT standard can be used in these environments, so there are again oportunities to apply TSS service over EDIFACT standard.

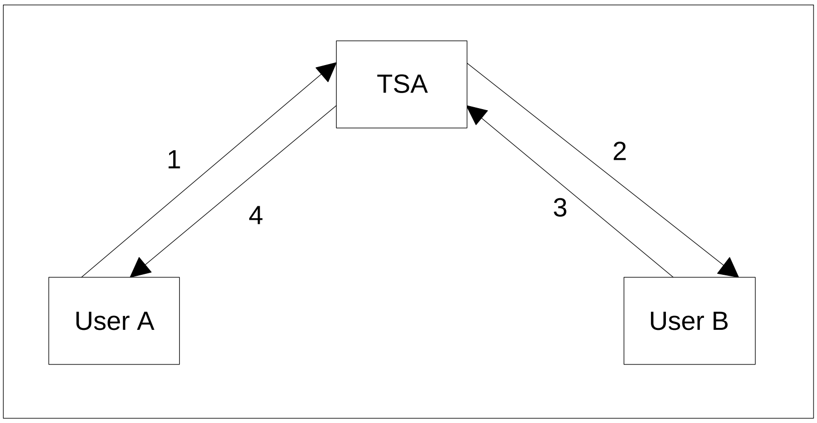
6.2 BASIC SCENARIOS

The resulting scenarios are exactly the same as specified in the previous deliverable [PKITS D3]. From the functional point of view we considered:

Non repudiation of origin: User A sends a document to user B. Non-repudiation of origin is requested by user B. When a user A wants to be able to demonstrate the ownership, authorship or just the knowledge of some information at a given time, then its s/he who must contact the TSA, prior to the publishing of that information or document. The procedure is exactly as described in details in [PKITS D3].

Non repudiation of recipient: This scenario corresponds to the situations where it is requested the non-repudiation of receipt of a document at a given time. User A sends a document to user B. Non-repudiation of receipt is requested by user A. The procedure is exactly as described in details in [PKITS D3].

Mutual non-repudiation: When both users require non-repudiation of the other's action, a combination of the two previously described scenarios may be necessary. However, this scenario differs from the one specified in [PKITS D3], because in the protocols defined in this proposal the document to be time-stamped is always encapsulated completely in the EDI interchanges. Because of this, this scenario is as follows:



Procedure:

1. User A sends the complete Document to TSA
2. TSA time stamp the original document and sends the resulting TS token (that also encapsulates the complete original document) to User B. The User B will have a proof of origin of Document by User A, who will not be able to repudiate the reception
3. User B sends an acknowledgement (a hash of the original document for instance) to the TSA in order to construct a receipt.
4. The TSA send the time-stamped acknowledgement to User A, so that User A will have a proof of reception of Document by User B, who will not be able to repudiate the reception.

7 APPENDIX A: DATA ELEMENT VALUES PROPOSED

This appendix sum up the data element values referenced in this proposal that are not supported by the syntax rules standard version 4 (shadowed values).

501 Security service coded

"13" Time Stamping renewal: The related security header indicates a time certificate renewal request to a TSA or time certificate token as a result of a time certificate renewal process from a TSA.

"14" Time Stamping verification: The related security header indicates a time certificate verification request to a TSA or a time certificate verification response from a TSA.

"15" Time Stamping retrieval: The related security header indicates a time certificate retrieval request to a TSA or a time certificate retrieval token from a TSA

579 Key management function qualifier

"300" Time Stamp renewal. It indicates that the S504 (List parameter) composite data element in USF (Key Management function) segment refers to time certificate serial numbers

575 List parameter qualifier

"TSN" Time Stamp Serial Number. It specifies in S504 (List parameter) composite data element that the list encapsulates time certificate serial numbers

0567 Security status, coded

"TSR" Time Stamp Retrieved. It specifies in USL (Security List Status) segment that the composite data element S504 (List parameter) encapsulates the serial numbers of the time certificate retrieved correctly from the TSA.

"TRE" Time Stamp Retrieval Error. It specifies in USL (Security List Status) segment that the composite data element S504 (List parameter) encapsulates the serial numbers of the time certificate that could not be retrieved correctly from the TSA.

8 APPENDIX B: EXAMPLES OF TIME STAMPING EDI INTERCHANGES

We present the following examples:

a) Time Stamping element service

a.1)Time stamping request in Simple protocol scheme and the resulting time certificate issued by the TSA

a.2)Time stamping request in Linking protocol scheme and the resulting time certificate issued by the TSA.

b)Time Stamping Renewal element service. Renewal in simple protocol scheme of the resulting time certificate in the previous example a.2 (linking protocol scheme)

8.1 TIME STAMPING ELEMENT SERVICE

8.1.1 Time Stamping in Simple protocol scheme

<u>Time Stamp Request EDI Interchange</u>

<u>Security Header and Trailer Group 1</u>

Segment group 1:USH-USA segments*:*

```
USH+x10+1++1++2+++1::RequesterIdentification:::RequesterName1:RequesterName2:RequesterName3'USA+1+++16'
```

The user requested time stamping element service with policy x (x10), in simple protocol scheme (second 1), ASCII 8 bit character set encoding (first 2). The first 1 is the security reference number, and the last one in USH segment is the security party qualifier as a message sender. The first 1 in USA segment indicates hash function usage of the algorithm coded with 16 (SHA1).

Segment group n: UST-USR segments:

```
UST+1+"Number of security segments" 'USR+1+"Digital Signature"
```

The first 1 after tag UST is the security reference number and matches with the related one in the USH. The first 1 in USR segment indicates RSA digital signature.

<u>Time Stamp token EDI interchange</u>

<u>Security Header and Trailer Group 1</u>

Segment group 1 USH-USA segments:

```
USH+x10+1++1++2+++3::RequesterIdentification:::RequesterName1:RequesterName2:R
equesterName3+1+1:980830: 19980830170420Z:0100'USA+1+++16
```

The TSA issued a new time certificate under policy x (x10), in Simple protocol scheme (second 1), ASCII 8 bit character set encoding (first 2). The user identified by RequestIdentification, RequesterNames 1,2,3 is the owner of the time certificate (first 3). The time certificate serial number is 1 (first 1 after RequesterName3), and the time encapsulated in S501 composite data field is qualified as Security TimeStamp (the following 1).
The first 1 after x10 value is the security reference number.

Segment group n: UST-USR segments:

```
UST+1+"Number of security segments"'USR+1+"Digital Signature"
```

The first 1 after the tag UST is the security reference number and matches with the related one in the USH

8.1.2 Time Stamping in Linking protocol scheme

Time Stamp Request EDI Interchange

Security Header and Trailer Group 1

Segment group 1:USH-USA segments:

```
USH+x10+2++2++2+++1::RequesterIdentification:::RequesterName1:RequesterName2:Req
uesterName3'USA+1+++16
```

The user requested time stamping element service with policy x (x10), in linking protocol scheme (second 2), ASCII 8 bit character set encoding (third 2). The first 2 is the security reference number, and the last one in segment USH is the security party qualifier as a message sender.

Segment group n: UST-USR segments:

```
UST+2+"Number of security segments"'USR+1+"Digital Signature"
```

The first 2 after tag UST is the security reference number and matches with the related one in the USH

Time Stamp token EDI interchange

Security Header and Trailer Group 1

Segment group 1 USH-USA segments:

```
USH+x10+2++2++2+++3::RequesterIdentification:::RequesterName1:RequesterName2:R
equesterName3+2+1:980831: 19980831170420Z:0100'USA+1+++16
```

The TSA issued a new time certificate under policy x (x10), in Linking protocol scheme (second 2), ASCII 8 bit character set encoding (third 2). The user identified by RequestIdentification, RequesterNames 1,2,3 is the owner of the time certificate (first 3). The

time certificate serial number is 2 (first 2 after RequesterName3), and the time encapsulated in S501 composite data field is qualified as Security TimeStamp (the following 1).
The first 2 after x10 value is the security reference number.

Segment group n: UST-USR segments:

```
UST+2+"Number of security segments"'USR+1+"Digital Signature"
```

The first 2 after the tag UST is the security reference number and matches with the related one in the USH

<u>Security Header and Trailer Group 2</u>

These "Security Header and Trailer" groups encapsulate the backward link of the current time certificate. In this example, the previous certificate issued by the TSA is the resulting time certificate of the previous example, this is, with serial number 1.

Segment group 1 USH-USA segments:

It is a copy of the Segment group 1of "Security Header Group 1" of the previous time certificate issued by the TSA.

```
USH+x10+1++1++2+++3::RequesterIdentification:::RequesterName1:RequesterName2:RequesterName3+1+1:980830: 19980830170420Z:0100'USA+1+++16
```

The previous time certificate issued by the TSA had serial number 1,it was issued under policy x (x10), in Simple protocol scheme (second 1), ASCII 8 bit character set encoding (first 2). The user identified by RequestIdentification, RequesterNames 1,2,3 is the owner of the time certificate (first 3). The time encapsulated in S501 composite data field is qualified as Security TimeStamp. The first 1 after x10 value is the security reference number.

Segment group n: UST-USR segments:

This segment group is a copy of the segment group n of the "Security Trailer Group 1"

```
UST+1+"Number of security segments"'USR+1+"Digital Signature"
```

The first 1 after the tag UST is the security reference number and matches with the related one in the USH

<u>Security Header and Trailer Group 3</u>

This "Security Header and Trailer" groups encapsulate the forward link of the current time certificate. In this example, the following certificate that the TSA will issue will have serial number 3.

Segment group 1 USH-USA segments:

```
USH+x10+3++++2+++3'
```

The serial number of the following time certificate issued by the TSA is 3 (last 3).
USA segment is omitted, because there is no security operation involved.

Segment group n: UST-USR segments:

```
UST+3+"Number of security segments"'
```

The first 1 after the tag UST is the security reference number and matches with the related one in the USH. USR segment is ommited.

8.2 TIME STAMPING RENEWAL ELEMENT SERVICE

Renewal in Simple protocol scheme of the resulting time certificate in the previous example a.2 (linking protocol scheme).

Time Stamp Renewal Request EDI Interchange

Security Header and Trailer Group 1

Segment group 1:USH-USA segments:

```
USH+x13+3++1++2+++1::RequesterIdentification:::RequesterName1:RequesterName2:Req
uesterName3+2'+USA+1+++16
```

The user requested time stamping renewal under policy x (x13), of the time certificate with serial number 2 (last 2), in Simple protocol scheme (first 1), ASCII 8 bit character set encoding (first 2). The first 3 is the security reference number, and the last 1 in segment USH is the security party qualifier as a message sender.

Segment group n: UST-USR segments:

```
UST+3+"Number of security segments"'+USR+1+"Digital Signature"
```

The first 3 after tag UST is the security reference number and matches with the related one in the USH

Time Stamp Renewal token EDI interchange

Security Header and Trailer Group 1

Segment group 1 USH-USA segments:

```
USH+x13+3++1++2+++3::RequesterIdentification:::RequesterName1:RequesterName2:R
equesterName3+3+1:980901: 19980901170420Z:0100'+USA+1+++16
```

The TSA issued a new time certificate under policy x (x13), in Simple protocol scheme (first 1), ASCII 8 bit character set encoding (first 2) in order to renew the certificate with serial number indicated in the "Security Header and Trailer Group 2" (see later). The user identified by RequestIdentification, RequesterNames 1,2,3 is the owner of the time certificate (second 3). The time certificate serial number is 3 (first 3 after RequesterName3), and the time encapsulated in S501 composite data field is qualified as Security TimeStamp (the following 1).
The first 3 after x13 value is the security reference number.

Segment group n: UST-USR segments:

```
UST+3+"Number of security segments"'USR+1+"Digital Signature"
```

The first 3 after the tag UST is the security reference number and matches with the related one in the USH.

<u>Security Header and Trailer Group 2</u>

Because Simple protocol scheme was requested, "Security Header and Trailer Group 2" shall be a copy of the "Security Header and Trailer Group 1" of the certificate to be renewed in order to link both time certificates. This is:

Segment group 1 USH-USA segments:

```
USH+x10+2++2++2+++3::RequesterIdentification:::RequesterName1:RequesterName2:R
equesterName3+2+1:980831: 19980831170420Z:0100'USA+1+++16
```

The renewed certificate was issued by the TSA under policy x (x10), in Linking protocol scheme (second 2), ASCII 8 bit character set encoding (third 2) and has serial number 2 (first 2 after RequesterName3).

Segment group n: UST-USR segments:

```
UST+2+"Number of security segments"'USR+1+"Digital Signature"
```

The first 2 after the tag UST is the security reference number and matches with the related one in the USH

9 APPENDIX C: AUTACK MESSAGE. SECURE AUTHENTICATION AND ACKOWLEDGEMENT MESSAGE

The TSA shall report any error or suspicious user behaviour detected during time-stamp service element processes. Different kind of errors can be considered: the TSA shall verify the digital signature of the request, the policy and service requested … and in some circumstances, for instance due to network transport errors or security attacks, some checks can fail. Moreover, the TSA shall check that the key with the user signed the request is length enough, the correctness of the algorithms applied and it also should be concerned about the amount of time it is willing to wait for a response in order to detect a "man-in-the-middle" attack.

An AUTACK message used as an acknowledgement message shall be sent by the recipient of one ore more previously received secured EDIFACT structures. In normal circumstances, if the user requests a new time certificate or a time certificate renewal, he will receive an EDI interchange message that encapsulates the new time stamp. However, if an error occurs, the TSA shall report these errors to the user through AUTACK message, instead of issuing a time certificate.

In this proposal, the ATUACK message shall also be used by the TSA in order to report to the user the status of a certificate in the verification service element. This is, when a user submits to the TSA a verification request EDI interchange with the information specified in chapter 4.2.3.1 (TSA Verification protocol) (serial number of the time certificate to be verified, the complete time certificate embedded in the message body…), he will receive an AUTACK message indicating the status of that time stamp. If the status is valid, data element 0571 (Security Error) shall be omitted. If not, it shall indicate the type of error the request generated.

The AUTACK message is as follows:

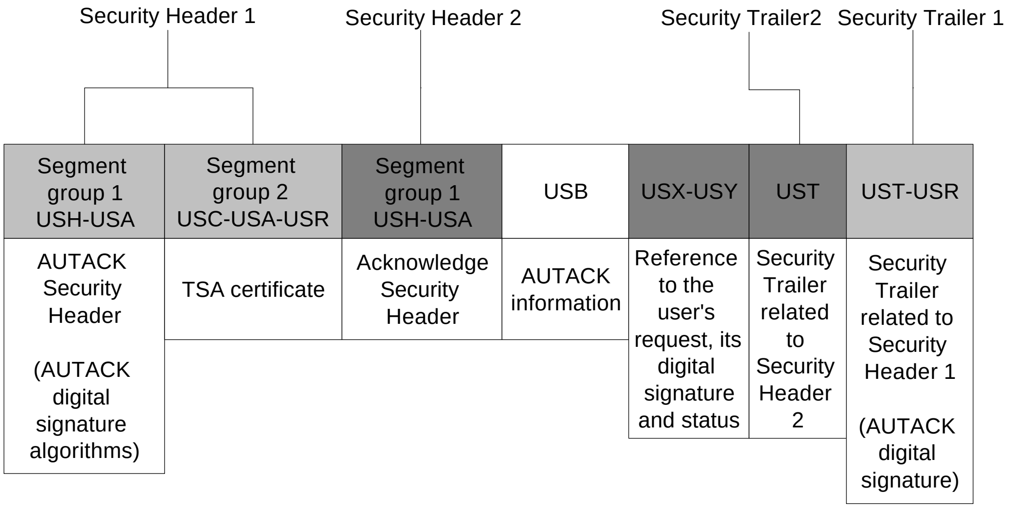
```
POS       TAG       Name                               S   R    Notes

0010      UNH       Message header                     M   1

0020      ----      Segment group 1 ------------       M   99   -------+

0030      USH       Security header                    M   1           |
0040      USA       Security algorithm                 C   3           |
                                                                       |
0050      -----     Segment group 2 ------------       C   2    ----+  |

0060      USC       Certificate                        M   1        |  |
0070      USA       Security algorithm                 C   3        |  |
0080      USR       Security result                    C   1    ----+--+

0090      USB       Secured data identification        M   1

0100      -----     Segment group 3 ------------       M   9999 ----+

0110      USX       Security references                M   1        |
0120      USY       Security on references             M   9    ----+

0130      -----     Segment group 4 ------------       M   99   ----+

0140      UST       Security trailer                   M   1        |
0150      USR       Security result                    C   1    ----+

0160      UNT       Message trailer                    M   1
```

Each "Segment group 1" encapsulates USH and USA segments. In this proposal, the first of them protects the AUTACK message from security attacks, and another will encapsulate information about the security service applied to the data structures referenced by the message, this is the request submit by the user to the TSA. In this proposal, the TSA shall digitally sign the request EDI interchange.

USX and USY segments are encapsulated in "Segment Group 3". The USX segment identifies those structures protected by the AUTACK message, this is the request interchange in this proposal. The USY segment encapsulates the results of the cryptographic process (digital signatures in this proposal) applied to the data structures secured (the request EDI interchange in this proposal).

"Segment group 4" encapsulates the security trailers related to USH segments. There shall be as UST as USH segments. However, there shall be only a single USR segment related to the USH segment that protect the complete AUTACK message, this is the digital signature of the AUTACK message.

The following illustration schematically exemplifies the AUTACK message used in this proposal:


Security Header 1
Security Header 2
Security Trailer2
Security Trailer 1
Segment group 1 USH-USA
Segment group 2 USC-USA-USR
Segment group 1 USH-USA
USB
USX-USY
UST
UST-USR
AUTACK Security Header (AUTACK digital signature algorithms)
TSA certificate
Acknowledge Security Header
AUTACK information
Reference to the user's request, its digital signature and status
Security Trailer related to Security Header 2
Security Trailer related to Security Header 1 (AUTACK digital signature)

The profiles proposed for each segment is as follows (shadowed):

```
USB    SECURED DATA IDENTIFICATION
```

Its function is to contain details related to the AUTACK

TAG	Name	S	R	Repr.	Value
0503	RESPONSE TYPE, CODED	M	1	an..3	“1”
S501	SECURITY DATE AND TIME	C	1		
0517	Date and time qualifier, coded	M		an..3	
0338	Event date	C		n8	
0314	Event time	C		an..15	
0336	Time offset	C		n4	
S002	INTERCHANGE SENDER	M	1		
0004	Interchange sender identification	M		an..35	AD
0007	Identification code qualifier	C		an..4	AD
0008	Interchange sender internal identification	C		an..35	
00042	Interchange sender internal sub-identification	C		an..35	
S002	INTERCHANGE RECIPIENT	M	1		
0010	Interchange recipient identification	M		an..35	AD
0007	Identification code qualifier	C		an..4	AD
0008	Interchange recipient internal identification	C		an..35	
0042	Interchange recipient internal sub-identification	C		an..35	

- 0503: Optional. Specification of the type of response expected from the recipient. It shall have value "1" in order to not request a secure receipt of the AUTACK message
- S501: It encapsulates the date end time when the AUTACK message was issued.
- S002 and S003: Optional. It should be used in order to identify the TSA that issued the AUTACK message and the recipient

USX SECURITY REFERENCES

USX encapsulate reference to the secured request EDI interchange the requester submitted to the TSA.

TAG	Name	S	R	Repr.	Value
0020	INTERCHANGE CONTROL REFERENCE	M	1	an..14	AD
S002	INTERCHANGE SENDER	C	1		
0004	Interchange sender identification	C		an..35	AD
0007	Identification code qualifier	C		an..4	AD
0008	Interchange sender internal identification	C		an..35	
0042	Interchange sender internal sub-identification	C		an..35	
S003	INTERCHANGE RECIPIENT	C	1		
0010	Interchange recipient identification	C		an..35	AD
0007	Identification code qualifier	C		an..4	AD
0008	Interchange recipient internal identification	C		an..35	
0042	Interchange recipient internal sub-identification	C		an..35	
0048	GROUP REFERENCE NUMBER	C	1	an..14	
S006	APLICATION SENDER IDENTIFICATION	C	1		
0040	Aplication sender identification	M		an..35	
0007	Identification code qualifier	C		an..4	
S007	APLICATION RECIPIENT IDENTIFICATION	C	1		
0044	Aplication recipient identification	M		an..35	
0007	Identification code qualifier	C		an..4	
0062	MESSAGE REFERENCE NUMBER	C	1	an..14	AD
S009	MESSAGE IDENTIFIER	C	1		
0065	Message type	M		an..6	
0052	Message version number	M		an..3	
0054	Message release number	M		an..3	
0051	Controlling agency, coded	M		an..3	
0057	Association assigned code	C		an..6	
0110	Code list directory version number	C		an..6	
0113	Message type sub-function identification	C		an..6	
0800	PACKAGE REFERENCE NUMBER	C	1	an..14	
S501	SECURITY DATE AND TIME	C	1		
0517	Date and time qualifier, coded	M		an..3	
0338	Event date	C		n8	
0314	Event time	C		an..15	
0336	Time offset	C		n4	

- 0020: Mandatory. It is a reference to the EDI interchange the requester submit to the TSA
- S002: Optional. The identification of the sender of the request EDI interchange, this is the user.
- S003: Optional. The identification of the recipient of the EDI interchange request, this is the TSA.
- 0062: Optional. A reference to the message (unique) embedded in the message body of the request EDI interchange the user sent to the TSA

USY SECURITY ON REFERENCES

It encapsulates the digital signature of the request EDI interchange the TSA received from the user and the reason why this request generated an error.

TAG	Name	S	R	Repr.	Value
0534	SECURITY REFERENCE NUMBER	M	1	an..14	AD
S508	VALIDATION RESULT	C	2		
0563	Validation value, qualifier	M		an..3	“1”
0560	Validation value	C		an..512	AP
0571	SECURITY ERROR, CODED	C	1	an..3	DEP

- 0534: Mandatory. It shall be the same value as the 0534 element in the second USH segment of the AUTACK message
- S508.0563: Identification of type of validation value in S508.0560.In this proposal, it shall be value "1": a RSA digital signature.
- S508.0560: The digital signature of the request EDI interchange submitted by the user to the TSA. It shall be calculated with the TSA private key and filtered as indicated in the USH segment of the AUTACK message.
- 0571: Status notification. This field shall specify the security error encountered by the TSA while processing the request. This field shall be omitted if no error has encountered in a verification procedure. If an error occurred, it shall be one of the following error codes:

  "1": Error checking digital signature. Wrong authenticator.
  "2": Error in user certificate. Wrong certificate
  "3": Incomplete certification path. Cannot verify
  "4": Signature algorithm not supported
  "5": Hashing method not supported
  "6": Protocol error

USH SECURITY HEADER

The second USH segment of the AUTACK message encapsulates information about the security service provided on the references of the AUTACK message.

The proposed profile is the same as proposed in chapter 4.1 (Interchanges in a secure environment), so implements a digital signature. However, the 0501 data element (security service coded) shall be the value as in the request EDI interchange that causes the error situation, this is "Time Stamp request", "Time Stamp Renewal" or "Time Stamp verification"

TAG	Name	S	R	Repr.	Value
0501	SECURITY SERVICE, CODED	M	1	an..3	DEP

.
.

10 APPENDIX D: RFC 1767 MIME ENCAPSULATION OF EDI OBJECTS

Network Working Group
Request for Comments: 1767
Category: Standards Track

D. Crocker
Brandenburg Consulting

March 1995

MIME Encapsulation of EDI Objects

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Table of Contents

1. Introduction

Electronic Data Interchange (EDI) provides a means of conducting structured transactions between trading partners. The delivery mechanism for these types of transactions in a paper world has been the postal system, so it is to be expected that electronic mail would serve as a natural delivery mechanism for electronic transactions. This specification permits formatted electronic business interchanges to be encapsulated within MIME messages [Bore92]. For the specification effort, the basic building block from EDI is an interchange.

This specification pertains only to the encapsulation of EDI objects within the MIME environment. It intends no changes in those objects from the primary specifications that define the syntax and semantics of them. EDI transactions take place through a variety of carriage and exchange mechanisms. This specification adds to that repertoire, by permitting convenient carriage through Internet email.

Since there are many different EDI specifications, the current document defines three distinct categories as three different MIME content-types. One is Application/EDI-X12, indicating that the contents conform to the range of specifications developed through the X12 standards organization [X125, X126, X12V]. Another is Application/EDIFACT, indicating that the contents conform to the range of specifications developed by the United Nations Working Party 4 Group of Experts 1 EDIFACT boards [FACT, FACV]. The last category covers all other specifications; it is Application/EDI-consent.

2. APPLICATION/EDIFACT SPECIFICATION

The Application/EDIFACT MIME body-part contains data as specified for electronic data interchange by [FACT, FACV].

Within EDIFACT, information is specified by:

MIME type name:	Application
MIME subtype name:	EDIFACT
Required parameters:	none
Optional parameters:	CHARSET, as defined for MIME
Encoding considerations:	May need BASE64 or QUOTED-PRINTABLE transfer encoding
Security considerations:	See separate section in the document.
Published specification:	Contained in the following section.
Rationale:	The EDIFACT specifications are accepted standards for a class of inter-organization transactions; this permits their transmission over the Internet, via email.
Contact-info:	See Contact section, below.

Detail specific to MIME-based usage:

> This is a generic mechanism for sending any EDIFACT interchange. The object is self-defining, in terms of indicating which specific EDI objects are included. Most EDI data is textual, but special characters such as some delimiters may be non-printable ASCII or some data may be

pure binary. For EDI objects containing such data, the MIME transfer mechanism may need to encode the object in Content-Transfer-Encoding:quoted-printable or base64.

3. APPLICATION/EDI-X12 SPECIFICATION

The Application/EDI-X12 MIME body-part contains data as specified for electronic data interchange by [X125, X12.6, EDIV].

Within MIME, EDI-X12 information is specified by:

MIME type name: Application

MIME subtype name: EDI-X12

Required parameters: none

Optional parameters: CHARSET, as defined for MIME

Encoding considerations: May need BASE64 or QUOTED-PRINTABLE transfer encoding

Security considerations: See separate section in the document.

Published specification: Contained in the following section.

Rationale: The ASC X12 EDI specifications are accepted standards for a class of inter-organization transactions; this permits their transmission over the Internet, via email.

Contact-info: See Contact section, below.

Detail specific to MIME-based usage:

This is a generic mechanism for sending any ASC X12 interchange. The object is self-defining, in terms of indicating which specific EDI objects are included. Most EDI data is textual, but special characters such as some delimiters may be non-printable ASCII or some data may be pure binary. For EDI objects containing such data, the MIME transfer mechanism may need to encode the object in Content-Transfer-Encoding:quoted-printable or base64.

4. APPLICATION/EDI-CONSENT SPECIFICATION

The Application/EDI-consent MIME body-part contains data as specified for electronic data interchange with the consent of explicit, bilateral trading partner agreement exchanging the EDI-consent traffic. As such, use of EDI-consent only provides a standard mechanism for "wrapping" the EDI objects but does not specify any of the details about those objects.

Within MIME, EDI-consent information is specified by:

MIME type name:	Application
MIME subtype name:	EDI-consent
Required parameters:	none
Optional parameters:	CHARSET, as defined for MIME
Encoding considerations:	May need BASE64 or QUOTED-PRINTABLE transfer encoding
Security considerations:	See separate section in the document.
Published specification:	Contained in the following section.
Rationale:	Existing practice for exchanging EDI includes a very wide range of specifications which are not part of the usual, accredited standards world. Nevertheless, this traffic is substantial and well-established. This content type provides a means of delimiting such content in a standard fashion.
Contact-info:	See Contact section, below.

Detail specific to MIME-based usage:

This is a generic mechanism for sending any EDI object explicitly agreed to by the trading partners. X12 and EDIFACT object must be sent using their assigned MIME content type. EDI-consent is for all other EDI objects, but only according to trading partner agreements between the originator and the recipient. Most EDI data is textual, but special characters such as some delimiters may be non-printable ASCII or some data may be pure binary. For EDI objects containing such data, the MIME transfer mechanism may need to encode the object in Content-Transfer-Encoding:quoted-printable or base64.

5. SAMPLE EDI USAGE IN MIME-BASED EMAIL

Actual use of EDI within MIME-based mechanisms requires attention to considerable detail. This section is intended as an example of the gist of the formatting required to encapsulate EDI objects within Internet mail, using MIME. To send a single EDIFACT interchange:

```
To:  <<recipient organization EDI email address>>
Subject:
From: <<sending organization EDI email address>>
Date:
Mime-Version: 1.0
Content-Type: Application/EDIFACT
Content-Transfer-Encoding:  QUOTED-PRINTABLE

<<standard EDIFACT Interchange goes here>>
```

6. REFERENCES

[Bore92] Borenstein, N., and N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, Bellcore, Innosoft, September 1993.

[Brad89] Braden, R., Editor, "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, Internet Engineering Task Force, October 1989.

[Croc82] Crocker, D., "Standard for the Format of Internet Text Messages", STD 11, RFC 822, UDEL, August 1982.

[Rose93] Rose, M., "The Internet Message: Closing the Book with Electronic Mail", PTR Prentice Hall, Englewood Cliffs, N.J., 1993.

[Post82] Postel, J., "Simple Mail Transfer Protocol". STD 10, RFC 821, USC/Information Sciences Institute, August 1982.

[X12V] Data Interchange Standards Association; sets of specific EDI standards are ordered by their version number; Washington D.C.

[X125] ANSI X12.5 Interchange Control Structure for Electronic Data Interchange, Washington D.C.: DISA

[X126] ANSI X12.6 Applications Control Structures for Electronic Data Interchange, Washington D.C.: DISA

[FACT] United Nations Economic Commission (UN/EC) Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT) - Application Level Syntax Rules (ISO 9735), 1991.

[FACV] Version sets contains the specific syntax documents, the element and segment dictionaries, and the transaction/message specifications.

7. SECURITY CONSIDERATIONS

EDI transactions typically include sensitive data, so that transmission often needs to attend to authentication, data integrity, privacy, access control and non-repudiation concerns. This specification permits transmission of such sensitive data via Internet mail and other services which support MIME object encapsulation. For transmission of sensitive data, it is essential that appropriate security services, such as authentication, privacy and/or non-repudiation be provided.

This specification does NOT, itself, provide any security-related mechanisms. As needed and appropriate, such mechanisms MUST be added, either via Internet MIME-based security services or any other services which are appropriate to the user requirements, such as those provided by EDI-based standards.

8. ACKNOWLEDGMENTS

Tom Jones offered introductory text and descriptions of candidate header options. Numerous working group participants provided review and comment, especially Walt Houser, Gail Jackson, and Jim Amster.

9. AUTHOR'S ADDRESS

David H. Crocker
Brandenburg Consulting
675 Spruce Dr.
Sunnyvale, CA 94086 USA

Phone: +1 408 246 8253
Fax: +1 408 249 6205
EMail: dcrocker@mordor.stanford.edu

10. APPENDIX - MIME FOR EDI USERS

To assist those familiar with EDI but not with Internet electronic mail, this Appendix is provided as a very brief introduction, primarily to give pointers to the relevant specifications. This section is in no way intended to be a thorough introduction. An excellent introductory text is [Rose93].

Internet electronic mail follows the classic user agent/mail transfer agent model. In this model, user software produces a standardized object which is transferred via standard exchange protocols.

An Internet electronic mail object comprises a collection of headers, followed by a (possibly structured) body. The headers specify such information as author and recipient addresses, subject summary, creation date, handling node names, and so on, and are defined by RFC822 and RFC1123 [Croc82, Brad89]. If the body is structured, it conforms to the rules of the Multipurpose Internet Message Exchange (MIME) [Bore92]. A structured body may have parts encoded in different text character sets, or even of entirely different types of data, such as voice or graphics.

The Simple Mail Transfer Protocol (SMTP) [Post82, Brad89] performs the primary task of message transmission. User posting and delivery interactions, between the user agent and the message transfer agent, on the same machine, are not standardized and are platform-specific.

An EDI-related use of Internet Mime email will have (at least) the following components:

```
Business Program/Data base -> EDI Translator ->
-> MIME encapsulation -> RFC822 packaging -> mail
submission ->
-> SMTP relaying ->
-> mail delivery -> RFC822 & Mime stripping ->
-> EDI Translator -> Business processing
```

The first and last lines show components normal to all EDI activities, so that it is only the EDI "transmission" components that are replaced with Internet modules.

Clarkson University Department of Mathematics and Computer Science Technical Report number TR-MCS-92-1. April 1992.

[BeMa93] J. Benaloh, M. de Mare, “One-Way Accumulators: A Decentralized Alternative to Digital Signatures (Extended Abstract)”, Proceedings of EuroCrypt `93. Lofthus, Norway. May 1993. ed. by T. Heleseth.

[DEC89] Digital Time Service Functional Specification Version T.1.0.5. Digital Equipment Corporation, 1989.

[EAN-1] EAN: "A guide to security for eancom messages".1997

[EDIINT-1] EDIINT:"Propuesta de implantación de servicios de seguridad a mensajes EDIFACT". March 98

[EDIRA-1] EDIRA: "Memorandum of understanding for the operation of EDI registration authorities".1993

[FIPS186] National Institute of Standards and Technology, “Digital Signature Standard”, U.S. Department of Commerce, May 1994. http://www.nist.gov:80/itl/div897/pubs/fip186.htm

[G.803] ITU-T Recommendation G.803 (6/97) Architectures of transport networks based on the synchronous digital hierarchy (SDH) http://www.itu.int/itudoc/itu-t/rec/g/g800up/g803_23488.html

[G.813] ITU-T Recommendation G.813 (8/96) Timing characteristics of SDH equipment slave clocks (SEC) http://www.itu.int/itudoc/itu-t/rec/g/g800up/g813_36313.html

[G.825] ITU-T Recommendation G.825 (3/93) The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH). http://www.itu.int/itudoc/itu-t/rec/g/g800up/g825_23272.html

[HaKaSt95] S.Haber, B. Kaliski, W. S. Stornetta, “How do Digital Time-Stamps Support Digital Signatures?”, RSA Laboratories’ Cryptobytes Newsletter, Volume 1, Number 3, Autumn 1995. http://www.rsa.com/rsalabs/pubs/cryptobytes/crypto1n3.pdf

[HaSt91a] S. Haber and W.S. Stornetta, “How to Time-Stamp a Digital Document”, Advances in Cryptology - Crypto’90 Proceedings, Springer-Verlag, 1991, pp. 437-455.

[HaSt91b] S. Haber and W.S. Stornetta, “How to Time-Stamp a Digital Document”, Journal of Cryptology, v.3 n.2, 1991, pp. 99-112.

[HaSt92a] S. Haber and W.S. Stornetta, “Digital Document Time-Stamping with Catenate Certificate”, U.S. Patent #5,136,646, 4 Aug. 1992.

[HaSt92b] S. Haber and W.S. Stornetta, “Method for Secure Time-Stamping of Digital Documents”, U.S. Patent #5,136,647, 4 Aug. 1992.

[HaSt94] S. Haber and W.S. Stornetta, “Method of Extending the Validity of a

Cryptographic Certificate”, U.S. Patent #5,373,561, 13 Dec. 1994.

[HaSt95] S. Haber and W.S. Stornetta, “Method for Secure Time-Stamping of Digital Documents”, U.S. Patent #Re 34,954, 30 May 1995.

[ISO 10181-4] ISO/IEC 10181-4:1997, Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Part 4: Non-repudiation framework.
http://www.iso.ch/cate/d23615.html

[ISO 13335] ISO/IEC TR 13335-1:1996, Information technology – Security techniques – Guidelines for the management of IT security (GMITS).
http://www.iso.ch/cate/d21733.html

[ISO 8824] ITU-Rec. X.680/ISO-IEC I.S. 8824-1, "ASN.1: Specification of Basic Notation", 1994.

[magerit] Spanish Ministery for Public Administrations (MAP), 'MAGERIT Versión 1.0 – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información', BOE, 1997.

[PKCS #12] RSA Laboratories, “PKCS #12 – Public Key User Information Syntax Standard”, version 1.0, Apr. 1995.
http://www.rsa.com/rsalabs/pubs/PKCS

[PKCS #6] RSA Laboratories, “PKCS #6 – Extended-Certificate Syntax Standard”, version 1.5, Nov. 1993.
http://www.rsa.com/rsalabs/pubs/PKCS

[PKIX] PKIX Working Group, “Internet Public Key Infrastructure - Part IX.509

http://www.ietf.org/html.charters/pkix-charter.html

[PKITS D3] Architecture of Time-Stamping Service and Scenarios of Use: Service and Features, Deliverable D3 of ETS Project 23.192 Public Key Infrastructure with Time-Stamping Authority, May, 1998.

[PKITS D4] Time-Stamping Service Functional Specification and Protocols for Unstructured Data, Deliverable D4 of ETS Project 23.192 Public Key Infrastructure with Time-Stamping Authority, July, 1998.

[Ray98] Ray, J.R., The IGP/BIPM time transfer project, in 1998 IGS Analysis Center Workshop Proceedings, European Space Operations Centre, Darmstadt, Germany, in press 1998.

[RFC 1305] D.L. Mills, “1305 Network Time Protocol (Version 3) Specification,

ftp://ds.internic.net/rfc/rfc1305.txt

[RFC 1319] B. Kaliski, "The MD2 Message-Digest Algorithm", Apr. 1992.
ftp://ds.internic.net/rfc/rfc1319.txt

[RFC 1320] R. Rivest, "The MD4 Message-Digest Algorithm", Apr. 1992.
ftp://ds.internic.net/rfc/rfc1320.txt

[RFC 1321] R. Rivest, "The MD5 Message-Digest Algorithm", Apr. 1992.
ftp://ds.internic.net/rfc/rfc1321.txt

[RFC 1422] S. Kent, “Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management”. February 1993.
ftp://ds.internic.net/rfc/rfc1422.txt

[RFC 1767] D.Crocker. “MIME encapsulation of EDI objects”, March 1995.
ftp:://ds.internic.net/rfc/rfc1767.txt

[RFC 1847] Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. J. Galvin, S. Murphy, S. Crocker & N. Freed. October 1995.

[RFC 2068] Hypertext Transfer Protocol – HTTP/1.1. R. Fielding et al. January 1997.

[RFC 2311] S/MIME Version 2 Message Specification. S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka. March 1998.

[RFC 2312] S/MIME Version 2 Certificate Handling:. S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein. March 1998.

[RFC 2313] RSA Laboratories, “PKCS #1 - RSA Encryption Standard”, version 1.5, Nov. 1993.
http://www.rsa.com/rsalabs/pubs/PKCS

[RFC 2314] RSA Laboratories, “PKCS #10 – Certification Request Syntax Standard”, version 1.0, Nov. 1993.
http://www.rsa.com/rsalabs/pubs/PKCS

[RFC 2315] RSA Laboratories, “PKCS #7 – Cryptographic Message Syntax Standard”, version 1.5, Nov. 1993.
http://www.rsa.com/rsalabs/pubs/PKCS

[RFC 781] Su, Z. A specification of the Internet protocol (IP) timestamp option. DARPA Network Working Group Report RFC-781. SRI International, May 1981.
ftp://ds.internic.net/rfc/rfc781.txt

[RFC 792] Defense Advanced Research Projects Agency. Internet Control Message Protocol. DARPA Network Working Group Report RFC-792, USC Information Sciences Institute, September 1981.
ftp://ds.internic.net/rfc/rfc792.txt

[RFC 867] Postel, J. Daytime protocol. DARPA Network Working Group Report RFC-867, USC Information Sciences Institute, May 1983.
ftp://ds.internic.net/rfc/rfc867.txt

[RFC 868] Postel, J. “Time protocol. DARPA Network Working Group Report, USC Information Sciences Institute, May 1983.
ftp://ds.internic.net/rfc/rfc868.txt

[RFC 959] File Transfer Protocol. J. Postel, J.K. Reynolds. Oct-01-1985.

[RIPE 95] RIPE Project. Ripe Integrity Primitives: Final Report on Race Integrity Primitives Evaluation; LNCS 1007, Springer-Verlag, 1995.

[Schneier96] B. Schneier, “Applied Cryptography”, 2nd ed. John Wiley & Sons, 1996.

[SJWG 1] SJWG: “EDIFACT CD-9735-1: Application level syntax rules. Part 1: Syntax rules common to all parts, together with syntax service directories for each of the parts.” 1997.

[SJWG 2] SJWG: “EDIFACT CD-9735-2: Application level syntax rules. Part2: Syntax rules specific to batch EDIecurity rules for batch EDI.” 1997.

[SJWG 3] SJWG: “EDIFACT CD-9735-5: Application level syntax rules: Security rules for batch EDI. Part 5: (authenticity, integrity and non-repudiation of origin)”. 1997.

[SJWG 4] SJWG: “EDIFACT CD-9735-6. Application level syntax rules: Part 6: Secure authentication and acknowledgement message (message type AUTACK) ”.

[SJWG 5] SJWG: “Recommendations for UN/EDIFACT message level security from the UN/EDIFACT Security JWG” 1993.

[SJWG 6] SJWG: “TRADE/WP4/R1026: EDIFACT SECURITY IMPLEMENTATION GUIDELINES”. 1994.

[SJWG 7] SJWG: “EDIFACT CD-9735-9. Application level syntax rules: Part 9: Security key and certificate management message (message type KEYMAN) ”.

[SPKI] Internet Engineering Task Force SPKI Working Group. SPKI Specifications.
http://www.ietf.org/html.charters/spki-charter.html

[X.509 v3] ITU Recommendation X.509, “The Directory – Authentication Framework”, version 3, Geneve 1996.
http://www.itu.ch/itudoc/itu-t/rec/x/x500up.html

[X.680] ITU-Rec. X.680/ISO-IEC I.S. 8824-1, "ASN.1: Specification of Basic Notation", 1994.