TeleSeC - a Solution to Implementing Digital Signature in EDI/EDIFACT

P. Fjelbye

Danish Payment Systems Ltd.
10, Lautrupbjerg, DK 2750 Ballerup, Denmark

ABSTRACT

This paper describes a practical and operational implementation of a Digital Signature scheme in a business application (Office Banking Application). The implementation is called TeleSeC.

In Denmark all banks and savings banks will use TeleSeC together with their Office Banking products allowing commercial clients to transfer funds between various account. It is anticipated that in the near future TeleSeC will establish the security standard for communication between clients and the financial infrastructure in Denmark.

This paper focuses on the protocols for administration of keys and certificates in TeleSeC.

Keyword Codes: E3; K.6.5; C.2.2;
Keywords: Data Encryption; Security and protection; Network Protocols;

1. BACKGROUND

TeleSeC was developed during 1990 - 1993 by the members of the Danish Banking Association and PBS (the common ACH of the Danish banks) in co-operation with cryptographic specialists from Cryptomathic Ltd and communication experts from danNet Ltd. The Danish Banking Association represents all banks and savings banks in Denmark.

The largest bank in Denmark, "Den Danske Bank", is now using TeleSeC in it's Office Banking application. The remaining banks and savings banks in the association plan to implement TeleSeC in their Office Banking application within the summer 1995. At that point of time TeleSeC will be established as the security standard for communication between Danish banks and their customers.

TeleSeC is a purely software based cryptosystem with a well-defined application programming interface API, facilitating implementation in almost every software platform imaginable. The development of the cryptographic mechanism is based on available international security standards wherever possible. The Digital Signature capability can be used to secure (end to end) EDIFACT messages and interchanges ref. [1], as well as ordinary file transfers in a point to point communication, independent of the communication protocols used. A combination of

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

symmetric (DES) ref. [2] and asymmetric (RSA) ref. [3,4] security algorithms are applied in TeleSeC in order to provide the security services desired.

Further to the TeleSeC security module the Danish Banking Association and PBS have developed and installed an operational Certification Authority. In Denmark it is called a Key Center (KC). It includes an on-line certificate generation equipment and a full package of instructions, procedures and legal agreements, specifying the entire rules and administration principles of the system. The certification organisation is based on ref. [5], but without the certification path. PBS is appointed as the Key Center for the Danish banks and savings banks and is furthermore responsible for maintenance of the TeleSeC software complex and the related documentation.

Although TeleSeC was developed for the banks in Denmark, the system structure and principles are general enough to easily suit other sectors than banks. TeleSeC is a suitable and practical solution that improves the existing security level for a variety of applications in open networks. An environment where the demand for security measures is still increasing.

2. IMPLEMENTATION CHARACTERISTICS

2.1 Key Mananagement

Each user is responsible for generation of a personal key pair. Upon generation the secret key is immediately stored on a disk, secured by means of DES encryption. A full 64 bit DES key is applied for the purpose. The DES key is derived from the 8 - 16 character password, selected by the user during the key generation. The user transmits the public key to the Registration Authority electronically and writes on a Key Check Form a hash total, derived from the public key. This is forwarded to the Registration Authority in a envelope as well, who compares the electronically forwarded public key with the hash total on paper. If the validation process is completed successfully, the credentials are transmitted to the KC by a secure path, whereupon a certificate is generated and returned to RA. The user receives the certificate at the RA. The secure path is established by means of IBM TSS 4755 or 4753 Cryptographic Adapters, installed in RA's and in the KC. Then RA sends a recommended letter to the user in order to acknowledge the certification. Finally RA sends the Key Check Form to KC which verifies, that the information on the form is identical with the information stored in the certificate.

2.2 EDIFACT

All service messages communicating keys and certificates, as well as data messages and interchanges, which are either secured by digital signatures or encrypted, are implemented based on EDIFACT segments and syntax [6] .

2.3 Independent of communication form

Conversion and filter functions are implemented in TeleSeC which ensure that TeleSeC security services are independent of the chosen communication form.

2.4 TeleSeC on various platforms

TeleSeC is primarily implemented in “C”, which ensures a very high degree of portability. Any platform which can execute C-programs can in principle use TeleSeC. The critical element in using any cryptographic system is the confidentiality of the cryptographic keys. In TeleSeC a client-server implementation based on LU6.2 and APPC is provided allowing TeleSeC to be installed on a dedicated server. Special physical and logical measures can then control the access to the server.

2.5 Multiple signatures

Several business sectors require two or more signatures in order to authorise a given transaction. TeleSeC has implemented a capability allowing users to attach a variable number of signatures to specific transactions.

2.6 Security rules and procedures

The TeleSeC software packages are developed, maintained and distributed in accordance with security rules to development environments and distribution practices. The security rules and instructions are specified in the TeleSeC Handbook.

3. CERTIFICATION HIERARCHY

The certification hierarchy is the organization which supports registration and certification of the users in TeleSeC. It consists of a Key Center and a variable number of Registration Authorities (see fig.1). The Key Center and the connected Registration Authorities constitute the certification organization. Users who want to secure their data communication with TeleSeC register at the Registration Authority and are certified at the Key Center.

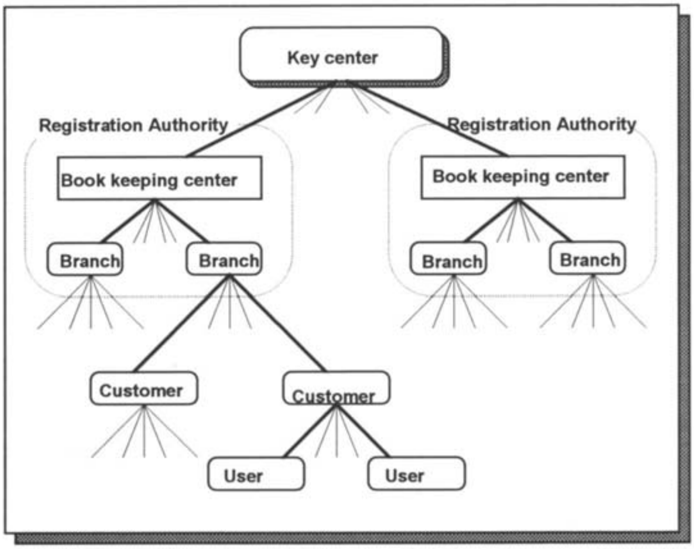

Figure 1: TeleSeC certifying hierarchy

TeleSeC can be distributed to any number of users. The users only use the certifying organization during registration, renewal of keys, and inquiry on and cancellation of certificates. The daily communication can take place between two arbitrary TeleSeC users, but of course also between a user and a Registration Authority. The Registration Authority functions then only as an ordinary TeleSeC user.

3.1 TeleSeC Key Center

The Key Center is the certifying authority, which has the responsibility to certify the TeleSeC users and to administrate the certificates. The Key Center's functions are:

- Production and forwarding of certificates
- Renewal of certificates
- Receipt of revokings of certificates
- Production of list of revoked certificates to Registration Authorities
- Distribution of receipts on inquiries about status of certificates
- Storage of software programs which the Registration Authorities have distributed to the users.
- Distributor of the TeleSeC diskette integrity check program

3.2 TeleSeC Registration Authority

The Registration Authority is the authority which has the responsibility of registration and approval of the TeleSeC users on behalf of the Key Center. The Registration Authority's functions are:

- Registration and approval of the users as TeleSeC users.
- Communication link between a user and the Key Center.
- Distributor of TeleSeC programs to the users.
- Guidance in the use of TeleSeC.

Any number of Registration Authorities can be connected to the TeleSeC Key Center.

3.3 TeleSeC user

The TeleSeC user is the employee who has been authorized to sign transactions on behalf of the organization using TeleSeC. The user's functions are:

- General administration of keys (certificates).
- Securing data transmissions with digital signature and/or encryption.

Any number of TeleSeC users in the certifying organization can be connected.

4. KEY AND CERTIFICATE ADMINISTRATION

In connection with the key- and certificate administration a number of service messages are implemented in TeleSeC. Service messages can be exchanged between 2 TeleSeC users, between a user and the Registration Authority (RA), and between Registration Authorities and the Key Center (KC).

4.1 TeleSeC Service Messages

There are the following service messages:

• DLVAFM	Cancellation list holding all cancelled certificates (KC⇒RA).
• DLVCRD	Delivery of credentials (RA⇒KC).
• DLVCRT	Delivery of certificate (KC⇒RA, RA⇒user, user⇒user)
• DLVPUB	Delivery of public key (user⇒RA).
• FSPCRT	Inquiry for certificate (user⇒RA), RA⇒KC).
• KVTFSP	Receipt on inquiry (KC⇒RA, RA⇒user).
• REQCRT	Request for certificate (user⇒user, user⇒RA, RA⇒KC).
• REQNCT	Request for new certificate (user⇒RA, RA⇒KC).

4.2 TeleSeC functions

A number of high-level 'C' functions are available to the user, the Registration Authority and the Key Center to manage keys- and the certificates.

There are the following functions:

• KEYGEN	RSA key pair generation functions (user/RA/KC)
• OIRCVMSG	General receive function for service messages at RA
• OIENROLL	Function for approval of credentials (RA)
• CARCVMSG	General receiving function for service messages (KC)
• CAVERIFY	Function for verification of issued certificates (KC)
• CACANCEL	Function for cancellation of certificate (KC)
• CACANLST	Function for generating cancellation list (KC)
• USRCVMSG	General receive function for service and data messages (user)
• USRNEWKE	Function for renewal of certificate (RSA key pair) (user)
• BLFSPCRT	Function for enquiry for certificate status (user)
• BLREQCRT	Function for requesting a certificate (user/RA)
• USRSDCRT	Function for forwarding of own certificate (user)

Functions for administration of local TeleSeC information:

• USRNEWPW	Function for changing the user's personal password for secret key encryption.
• ARCXXXXX	A number of functions for administration of database information.

Data message functions

Data messages are used at the usual communication between two users or between a user and the Registration Authority. Three main categories of data messages are applied:

• EDIINT	EDIFACT - interchanges
• EDIMSG	EDIFACT - messages
• NONEDI	Free formatted data (also binary)

This type of messages can be secured in three different ways: signing, encryption, and signing and encryption.

4.3 TeleSeC Scenarios

The following scenarios describe the service message types and functions, which are used in TeleSeC in relation with the key- and certificate administration. Communication between the user and the Key Center is always conducted via the Registration Authority. Consequently, the users only "see" the Registration Authority (the bank) when service messages are communicated to the Key Center. It was an important issue during the design of the protocols that every bank and savings bank was able to profile themselves to their customers.

4.3.1 Registration and Certification of a TeleSeC User

The scenario in figure 2 describes the protocols implemented in order to register and certify a user in the TeleSeC system.

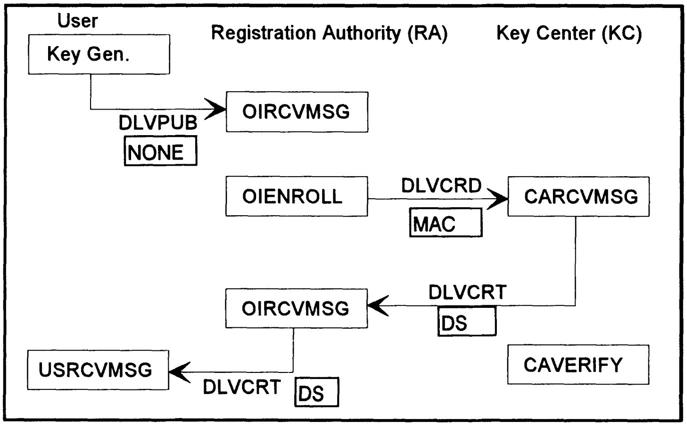

Figure 2: Registration of a TeleSeC user.

MAC: Message Authentication Code DS: Digital Signature

- A User sends *DLVPUB* to RA.
- RA receives *DLVPUB* with the function *OIRCVMSG*. After approval of the user, RA produces a *DLVCRD* by means of the function *OIENROLL*. RA sends *DLVCRD* to KC.
- KC receives *DLVCRD* with the function *CARCVMSG*. KC produces a *DLVCRT*, which is sent to RA.
- RA receives *DLVCRT* with the function *OIRCVMSG* and sends *DLVCRT* on to the user.
- User receives his certificate with *USRCVMSG* and stores it in the archive.

The administrative procedures which support the certification process are not included in the diagram.

4.3.2 Inquiries for certificate(s)

The scenario in figure 3 describes the protocol which allows the user to get the current status of one or several certificates from the Key Center. The receipt to the user is signed by the Key Center.

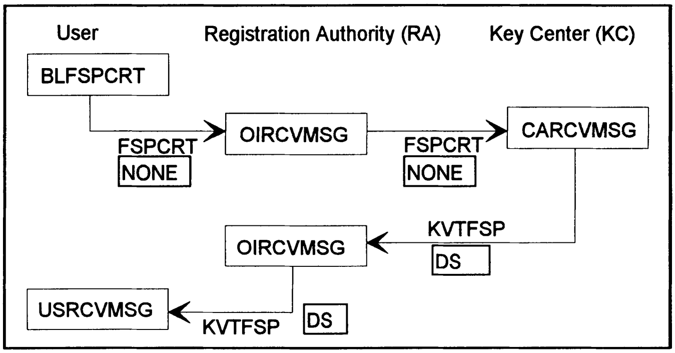

Figure 3: Inquiries of certificate(s).

DS: Digital Signature

- The user produces an inquiry for one or several certificates with the function *BLFSPCRT* which produces a *FSPCRT*. The *FSPCRT* is sent to RA.
- RA receives the message with *OIRCVMSG* and sends *FSPCRT* unchanged on to KC.
- KC receives *FSPCRT* with *CARCVMSG* and produces a *KVTFSP* which is sent to RA.
- RA receives *KVTFSP* with *OIRCVMSG* - and stores the message in the user's mailbox.
- The user receives *KVTFSP* with the function *USRCVMSG.*

4.3.3 Renewal of certificate

This figure describes the protocol which enables a user to renew a certificate.

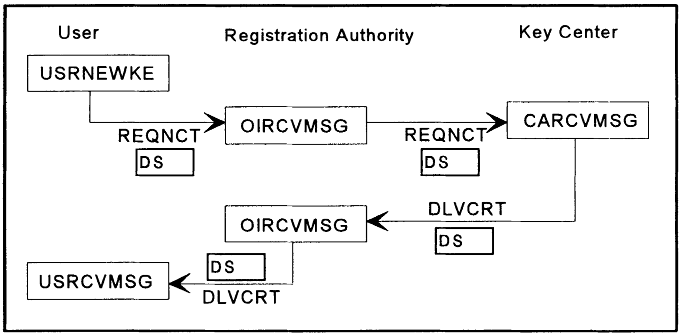

Figure 4: Renewal of certificate

DS: Digital Signature

- A User sends *REQNCT* to RA.
- RA receives *REQNCT* with the function *OIRCVMSG*. RA functions here simply as a switchboard and sends REQNCT further on to KC.
- KC receives *REQNCT* with the function *CARCVMSG* and produces a *DLVCRT*. KC sends *DLVCRT* to RA.
- RA receives *DLVCRT* with the function *OIRCVMSG* and sends *DLVCRT* further on to the user.

- The user receives his certificate with the function *USRCVMSG.*

4.3.4 Request for another user's certificate

This figure describes the protocol which enables a user to get another user's certificate. This would be necessary, if the user wants to encrypt a transmission.

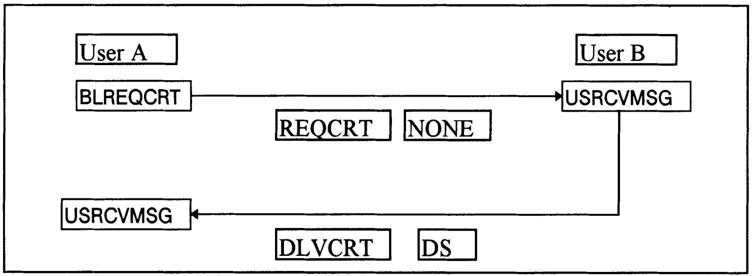

Figure 5: Request for another user's certificate.

DS: Digital Signature

- User A sends *REQCRT* to user B
- User B receives *REQCRT* with the function *USRCVMSG* which produces a *DLVCRT* User B sends *DLVCRT* to user A.
- User A receives the certificate from B with the function *USRCVMSG* that stores the certificate in the archive.

4.3.5 Cancellation of certificate

This diagram describes the certificate cancellation procedures.

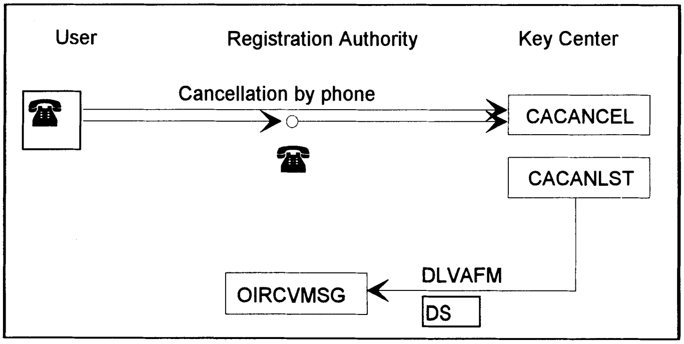

Figure 6: Cancellation of certificate.

- Cancellation of a certificate takes place by phoning the KC or the RA.
- KC carries out the function *CACANCEL,* which cancels the certificate. Subsequently the KC carries out the function *CACANLST,* which produces a *DLVAFM,* that is sent to all RA's.
- The RAs receives *DLVAFM* with the function *OIRCVMSG.*

4.3.6 Data Formats

Service- and data messages are implemented based on ref. [1,6]. Standards on security in EDIFACT were not available during development of TeleSeC. Therefore, the project team developed a scheme on how to implement security services in EDIFACT messages and interchanges without affecting the existing EDIFACT syntax. The result was documented in ref. [1]. The work carried out in UN/EDIFACT Security Joint Working Group is followed and when stable standards are available, they will be integrated in TeleSeC.

An example of the format of one of the service- and data messages in TeleSeC is outlined below:

DLVAFM - Cancellation List

The cancellation list is sent from the Key Center to the Registration Authority when a certificate is canceled at the Key Center. The cancellation list includes all certificates, which are cancelled, but not expired. The cancellation list is secured with the Key Center's signature.

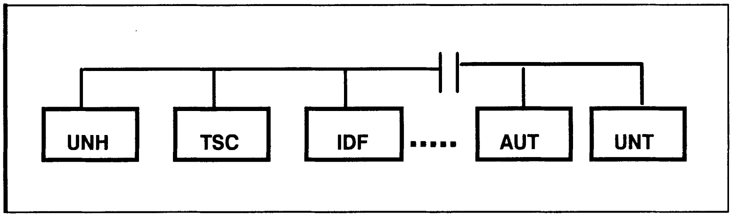

Figure 7: Cancellation List

UNH: Message header
TSC: Security header
IDF: Segment for transmission of user identification, certificate or status of certificate,
AUT: Segment for transmission of the Key Center's signature of the cancellation list.
UNT: Message trailer

SGNMSG - Signed EDIFACT message

The application must ensure that the EDIFACT message contains a TSC, an AUT, and a CER segment before calling TeleSeC. TeleSeC fills these segment with the relevant information during the signing process.

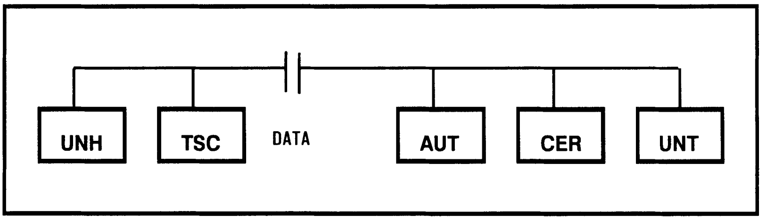

Figure 8: Signature in EDIFACT message

UNH: Message header
TSC: Security header
AUT: Segment for transmission of digital signature

CER: Segment for transmission of certificate
UNT: Message trailer.

5. TELESEC SOFTWARE MODULES

TeleSeC includes a general security module "TeleSeC basis" which is part of the Key Center, the Registration Authority and the user installation. In addition TeleSeC includes a number of modules, which are specific to the installations concerned, for example the database module.

TeleSeC Basis Modules
TeleSeC basis contains the general interface to TeleSeC and the basic security functions. The security functions are grouped in underlying modules, which each carries out logical independent functions (see figure 9).

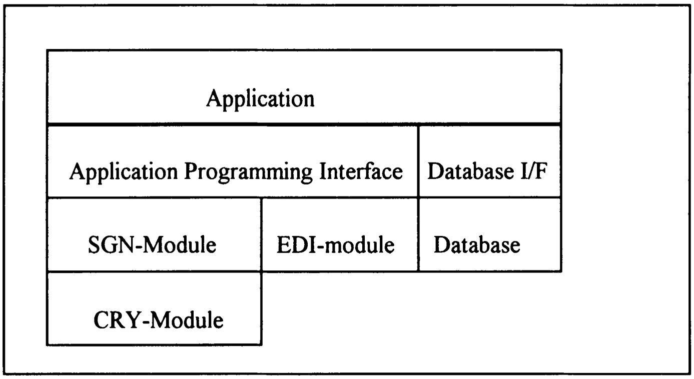

Figure 9: TeleSeC basis modules

The CRY-module
The CRY- module carries out the fundamental cryptographic functions such as:

- Key generation, RSA in accordance to ref. [4].
- Hash value calculation MDC2 in accordance to ref. [3].
- Generation and verification of digital signatures
- Encryption and decryption functions, RSA and DES

Other algorithms such as NIST/SHS: Secure Hash Standard and NIST/DSS: Digital Signature Standard can be incorporated.

The SGN-module
The SGN-module is a superstructure to the CRY-module, which secures a correct use of the cryptographic functions. The module secures among others, that the secret key is deleted from memory after use.

The EDI-module

The module inserts digital signatures in EDIFACT messages and interchanges and encrypts data in accordance with [1].

The module is not an EDIFACT translator (translator of in-house format to EDIFACT), but an EDIFACT security module which can fill out and interpret certain security elements in EDIFACT messages and insert specific security messages in EDIFACT interchanges.

When EDIFACT security standards reach a stable level, they will be included in the EDI-module.

Database Interface

The interface gives the application the possibility of storing, searching and getting:

- TeleSeC messages
- Certificate information

The application can further get information about the latest time of use of the user's secret key. This function can be used, if the user wants to check whether the secret key has been used since the last time, the user received or sent TeleSeC messages.

Furthermore, TeleSeC uses the database internally to store:

- Certificates,
- The user's secret key,
- Index for the message archive
- GREP tables (Reference code tables)
- Replay information

The API Module

The API module constitutes together with the database interface the authorized interface to TeleSeC. Applications apply this interface to get access to TeleSeC.

6. ADMINISTRATIVE PROCEDURES

Every security measure needs a supporting administrative procedure. That is also the case with TeleSeC. In the TeleSeC Handbook all security instructions and procedures are collected. The Key Center and every Registration Authority must obey the rules specified in the TeleSeC Handbook. This ensures that all activities performed by any Registration Authority and the Key Center is conducted in a harmonised and well-defined manner.

Each RA must every year send an auditor's declaration specifying the degree to which the procedures are followed.

7. LEGAL AGREEMENTS

Legal agreements have been specified parallel with the development of TeleSeC. One agreement specifies the obligations and responsibilities to the Key Center and to the

Registration Authorities. Another agreement specifies the obligations and responsibilities to the users. This agreement is tailored to the existing interchange agreement between the bank and its customers.

8. STATUS

All the Danish banks and saving banks have last year announced, that they will integrate TeleSeC in their Office Banking application within the summer 1995. The largest bank in Denmark 'Den Danske Bank" has now used TeleSeC for 15 months in a minor region in Demark. In the next 2- 3 months 'Den Danske Bank" will introduce TeleSeC to all their Office Banking customers.

It is planned to improve TeleSeC by smart cards in order to satisfy those customers who require additional security measures at their premises and those who find that a software solution is insufficient.

REFERENCES

[1] The TEDIS Programme "A proposal concerning the use of Digital Signatures in EDIFACT, Brussels, 29 November, 1990.

[2] Data Encryption Standard FIPS PUB 46 National Bureau of Standards, Washington, DC, 15 January 1977.

[3] ISO/IEC 10118-2:92 Hash function for digital signatures Part 2: Hash Functions using a symmetric block - cipher algorithm.

[4] ISO/IEC 9796:91 "Information technology - Security Techniques - Digital signature scheme giving message recovery (in accordance to annex).

[5] ISO/IEC DIS 9594-8 Information processing systems - Open Systems Interconnection - The Directory - Part 8: Authentication framework.

[6] ISO/IEC 9735 Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules.