

# **Sicherer Elektronischer Meldungsverkehr im Bereich der Finanzinstitute der Schweiz**

Autoren: Armin Müller Dr., Andreas Galle, Paul Sutter, Istvan Teglas  
Datum: Februar 2003  
Version: 1.1

## Change Control

Version	Datum	Initials	New/Changes
0.2	15.3.1999	MUL	1 <sup>st</sup> Draft: Kapitel 1 bis 3
0.4	19.4.1999	MUL	Kapitel 4, update Kapitel 1 bis 3 gemäss Besprechung 1. April 1999
0.9	11.6.1999	MUL	Kapitel 5 und 6, Referenzen, Glossar, update Report gemäss Besprechung 23. April 1999
1.0	18.6.1999	MUL	Überarbeitung gemäss Besprechung 15. Juni 1999.
1.0	26.10.1999	TEG	Überarbeitung gemäss Besprechung 19.10.1999.
1.1	18.02.2003	TEG	Aktualisieren und ergänzen Kapitel „EDIFACT CH“ und „Applikationen im Bankenumfeld Schweiz“, entfernen Beschreibungen zu Swisskey, diverse andere Teilaspekte.

## Inhaltsverzeichnis

<b>1. <u>EINLEITUNG</u></b>	<b>3</b>
<b>2. <u>SICHERHEITSDIENSTE UND -TECHNIKEN</u></b>	<b>4</b>
2.1 GEFAHREN	4
2.2 SICHERHEITSDIENSTE	5
2.3 SICHERHEITSTECHNIKEN	6
<b>3. <u>SICHERHEITSARCHITEKTUREN</u></b>	<b>8</b>
3.1 SCHICHTENMODELL	8
3.2 PROTOKOLLSCHICHTEN UND KOMMUNIKATIONSSICHERHEIT	10
3.2.1 SICHERUNG AUF DER ANWENDUNGSSCHICHT (MELDUNGSSICHERUNG)	10
3.2.2 SICHERUNG AUF DER TRANSPORTSCHICHT	11
3.2.3 SICHERUNG AUF DER NETZWERKSCHICHT	12
3.2.4 SICHERUNG AUF DER VERBINDUNGSSCHICHT	13
3.2.5 ZUSAMMENFASSUNG	14
3.3 WEITERE SICHERHEITSARCHITEKTUREN	14
<b>4. <u>SICHERHEITSLÖSUNGEN</u></b>	<b>15</b>
4.1 MELDUNGSSICHERUNG	15
4.1.1 EDIFACT	15
4.1.2 XML	22
4.1.3 PGP	23
4.1.4 S/MIME	24
4.2 KANALSICHERUNG	25
4.2.1 SECURE SOCKET LAYER (SSL)	25
4.2.2 TRANSPORT LAYER SECURITY (TLS)	26
4.2.3 IP-SICHERUNG UND VPN	26
4.2.4 LEITUNGSVERSCHLÜSSELUNG	27
4.3 HYBRIDLÖSUNGEN	28
4.4 SCHLUSSFOLGERUNGEN	28
<b>5. <u>KEYMANAGEMENT</u></b>	<b>29</b>
5.1 PROBLEMATIK	29
5.2 ZERTIFIKAT UND ZERTIFIZIERUNGS AUTORITÄT	29
<b>6. <u>APPLIKATIONEN IM BANKENUMFELD SCHWEIZ</u></b>	<b>31</b>
<b>7. <u>REFERENZEN</u></b>	<b>33</b>
<b>8. <u>GLOSSAR</u></b>	<b>35</b>

# 1. Einleitung

Kaum ein Bereich hat in den letzten Jahren so dramatische Entwicklungen durchlaufen wie die Informationsverarbeitung. Mit den zunehmenden Möglichkeiten sind die Komplexität der Konzepte und Techniken enorm gewachsen. Dieser Report hat zum Ziel, eine Übersicht über Sicherheitslösungen für das elektronische Banking zu vermitteln. Dazu werden auch die Zusammenhänge zwischen den verschiedenen Sicherheitsdiensten, Sicherheitstechniken und den realisierten Anwendungen aufgezeigt. Das Dokument ist eine reine Beschreibung zum Thema Sicherheit im Bereich des elektronischen Meldungsverkehrs, es hat keinen Weisungscharakter.

Der Report ist in folgende Kapitel gegliedert:

- Kapitel 2 erläutert mögliche Attacken sowie Sicherheitsdienste und die zugehörigen Sicherheitstechniken;
- Kapitel 3 zeigt den allgemeinen Zusammenhang zwischen Protokollschichten und Kommunikationssicherheit auf und soll damit ein tieferes Verständnis für die verschiedenen Sicherheitslösungen erleichtern;
- Kapitel 4 beschreibt verschiedene konkrete Sicherheitslösungen und -standards, wobei die wesentlichen Merkmale jeweils mit einer Tabelle zusammengefasst werden;
- Kapitel 5 weist auf die zunehmende Bedeutung von Zertifikaten und deren Management hin;
- Kapitel 6 enthält eine Übersicht über die Sicherheitsanwendungen in der Schweiz und deren Sicherheitsdienste sowie die zugehörigen Sicherheitstechniken.

Die Einbindung der Sicherheit bei elektronischem Meldungsverkehr auf der Basis von UN-EDIFACT Meldungen ist im Dokument „Recommended practice for message flow and security for edifact payments“ der „UN/EDIFACT Finance Group SWG D6“ beschrieben [Ref. 10].

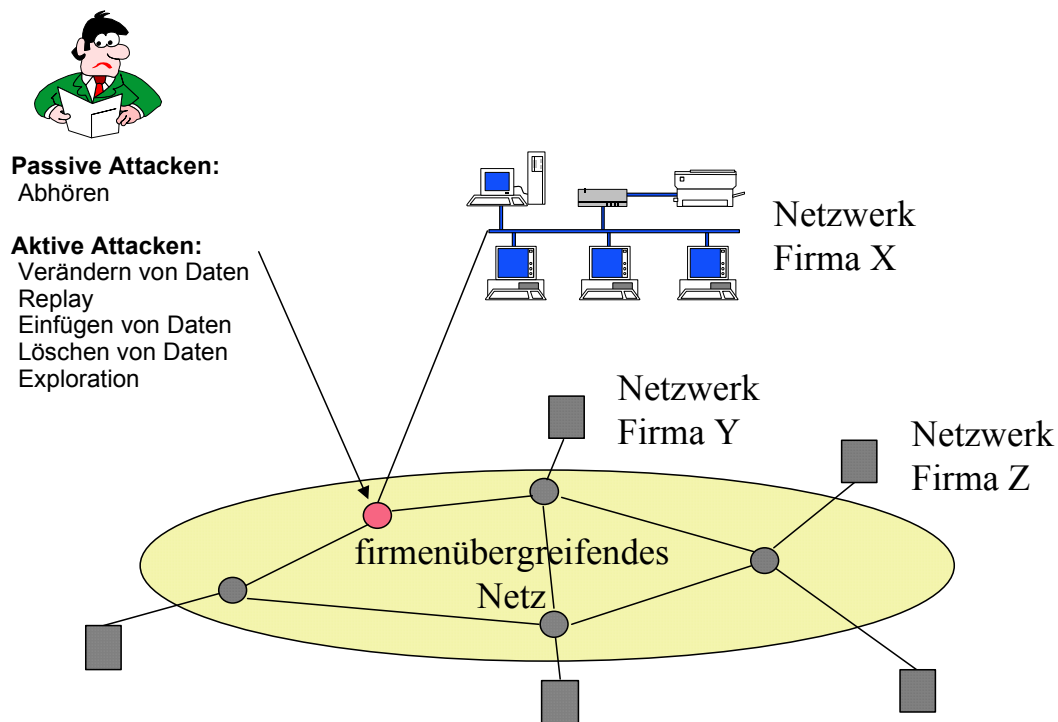
## 2. Sicherheitsdienste und -techniken

### 2.1 Gefahren

Die Sicherheit von Daten ist durch eine Reihe von Attacken gefährdet, insbesondere in Netzwerken (sehen Sie dazu Figur 1). Bei der passiven Attacke werden die zu übertragenden Daten von Unbefugten aufgezeichnet. Damit können z.B. ungesicherte Passwörter und Zahlungsaufträge in fremde Hände gelangen. Bei der aktiven Attacke werden die Daten manipuliert. Es wird z.B. ein Zahlungsauftrag oder die Identifikation eines Absenders verändert. Zu den aktiven Attacken zählen auch die Datenaufzeichnung und die damit mögliche Mehrfacheinreichung (Replay) oder die Exploration von Systemen und deren Daten. Bei der Exploration wird das Computersystem vom Angreifer auf Sicherheitsschwächen untersucht, um die Kontrolle über ein System zu erreichen. Ist ein System unter seiner Kontrolle, so kann er ausgehend von diesem System versuchen, zusätzliche Systeme zu attackieren.

Attacken sind in firmeneigenen und firmenübergreifenden Netzen nicht auszuschliessen, insbesondere wenn ein Anschluss an das globale Internet vorhanden ist.

Daten sind besonders gefährdet während der Übertragung. Aber auch abgespeicherte Daten sind vor Attacken nicht ausgenommen: Unberechtigte können die gespeicherten Daten verändern, löschen, kopieren oder analysieren.



Figur 1: Aktive und passive Attacken als Gefahrenquellen.

## 2.2 Sicherheitsdienste

Für die Kommunikation zwischen Geschäftspartnern bestehen häufig Anforderungen an die Sicherheitsdienste. So ist z.B. bei Finanztransaktionen die Vertraulichkeit der Information zu gewährleisten oder bei einem elektronisch unterschriebenen Vertrag die Nicht-Abstreitbarkeit der Signatur. Sicherheitsanforderungen können auch eine gesetzliche Basis haben (Bankgeheimnis, Datenschutz).

Wir werden uns nun auf die Gewährleistung folgender Sicherheitsdienste konzentrieren:

- **Vertraulichkeit der Daten (Confidentiality):**  
Die Vertraulichkeit verlangt, dass die Daten von Dritten nicht eingesehen werden können. Die Vertraulichkeit der Daten kann für die Übermittlung der Daten und/oder für die Speicherung der Daten gefordert sein.
- **Datenintegrität (Data Integrity):**  
Die Datenintegrität stellt sicher, dass Änderungen an den Daten während der Übermittlung und/oder der Speicherung entdeckt werden bzw. ausgeschlossen werden können.
- **Authentifizierung (Entity Authentication):**  
Die Kenntnis der Identität des Kommunikationspartners (z.B. Geschäftspartners!) ist häufig eine Voraussetzung, sowohl für den Sender wie auch für den Empfänger (gegenseitige Authentifizierung). Bei Mehrparteienprotokollen kann sich diese Anforderung auf alle Kommunikationspartner ausweiten.<sup>1</sup>
- **Nicht-Abstreitbarkeit (Non-Repudiation):**  
Die Nicht-Abstreitbarkeit oder Verbindlichkeit kann sich auf den Sender beziehen und/oder auf den Empfänger:
  - **Nicht-Abstreitbarkeit des Ursprungs (Non-Repudiation of Origin)**  
bezeichnet die Nachweisbarkeit für den Empfänger, dass er die Nachricht tatsächlich vom entsprechenden Sender erhalten hat. Damit ist für den Empfänger gewährleistet, dass der Sender nicht abstreiten kann, dass er die Nachricht geschickt hat.
  - **Nicht-Abstreitbarkeit des Empfangs (Non-Repudiation of Receipt)**  
bezeichnet die Nachweisbarkeit für den Sender, dass die Nachricht tatsächlich vom entsprechenden Empfänger erhalten wurde. Damit ist für den Sender gewährleistet, dass der Empfänger nicht abstreiten kann, dass er die Nachricht erhalten hat. Die Nachweisbarkeit kann auf einer nicht-abstreitbaren Quittungsnachricht basieren, die vom Empfänger an den Sender geschickt wurde.

Eine Voraussetzung für die Nicht-Abstreitbarkeit ist die Authentifizierung des Senders oder Empfängers und die Integrität der Nachricht. Die Sicherheitsdienste

---

<sup>1</sup> In der Praxis kann auch die Anforderung nach Anonymität aufkommen, z.B. bei Kunden, welche eine ähnliche Anonymität wie beim Bargeld wünschen.

Authentifizierung und Integrität sind deshalb in der Nicht-Abstreitbarkeit enthalten (Tabelle 1). Die Vertraulichkeit ist in der Nicht-Abstreitbarkeit nicht enthalten; die Vertraulichkeit kann aber als zusätzlicher Sicherheitsdienst zur Nicht-Abstreitbarkeit hinzukommen.

	Vertraulichkeit	Datenintegrität	Authentifizierung
<b>Nicht-Abstreitbarkeit</b>	N	✓	✓

Tabelle 1: Nicht-Abstreitbarkeit gewährleistet die Datenintegrität und Authentifizierung (N = nicht enthalten, ✓ = enthalten).

## 2.3 Sicherheitstechniken

Zu den oben aufgeführten Sicherheitsdiensten werden untenstehend die entsprechenden kryptographischen Sicherheitstechniken vorgestellt. Mehr Informationen sind in [Ref. 1] enthalten. Die Tabelle 2 fasst die Sicherheitsdienste und die zugehörigen Sicherheitstechniken zusammen.

- Vertraulichkeit der Daten: Verschlüsselung (Encryption)**  
 Die Vertraulichkeit wird gewährleistet, indem die Daten beim Sender verschlüsselt und beim Empfänger entschlüsselt werden. Für die Verschlüsselung werden symmetrische Verschlüsselungsverfahren eingesetzt. Bekannte Verfahren sind IDEA, DES, Triple-DES, CAST und RC2. Die Schlüssellänge sollte 128 Bit oder mehr betragen, damit der Schlüssel nicht mit einer Brute-Force Attacke gebrochen werden kann (bei der Brute-Force Attacke werden alle möglichen Schlüsselvarianten ausprobiert, bis der gesuchte Schlüssel gefunden ist). Exportrestriktionen können den Export von Produkten mit starker Verschlüsselung (128 Bit Schlüssellänge) aus z.B. den USA verbieten.
- Datenintegrität: Berechnung des Hashwerts (Hash Value, Fingerprint, Message Digest, Message Integrity Check)**  
 Der Sender berechnet den Hashwert zu einer Meldung (ähnlich einer Checksum) und übermittelt diesen dem Empfänger zusammen mit der Meldung. Der Empfänger bestimmt seinerseits den Hashwert der empfangenen Daten und vergleicht diesen mit dem vom Sender direkt erhalten Hashwert. Die Integrität der Meldung ist gewährleistet, wenn der berechnete und der empfangene Hashwert identisch sind. Da der Hashwert selbst ungeschützt übermittelt werden kann, werden häufig weitergehende Sicherheitstechniken eingesetzt wie z.B. die digitale Signatur.
- Authentifizierung: Berechnung eines Meldungsursprungswerts (Message Origin Authentication Value)**  
 Der Sender berechnet mit seinem privaten (geheimen) Schlüssel den Meldungsursprungswert und übermittelt diesen dem Empfänger. Der Empfänger prüft seinerseits mit einem entsprechenden Schlüssel (öffentlicher Schlüssel des Senders), ob der empfangene Meldungsursprungswert zur entsprechenden Meldung passt. Die Authentifizierung der Identität des Senders ist gewährleistet, wenn der berechnete und der empfangene Kontrollwert zusammenpassen (entspricht dem TBSS [Ref. 12]).

- Nicht-Abstreitbarkeit des Ursprungs:** Berechnung der digitalen Signatur durch den Sender

Der Sender berechnet mit seinem privaten Schlüssel (asymmetrisches Verschlüsselungsverfahren) die digitale Signatur zu der zu übertragenden Nachricht. Der Empfänger prüft, ob die digitale Signatur zur empfangenen Nachricht passt (der Empfänger kann die Signatur des Senders prüfen, aber nicht selbst erzeugen). Der Empfänger benötigt dazu den öffentlichen Schlüssel (Public Key) des Senders. Da nur der Sender die digitale Signatur erzeugen kann, stellt die digitale Signatur den Beweis dar, dass die Meldung ausschliesslich vom entsprechenden Sender stammt. Damit kann die Nicht-Abstreitbarkeit des Ursprungs der Nachricht gewährleistet werden.
- Nicht-Abstreitbarkeit des Empfangs:** Berechnung der digitalen Signatur durch den Empfänger

Die Nicht-Abstreitbarkeit des Empfangs bedingt eine Quittungsnachricht, die vom Empfänger der zu quittierenden Nachricht an den Sender zurückgeschickt wird. Diese Quittungsnachricht wird vom Empfänger mit seiner digitalen Signatur versehen. Dazu benötigt der Empfänger seinen eigenen privaten Schlüssel. Der Sender prüft, ob die digitale Signatur zur Quittungsnachricht passt. Der Sender benötigt dazu den öffentlichen Schlüssel (Public Key) des Empfängers. Die digitale Signatur der Quittungsnachricht stellt den Beweis dafür dar, dass die Quittungsnachricht ausschliesslich vom entsprechenden Empfänger stammen muss. Mit der digital signierten Quittung kann die Nicht-Abstreitbarkeit des Empfangs der Nachricht gewährleistet werden.

Sicherheitsdienst	Sicherheitstechnik
Vertraulichkeit	Verschlüsselung
Datenintegrität	Berechnung Hashwert
Authentifizierung	Berechnung Meldungsursprungswert
Nicht-Abstreitbarkeit des Ursprungs	Berechnung der digitalen Signatur durch den Sender
Nicht-Abstreitbarkeit des Empfangs	Berechnung der digitalen Signatur durch den Empfänger (Quittungsnachricht)

Tabelle 2: Sicherheitsdienste und anwendbare Sicherheitstechnik.

Bei digitalen Signaturen wird für jede Partei ein Schlüsselpaar mit einem privaten Schlüssel (Private Key) und einem öffentlichen Schlüssel (Public Key) vorausgesetzt. Der private Schlüssel darf unter keinen Umständen einer anderen Partei zugänglich sein, ansonsten kann die Nicht-Abstreitbarkeit nicht mehr gewährleistet werden. Der öffentliche Schlüssel dagegen soll für jedermann verfügbar sein, nämlich zur Überprüfung der digitalen Signatur. Sehen Sie dazu auch Kapitel 5.

## 3. Sicherheitsarchitekturen

### 3.1 Schichtenmodell

Eine Menge von Aufgaben, Funktionen und Leistungen stecken hinter der modernen Datenkommunikation. Wie kann man da einen Überblick gewinnen?

Das OSI-Referenzmodell der Internationalen Standardisierungs-Organisation (ISO) bringt Ordnung in diese Menge. Es ordnet die Aufgaben, Funktionen und Leistungen in sieben Schichten (sehen Sie dazu auch die Tabelle 3):

- Die Anwendungsschicht (Application Layer) ist die oberste Schicht mit der Nummer 7. Sie stellt den verteilt realisierten Anwendungen die logisch-kommunikationstechnische Unterstützung in Form bestimmter Services zur Verfügung wie Electronic Mail (Basis, ohne Oberfläche) und File Transfer. Der Anwendungsprozess selbst befindet sich ausserhalb des Betrachtungsbereichs des Schichtenmodells.
- Die Datendarstellungsschicht (Presentation Layer, Schicht 6) transformiert die Daten auf ein vereinbartes Standardformat und sorgt für eine einheitliche Interpretation (z.B. ASN.1 [Abstract Syntax Notation], Datenkomprimierung). Die Abgrenzung zwischen Schicht 7 und 6 ist oftmals nicht ganz klar, da sie recht stark miteinander verbunden sind (die Applikationsebene impliziert im allgemeinen gewisse Datenstrukturen).
- Die Kommunikationssteuerschicht (Session Layer, Schicht 5) synchronisiert die an der Kommunikation beteiligten Prozesse und enthält u.a. die Dienste für die Session-Daten-Transfer-Kontrolle.  
Die Schichten 5 bis 7 arbeiten applikationsbezogen und haben deshalb einen *Ende-zu-Ende-Charakter auf der Applikationsebene*.
- Mit der Schicht 4 (Transport Layer) wird der benachbarten Schicht 5 ein universeller Ende-zu-Ende-Transportdienst zwischen zwei kommunizierenden Stationen zur Verfügung gestellt. Die Transportschicht befreit die obere Schicht von der Bestimmung des optimalen Weges, der Flusskontrolle, Überlastkontrolle und der Fehlerkorrektur auf tiefem Niveau.  
Die Schicht 4 hat einen *Ende-zu-Ende-Charakter auf der Workstationebene* und nicht mehr auf der Applikationsebene. Die Dienste der Transportschicht können von verschiedensten Applikationen genutzt werden. Die Schicht 4 gehört zusammen mit den darunterliegenden Schichten zu den transportorientierten Schichten.
- Die Vermittlungsschicht (Network Layer, Schicht 3) hat als wichtigste Aufgabe das Routing zu übernehmen, d.h. die Bestimmung des optimalen Weges durch ein eventuell verzweigtes Netzwerk.
- Die Sicherungsschicht (Link Layer, Schicht 2) enthält meist eine Sicherungsfunktion, indem sie Daten in Paketform überträgt und dabei elementare fehlererkennende und -korrigierende Funktionen übernimmt. Die Sicherungsschicht betrachtet bei Netzwerken im wesentlichen Zweipunktverbindungen und nicht Ende-zu-Ende-Verbindungen zwischen den kommunizierenden Workstations.

- Die Schicht 1 (Physical Layer) ist die Bitübertragungsschicht. Hier werden die Methoden der Übertragung und Bedeutung der einzelnen Bits festgelegt.

Schicht	Name	Beispiel	Verbindungscharakter
7	Anwendungsschicht (Application Layer)	SMTP, FTP, Telnet	Ende-zu-Ende-Charakter auf Applikationsebene
6	Datendarstellungsschicht (Presentation Layer)	ASN.1	
5	Kommunikationssteuerschicht (Session Layer)		
4	Transportschicht (Transport Layer)	TCP	Ende-zu-Ende-Charakter auf Workstationebene (z.B. PC)
3	Vermittlungsschicht (Network Layer)	IP	transportorientierte Schichten
2	Verbindungssicherungsschicht (Link Layer)	Ethernet, FDDI, PPP, X.25	
1	Bitübertragungsschicht (Physical Layer)		

Tabelle 3: Schichten des OSI-Referenzmodells.

Die Schichten können ganz unterschiedlich realisiert und implementiert sein. Die Funktionen von einzelnen Schichten können durch andere Realisierungen ersetzt werden. Wichtig ist dabei einzig, dass die Schnittstellenbeschreibungen zu den darüber- und daruntergelegenen Schichten eingehalten werden.

## 3.2 Protokollschichten und Kommunikationssicherheit

Das Schichtenmodell hilft uns nun, die verschiedenen Sicherheitslösungen besser einzuordnen und die Eigenschaften in einem grösseren Rahmen zu verstehen.

### 3.2.1 Sicherung auf der Anwendungsschicht (Meldungssicherung)

Bei der Sicherung auf der Anwendungsschicht werden die *einzelnen Meldungen* (z.B. Email [S/MIME, PGP], EDIFACT Nachrichten, sehen Sie dazu Kapitel 4.1) vom Anwendungsprozess vor der Übertragung gesichert (sehen Sie dazu bitte die untenstehende Figur). Das Resultat ist eine *Ende-zu-Ende Sicherung auf der Applikationsebene* ('Writer-to-Reader Security'). Die Meldungen können mit allen in Kapitel 2.2 beschriebenen Sicherheitsdiensten gesichert sein. *Die Nicht-Abstreitbarkeit ist nur mit der Sicherung auf der Anwendungsschicht realisierbar.*

Bei der Sicherung auf der Anwendungsebene werden in der Regel die Meldungen beim Empfänger erst bei Bedarf entschlüsselt und/oder die Integrität und/oder die Signatur geprüft. Bis zu diesem Zeitpunkt *bleiben die Daten auf dem Computersystem des Empfängers gesichert, insbesondere verschlüsselt.*

Der Nachteil der Sicherung auf der Anwendungsschicht ist, dass die Sicherheitsdienste für jede Applikation separat implementiert werden müssen, was erheblichen Aufwand bedeuten kann. Die Umsetzung der Sicherheitsdienste erfolgt für das Netz transparent.

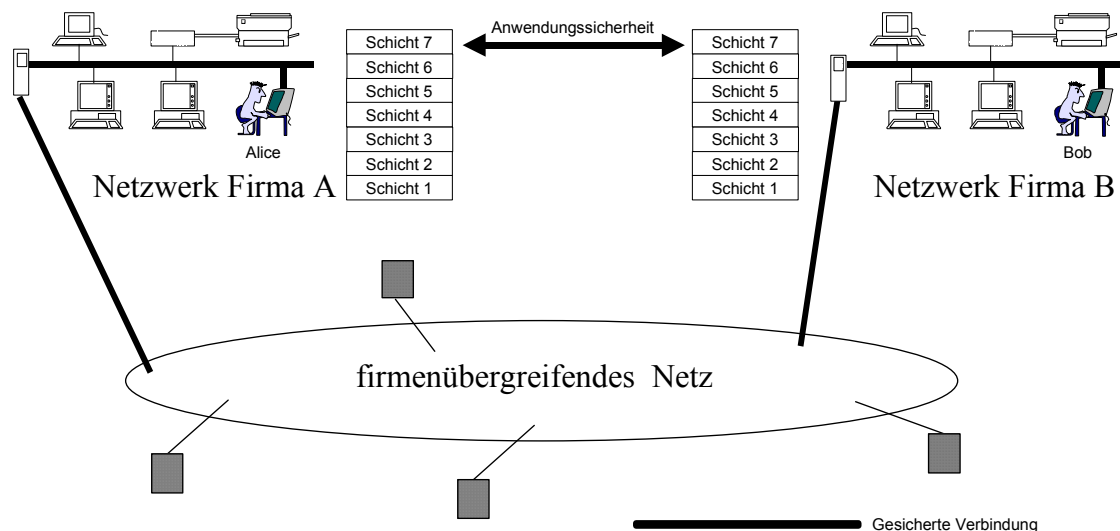


Figure 2: Ende-zu-Ende Sicherung auf der Anwendungsebene zwischen Alice und Bob.

### 3.2.2 Sicherung auf der Transportschicht

Die Sicherheitsdienste werden hier auf der Transportschicht realisiert (z.B. mit Secure Socket Layer [SSL], sehen Sie dazu Kapitel 4.2.1). Es wird ein sicherer Kanal auf der Ebene der Transportschicht aufgebaut, der eine *Ende-zu-Ende Sicherung auf der Workstationebene* darstellt (sehen Sie dazu bitte die untenstehende Figur). Der sichere Kanal kann von verschiedenen darüberliegenden Applikationen genutzt werden.

Da die Transportschicht die einzelnen Meldungen der Applikationsebene nicht mehr erkennen kann, ist die Nicht-Abstreitbarkeit des Empfangs einer Meldung mit der Sicherung der Transportschicht nicht realisierbar, wohl aber die Vertraulichkeit, Datenintegrität und die Authentifizierung von Sender und Empfänger. Bei der Sicherung auf der Transportschicht werden die Daten *ungesichert* auf die Computersysteme abgelegt, d.h. *unverschlüsselt*.

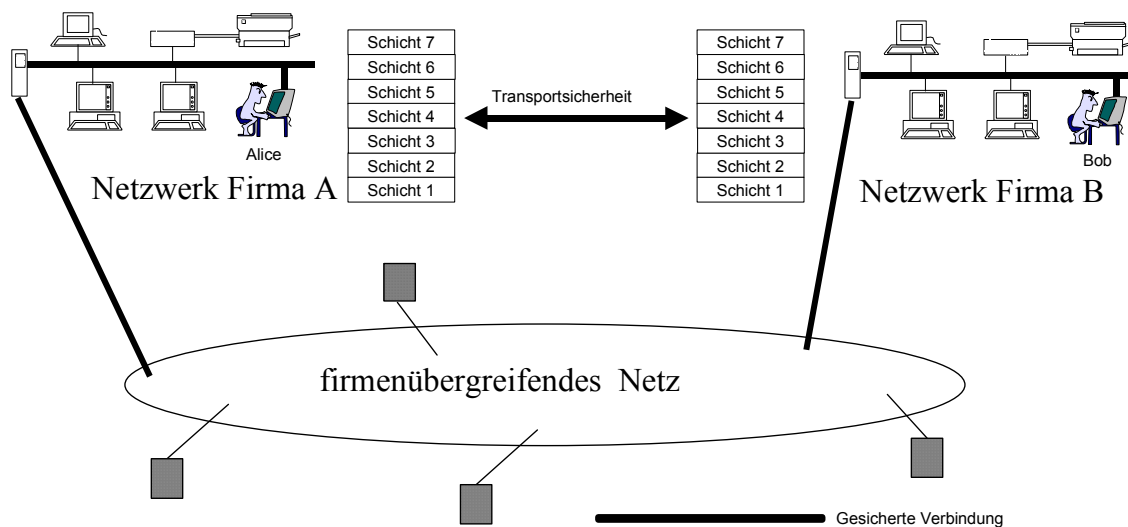
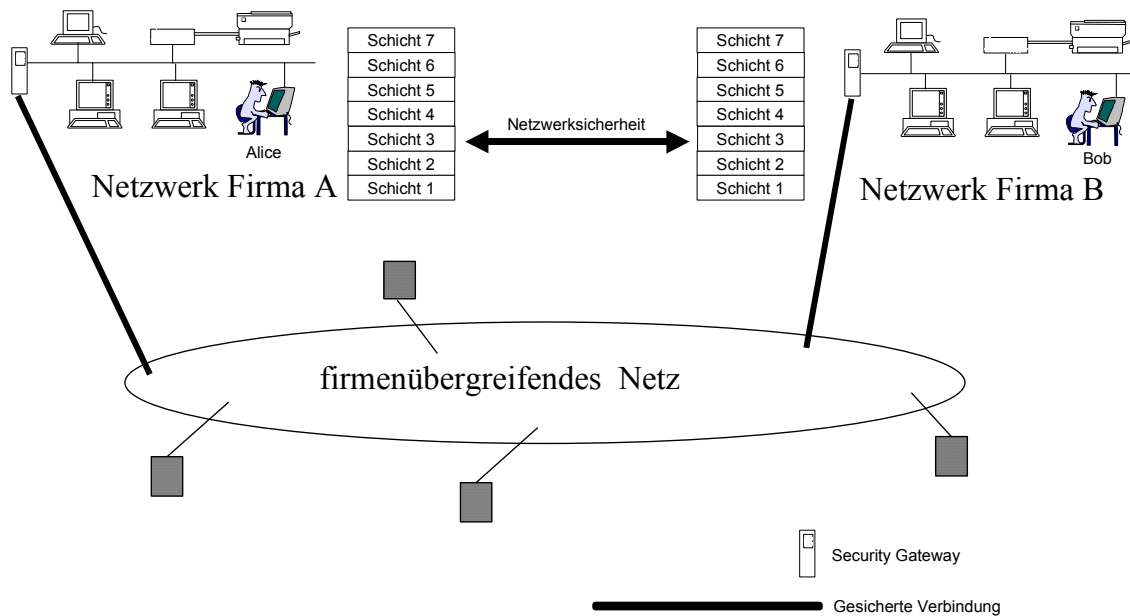


Figure 3: Ende-zu-Ende Sicherung auf der Workstationebene (Schicht 4) zwischen Alice und Bob.

### 3.2.3 Sicherung auf der Netzwerkschicht

Die Sicherung auf der Netzwerkschicht (Vermittlungsschicht oder Network Layer, sehen Sie dazu auch Kapitel 4.2.3) erfolgt häufig mit Sicherheits-Gateways, die zwischen zwei Netzwerken eingesetzt werden. Zwischen den Sicherheits-Gateways werden die einzelnen Übertragungspakete (z.B. IP Datagrams) gesichert. Das Resultat ist ein Virtual Private Network [VPN]. Es resultiert ein sicherer Kanal zwischen den kommunizierenden Sicherheits-Gateways, d.h. eine *Ende-zu-Ende Sicherung zwischen den Gateways*.

Bei der Sicherung auf der Netzwerkschicht sind *alle auf der Schicht 3 aufsetzenden Anwendungen gesichert*, auch wenn die Kommunikation über mehrere Zwischenknoten läuft (z.B. über das Internet). Die Sicherung bezieht sich aber nur auf die Verbindung *zwischen* den Sicherheits-Gateways. Da die Netzwerkschicht die einzelnen Meldungen der Applikationsebene nicht mehr erkennen kann, ist die Nicht-Abstreitbarkeit des Empfangs einer Meldung mit der Netzwerksicherheit nicht realisierbar, wohl aber die Vertraulichkeit, Datenintegrität und Authentifizierung (der Sicherheits-Gateways, nicht der Endbenutzer). Bei der Sicherung auf der Netzwerkschicht werden die Daten *unverschlüsselt* auf dem firmeneigenen Netzwerk übertragen (Netzwerk Firma A und Netzwerk Firma B in untenstehender Figur) und auch unverschlüsselt auf die Computersysteme abgelegt.

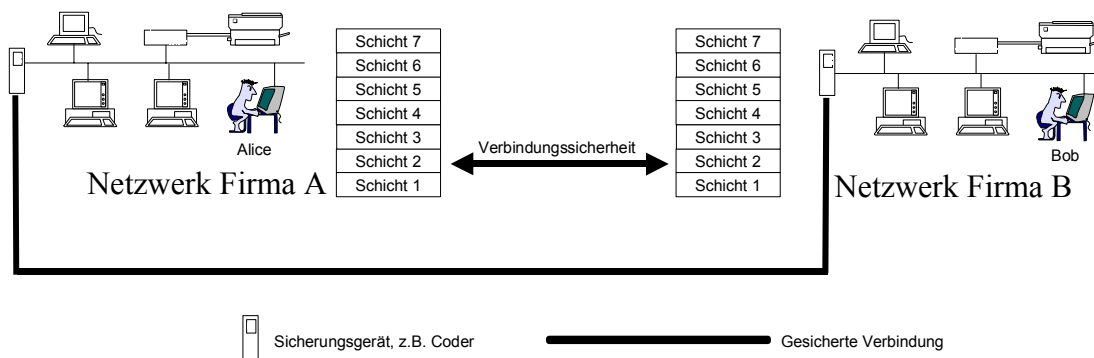


Figur 4: Sicherung auf der Netzwerkschicht: Ende-zu-Ende Sicherung auf der Ebene der Security-Gateways.

### 3.2.4 Sicherung auf der Verbindungsschicht

Die Sicherung auf der Schicht 2 wird üblicherweise zwischen zwei Netzwerken mit Sicherungsgeräten realisiert (z.B. Gretacodern mit Chiffrierboxen, sehen Sie dazu auch Kapitel 4.2.4), wobei zwischen den Netzwerken keine weiteren Knoten liegen. *Alle Applikationen werden gesichert, welche über dieser Schicht 2 liegen.* Die auf diese Weise erreichte Konfiguration kann so betrachtet werden, als ob die einzelnen Organisationseinheiten unmittelbar nebeneinander stehen würden.

Da bei der Sicherung der Verbindungsschicht die einzelnen Meldungen der Applikationsebene nicht mehr erkennbar sind, ist die Nicht-Abstreitbarkeit des Empfangs einer Meldung und die Authentifizierung von Sender und Empfänger (Alice und Bob) mit der Verbindungssicherheit nicht realisierbar, wohl aber die Vertraulichkeit. Bei der Sicherheit auf der Verbindungsschicht werden die Daten wohl gesichert übertragen, aber nur *zwischen* den Sicherungsgeräten. Das hat zur Folge, dass die Daten *unverschlüsselt* auf dem firmeneigenen Netzwerk (Netzwerk Firma A und Netzwerk Firma B in untenstehender Figur) übertragen werden und auch unverschlüsselt auf die Computersysteme abgelegt werden.



Figur 5: Sicherung auf der Verbindungsschicht: Ende-zu-Ende Sicherheit auf der Ebene der Sicherungsgeräte (Coder).

### 3.2.5 Zusammenfassung

Die nachfolgende Tabelle 4 fasst die Zusammenhänge zwischen Protokollschichten und Kommunikationssicherheit zusammen.

Schicht	Name	Ende-zu-Ende Sicherung auf der Ebene von	Meldungs-/Kanal- sicherung	Verschlüsselung	Datenintegrität	Authentifizierung	Nicht-Abstreitbarkeit
7	Anwendungs- schicht	Applikation	Meldungssicherung	✓	✓	✓	✓
6	Datendarstellungs- schicht						
5	Kommunikations- steuerschicht						
4	Transportschicht	Workstation	Kanalsicherung	✓	✓	✓	N
3	Vermittlungs- schicht	Sicherheits- Gateways					
2	Verbindungs- sicherungsschicht	Sicherungs- geräte (Coder)					
1	Bitübertragungs- schicht						

Tabelle 4: Protokollschichten und Kommunikationssicherheit (✓ = möglich, N = nicht möglich).

### 3.3 Weitere Sicherheitsarchitekturen

Wir haben bisher die Realisierung von Sicherheit *in einer einzigen Schicht* betrachtet. Es sind aber auch Kombinationen möglich. Es ist denkbar, dass z.B. die Meldung auf Applikationsebene mit einer digitalen Signatur gesichert wird und auf der Netzwerkebene mit Verschlüsselung.

## 4. Sicherheitslösungen

In diesem Kapitel werden nun konkrete Realisierungen und Standards für Sicherheitslösungen beschrieben und charakterisiert. Bei Sicherheitslösungen steht im allgemeinen nicht eine maximale Sicherheit im Vordergrund, sondern eine optimale Sicherheit bezogen auf die spezifischen Anforderungen. Aus diesem Grunde sind unterschiedlichste Sicherheitslösungen realisiert worden.

### 4.1 Meldungssicherung

Bei der Meldungssicherung werden die einzelnen Meldungen zuerst gesichert (z.B. digital unterschrieben und verschlüsselt) und erst danach übertragen (Kapitel 3.2.1). Als konkrete Beispiele für die Meldungssicherung werden in den folgenden Kapiteln EDIFACT und sichere Email-Systeme beschrieben.

#### 4.1.1 EDIFACT

EDIFACT dient dem Austausch von Geschäftsdaten, Bestellungen, Rechnungen und der Abwicklung von Finanztransaktionen. Bei EDIFACT werden die Meldungen ausgetauscht und *weiterverarbeitet*, z.B. werden vom Finanzinstitut entsprechende Finanztransaktionen ausgelöst. Bei EDIFACT müssen deshalb die Meldungen eine bestimmte Struktur aufweisen (nicht aber bei Email, wo der unstrukturierte Dokumentenaustausch im Vordergrund steht).

##### 4.1.1.1 EDIFACT Syntax-Version 3

Heute wird die EDIFACT Syntax-Version 3 (ISO 9735) auf breiter Basis eingesetzt. Sehr strikt betrachtet, unterstützt die Syntax-Version 3 gemäss dem ISO-Standard keine Sicherheitsdienste, d.h. keine Vertraulichkeit, keine Datenintegrität, keine Authentifizierung und keine Nicht-Abstreitbarkeit. Werden aber die UN Directories zum Standard hinzugezählt, so steht für die Sicherheit ein AUT-Segment zur Verfügung [Ref. 4]. Das AUT-Segment ermöglicht die Berechnung eines Datenintegritätswerts, wobei der verwendete Algorithmus mit einem Authentisierungsschlüssel aktiviert wird. Der Aktivierungskey ist ein symmetrischen Schlüssel, der sowohl dem Sender wie auch dem Empfänger bekannt ist. Mit dem AUT-Segment kann die Datenintegrität gewährleistet werden, sowie eine (nicht strenge) Authentifizierung. Wir haben damit bei der EDIFACT Syntax-Version 3 die Sicherheitsmerkmale gemäss nachfolgender Tabelle:

Sicherheitsmerkmal	EDIFACT Syntax-Version 3
Vertraulichkeit	N
Datenintegrität	✓
Authentifizierung	(✓)
Nicht-Abstreitbarkeit des Ursprungs	N
Nicht-Abstreitbarkeit des Empfangs	N
Ende-zu-Ende Sicherheit	Applikationsebene
Key Management	symmetrische Schlüssel für AUT

Tabelle 5: Sicherheitsmerkmale bei EDIFACT Syntax-Version 3; ✓ = möglich, (✓) = nicht strenge Authentifizierung, N = nicht möglich).

#### 4.1.1.2 EDIFACT Syntax-Version 4

Die EDIFACT Syntax-Version 4 (ISO 9735) wurde kürzlich verabschiedet und steht als Standard zur Verfügung (genauer: Part 1 bis 6 sowie Part 8 und 9 wurden standardisiert, nicht aber Part 7, der die Vertraulichkeit betrifft). Die Syntax-Version 4 definiert Konstruktionen, welche die Sicherheitsdienste Vertraulichkeit, Datenintegrität, Authentifizierung sowie Nicht-Abstreitbarkeit des Ursprungs und des Empfangs unterstützen. Die Sicherheit wird für die verschiedenen Dienste mit ähnlichen Konstruktionen realisiert, welche je eine Segmentgruppe für einen Security-Header und einen Security-Trailer einschliessen. Für die Authentifizierung können EDIFACT-Zertifikate eingesetzt werden. Für das Keymanagement spezifiziert EDIFACT eine spezielle Nachricht, die KEYMAN [Ref. 5].

##### 4.1.1.2.1 Verschlüsselung

Eine EDIFACT Struktur kann verschlüsselt werden, indem die zu verschlüsselnde Struktur in ein USD (Data Encryption Header) und USU (Data Encryption Trailer) Segmentpaar eingeschlossen wird [Ref. 6]. Es können damit Meldungen, Pakete, Gruppen und Interchanges gesichert werden. Die zu verschlüsselnden Daten können optional vor der Verschlüsselung komprimiert werden. Vor der Übertragung der verschlüsselten Daten werden diese je nach Anforderung noch gefiltert.

#### 4.1.1.2.2 Security Header/Trailer

Security Header/Trailer [Ref. 7] kann EDIFACT Konstruktionen (Meldungen, Pakete, Gruppen und Interchanges) sichern bezüglich Authentifizierung, Datenintegrität und Nicht- Abstreitbarkeit des Ursprungs. Die EDIFACT Konstruktionen werden gesichert, indem zusätzliche Segmente eingebaut werden. Z.B. kann eine digitale Signatur für die Nicht-Abstreitbarkeit des Ursprungs mittels Security Header/Trailer zur EDIFACT Meldung hinzugefügt werden (sehen Sie dazu die nachfolgende Figur):

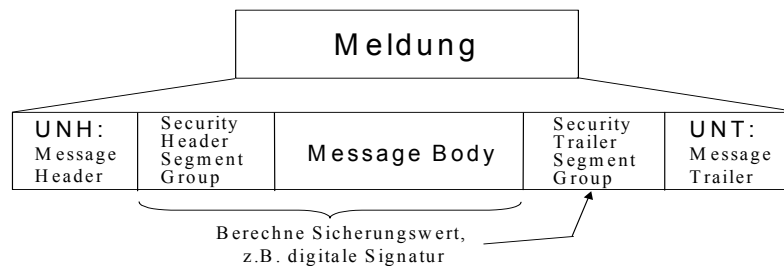


Figure 6: Beispiel einer Meldung gesichert mit Security Header/Trailer.

Security Header/Trailer lässt die mehrfache Sicherung von EDIFACT Konstruktionen zu (mit bis zu 99 Signaturen). Die Sicherungswerte können dabei voneinander unabhängig oder abhängig sein. Bei abhängigen Unterschriften kann einer ersten Signatur von Person A eine zweite Unterschrift von Person B hinzugefügt werden, so dass mit der Signatur von B die bereits vorhandene Signatur von A mituntersrieben wird. Ein Szenario wäre der Service eines Notars (Person B), der mit seiner Unterschrift bezeugt, dass die Person A eine Meldung tatsächlich unterschrieben und abgeschickt hat.

Bei der Sicherung mit Security Header/Trailer werden die Sicherheitselemente in den ursprünglichen Interchange eingebaut (bei der AUTACK ist dies nicht zwingend).

#### 4.1.1.2.3 AUTACK

Die AUTACK Meldung kann die Sicherheitsdienste Datenintegrität, Authentifizierung und Nicht-Abstreitbarkeit des Ursprungs und/oder Nicht-Abstreitbarkeit des Empfangs gewährleisten [Ref. 8]. Die Sicherung kann sich auf Meldungen, Pakete, Gruppen oder Interchanges beziehen. Die Sicherung eines Interchanges mit einer AUTACK Meldung wird mit der untenstehenden Figur dargestellt.

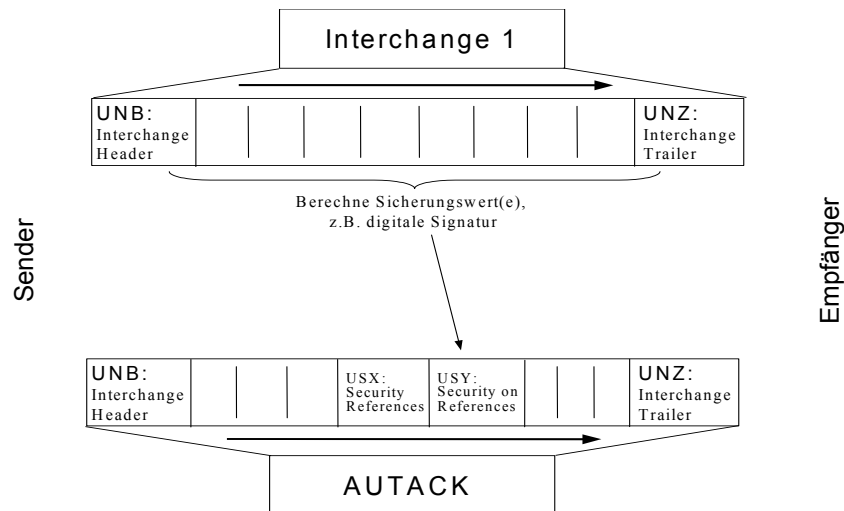


Figure 7: Beispiel AUTACK für die Sicherung eines Interchanges.

Die AUTACK Meldung *kann separat* von den gesicherten EDIFACT Strukturen übermittelt werden und eignet sich deshalb auch als *Quittungsnachricht* für die Nicht-Abstreitbarkeit des Empfangs. Eine Quittungsnachricht setzt voraus, dass zuvor eine gesicherte Nachricht erhalten wurde (gesichert mit AUTACK oder Security Header/Trailer). Die nachfolgende Figur stellt eine AUTACK als Quittungsnachricht auf eine Meldung gesichert mit Security Header/Trailer dar:

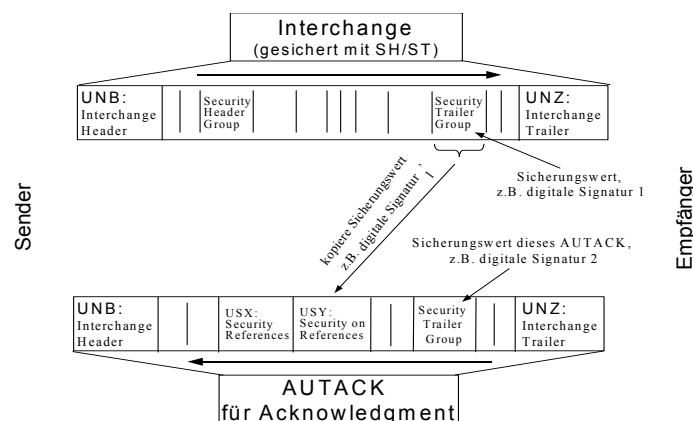


Figure 8: Beispiel einer AUTACK als Quittungsnachricht.

Wie bei Security Header/Trailer sind bei der Verwendung der AUTACK mehrere Sicherungswerte zugelassen. Die Sicherungswerte (z.B. Unterschriften) können wieder abhängig oder voneinander unabhängig sein.

#### 4.1.1.2.4 Key Management

Die für das Keymanagement spezifizierte EDIFACT Nachricht KEYMAN [Ref. 5] soll gemäss ISO9735-9 zwischen den beteiligten Partnern für „requests“ und „deliveries or notices“ verwendet werden

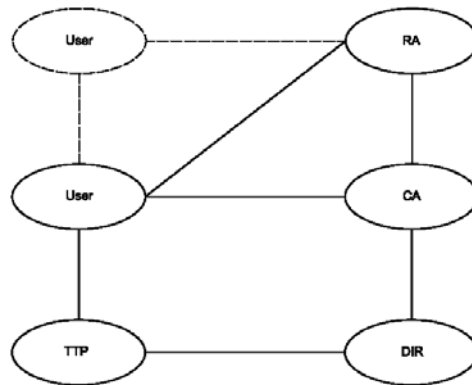


Figure 9: Am Key Management beteiligte Parteien

(Diese Szenarien sind heute nicht implementiert, der KEYMAN wird für den bilateralen Austausch von public Keys verwendet.)

#### 4.1.1.2.5 Zusammenfassung

Die EDIFACT Syntax-Version 4 bietet Konstruktionen für die Vertraulichkeit, Datenintegrität, Authentifizierung sowie Nicht-Abstreitbarkeit des Ursprungs und Nicht-Abstreitbarkeit des Empfangs. Dabei können die verschiedenen Konstruktionen auch kombiniert werden. So kann z.B. eine signierte Nachricht verschlüsselt übertragen werden.

Der Standard ISO 9735 lässt sehr komplexe Konstruktionen zu (bis zu 99 verschachtelte Verschlüsselungen und Unterschriften, wobei unterschiedlichste Algorithmen zulässig sind). Daher werden Implementation Guidelines spezifiziert, welche die Details der Nutzung genau festlegen und damit den Implementierungsaufwand in Grenzen halten. Die nachfolgende Tabelle fasst die Sicherheitsmerkmale der EDIFACT Syntax-Version 4 zusammen:

Sicherheitsmerkmal	EDIFACT Syntax-Version 4
Vertraulichkeit	✓
Datenintegrität	✓ (SH/ST oder AUTACK)
Authentifizierung	✓ (SH/ST oder AUTACK)
Nicht-Abstreitbarkeit des Ursprungs	✓ (SH/ST oder AUTACK)
Nicht-Abstreitbarkeit des Empfangs	✓ (nur AUTACK)
Ende-zu-Ende Sicherheit	Applikationsebene
Key Management	Einsatz der Meldung KEYMAN in definierten Szenarien

Tabelle 6: Sicherheitsmerkmale bei EDIFACT Syntax-Version 4 (SH/ST = Security Header/Trailer).

#### **4.1.1.3 EDIFACT CH**

In der Schweiz werden verschiedene Sicherheitsdienste für EDIFACT genutzt. So wird auf der Basis der Syntax-Version 3 das AUT-Segment seit 1992 für die Sicherung von Transaktionen zwischen Kunden und Finanzinstituten eingesetzt. Security Header/Trailer und CIPHER werden in der Praxis ebenfalls von mehreren Applikationen genutzt (sehen Sie dazu bitte auch Kapitel 6).

##### **4.1.1.3.1 AUT**

Das AUT-Segment wird gemäss Kapitel 4.1.1.1 verwendet [Ref. 4].

##### **4.1.1.3.2 CIPHER**

Damit die Vertraulichkeit innerhalb der Syntax-Version 3 möglich ist, wurde eine CIPHER-Meldung definiert [Ref. 9]. Sie enthält eine Segmentgruppe für einen Security-Header und einen Security-Trailer und ist damit gleich aufgebaut wie die Sicherheitskonstrukte der Syntax-Version 4. Die CIPHER-Meldung ermöglicht einen ganzen Interchange zu verschlüsseln (und zu komprimieren sowie zu filtern). Die verschlüsselten Daten werden in USM-Segmente von je 512 Bytes verpackt. Damit werden die strengen Syntaxregeln der Version 3 respektiert. Eine zweite ebenfalls im Einsatz befindliche Lösung verwendet statt den USM-Segmenten (mit je 512 Bytes der verschlüsselten Daten pro USM-Segment) die Segmente USD/USU analog ISO9735-7. Hier befinden sich die verschlüsselten Daten in einem Block zwischen den Segmenten USD und USU.

Für die Verschlüsselung existiert auch eine CONFID-Meldung. Diese wird aber im Bankenumfeld zur Zeit nicht eingesetzt.

##### **4.1.1.3.3 Security Header/Trailer**

Die Technik mit Security Header/Trailer ermöglicht den Sicherheitsdienst der Nicht-Abstreitbarkeit des Ursprungs. Dabei wird die Technik des Security Header/Trailer der Syntax-Version 4 (Kapitel 4.1.1.2.2) in die Syntax-Version 3 abgebildet. Die Nutzung von Security Header/Trailer innerhalb der Version 3 ist auf Meldungen beschränkt. Security Header/Trailer ist bei PayNet bzw. BSP/CSP mit Kunden und Rechnungsteller im Einsatz, ausserdem bei der SIC im Bereich Interbanksicherheit.

#### 4.1.1.3.4 AUTACK

Der AUTACK wird von einzelnen Finanzinstituten als „Embedded AUTACK“ verwendet für den Transport der digitalen Signatur der mitgelieferten Zahlungen (Dienst NRO). Hierbei wird zunächst über das zu Sichernde Interchange (bzw. über deren Meldungen, vom ersten UNH bis zum letzten UNT) ein Hashwert gerechnet und mit den entsprechenden Informationen in einer AUTACK Meldung abgelegt. Diese AUTACK Meldung wird anschliessend signiert gemäss Security Header / Trailer Ansatz und im gleichen Interchange wie die Meldungen angefügt.

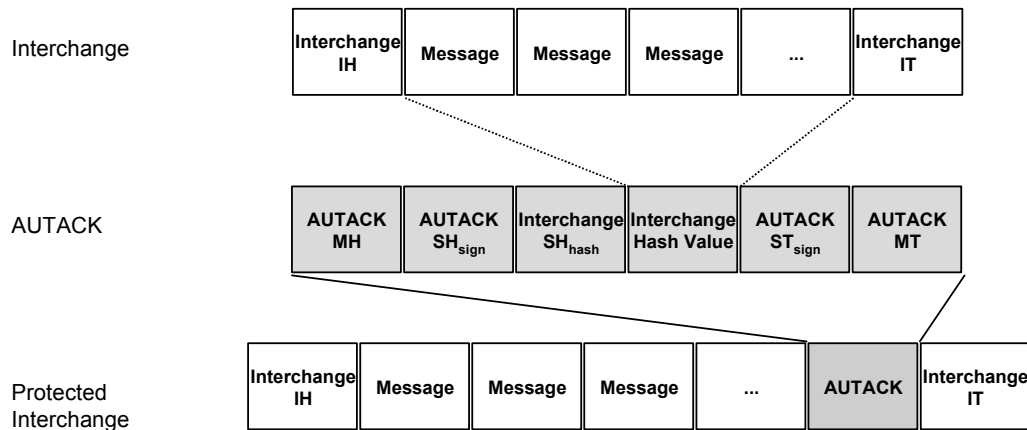


Figure 10: Embedded AUTACK

Der NRR-Dienst mittels AUTACK wird bei PayNet in Zusammenhang mit der Dienstleistung für Gutschriften verwendet (nicht zu verwechseln mit Gutschriftenanzeigen).

#### 4.1.1.3.5 Einsatz Public Keys

Auf der Basis von eingesetzten Software-Produkten werden Public Keys bilateral ausgetauscht. Dabei generiert der Sender den Private- und Public Key, speichert den Private Key in seinem System (dieser wird für die Generierung der digitalen Signatur des Senders verwendet) und schickt den Public Key mittels KEYMAN an den Receiver. Mit dem gespeicherten Public Key des Senders kann der Receiver die digitale Signatur des Senders verifizieren.

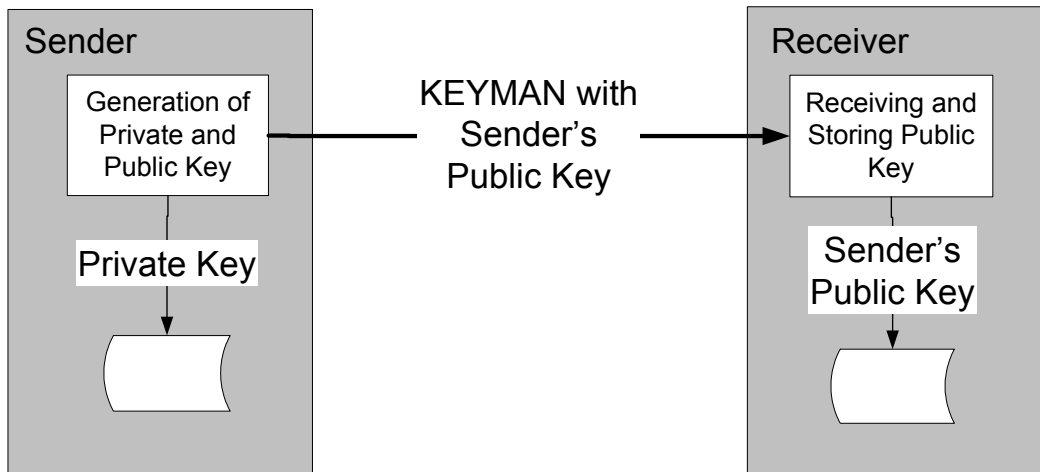


Figure 11: Einsatz KEYMAN für bilateralen Austausch des Public Key

#### 4.1.1.3.6 Zusammenfassung

Sicherheitsmerkmal	EDIFACT CH
Vertraulichkeit	✓ (CIPHER)
Datenintegrität	✓ (AUT und SH/ST)
Authentifizierung	✓ (SH/ST) (✓) (AUT)
Nicht-Abstreitbarkeit des Ursprungs	✓ (SH/ST)
Nicht-Abstreitbarkeit des Empfangs	✓ *
Ende-zu-Ende Sicherheit	Applikationsebene
Key Management	symmetrische Schlüssel für AUT, asymmetrische Schlüssel, bilateraler Schlüsselaustausch mittels KEYMAN

Tabelle 7: Sicherheitsmerkmale bei EDIFACT CH (SH/ST = Security Header/Trailer, (✓) = nicht strenge Authentifizierung, \* = bei PayNet mit AUTACK bei Dienstleistung für Gutschriften, in EVA mit signierter Rückmeldung realisiert).

#### 4.1.2 XML

Alle Informationen im Zusammenhang mit XML (eXtensible Markup Language) sind zur Zeit der Erstellung dieses Reports sehr neu. Die Spezifikationen für die Version 1 von XML sind erst seit 1998 verfügbar [Ref. 15].

XML und HTML (HyperText Markup Language, wird üblicherweise für Web-Dokumente benutzt) sind verwandt. Beide sind ein Subset von SGML (Standard Generalized Markup Language), dem internationalen Standard ISO 8879 für die Definition der Beschreibung von Struktur und Inhalt von verschiedenen Typen von Dokumenten. HTML beschreibt mit sogenannten *Tags* das Format eines Dokuments und dessen Darstellung ('Aussehen'). XML beschreibt mit Tags den Inhalt und die

Struktur eines Dokuments ('Inhalt'). Applikationen können deshalb in XML-Dokumenten gewisse Teile erkennen (z.B. einen Zahlenwert als Preis oder einen Textteil als Zusammenfassung) und damit das Dokument auch in einer anderen Form darstellen oder weiterverarbeiten. XML ermöglicht neue Anwendungen, die auf der Basis von HTML nicht realisierbar wären.

Die Sicherheitsdienste Datenintegrität, Authentifizierung und Nicht-Abstreitbarkeit des Ursprungs werden mit dem Internet Draft *Digital Signatures for XML* vom Januar 1999 angegangen. Aktuelle Informationen sind über die *ETF/W3C XML-Signature Working Group* [Ref.16] verfügbar. Für den Sicherheitsdienst der Vertraulichkeit kann SSL eingesetzt werden oder auf der Meldungsebene auch S/MIME.

### 4.1.3 PGP

In diesem Kapitel wird das klassische PGP beschrieben. PGP (Pretty Good Privacy) [Ref. 3] war eine der ersten Anwendungen für sicheres Email. Heute sind PGP-Versionen mit einer benutzerfreundlichen Oberfläche verfügbar, z.B. als Plug-In für Windows Email-Anwendungen. Die Sicherheitsmechanismen umfassen die Verschlüsselung (z.B. mit dem IDEA Algorithmus, 128 Bit) und die digitale Signatur. Diese Mechanismen gewährleisten die Sicherheitsdienste Vertraulichkeit, Datenintegrität, Authentifizierung und Nicht-Abstreitbarkeit des Ursprungs (Tabelle 8).

Ein Vorteil und zugleich ein Nachteil von PGP ist die Zertifizierung. PGP benötigt *keine* zentrale Zertifizierungsinstanz. Jede Person kann den öffentlichen Schlüssel eines anderen PGP-Benutzers unterschreiben und damit ein Zertifikat ausstellen (d.h. die Übereinstimmung von öffentlichem Schlüssel und Namen des Schlüsselbesitzers bezeugen). Bei PGP kann nun eingestellt werden, ob öffentliche Schlüssel, die von einer Person zertifiziert wurden, als vertrauenswürdig betrachtet werden sollen. Damit wird ein 'Web of Trust' aufgebaut. Dieses 'Web of Trust' macht PGP zu einem geeigneten Email-System für den 'privaten Gebrauch' und den Gebrauch innerhalb kleiner Gruppen. Für die kommerzielle Nutzung mit Tausenden von Benutzern fehlt aber eine zentrale Zertifikatsautorität CA (Kapitel 5.2), welche die Zertifikate nach klaren Kriterien ausstellt und die Gültigkeit der Zertifikate überwacht (z.B. mit Revocation-Lists).

Bei PGP ist die Skalierbarkeit und die Identifikation des Zertifikatseigentümers problematisch. Das erschwert den Einsatz von PGP im kommerziellen Bereich.

Sicherheitsmerkmal	PGP
Vertraulichkeit	✓
Datenintegrität	✓
Authentifizierung	✓
Nicht-Abstreitbarkeit des Ursprungs	✓
Nicht-Abstreitbarkeit des Empfangs	N
Ende-zu-Ende Sicherheit	Applikationsebene
Key Management	PGP-Zertifikate, keine zentrale PKI

Tabelle 8: Sicherheitsmerkmale des klassischen PGP.

#### 4.1.4 S/MIME

S/MIME (Secure Multipurpose Internet Mail Exchange) [Ref. 2] wird von vielen grossen Benutzergruppen eingesetzt und ist weltweit sehr verbreitet. S/MIME wurde von RSA Data Security Inc entwickelt und wird heute von Microsoft, Netscape, Lotus, ConnectSoft, Entrust und vielen weiteren Firmen unterstützt. *S/MIME ist ein de facto Standard für die Signierung und Verschlüsselung von Mail-Meldungen im MIME-Format.*

S/MIME unterstützt die Sicherheitsdienste für die Vertraulichkeit und die Nicht-Abstreitbarkeit des Ursprungs und damit auch für die Datenintegrität und Authentifizierung (Tabelle 9). Das sichere Meldungsformat von S/MIME kann für unterschiedliche Anwendungen genutzt werden, z.B. für sicheren elektronischen Datenaustausch (EDI): EDIFACT Interchanges können in MIME Objekte eingepackt werden und damit auch in S/MIME.

Obwohl die Verbreitung von S/MIME zunimmt, muss doch berücksichtigt werden, dass häufig US-Produkte angeboten werden, welche mit Exportrestriktionen belegt sein können.

S/MIME verwendet X.509-Zertifikate. Solche Zertifikate werden z.B. von Verisign angeboten oder von PKI-Produkten unterstützt.

Sicherheitsmerkmal	S/MIME
Vertraulichkeit	✓
Datenintegrität	✓
Authentifizierung	✓
Nicht-Abstreitbarkeit des Ursprungs	✓
Nicht-Abstreitbarkeit des Empfangs	N
Ende-zu-Ende Sicherheit	Applikationsebene
Key Management	X.509v3, zentrale PKI

Tabelle 9: Sicherheitsmerkmale bei S/MIME.

Bemerkung: Das 'From'-Feld eines Email-Systems gibt üblicherweise den Absender an. Damit ist aber eine Authentifizierung des Absenders in keiner Weise gewährleistet. Der Sender kann bei nicht gesicherten Email-Systemen für den Absender irgendeine Email-Adresse angeben (z.B. beim Netscape Communicator).

## 4.2 Kanalsicherung

Die Sicherung des Verbindungskanals ermöglicht die Übertragung beliebiger Daten über den Kanal. Die Kanalsicherung kann neben der Verschlüsselung auch eine Sicherung der Integrität und eine Authentifizierung enthalten. Bei der Kanalsicherung ist es jedoch nicht möglich, diejenigen Sicherheitsdienste zu implementieren, welche direkt an Meldungen angebracht werden müssen, z.B. digitale Signaturen für die Nicht-Abstreitbarkeit.

Bei der Kanalsicherung werden die Daten wohl gesichert übertragen, stehen aber danach ungesichert zur Verfügung. So werden z.B. die Daten verschlüsselt übertragen und danach auf Computersystemen nicht verschlüsselt abgelegt.

### 4.2.1 Secure Socket Layer (SSL)

Das SSL-Protokoll [Ref. 3] bietet für die Kanalsicherung drei Sicherheitsdienste an. SSL gewährleistet die gegenseitige Authentifizierung von Server und Client. Die Authentifizierung des Clients ist dabei optional und erfordert ein Client-Zertifikat. Weiter sichert SSL die Vertraulichkeit der Kommunikation (nach dem initialen Verbindungsaufbau) und die Datenintegrität mittels einer Hash-Funktion.

SSLv3 wird sowohl vom Netscape Navigator wie auch vom Internet Explorer unterstützt und ist deshalb weltweit sehr verbreitet. In der Exportversion wird jedoch die Verschlüsselung nur mit 40-bit Schlüssellänge unterstützt. SSL wird häufig für die Sicherung der Verbindung zu einem Web-Server genutzt, z.B. bei Kreditkartenzahlungen (obwohl das SET Protokoll für Kreditkartenzahlungen aus technischer Sicht viel mehr Sicherheit mittels digitaler Signaturen bieten könnte). Mit SSL gesicherte Web-Server werden mit einer URL angesprochen, die mit 'https' beginnt, z.B. <https://www.example.com/document.html>. HTTPS entspricht HTTP über SSL.

SecureNet, welches von Swiss Online und vielen schweizerischen Banken eingesetzt wird, unterstützt SSL (SSLv2) mit 128-bit Schlüssellänge (IDEA).

Sicherheitsmerkmal	Secure Socket Layer (SSL)
Vertraulichkeit	✓
Datenintegrität	✓
Authentifizierung (Client: optional)	✓
Nicht-Abstreitbarkeit des Ursprungs	N
Nicht-Abstreitbarkeit des Empfangs	N
Ende-zu-Ende Sicherheit	Workstationebene (Session)
Key Management	Zertifikate X509.v3, zentrale PKI

Tabelle 10: Sicherheitsmerkmale bei Secure Socket Layer (SSL).

## 4.2.2 Transport Layer Security (TLS)

TLS entspricht im wesentlichen SSL; TLS bezeichnet sich selbst als SSL Version 3.1. TLS unterscheidet sich von SSL nur unwesentlich, z.B. in den Meldungsformaten und den verwendeten Algorithmen. TLS wird von der IETF (Internet Engineering Task Force) entwickelt während SSL von Netscape kommt.

## 4.2.3 IP-Sicherung und VPN

Das Internet Protokoll (IP) ist ein Basisprotokoll auf der Schicht 3 für viele Netzwerke. IP zerlegt die Datenströme in kleine Pakete, die voneinander unabhängig durch das Netzwerk geleitet werden, eventuell über eine ganze Reihe von Zwischensystemen. Diese Datenpakete sind nicht gesichert: die Nutzdaten wie auch die Absender- und Empfängerinformationen könnten auf Zwischensystemen verändert werden.

IPsec (IP Security) definiert Erweiterungen zum IP Protokoll für die Sicherung der Daten auf der Netzwerkebene. Die ursprünglichen IP Datenpakete (Datagrams) können mit IPsec verschlüsselt und digital unterschrieben werden (für die Authentifizierung). IPsec kann damit die Vertraulichkeit, Datenintegrität und Authentifizierung gewährleisten. IPsec kann über *bestehende* IP-Netzwerke kommunizieren.

IPsec ermöglicht die Realisierung von Virtual Private Networks (VPNs), d.h. die Isolierung eines sicheren und privaten Subnetzwerks aus einem unsicheren und öffentlichen IP-Netzwerk. VPNs können z.B. eine Verbindung über das Internet herstellen, die ähnlich sicher ist wie eine Verbindung, die ausschliesslich über private Kommunikationslinien abläuft. Die Kosten für eine mit IPsec gesicherte Verbindung sind aber im allgemeinen wesentlich günstiger als eine private Kommunikationslinie (z.B. Standleitung).

Eine Anwendung ist die sichere Verbindung von zwei (oder auch mehreren) Firmen-LANs über das Internet. Dabei wird die Verbindung zwischen zwei Security-Gateways gesichert (Figur 4) bezüglich Vertraulichkeit, Datenintegrität und Authentifizierung (der Security-Gateways, nicht der Endbenutzer). Für den Benutzer in der Firma scheinen die beiden Firmen-LANs direkt verbunden zu sein (Virtual Private Network).

IPsec kann auch für die Sicherung eines externen Arbeitsplatzes eingesetzt werden. So kann z.B. ein Firmenangestellter über das Internet (d.h. seinen Internetprovider) mit der Firma eine Verbindung aufbauen als wäre er direkt am Firmen-LAN angeschlossen. Die Kommunikation wird für alle Applikationen gesichert (die über IP ablaufen).

Beim *IP-Tunneling* werden die ganzen IP-Pakete gesichert übertragen, wobei auch die ursprünglichen Absender- und Empfängeradressen verschlüsselt werden. Der empfangende Security-Gateway entschlüsselt die ursprünglichen Absender- und Empfängeradressen und leitet das IP-Paket zum Endempfänger weiter. Damit sind die ursprünglichen Absender- und Empfängeradressen unsichtbar während dem Transport über das öffentliche Netz (Tunneling).

Für die IP-Sicherung sind viele Produkte verfügbar, z.B. von Cisco, 3Com, Axent/Raptor, Bay Networks, TimeStep, Nortel Networks, CheckPoint, Entrust usw.

Diese Produkte erlauben eine kostengünstige Verbindung zwischen geographisch entfernten LANs.

Sicherheitsmerkmal	IP-Sicherung
Vertraulichkeit	✓
Datenintegrität	✓
Authentifizierung (Security Gateway)	✓
Nicht-Abstreitbarkeit des Ursprungs	N
Nicht-Abstreitbarkeit des Empfangs	N
Ende-zu-Ende Sicherheit	auf Ebene der Security Gateways
Key Management	X.509v3, zentrale PKI (alternativ: 'shared secret', proprietäre Ansätze)

Tabelle 11: Sicherheitsmerkmale bei IP-Sicherung und VPN.

#### 4.2.4 Leitungsverschlüsselung

Unternehmen bauen häufig ihre eigenen Kommunikationsnetze auf. Derartige Netzwerke können Standleitungen einschliessen. Diese Standleitungen sind in der Praxis oftmals auch Satellitenverbindungen oder Richtfunkstrecken, die besonders leicht abgehört werden können.

Um die Vertraulichkeit zu gewährleisten, wird gerne auf die Leitungsverschlüsselung zurückgegriffen. Alle Daten werden mit Verschlüsselungseinrichtungen beim Sender verschlüsselt und beim Empfänger entschlüsselt. Diese Verschlüsselung realisiert die Vertraulichkeit auf der Schicht 2.

Leitungsverschlüsselung gewährleistet die Vertraulichkeit der Daten (während der Datenübertragung). Im allgemeinen werden keine speziellen Massnahmen für die Gewährleistung weiterer Sicherheitservices getroffen (siehe Tabelle 12).

Typische Vertreter sind hier Gretacoder mit Chiffrierboxen [Ref. 11].

Sicherheitsmerkmal	Leitungsverschlüsselung
Vertraulichkeit	✓
Datenintegrität	N
Authentifizierung	N
Nicht-Abstreitbarkeit des Ursprungs	N
Nicht-Abstreitbarkeit des Empfangs	N
Ende-zu-Ende Sicherheit	auf Ebene der Sicherungsgeräte (Coder)
Key Management	N

Tabelle 12: Sicherheitsmerkmale bei Leitungsverschlüsselung.

### 4.3 Hybridlösungen

Eine Kanalsicherung kann auch mit einer zweistufigen Hybridlösung aufgebaut werden. Da die Web-Browser in Exportstärke keine genügend starke Verschlüsselung unterstützen (nur 40 Bit), kann nach dem Verbindungsaufbau zu einem Web-Server zuerst ein Java Applet (plattformunabhängige Softwarekomponente) über das Internet heruntergeladen werden. Dieses Java Applet kann nun seinerseits die Daten stark verschlüsseln (128 Bit) und damit eine wesentlich stärker verschlüsselte Verbindung zwischen Web-Server und Web-Client etablieren.

Bei der Java-Lösung stellt sich allerdings das Problem, dass das Herunterladen des Applets gesichert werden muss, vor allem sind Datenintegrität und Authentifizierung gefordert. Dies kann auf folgende Arten geschehen:

- Verwendung eine der oben beschriebenen Kanalsicherungen (SSL in Exportstärke kann für die Authentifizierung des Applets genügen);
- Verwendung von signierten Applets. Mit der Möglichkeit, Java-Applets zu signieren, kann die Authentifizierung und Integrität auf Applet-Ebene sichergestellt werden. Als Problempunkt (oder als Chance für die Applikation) kann sich erweisen, dass signierten Applets auf dem lokalen Rechner (Client) zusätzliche Rechte zugewiesen werden können.

Eine Hybridlösung wird von Brokat mit dem Produkt Xpresso angeboten. Via eine 40-bit SSL-Verschlüsselung wird das Applet heruntergeladen, welches dann eine 128-bit Verschlüsselung aufbaut. Das Produkt Xpresso wird von einer Reihe von Banken eingesetzt (als Alternative zu SecureNet).

### 4.4 Schlussfolgerungen

Vereinfachend werden nun lediglich Meldungs- und Kanalsicherung betrachtet. Beide Sicherungsvarianten bieten Vor- und Nachteile. Sie können bei der Realisierung von Sicherheitslösungen entscheidenden Einfluss haben. Diese Vor- und Nachteile sind in der folgenden Tabelle 13 aufgeführt.

	<b>Vorteil</b>	<b>Nachteil</b>
<b>Meldungs-sicherung</b>	Verbindlichkeitsdienste wie Nicht-Abstreitbarkeit sind realisierbar.  Sicherheitsdienste sichern die Datenkommunikation bis zur Applikation beim Endbenutzer (Daten können auch verschlüsselt abgespeichert werden).	Hoher Aufwand: für jede Applikation müssen die Sicherheitsdienste separat definiert, spezifiziert und implementiert werden
<b>Kanal-sicherung</b>	Applikationsprogramme müssen (meist) nicht geändert werden.	Keine Verbindlichkeitsdienste. Sicherheitsdienste sichern die Datenkommunikation nicht bis zur Applikation des Endbenutzers.

Tabelle 13: Vor- und Nachteile bei Meldungs- und Kanalsicherung.

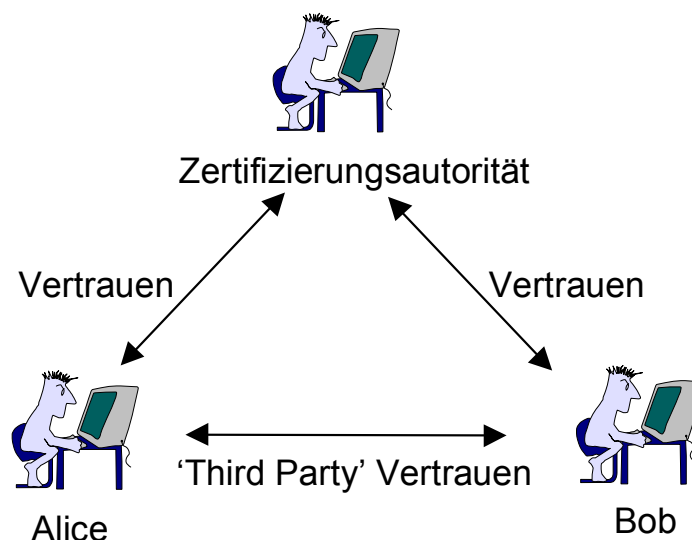
## 5. Keymanagement

### 5.1 Problematik

Die Gewährleistung von Sicherheitsdiensten wie Vertraulichkeit, Authentifizierung und Nicht-Abstreitbarkeit auf der Basis von kryptographischen Verfahren setzt für jeden Benutzer entsprechende Schlüssel voraus. So ist für den gegenseitigen Austausch von digitalen Signaturen für jede Partei ein Schlüsselpaar erforderlich, das einen privaten Schlüssel (Private Key) und einem öffentlichen Schlüssel (Public Key) umfasst. Der private Schlüssel darf unter keinen Umständen einer anderen Partei zugänglich sein, ansonsten kann die Nicht-Abstreitbarkeit nicht mehr gewährleistet werden. Der öffentliche Schlüssel dagegen soll für jedermann verfügbar sein, nämlich zur Überprüfung der digitalen Signatur. Das setzt ein Schlüsselmanagement voraus. Bei einer grösseren Benutzergruppe oder in einem offenen System darf das Schlüsselmanagement nicht unterschätzt werden.

### 5.2 Zertifikat und Zertifizierungsautorität

Für das Schlüsselmanagement können Zertifikate verwendet werden. Das Zertifikat enthält gesicherte Informationen für das Verifizieren der Identität des Besitzers. Dazu gehören u.a. der Name des Besitzers und dessen Public Key. Das Zertifikat wird von einer Zertifizierungsautorität (Certification Authority, CA) digital unterschrieben. Mit der Unterschrift bestätigt die CA die Zusammengehörigkeit von Public Key und Name des Besitzers sowie weiterer Informationen. Da die Zertifikatsinhaber der CA vertrauen, entsteht zwischen den Zertifikatsinhabern ein indirektes Vertrauensverhältnis über die Zertifizierungsautorität, das 'Third Party' Vertrauen (Figur 12). Für weitere Informationen verweisen wir auf den TBSS (Telematic Base Security Services) [Ref. 12].



Figur 12: 'Third Party' Vertrauen und Zertifizierungsautorität.

Einige Firmen und Finanzinstitute bauen eigene Public Key Infrastrukturen (PKI) auf, deren Schlüsselmanagement zusätzliche wichtige Funktionen übernehmen, wie z.B.

die automatische Schlüsselerneuerung (vor dem Erreichen des Ablaufdatums), Schlüsselwiederherstellung (bei Verlust des Schlüssels oder Passworts), Verwaltung der Key History (damit die abgelaufenen Schlüssel weiterhin zur Verfügung stehen, z.B. für die Entschlüsselung von 'alten' Emails), der Widerruf von Zertifikaten (z.B. bei Verdacht, dass der private Schlüssel einer anderen Partei zugänglich war).

## 6. Applikationen im Bankenumfeld Schweiz

Die nachfolgende Tabelle gibt eine Übersicht über die in der Schweiz verfügbaren Applikationen im Bankenumfeld und die realisierten Sicherheitsdienste sowie die zugehörigen Sicherheitstechniken.

Anwendung CH	Sicherheitsdienst	Technik/Verfahren
<b>Kunden an Schweizer Finanzinstitute</b> (seit 1992, UBS, CS, ZKB, PostFinance)	Datenintegrität, Authentifizierung <sup>1</sup>	MAC im AUT-Segment auf Meldungsebene
<b>Zwischen Kunden und UBS, CS</b>	Vertraulichkeit	Spezielle Ausprägung der CIPHER-Meldung
<b>PayNet</b> [Ref. 14] mit Kunden	Datenintegrität, Authentifizierung, NRO	Digitale Signatur mit Security Header/Trailer
<b>Yellowbill</b> mit Kunden	Vertraulichkeit, Datenintegrität	SSL-Verschlüsselung über HTTPS
<b>PayNet</b> mit Kunden	Vertraulichkeit, Datenintegrität	SSL-Verschlüsselung über HTTPS
<b>PayNet</b> mit Kunden	NRR	AUTACK <sup>2</sup> als Antwortmeldung auf digital signierte Meldungen
<b>PayNet</b> mit Finanzinstituten	Datenintegrität, Authentifizierung <sup>1</sup>	MAC im AUT-Segment auf Meldungsebene
<b>EVA</b> mit Finanzinstituten	Datenintegrität, Authentifizierung <sup>1</sup>	MAC im AUT-Segment auf Meldungsebene
<b>EVA</b> mit Finanzinstituten (Filetransfer)	Vertraulichkeit	CIPHER
<b>EVA</b> mit Kunden (PayCom3)	Datenintegrität, Authentifizierung, NRO	Digitale Signatur (payCOM <sup>web</sup> mit Zertifikat auf Smartcard plus HTTPS)
<b>SIC/euroSIC</b> (Interbanksicherheit)	Datenintegrität, Authentifizierung, NRO	Digitale Signatur mit Security Header/Trailer
<b>SIC/euroSIC</b> (Interbanksicherheit)	NRR	Digital signierte applikatorische Quittung mit Security Header/Trailer
<b>SIC/euroSIC</b> (Interbanksicherheit)	Vertraulichkeit	CIPHER oder Leitungsverschlüsselung

Tabelle 14: Übersicht über die Applikationen im Bankenumfeld der Schweiz sowie die realisierten Sicherheitsdienste und die zugehörigen Sicherheitstechniken (NRO = Nicht-Abstreitbarkeit des Ursprungs, NRR = Nicht-Abstreitbarkeit des Empfangs).

<sup>1</sup> Authentifizierung mit MAC im AUT-Segment: Bei dem in der Schweiz verwendeten MAC-Verfahren im AUT-Segment handelt es sich nicht um eine Authentifizierung im strengen Sinn, da

symmetrische Schlüssel eingesetzt werden. Somit ist sowohl der Sender wie auch der Empfänger im Besitz des gleichen Schlüssels (aber kein dritter).

<sup>2</sup> Der NRR-Dienst mittels AUTACK ist bei PayNet für die Dienstleistung Gutschriften im Einsatz.

## 7. Referenzen

Ref. 1: Applied Cryptography, Second Edition, Bruce Schneier, John Wiley & Sons, ISBN 0-471-12845-7, 1996.

Ref. 2: Digital Certificates, Applied Internet Security, Jalal Feghhi, Jalil Feghhi, Peter Williams, Addison-Wesley, ISBN 0-201-30980-7, 1998.

Ref. 3: Web Security & Commerce, Simson Garfinkel with Gene Spafford, O'Reilly & Associates, ISBN 1-56592-269-7, 1997.

Ref. 4: EVA/EEA-Handbuch, Teil F – Sicherheitssystem, Version 1.4, IBO 903 250, 8.2.99.

Ref. 5: ISO 9735-9, Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules; Syntax version number: 4, Release 1, 2002; Part 9: Security key and certificate management message (message type - KEYMAN).

Ref. 6: ISO 9735-7, Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules; Syntax version number: 4, Release 1, 2002; Part 7: Security rules for batch EDI (confidentiality).

Ref. 7: ISO 9735-5, Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules; Syntax version number: 4, Release 1, 2002; Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin).

Ref. 8: ISO 9735-6, Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules; Syntax version number: 4, Release 1, 2002; Part 6: Secure authentication and acknowledgment message (message type - AUTACK).

Ref. 9: CIPHER: Gemäss Implementierung im Produkt safeX der R&L AG (<http://www.rl-ag.com/>)

Ref. 10: „Recommended practice for message flow and security for edifact payments“ der „ UN/EDIFACT Finance Group SWG D6“ Version 2v02 vom 01.04.1999.

Ref. 11: Gretacoder mit Chiffrierboxen: <http://www.gds.ch/>

Ref. 12: TBSS (Telematic Base Security Services), Version 1.2, IBO 920 353 12.96, 6.12.1996.

Ref. 14: PayNet Handbuch Version 4.0, PayNet (Schweiz) AG, Hertistrasse 27 CH-8304 Wallisellen, 2002, <http://www.paynet.ch/>

Ref. 15: Extensible Markup Language (XML) 1.0 Specification, T. Bray, J. Paoli, C. M. Sperberg-McQueen, available at: <http://www.w3.org/TR/REC-xml>, 10.2.1998.

Ref. 16: ETF/W3C XML-Signature Working Group  
<http://www.w3.org/Signature/Overview.html>

## 8. Glossar

### **Applet:**

In Java geschriebener Programmcode, der auf dem lokalen Rechnersystem innerhalb einer eigenen Umgebung (Sandbox) ausgeführt wird.

### **Asymmetrisches Verfahren:**

Kryptographisches Verfahren mit zwei verschiedenen zusammengehörigen Schlüsseln (privater und öffentlicher Schlüssel). Das asymmetrische Verfahren kann für die Verschlüsselung oder die digitale Signatur genutzt werden. Die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel und die Entschlüsselung mit dem entsprechenden privaten Schlüssel. Das Signieren erfolgt mit dem privaten Schlüssel, das Verifizieren der Signatur mit dem öffentlichen Schlüssel.

### **Authentifizierung:**

Prozess, bei dem überprüft wird, ob 'jemand' oder 'etwas' echt oder berechtigt ist. Authentifizierung bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität.

### **Brute-Force Attacke:**

Bei der Brute-Force Attacke werden alle möglichen Schlüsselvarianten ausprobiert, bis der gesuchte Schlüssel gefunden ist. Schlüssellängen von 128 Bit gelten heute als sicher vor dieser Attacke, nicht aber 64 Bit.

### **CA:**

Certification Authority: Zertifizierungsstelle, die Zertifikate ausgibt. Damit können Daten authentisch übermittelt und vom Empfänger zur Identitätsprüfung des Urhebers verwendet werden.

### **DES:**

Data Encryption Standard: eines der bekanntesten und meist verbreiteten symmetrischen Verschlüsselungsverfahren. Der DES wurde 1978 in den USA normiert (ANSI X3.92).

### **Digitale Signatur:**

Die digitale Signatur kann die Nicht-Abstreitbarkeit des Ursprungs einer Nachricht (oder sonstigen Datenquelle, auch Softwarehersteller) ermöglichen. Die digitale Signatur entspricht also einer manuellen Unterschrift, die den Absender eindeutig identifiziert und zusätzlich sicherstellt, dass die empfangenen Daten nicht verfälscht wurden (Datenintegrität).

### **EDIFACT:**

Electronic Data Interchange For Administration, Commerce and Transport.

### **HTML:**

HyperText Markup Language, wird üblicherweise für die Beschreibung von Web-Dokumenten benutzt.

### **HTTPS:**

HTTP über SSL.

### **IDEA:**

International Data Encryption Algorithm; 1990 von Lai und Massey als Alternative

zum DES vorgestelltes symmetrisches Verschlüsselungsverfahren mit einer Schlüssellänge von 128 Bit.

**IP:**

Internet Protocol; Netzwerkprotokoll im Internet.

**Java:**

Von Sun entwickelte plattformunabhängige Programmiersprache für das Internet. Java-Programme (Applets) können von einem Web-Server auf das lokale Rechner-system übertragen und dort ausgeführt werden.

**MAC:**

Message Authentication Code: Authentifizierung auf der Basis eines symmetrischen Schlüssels.

**NRO:**

Sicherheits Dienst für „Nicht-Abstreitbarkeit des Ursprungs“.

**NRR:**

Sicherheits Dienst für „Nicht-Abstreitbarkeit des Empfangs“.

**PGP:**

Pretty Good Privacy.

**SSL:**

Secure Socket Layer.

**Symmetrische Verschlüsselung:**

Verschlüsselungsverfahren, bei dem für die Verschlüsselung der Daten der gleiche Schlüssel verwendet wird wie für ihre Entschlüsselung. Bekannte symmetrische Verschlüsselungsverfahren sind DES und IDEA.

**TCP:**

Transmission Control Protocol: Standard-Transportprotokoll zur Datenübertragung im Internet.

**TLS:**

Transport Layer Security.

**XML:**

eXtensible Markup Language.

**SGML:**

Standard Generalized Markup Language.

**S/MIME:**

Secure Multipurpose Internet Mail Exchange.

**VPN:**

Virtual Private Network.

**Zertifikat:**

Ein Zertifikat ist eine Bestätigung einer zertifizierenden Stelle, dass ein öffentlicher Schlüssel oder ein Attribut zu einer bestimmten Person oder Institution gehört. Die Bestätigung erfolgt mit der digitalen Unterschrift der Zertifizierungsinstanz. Die Signatur schützt auch vor Manipulationen am Zertifikat.