**Nachrichtenarten**

Um welche Nachrichtenart es sich handelt, wird in einem 6-stelligen Schlüssel angegeben, z.B. ORDERS, DELFOR, ORDRSP, ORDCHG, DESADV, INVOIC etc.

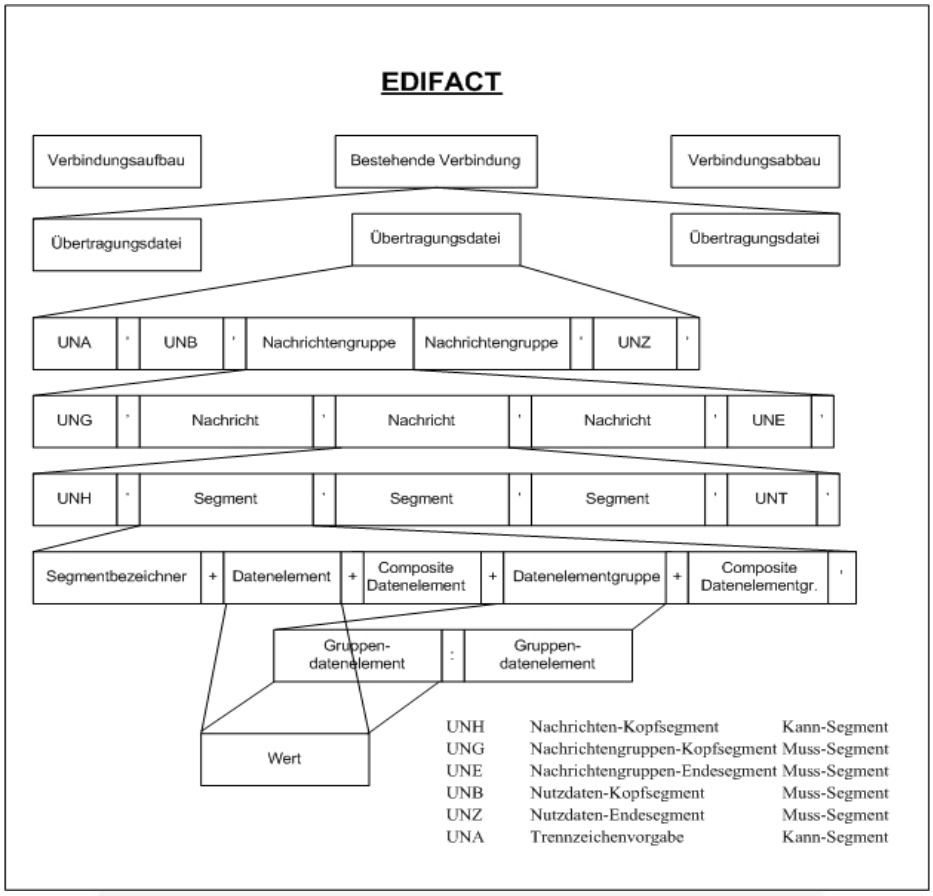


Abbildung 5.1: EDIFACT-Nachrichtenstruktur Quelle: [Petri1990] Seite 181

**Kann- u. Muss-Segmente**

EDIFACT benötigt nicht alle in einer Nachrichtendefinition enthaltenen Segmente, bzw. Datenelemente und bietet die Möglichkeit diese auszulassen. Das führt zur Unterscheidung von obligatorischen und optionalen Segmenten bzw. Datenelementen. Ist für ein Kann-Segment innerhalb einer Nachricht kein Inhalt vorhanden, so wird dieses ausgelassen. Dahingegen wird beim Weglassen eines Kann-Datenelementes innerhalb eines Segments das Datenelement-Trennzeichen (+) angegeben.

Da EDIFACT variable Datenfeldlängen zulässt und der Inhalt im Gegensatz zur Codierung mit festen Längen, nicht mit Leerzeichen oder Nullen aufgefüllt werden muss, ist eine deutliche Einsparung in der Datenübermittlung möglich.

Die folgende Abbildung zeigt den Anfang einer EDIFACT-Nachricht:

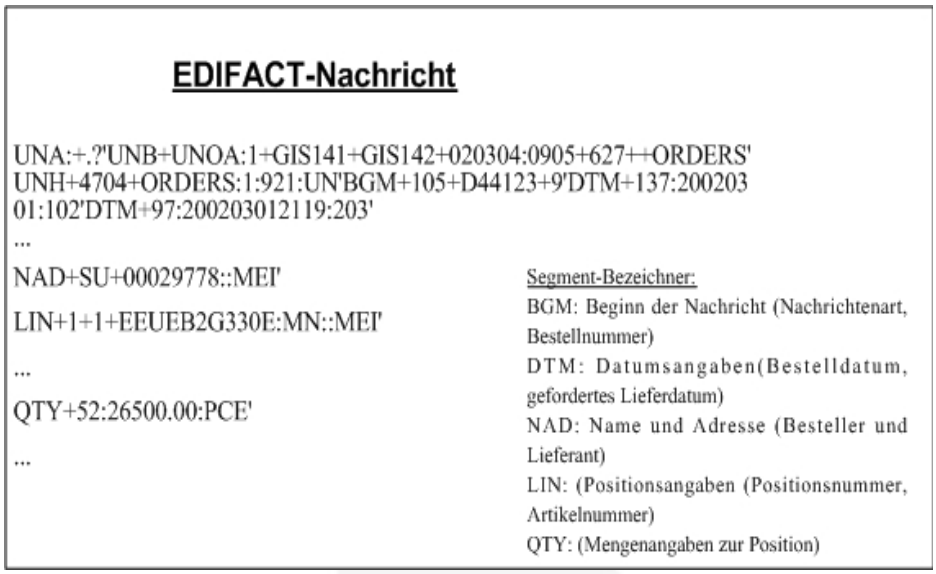


Abbildung 5.2: Ausschnitt einer EDIFACT-Nachricht

## 5.2.2 XML

**XML < SGML**

XML ist eine Teilmenge der Standard Generalized Markup Language (SGML). Bei XML handelt es sich, genau wie bei SGML, um eine Metasprache, wobei zur Reduzierung der Komplexität einige Eigenschaften weggelassen wurden.[1] XML erlaubt die Beschreibung, den Austausch, die Darstellung und die Manipulation von strukturierten Daten, sodass diese von einer Vielzahl von Anwendungen genutzt werden kann.[2]

**CSS u. XSL**

Zur Präsentation von XML-Dokumenten können diese mittels Cascading Style Sheets (CSS) oder der Extensible Style Language[3] (XSL) optisch aufbereitet werden. Für den Austausch von Daten im XML-Format ist dieses jedoch nicht weiter wichtig.

**DTD u. Schablone**

Mit Hilfe einer Document Type Definition (DTD) oder eines XML Schemas[4] wird eine formale Grammatik definiert. Sie stellt eine explizite Definition der nötigen, bzw. möglichen Tags und ihre Struktur dar.[5]

**parsen u. validieren**

Um XML als Datenaustauschformat zu nutzen, müssen beide Partner die gleichen Bezeichner (Tags) zum Markieren der Inhalte einsetzen. Deshalb ist es notwendig, dass sie sich auf gemeinsame Dokumentenklassen und somit auf gemeinsame Bezeichner einigen. Dies geschieht durch die Definition gemeinsamer DTDs oder XML Schemata,[6] welche in Repositories zur Verfügung stehen, damit Dokumente von der empfangenen Anwendung geparst, validiert und verarbeitet werden können.[7]

1. Vgl. [Weitzel2001] Seite 18.
2. Vgl. [Weitzel2001] Seite 19.
3. Nähere Informationen dazu unter http://www.w3.org/TR/xslt (Zugriff: 28-Mai-2002).
4. Nähere Informationen dazu unter http://www.w3.org/XML/Schema (Zugriff: 28-Mai-2002).
5. Vgl. [Weitzel2001] Seite 25.
6. Vgl. [Berthold1999] Seite 353.
7. Vgl. [Weitzel2001] Seite 59.

**Normierung**

DTDs und XML Schemata sind mit der Nachrichtendefinition von EDIFACT zu vergleichen. Es gibt etwa 200 genormte EDIFACT-Nachrichtentypen. Um eine zeit- und kostenaufwendige Normierung zu vermeiden, ist eine Migration der EDIFACT-Nachrichtentypen in DTDs und Schemata zu beobachten.

Da eine Vielzahl nicht kompatibler EDI-Standards, wie EDIFACT und ANSI ASC X.12, für Inkompatibilität gesorgt haben, wird durch XML die Einbindung neuer Partner in bestehende Geschäftsnetze und Informationsflüsse einfacher.[1]

**einheitlicher Standard?**

Auch wenn eine Übernahme der EDIFACT-Strukturen zu beobachten ist, stellt die Bildung eines einheitlichen Standards eine große Herausforderung dar, da die XML-Tags zur Zeit nicht standardisiert sind. Es existieren unterschiedliche Initiativen (zusammengesetzt aus namhaften Unternehmen), die daran arbeiten, einen neuen Standard auf XML-Basis zu definieren, der die Semantik zum Austausch von Nachrichten beschreibt.[2] Zu Unterscheiden sind die Initiativen im wesentlichen in Frameworks, Functions und Verticals.

BizTalk[3], RosettaNet[4], Electronic Business XML[5] (ebXML), Commerce XML[6] (cXML) arbeiten beispielsweise an Frameworks. Ziel ist es eine Infrastruktur bereitzustellen, damit beliebige Geschäftsdokumente automatisiert, auf XML-Basis ausgetauscht werden können.[7]

Sogenannte Functions, die beispielsweise von Common Business Library[8] (xCBL) und Guideline XML[9] (gXML) erarbeitet wurden, bilden Spezifikationen für typische Geschäftsoperationen über Branchengrenzen hinweg. Verticals leisten das gleiche innerhalb einer Branche, beziehungsweise innerhalb von Lieferketten. Beispiele sind hier CML[10] und Open Software Description (OSD)[11].[12]

**EDIFACT vs. XML**

Im Gegensatz zum EDIFACT-Format, bei dem sich die Bedeutung der Nachrichteninhalte aus der Reihenfolge der Felder innerhalb der Nachricht ergibt, sind für XML zusätzlich beschreibende Elemente (z.B. <Bestellung>) notwendig. Dadurch steigt das Übertragungsvolumen bis zum Faktor zehn an.[13] Dies ist allerdings angesichts hoher Bandbreiten bei der Übertragung nicht als Problem dazustellen, lediglich bei einer sehr hohen Anzahl von auszutauschenden Nachrichten.

---

1. Vgl. [Weitzel2001] Seite 3.
2. Vgl. [Weitzel2001] Seite 68.
3. Nähere Informationen dazu unter http://www.biztalk.org (Zugriff: 25-Mai-2002).
4. Nähere Informationen dazu unter http://www.rosettanet.org (Zugriff: 25-Mai-2002).
5. Nähere Informationen dazu unter http://www.ebxml.org (Zugriff: 25-Mai-2002).
6. Nähere Informationen dazu unter http://www.cxml.org (Zugriff: 25-Mai-2002).
7. Vgl. [Weitzel2001] Seite 76.
8. Nähere Informationen dazu unter http://www.xcbl.org (Zugriff: 25-Mai-2002).
9. Nähere Informationen dazu unter http://www.oasis-open.org/cover/gxml.html (Zugriff: 25-Mai-2002).
10. Nähere Informationen dazu unter http://www.chem.uni-potsdam.de/inet_kurs/cml/cml-3a.html (Zugriff: 25-Mai-2002).
11. Nähere Informationen dazu unter http://www.w3.org/TR/NOTE-OSD.html (Zugriff: 25-Mai-2002).
12. Vgl. [Weitzel2001] Seite 77.
13. Vgl. [Cowo25052001]Seite 26-27.

**EDIFACT vs. XML**

Positionsangaben in EDIFACT und XML

| EDIFACT | XML |
|---|---|
| BGM+220+396 | <BGM ID="220"><DokumentNumber>396</DokumentNumber></BGM> |
| LIN+1+2329-S' | <Positionsangaben><Positionsnummer>1</Positionsnummer> |
| QTY+21+100+PCE' | <Artikelnummer>2329-S</Artikelnummer> |
| | <Bestellmenge>100</Bestellmenge> |
| | <Mengeneinheit>Stueck</Mengeneinheit> |
| | </Positionsangaben> |

Abbildung 5.3: EDIFACT vs. XML

XML-Schnittstellen sind besonders für KMUs interessant, für die eine traditionelle EDI-Lösung bisher aufgrund hoher Setup- und Betriebskosten zu teuer war.[1] Für Großunternehmen mit bestehenden Geschäftsbeziehungen und einem hohen Transaktionsvolumen erscheint derzeit eine Ablösung durch XML nicht unbedingt sinnvoll, da zum einen Implementierungs-Kosten entstehen und zum anderen eine einheitliche Norm nicht geboten ist.

Viele dieser großen Unternehmen haben jedoch begonnen, sich mit XML auseinanderzusetzen und werden nach dem Etablieren von Standards den Geschäftspartnern die Möglichkeit bieten, XML-Daten auszutauschen.

### 5.2.3 XML mit SAP

SAP stellt mit dem Business Connector eine XML-Schnittstelle im R/3-System zur Verfügung (siehe auch Kapitel 4.8).

**Business Connector**

Damit Geschäftsdaten vom SAP-System an den Business Connector versendet werden können, ist es notwendig, dass im R/3-System eine Partnervereinbarung angelegt wird. In dieser ist festgelegt, welche Datentypen ausgetauscht werden und wie die IDoc-Struktur zwischen den Partnern definiert ist. IDocs können mittels transaktionalem RFC direkt an das externe System weitergegeben, oder als Datei in ein Verzeichnis geschrieben.

Im Business Connector werden ebenfalls Partnervereinbarungen angelegt, so dass nach Auslesen des Senders, Empfängers und der Nachrichtenart aus dem IDoc die zugeordnete Verarbeitungsmethode aufgerufen und die Konvertierung der Empfangsdatei vorgenommen werden kann. Zudem muss für jeden Kunden oder Lieferanten ein sogenannter XML Port definiert und in der Partnervereinbarung hinterlegt werden. Dieser Port besteht

1. Vgl. [Weitzel2001] Seite 7.

aus einem Verzeichnis in dem die Nachrichten abgelegt werden und einer Umsetzungstabelle für das Mapping.[1]

**XML-Struktur**

Die XML-Struktur basiert auf den bereits bestehenden IDoc-Strukturen. Die Konvertierung in ein allgemeingültiges XML-Format kann mittels XSLT oder einem XML-fähigen, kommerziellen Konverter durchgeführt werden.

Abbildung 5.4 zeigt eine Beispielkonvertierung einer IDoc-Bestellung. Es ist zu erkennen, dass die Segmente des IDocs in hierarchische XML-Tags umgewandelt sind, die die Darstellung eines strukturierten Dokumentes, ähnlich einem IDoc, ermöglicht.

**SAP-XML**

```
<?xml version="1.0" encoding="iso-8859-1" ?>
        <ORDERS01>
                <IDOC BEGIN="1">
                        <EDI_DC40 SEGMENT="1">
                                <TABNAM>EDI_DC40</ TABNAM >
                                <MANDT>100</MANDT>
                                <DOCNUM>00205015</DOCNUM>
                                <DOCREL>46B</DOCREL>
                                <STATUS>30</STATUS>
                        </EDI_DC40>
                        <E1EDK01 SEGMENT="1">
                                <CURCY>DEM</CURCY>
                                <WKURS>1.00000</WKURS>
                                <E1EDP20 SEGMENT="1">
                                        <WMENG>100.000</WMENG>
                                        …
```

Abbildung 5.4: SAP-XML (Beispielkonvertierung einer IDoc Orders01)

## 5.3 Datenmapping

**Konvertersysteme**

Bei der Umsetzung des SAP-internen IDoc-Formats in ein standardisiertes Format, wie beispielsweise EDIFACT oder ein XML-basiertes Format, ist eine Konvertierung der Felder notwendig. Das Konvertieren übernehmen in der Regel spezielle Konvertersysteme, die zuvor erzeugte Konvertierungsvorschriften, sogenannte Mappings, auf die Daten anwenden, und eine Überführung in das entsprechende Format vornehmen. Dabei besteht auch die Möglichkeit, den Inhalt der Felder durch andere Inhalte zu ersetzen.[2]

**Mapping Ja o. Nein?**

Grundsätzlich ist immer ein Mapping der Felder erforderlich. Es sei denn, dass beide Geschäftspartner die gleichen Stammdaten und die gleichen Schlüssel für Lieferbedingungen, Zahlungsbedingungen, Maße, etc. verwenden, so dass keine Formatumwandlungen vorgenommen werden müssen.

**ISO-Codes**

Für die Codes der Maßeinheiten wäre beispielsweise kein Mapping erforderlich, wenn sich alle Unternehmen an die ISO-Codes halten würden. Es

1. Vgl. [Weitzel2001] Seite 169.
2. Vgl. [Deutsch1995] Seite 147.

gibt jedoch Gründe, die Unternehmen zwingen, eigene Codes anzulegen. So benutzt das SAP-System für die Mengeneinheit Stück den ISO-Code "PCE". Allerdings wird diese Einheit ohne Nachkommastellen geführt. ECOM benötigt, da immer mehrere Komponenten zusammen verpackt werden, die Mengeneinheit Stück mit Nachkommastellen. Deshalb wurde für die Verpackungsmaterialien der Code "STK" angelegt.

Benutzen beide Partner die ERP-Software SAP R/3, so ist keine Konvertierung der Formate erforderlich. Die Dokumente können direkt im SAP-eigenen IDoc-Format übertragen werden. Das Mapping für die Lieferbedingungen, Zahlungsbedingungen, etc. sind jedoch weiterhin notwendig. Deshalb bietet SAP mit der Transaktion BD79 die Möglichkeit, Umsetzungsregeln für einzelne Segmentfelder zu definieren. Dabei wird eine eindeutige Zuordnung vom Empfänger- zum Senderfeld hergestellt und mit Regeln bzw. Bedingungen belegt.

### 5.3.1 Vorgehensweise beim Mapping

Zunächst wird im Konvertersystem die Struktur des IDoc-Formats abgebildet, die als Schnittstelle aus dem SAP-System erstellt wird. SAP bietet an dieser Stelle die Möglichkeit, die IDoc-Struktur herunterzuladen[1] und in das Mapping-Tool einzuspielen. Die Struktur besteht aus den intern zu füllenden Feldern, und den Satzarten, die aus den Feldern zusammengesetzt werden, sowie einer Reihenfolge, die das Auftreten der Satzarten festlegt.

**Zuordnungstabelle**

Die einzelnen Felder innerhalb der Satzarten werden den entsprechenden Elementen und Segmenten der EDIFACT-Nachricht zugeordnet, wobei sogenannte Zuordnungstabellen entstehen. An dieser Stelle spricht man vom Mapping.

Bei der Umsetzung wird nach einer logischen Identifikation der IDoc-Felder und der EDIFACT-Elemente eine Prozedur durchgeführt, die über die Zuordnungstabellen die Felder mappt.

**Eingangs- u. Ausgangsverarbeitung**

Beim Eingang, bzw. Ausgang, einer Nachricht wird vom Konvertersystem zunächst der Nachrichtentyp und der Absender, bzw. Empfänger, durch parsen des Dokuments ermittelt. Aufgrund der angelegten Partnervereinbarungen erfolgt die Auswahl der Zuordnungstabellen, anhand derer das Mapping vorgenommen wird.

### 5.3.2 Herausforderungen bei ECOM

**nicht abbildbare Strukturen**

Kann der Konverter eine Nachricht nicht in ein anderes Format überführen, da er die abgebildeten Strukturen nicht verstehen kann, ist es notwendig, dass ein vorgeschaltetes Programm (i.d.R. selbst zu erstellen) die Aufgabe übernimmt.

ECOM bekommt Nachrichten im EDIFACT-Format von der Panasonic Industrial Europe GmbH, intern PIE, wobei in einer Nachricht mehrere Bestellungen enthalten sein können. Generell bietet EDIFACT die Mög-

1. Das Herunterladen der IDoc-Struktur erfolgt über die Transaktion WE60.

lichkeit, am Anfang einer Nachricht die Trennzeichen mit dem UNA-Segment bekannt zumachen. Wenn in einer Nachricht mehrere Bestellungen enthalten sind, wird von PIE das UNA-Segment am Anfang jeder Bestellung übertragen und ist somit mehrfach in einer Nachricht vorhanden. Leider kann das Mapping-Tool von PIE nicht für jeden Lieferanten individuelle Einstellungen vornehmen, so dass entweder für alle oder für keinen Lieferanten dieses Segment mehrfach übertragen wird.

Das Konvertierungsprogramm von ECOM akzeptiert in Nachrichten das UNA-Segment nur am Anfang einer Nachricht. Jede Nachricht, die mehr als ein UNA-Segment enthält, führt zu einem Fehler bei der Konvertierung. Deshalb besteht seitens ECOM die Notwendigkeit, ein Zusatzprogramm zu schreiben, das im Vorfeld alle zusätzlichen UNA-Segmente löscht. Im Rahmen dieser Diplomarbeit entstand ein Programm in der Programmiersprache C, dass das geschilderte Problem löst. Der Quellcode ist der Diplomarbeit in Anhang A1 beigefügt und auf der CD im Verzeichnis "CD:\Diplomarbeit\Quellcode\" ebenfalls vorhanden.

## 5.4 EDI bei ECOM

**SAP-Subsystem von FIS**

Seit ca. 2 Jahren wird bei ECOM die herkömmliche Übertragung von Bestellungen, Rechnungen, etc. per Post oder Telefax mehr und mehr über EDI abgewickelt. Ausschlaggebend war das Einrichten eines Stockpointes in Lüneburg, der eine weitgehende Automatisierung von Geschäftsdokumenten verlangt. Da das SAP-System, wie in Kapitel 5.1.4 beschrieben, selbst nicht EDI-fähig ist, wurde das Produkt FIS/edi der Firma FIS Informationssysteme und Consulting GmbH zum Empfangen, Versenden und Konvertieren der EDI-Daten als SAP-Subsystem eingeführt. Dieses System setzt sich aus einem Server, einem Konverter und einem dritten Teil, der über ALE mit dem SAP-System verbunden ist, zusammen und verwaltet seine gesamten Daten direkt im SAP-System. Das Subsystem findet sowohl für den EDI Austausch bei ECOM als auch in dem Tochterunternehmen in der Slowakei (ECOM-SK) Anwendung.

**Konfiguration u. Monitoring**

Über die Transaktion J6TE lassen sich Partnervereinbarungen konfigurieren und das Mapping überwachen. Der EDI-Server empfängt und versendet die Nachrichten. Dabei wird festgestellt, von wem die Nachricht kommt, und in welchem Nachrichtenformat sie gesendet wurde. Da alle Nachrichten in einer Datei enthalten sind, wird gegebenenfalls ein Empfängersplit durchgeführt. Zudem wird eine Umsetzung der notwendigen Felder vorgenommen, indem ein Mapping durchgeführt wird, das zuvor mit dem Konverter-Tool erstellt wurde.

Zur Kommunikation benutzt ECOM die Dateischnittstelle und die Telebox 400 Schnittstelle des Subsystems.

### 5.4.1 EDI-Eingangsverarbeitung

**X.400 u. Pananet**

In Abbildung 5.5 sind die Vorgänge des Nachrichteneinganges dargestellt. Die Daten werden zunächst per FTP vom Pananet abgeholt und in die Verzeichnisse ".../data" für ECOM und ".../data2" für ECOM-SK gestellt.

Nachrichten, die per X.400 übertragen wurden gelangen direkt zum EDI-Server.

Über den GIS-Server empfangene Nachrichten können auf zwei Wege weiterverarbeitet werden.

Zum einen können die Daten direkt über den EDI-Server im SAP-System verarbeitet werden (blaue/durchgezogene Linie), auf dem anderen Weg werden die empfangenen Daten vor der Verarbeitung interaktiv eingesehen und editiert (rote/gestrichelte Linie).

Da zur interaktiven Verarbeitung im SAP-Standard keine Möglichkeiten vorgesehen sind, wurde im Rahmen der Diplomarbeit ein Programm zur Verarbeitung von EDIFACT-Bestellungen entwickelt. Im Anhang A2 befindet sich eine Sequenz der Bildschirmmasken. Der Quellcode des Programms und die Ablauflogik sind auf der CD im Verzeichnis "CD:\Diplomarbeit\Quellcode" enthalten.

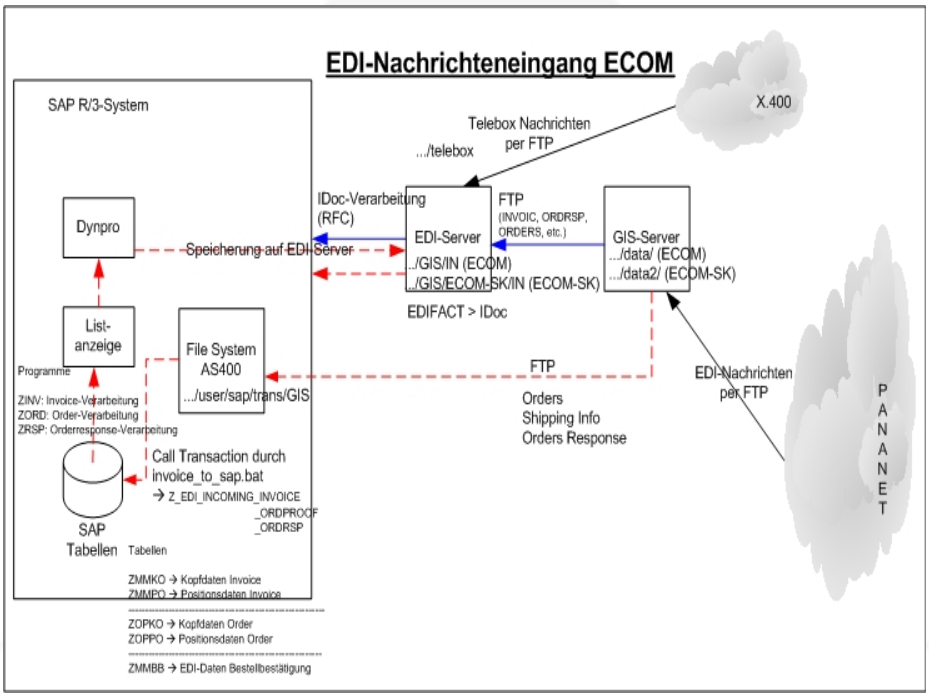


Abbildung 5.5: EDI-Nachrichteneingangsverarbeitung

Die folgenden Unterkapitel erläutern die unterschiedliche Verarbeitung am Beispiel der Nachrichtenart ORDERS.

#### 5.4.1.1 Direkte Eingangsverarbeitung

Bei dem direkten Weg werden die Daten vom GIS-Server zum EDI-Server weitergeleitet. Es folgt ein Mapping und die Umwandlung der Nachrichten vom EDIFACT-Format in das SAP-interne IDoc-Format. Nach Übertragung der Nachrichten mittels RFC in das SAP-System, erfolgt die Verarbeitung in den entsprechenden Tabellen. Eine Interaktion mit dem User findet nicht statt.

**IDoc-Liste u. IDoc-Statistik**

Über die Transaktionen WE05 (IDoc-Listen) und WE07 (IDoc-Statistik) kann anhand der Statusmeldung überprüft werden, ob die IDocs ordnungsgemäß verarbeitet wurden. Informationen über die enthaltenen Materialnummern, Mengen und Preise sind nicht ohne weiteres den Listen und Statistiken zu entnehmen.

An dieser Stelle bietet SAP wenig Funktionalität. Wünschenswert ist ein ausführliches Protokoll über die verarbeiteten Nachrichten mit Informationen über Bestellnummer, Materialnummer, Lieferdatum, Menge, etc.

Im Fehlerfall bietet SAP über den Workflow die Möglichkeit, betreffende Bearbeiter zu informieren. Dazu bedarf es aber einer Anpassung der Workflow Ablauflogik.

#### 5.4.1.2 Indirekte Eingangsverarbeitung

Der zweite Weg ist die indirekte Verarbeitung der eingegangenen Nachrichten (rote/gestrichelte Linie). Das heißt, der Benutzer hat die Möglichkeit, die Daten vor dem Einspielen zu prüfen und zu modifizieren. Dafür gibt es unterschiedliche Gründe.

**Gründe für indirekte Verarbeitung**

Zunächst wird von einigen Abteilungen die Prüfung verlangt, um nicht die Kontrolle und Übersicht zu verlieren, da, wie bereits erwähnt, SAP an dieser Stelle kaum Möglichkeiten der Protokollierung bietet.

Weiterhin stimmen die in den Bestellungen genannten Materialnummern nicht mit den internen Materialnummern von ECOM überein, da für selbsthergestellte Komponenten das Kürzel "-C" und für zugekaufte das Kürzel "-S" als Suffix ergänzt wird.

Dazu kommt, dass die Sparten bei ECOM nach Produkten, statt nach Kunden organisiert sind. Da der Kunde durchaus Materialien unterschiedlicher Sparten ordert, das SAP-System auf der anderen Seite allerdings verlangt, dass alle Materialien der Bestellung zu einer Sparte gehören, können folglich keine Bestellungen in das System gespielt werden, dessen Materialien zu unterschiedlichen Sparten gehören. Der einzige Weg ist die Aufteilung der Bestellung, so dass für jede Sparte eine neue EDIFACT-Bestellung erzeugt wird.

Das im Rahmen dieser Diplomarbeit entwickelte Programm läßt die erforderlichen Modifikationen für Bestellungen zu und erzeugt für jede Sparte unterschiedliche EDIFACT-Dateien.

**Abholen der Nachrichten**

Die Daten werden zunächst per FTP vom GIS-Server zum File-System der AS400 in das Verzeichnis ".../user/sap/trans/GIS" gestellt und von dort mit dem Programm "invoice_to_sap.bat", das über den ABAP-Befehl CALL TRANSACTION den SAP-Funktionsbaustein "Z_EDI_DATA_INCOMING_ORDPROOF" aufruft, in spezielle SAP-Tabellen (siehe Abbildung 5.5) übergeben.

**Programmablauf**

Zum Starten des speziell entwickelten Programmes, wird vom Benutzer die Transaktion ZORD aufgerufen. Es erscheint zunächst eine Liste der eingegangenen Bestellungen mit entsprechendem Verarbeitungsstatus (verarbeitet / nicht verarbeitet). Nach Auswahl der zu verarbeitenden Bestellungen wird diese mit allen Details angezeigt.

Nach Begutachtung gelangt man zu dem Dynpro, in dem die Sparte, Materialnummer und das Lieferdatum geändert werden können. Wurden die Änderungen vollzogen, erfolgt nach Plausibilitätsprüfung die Verarbeitung der Bestellungen.

Das heißt, es werden EDIFACT-Bestellungen erzeugt, die in das Verzeichnis ".../GIS/IN" für ECOM bzw. ".../GIS/ECOM-SK/IN" für ECOM-SK auf dem EDI-Server übertragen werden. Nach dem Mapping und der Konvertierung der Nachrichten zu IDocs, erfolgt die Übergabe und Verarbeitung ins SAP-System.

**IDoc-Kontrolle bei ECOM**

Die Abteilungen fordern mehr und mehr eine Benachrichtigung ihrer User nach dem Einspielen der IDocs. Da zur Zeit Statistiken nur manuell aufgerufen werden können und viel technisches Know How zum Beseitigen von Fehlern notwendig ist, wird die Kontrollarbeiten zum größten Teil in der EDV-Abteilung von ECOM durchgeführt. Abhilfe kann hier das Einrichten eines automatisierten Workflows schaffen, der die User über EDI-Nachrichten, bzw. aufgetretene Fehler beim Einspielen informiert.

## 5.4.2 EDI-Ausgangsverarbeitung

Wie in Abbildung 5.6 zu erkennen ist, stellt sich die Ausgangsverarbeitung bei ECOM übersichtlicher als die Eingangsverarbeitung dar.

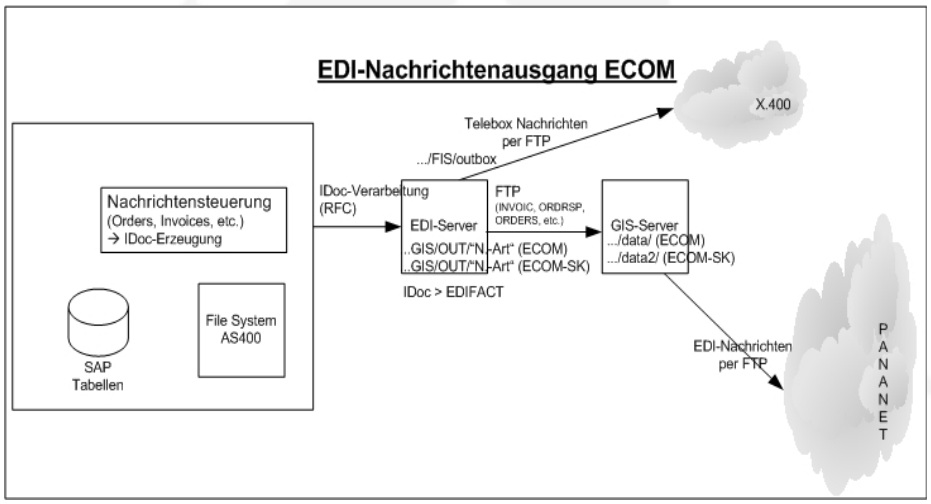


Abbildung 5.6: EDI-Ausgangsverarbeitung

Die ausgehenden Nachrichten werden durch die Nachrichtensteuerung des SAP-Systems, in Form von IDocs, automatisch erzeugt. Über einen RFC erfolgt die Weiterleitung an den EDI-Server. Dort findet das Mapping und eine Konvertierung des IDocs in das EDIFACT-Format statt.Nach erfolgreicher Verarbeitung werden die Nachrichten, je nach Versendungsart, in die entsprechenden Verzeichnisse auf den EDI-Server gestellt. Die Versendung erfolgt entweder direkt über X.400 oder indirekt nach Übertragung der Daten zum GIS-Server mit anschließendem Transport in das Pananet.

# 6

# Security-Aspekte für das R/3-System

**Datenschutz vs. Datensicherheit**

Im Grunde betreffen die Security-Aspekte die Datensicherheit und den Datenschutz. Unter Datenschutz versteht man alle gesetzlichen und betrieblichen Maßnahmen zum Schutz personenbezogener Daten. Datensicherheit beinhaltet dagegen die Verhinderung von Datenverlusten und Verfälschungen.

Dieses Kapitel befasst sich überwiegend mit der Datensicherheit, wobei unter SAP-technischen Gesichtspunkten eine Unterteilung innerhalb des SAP-Systems und zwischen SAP-Systemen vorgenommen wurde. Dabei sind in geschlossenen Systemen und Netzen in der Regel die gleichen Sicherheitsanforderungen notwendig, wie sie auch in globalen und offenen Systemen gelten.

**Schutz auf allen Ebenen**

Die Sicherheit unternehmerischer Daten nimmt einen erheblichen Stellenwert ein, da der Mißbrauch sensitiver Daten zu immensen wirtschafltlichen Schäden führen kann. Aus diesem Grunde müssen Daten und Informationen auf allen Ebenen unternehmerischer Schnittstellen geschützt werden.[1] Dazu gehören auch der elektronische Datenaustausch und die Client/Server-Kommunikation zwischen SAPGUI und R/3-System, bzw. zwischen R/3-Systemen.

**Sniffing u. Spoofing**

So ist die Datensicherheit, beispielsweise durch frei erhältliche Werkzeuge, wie "LAN Sniffer", die Übertragungsdaten mithören, aufzeichnen und anzeigen, ohne dass dies von der sendenden oder der empfangenden Station bemerkt wird, gefährdet.[2] Eine weitere Möglichkeit ist das IP Spoofing. Dabei wird unter der Identität einer Systemkomponente, oder eines Partnersystems, eine Verbindung aufgebaut und die Daten direkt ausgetauscht.

**„geschwätzige Dienste“**

Nicht zu unterschätzen ist die Informationsgewinnung aufgrund „geschwätziger“ Dienste, die von einem Webserver angeboten werden. Diese geben oftmals unnötig viele Informationen preis, die für einen Angriff missbraucht werden können.[3]Dazu gehören beispielsweise die Versionsnummer, die genutzt werden kann, um spezielle Fehler auszunutzen, die nur in dieser Version vorhanden sind oder die Fehlermeldungen, die bei vielen HTTP-Servern sehr aussagekräftig sind, so dass ein Angreifer anhand dieser Meldungen Rückschlüsse ziehen kann.[4]

**Aufwand u. Kosten**

Aus betriebswirtschaftlicher Sicht ist die Sicherheit für ein Unternehmen stets mit Aufwand und Kosten verbunden. Entweder durch die Pflege oder

1. Vgl. [Hantusch1997] Seite 99.
2. Vgl. [Hornberger/Schneider2000] Seite 87.
3. Vgl. [Fuhrberg2001] Seite 58.
4. Ein konkretes Beispiel ist die HTTP-Fehlermeldung 401: Sie sind nicht berechtigt, diese Seite anzuzeigen. Das heisst, diese Seite ist existent. Hacker wissen was zu tun ist, um diese Seite dann zur Anzeige zu bringen.

die Integration und Auswahl von neuen Sicherheitsfunktionalitäten. Scheut ein Unternehmen jedoch die Investitionen, kann der verursachte Schaden durch Datenverlust und Datenmanipulation in vielen Fällen weitaus größer sein, als die Aufwendungen für Sicherheitsprodukte.

## 6.1 Anforderungen an die Sicherheit

Sicherheitsanforderungen können in die unten folgenden Bereiche eingeteilt werden. Wichtig ist, ihren gewünschten Erfüllungsgrad innerhalb der unternehmerischen Sicherheitsstrategie festzulegen und auf die einzelnen Anforderungen einzugehen.

Um die Sicherheitsanforderungen zu erfüllen, sollte ein Sicherheitskonzept eingeführt werden, dass sowohl von der Geschäftsleitung als auch von den Mitarbeitern unterstützt und gefordert wird.[1]

### 6.1.1 Identität und Authentizität

Damit sich niemand für das System oder einen seiner Benutzer ausgeben und entsprechende Aktionen im System unter einer falschen Identität auslösen kann, gilt es diese zu schützen.

Die Benutzer des Systems, die Systemkomponenten und ihre Kommunikationspartner müssen jederzeit korrekt authentifiziert werden. [2]

### 6.1.2 Integrität und Vertraulichkeit

Im System gespeicherte und verarbeitete Daten sollten nicht unberechtigt eingesehen oder manipuliert werden können. Dies gilt auch für die, mit dem System oder innerhalb des Systems, ausgetauschten Daten während der Übertragung über Netzwerke.

### 6.1.3 Verfügbarkeit

Das System sollte jederzeit zur Informationsverarbeitung und zum Dialog mit seinen Benutzern verfügbar sein. Das heißt, das System darf nicht ausfallen. Dabei ist auch sicherzustellen, dass es nicht zu einer Überlastung und somit ebenfalls zu einem Ausfall kommt.

### 6.1.4 Prüfbarkeit und Nachvollziehbarkeit

Vorgänge und Änderungen im System sollten für eine gewisse Zeit nachvollziehbarsein. Dies ist nicht nur aus rechtlichen Gründen notwendig. Protokolle und Prüfungen erweisen sich für die Überwachung der Systemsicherheit und die Verfolgung von Ereignisssen bei Problemen als unentbehrlich.[3]

---

1. Vgl. SAP Sicherheitsleitfaden Band I Version 2.0a vom 6. Juli 1999 Seite 1-1.
2. Vgl. [Hornberger/Schneider2000] Seite 36.
3. Vgl. SAP Sicherheitsleitfaden Band I Version 2.0a vom 6. Juli 1999 Seite 2-3.

### 6.1.5 Verbindlichkeit und Beweisbarkeit

Um die Verleugnung eines Geschäftsvorganges vorzubeugen, sollten verbindliche Daten vorhanden sein, die, unter anderem, eine eindeutige Beweisbarkeit des Vorganges unterstützen. Dieses ist für den elektronischen Handel unverzichtbar und notwendig, um sich in der heutigen Geschäftswelt zu etablieren.[1]

## 6.2 Kryptologie

**Kryptologie u. Kryptographie**

Kryptologie bezeichnet die Wissenschaft, die sich mit der Sicherheit von Kommunikationssystemen befasst. Der Begriff kommt aus dem Griechischen und setzt sich aus "kryptós" (versteckt) und "lógos" (Wort) zusammen. Dahingegen befasst sich der Unterbegriff Kryptographie (griechisch: "graphein" = schreiben) mit die Techniken zur Verschlüsselung von Kommunikation. Mit Hilfe kryptographischer Methoden und Algorithmen können die Sicherheitsanforderungen erfüllt bzw. ein wesentlich höheres Sicherheitsniveau erreicht werden. Zur Anwendung kommen symmetrische und asymmetrische Verfahren, sowie Hashverfahren.

Durch die Verschlüsselung von Daten wird Vertraulichkeit erreicht, da die Daten nur noch durch Empfänger, die Zugriff auf den dafür erforderlichen Schlüssel haben, entschlüsselt werden können. Zur Authentifizierung kann die Kenntnis eines geheimen Schlüssels verwendet werden. Auf diese Weise kann z.B. die Identität einer Person festgestellt werden. Mit digitalen Signaturen wird zu gegebenen Daten ein mathematisches Siegel berechnet, mit dem die Integrität und die Urheberschaft geschützt werden.

Kryptographische Hashverfahren berechnen zu gegebenen Daten eindeutige "Fingerabdrücke", die die Integrität der Daten schützen können, ohne dass Rückschlüsse auf die ursprünglichen Daten möglich sind (Einwegfunktion).

### 6.2.1 Symmetrische Verfahren

**geheimer Schlüssel**

Bei symmetrischen Verfahren verfügen Sender und Empfänger über den gleichen geheimen Schlüssel. Angewendet wird eine Verschlüsselungsfunktion mit dem geheimen Schlüssel auf eine Klartextnachricht; das Ergebnis ist die verschlüsselte Nachricht. Die Entschlüsselung wird mit dem gleichen Schlüssel auf die verschlüsselte Nachricht angewandt; das Ergebnis ist die Nachricht im Klartext. Sender und Empfänger müssen sich vor dem sicheren Datenaustausch über den einzusetzenden Schlüssel einigen. Da die Sicherheit im Schlüssel liegt, ist darauf zu achten, dass dieser Schlüssel unbefugten Personen nicht bekannt wird.

**Anzahl der Schlüssel**

Erforderlich ist ein Schlüssel für jeweils zwei Kommunikationspartner. Steigt die Anzahl der Benutzer, nimmt auch die Anzahl der benötigten Schlüssel zu. Bei n Benutzern sind n(n-1)/2 Schlüssel erforderlich.

---

1. Vgl. SAP Sicherheitsleitfaden Band I Version 2.0a vom 6. Juli 1999 Seite 2-3.

Am häufigsten kommen die Verfahren Triple-DES[1], RC2[2], RC4[3] oder IDEA[4] zum Einsatz.

### 6.2.2 Asymmetrische Verfahren

**geheimer und öffentlicher Schlüssel**

Asymmetrische Verfahren verwenden Schlüsselpaare, die aus einem privaten (geheimen) und einem öffentlichen Schlüssel bestehen. Beide Schlüssel stehen in einer festen mathematischen Beziehung. Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur noch mit dem dazugehörigen privaten Schlüssel entschlüsselt werden. Umgekehrt können Daten, die mit dem privaten Schlüssel signiert wurden, mit dem dazugehörigen öffentlichen Schlüssel geprüft werden (digitale Signatur[5]). Mit dem Siegel kann die Integrität der Daten geprüft werden, da über die darin enthaltenden Zusatzinformationen jegliche Änderungen an den Daten erkannt werden können. Außerdem bezeugt die Signatur, dass die abgegebene Erklärung von demjenigen stammt, der sich als Verfasser ausgibt (Authentifizierung). Desweiteren kann sie zur Unwiederrufbarkeit von Nachrichten verwendet werden. Das am weitesten verbreitete Verfahren ist RSA[6].

In allen Fällen ist für jeden Benutzer ein Schlüsselpaar aus öffentlichen und privaten Schlüssel notwendig.

### 6.2.3 Hashverfahren

Das Hashverfahren erzeugt auf Basis einer Nachricht den charakteristischen Hashwert, der auch als digitaler Fingerabdruck bezeichnet wird.

Eine Hash-Funktion verarbeitet beliebig lange Nachrichten und erzeugt, je nach Hashverfahren, einen 128 Bit oder 160 Bit langen Ausgabewert, der unabhängig von der Größe der ursprünglichen Nachricht ist. Deshalb wird das Hashverfahren häufig anstelle von asymmetrischen Verfahren genutzt, die im Vergleich aufwendiger und zeitintensiver sind. Ermittelt wird der Wert in Iterationen, in die die Ausgangsnachricht und die Zwischenergebnisse eingehen.

Eingesetzt werden häufig die Verfahren MD5[7] und RIPEMD[8]

---

1. Nähere Informationen dazu unter http://home.in.tum.de/~atterer/uni/crypto.html (Zugriff: 26-Mai-2002).
2. Nähere Informationen dazu unter http://mitglied.lycos.de/cthoeing/crypto/rc2.htm (Zugriff: 26-Mai-2002).
3. Nähere Informationen dazu unter der URL http://mitglied.lycos.de/cthoeing/crypto/rc4.htm (Zugriff: 26-Mai-2002).
4. Nähere Informationen dazu unter http://home.in.tum.de/~atterer/uni/crypto.html (Zugriff: 26-Mai-2002).
5. Mit dem Signaturgesetz (SigG) hat der deutsche Gesetzgeber am 1. August 1997 ein Gesetz erlassen, welches die Rahmenbedingungen für technisch sichere digitale Signaturen beinhaltet. Dazu kommt die Signaturrichtlinie 99/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 13. Dezember 1999, die das Signaturgesetz im Rahmender Richtlinienumsetzung neu fasst und die Anerkennung elektronischer Signaturen fördern soll.
6. Nähere Informationen dazu unter http://rsasecurity.com/rsalabs/rsa_algorithm/index.html (Zugriff: 26-Mai-2002).
7. Nähere Informationen dazu unter http://rfc.net/rfc1321.html (Zugriff: 26-Mai-2002).
8. Nähere Informationen dazu unter http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html (Zugriff: 26-Mai-2002).

### 6.2.4 Schlüsselverteilung

Mit der Schlüsselverteilung steht und fällt die Sicherheit. Deshalb sollte ihr eine besondere Aufmerksamkeit gewidmet werden. Die postalische, telefonische oder persönliche Übermittlung des Schlüssels, ist bei der Verwendung symmetrischer Verfahren aus Gründen der Sicherheit vorzuziehen.

**Trustcenter**

Werden asymmetrische Verfahren eingesetzt, ist sicherzustellen, dass die öffentlichen Schlüssel authentisch übertragen werden. Dabei muss die Zuordnung des öffentlichen Schlüssels zu einer Person verifizierbar sein. Dies wird durch sogenannte Zertifikate[1] ermöglicht, die von Trusted Third Partys verwaltet werden. Die SAP AG hält einen Trustcenter auf dem mySAP.com Workplace bereit, in dem Kunden die Möglichkeit zur kostenlosen Nutzung der Zertifizierungstechnologie haben, wobei die verteilten Zertifikate dem X.509-Standard[2] entsprechen.[3]

## 6.3 Sicherheit zwischen SAP R/3-Systemen

Um Daten zwischen SAP R/3-Systemen auf sicherem Wege austauschen zu können, ist deren Kommunikation mittels Verschlüsselung zu schützen.

### 6.3.1 Verschlüsselung im Internet

Die Verschlüsselung im Internet kann auf verschiedenen Systemebenen erfolgen. SSL (Secure Socket Layer) baut auf der Netzwerkebene auf und kann dadurch mehrere überlagerte Protokolle bedienen, wodurch Anwendungen, wie beispielsweise FTP und WWW ein sicherer Übertragungsdienst zur Verfügung gestellt wird. Secure-HTTP (S-HTTP) ist eine weitere Möglichkeit zur Verschlüsselung. Es bildet eine Erweiterung des HTTP-Standards und ist somit nachrichtenbasiert.

#### 6.3.1.1 SSL-Verschlüsselung

Secure Socket Layer (SSL) ist ein Sicherheitsprotokoll, das zwischen TCP/IP und der Applikation "sitzt" und dort eine Ver- und Endschlüsselung auf Paketebene anwendet. Dadurch werden verschlüsselte Verbindungen, Echtheitsbestätigungen mit Zertifikaten nach dem X.509[4] Standard sowie die Sicherstellung der Nachrichtenintegrität ermöglicht.

Um die Integrität der übermittelten Nachrichten, sowie die rechtmäßige Server- und Client-Authentizität zu gewährleisten, verwendet SSL den RC4-Verschlüsselungsmechanismus von RSA Data Security.[5]

---

1. Nach §2 Abs. 3 des SigG(angeben als Quelle) ist ein Zertifikat eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person.
2. Das X.509-Zertifikat ist ein internationaler Standard für Zertifikate, der von der ISO im Rahmen des X.509-Protokolls 1988 definiert wurde. Es beschreibt den Inhalt von Zertifikaten und die Struktur von Zertifizierungsinstanzen, definiert aber keine Algorithmen.
3. Vgl. [ISelling2001] Seite 274.
4. X.509 ist ein Standardformat der International Telecommunication Union - Telecommunications (ITU-T) für Zertifikate. Es beinhaltet den Name des Ausstellers, eine Certification Authority, Informationen über die Identität des Inhabers sowie die digitale Signatur des Ausstellers.
5. Vgl. [Hantusch1997] Seite 105.

Die Verständigung zwischen Client und Server geschieht dabei über ein sogenanntes "Handshake"-Verfahren, bei dem sich beide zunächst authentisieren, um dann die Nachrichten untereinander verschlüsselt zu übermitteln. Je nachdem welche Anwendung mittels SSL verschlüsselt wird, wird ein anderes URL-Kürzel und ein anderer Port benutzt (siehe Tabelle 6.1).

**TLS** Die aktuelle Version SSL-Version 3.0 wird derzeit unter dem Namen Transport Layer Security (TLS) standardisiert.

| Portnummer | Bedeutung | URL-Kürzel |
|---|---|---|
| 443 | HTTP via SSL | HTTPS |
| 465 | SMTP via SSL | SSMTP |
| 992 | Telnet via SSL | TELNETS |
| 995 | POP3 via SSL | SPOP3 |

Tabelle 6.1: SSL-Portnummern und URL-Kürzel Quelle: Internetsicherheit Seite 106

#### 6.3.1.2 S-HTTP

Dieses Protokoll beruht ebenfalls auf Verschlüsselungsmechanismen von RSA Data Security. Es unterstützt verschiedene Verfahren für Verschlüsselung, Authentifizierung und digitale Unterschrift.[1] Bei Aufnahme der Kommunikation geben Server und Client an, mit welchen Verschlüsselungen sie arbeiten wollen. Die URLs beginnen bei diesem Protokoll mit shttp://.

### 6.3.2 Virtual Private Network

Ein Virtual Private Network (VPN) ist eine sichere Zugriffsmöglichkeit, von ausserhalb des Local Area Networks, auf Daten und Systeme, die sich innerhalb des Netzwerkes befinden. VPNs setzen einen weiteren, privaten TCP/IP-Stack auf den öffentlichen TCP/IP-Stack und simulieren dadurch private Netzwerke. Dadurch hat ein VPN die Möglichkeit, Daten auf physischer Ebene zu ver- und entschlüsseln und somit eine sichere Übertragung völlig unabhängig von den verwendeten Applikationen, durchzuführen.[2]

1. Vgl. [Hantusch1997] Seite 105.
2. Vgl. [Daum/Scheller2000] Seite 60.

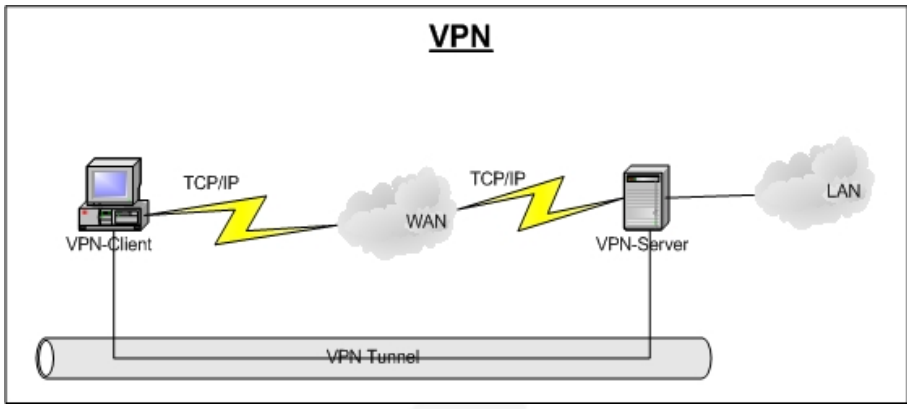


Abbildung 6.1: VPN-Verbindung

Zunächst muss sich der VPN-Client gegenüber dem VPN-Server per Username und Password authentisieren. Nach erfolgreicher Authentisierung wird der verschlüsselte VPN-Tunnel aufgebaut. Da der VPN-Client eine IP-Adresse aus dem firmeninternen Netzwerk zugewiesen bekommt, besitzt er dann keine direkte Verbindung mehr zum Internet und kann von dort auch nicht angesprochen werden.

VPN setzt in der Regel die Sicherheitsprotokolle Point-to-Point Tunneling Protocol und Internet Protocol for Security ein.

#### 6.3.2.1 PPTP

**PPP-Erweiterung**

Das Point-to-Point Tunneling Protocol (PPTP) ist eine Erweiterung des Point-to-Point Protocol (PPP). Bei PPTP werden PPP-Pakete in IP-Pakete gekapselt und über das Internet getunnelt versendet. PPTP ermöglicht den Aufbau eines sicheren Tunnels, in dem die Daten verschlüsselt transportiert werden.[1] Zur Sicherung der Datenübertragung verfügt PPTP über eine 40- oder 128-bit großen RC4-Verschlüsselung.[2]

#### 6.3.2.2 IPSec

**Authentification Header u. Encapsulated Security Payload**

IPSec kann als Rahmen bezeichnet werden, der aus einem Authentification Header (AH) und einem Encapsulated Security Payload (ESP) besteht. Mit Hilfe des AH wird die Integrität der übertragenen Daten geschützt und die Authentizität durch eine digitale Signatur gewährleistet. Der ESP dient zur Verschlüsselung der Nutzdaten, die in einem Paket übertragen werden. Dabei kapselt er die zu schützenden Daten ein und sichert deren Vertraulichkeit.[3]

### 6.3.3 Filter und Firewall als Sicherheitstools

**Zugangskontrolle**

Eine Firewall kontrolliert den Zugang zu vorhandenen Diensten und beschränkt die Nutzung auf einen erlaubten Nutzerkreis. Es werden interne

1. Vgl. http://www.lf69.at/grundlagen_vpn.htm (Zugriff: 23-Mai-2002).
2. Vgl. http://www.networkworld.de/onlinelexikon/8/f008988.htm (Zugriff: 23-Mai-2002).
3. Vgl. http://www.lf69.at/grundlagen_vpn.htm (Zugriff: 23-Mai-2002).

Systeme durch einen kontrollierten Eingangspunkt von externen getrennt und somit geschützt. Dadurch besteht die Möglichkeit, den Netzverkehr, sowohl von intern nach extern, als auch umgekehrt, zu beschränken. Dabei werden für die gewünschte Kommunikation sogenannte Ports geöffnet.

#### 6.3.3.1 Paket-Filter basierende Firewalls

Filter-Firewalls kontrollieren den Netzverkehr über die ein- und ausgehenden IP-Pakete.[1] Dabei werden bei Filtern in der Regel unerwünschte Situationen definiert und alles andere automatisch erlaubt. Sollte ein durchlaufendes Paket gegen die zuvor definierten Regeln verstoßen, wird die Verbindung unterbrochen.

**Aufgabe**

Die Implementierung von Filtern kann innerhalb von Routern, aber auch auf eigenständigen Rechnern mittels Filter-Software, erfolgen. Aufgabe der Router ist es, eine direkte IP-Verbindung zwischen zwei Host-Systemen herzustellen. Durch Filter wird letztlich die Nutzung unerwünschter Dienste anderer Hosts ausgeschlosssen, bzw. der Zugang ins interne Netz von unerwünschten Hosts verhindert.

#### 6.3.3.2 Applikations-Gateways

**Informationskontrolle**

Applikations-Gateways prüfen im Gegensatz zu Paket-Filter basierenden Firewalls nicht IP-Pakete, sondern den allgemeinen Informationsfluß, bzw. Datenstrom auf Applikationsebene.[2] Alle Aktionen können durch Applikations-Gateways aufgezeichnet, erlaubt oder verboten werden. Es besteht beispielsweise die Möglichkeit, bestimmte FTP-Befehle für externe Benutzer zu verbieten.

**SAProuter**

Zu den Applikations-Gateways gehört auch der SAProuter, der i.d.R. zusammen mit einer Paket-Filter basierenden Firewall installiert wird. Der SAProuter ermöglicht eine genaue Steuerung der Zugriffe innerhalb des Netzwerkes und die Kontrolle des Zugangs zum R/3-System, da er die SAP-Protokolle versteht. So kann beispielsweise die Firewall für das SAP-Protokoll DIAG geöffnet sein, vom SAProuter wird allerdings festgelegt, welche Benutzer mit DIAG auf das R/3-System zugreifen dürfen. Jeder SAProuter arbeitet mit einer Route-Permission-Tabelle[3], die bestimmt, welche Routen benutzt werden können und welche Kennwörter für den Zugang erforderlich sind.[4] Der eingehende Verbindungsaufbauwunsch endet zunächst im SAProuter, und wird mit einer neuen vom Router aufgebauten Verbindung zum Applikationsserver des Backend-Systems assoziiert. Während der folgenden Kommunikationsphase werden die einzelnen Datenpakete vom SAProuter über die von ihm gebildete Brücke transportiert. SAProuter können eingesetzt werden, um SAP-Systeme unterschiedlicher Local Area Networks, die über RFC miteinander kommunizieren, zu koppeln, sowie zur Verbesserung der Sicherheit innerhalb des Local Area Networks, bzw. für Zugriffe von Geschäftspartnern

1. Vgl. [Hantusch1997] Seite 107.
2. Vgl. [Hantusch1997] Seite 107.
3. Die Route-Permission-Tabelle enthält Hostnamen, Portnummern des Vorgänger- und Nachfolgerpunktes der Route sowie die Kennwörter, die für die Herstellung der Verbindung erforderlich sind. Gesucht wird in der Tabelle nach dem First-Match-Verfahren Des weiteren wird dort festgelegt, ob und welche SNC-Verbindungen aufgebaut werden.
4. Vgl. OSS-Hinweis 30289 (SAProuter Dokumentation) Seite 5.

von ausserhalb (siehe auch Kapitel 6.3.3.2). SAProuter unterstützen zudem die Nutzung von SNC – Secure Network Communication (siehe auch Kapitel 6.5.1)

## 6.4 Sicherheit innerhalb des SAP R3-Systems

Das SAP R/3-System zur rechnergestützten Unternehmenssteuerung benötigt geeignete Sicherheitsfunktionen, die nicht unmittelbar von Betriebssystemen oder Datenbanken bereitgestellt werden. Das liegt daran, dass die zu schützenden Objekte und Vorgänge nicht mit den Ressourcen auf der Ebene des Betriebssystems identisch sind. Allein mit den Mitteln der Datenbank können Tabellen und Felder lediglich unabhängig vom logischen Zusammenhang im Programm geschützt werden. Nur die Anwendung kennt die betriebswirtschaftliche Sicht und somit die eindeutige Zuordnung der Berechtigungen.

**Ansatz**

Daher wurde der Ansatz verfolgt, für das System selbst die Schutzfunktionen der Betriebssysteme und der Datenbanken zu nutzen. Innerhalb des R/3-Systems sind allerdings eine eigene Benutzerverwaltung, ein auf betriebswirtschaftliche Belange zugeschnittenes Berechtigungswesen und ein eigenes Auditing und Logging auf Anwendungsebene implementiert.[1]

**kryptographische Zusatzprodukte**

Weitere Sicherheitsfunktionen, wie digitale Signatur und Verschlüsselung werden durch kryptographische Zusatzprodukte, die über direkte Schnittstellen an das SAP-System angebunden werden, zur Verfügung gestellt.

### 6.4.1 Benutzerauthentifizierung

**Passwörter**

Zur Authentifizierung des Benutzers, bei der Anmeldung am System, werden im SAP-Standard Passwörter benutzt. Damit wird sichergestellt, dass nur bestimmte Benutzer, zu festgelegten Zeiten, Zugang zum System haben. Im Benutzerstamm ist der Hashwert des Paßwortes abgelegt. Die Übertragung des Passwortes vom Frontend zum Server erfolgt komprimiert. Der Zeitpunkt der letzten Anmeldung wird zur Mißbrauchskontrolle gespeichert und dem Benutzer beim Systemzugang angezeigt. Jeder Benutzerstammsatz enthält auch einen Status, damit einzelne Benutzer gesperrt werden können.

**Anmeldeversuche**

Es besteht die Möglichkeit, die Anmeldeversuche zu begrenzen. Die Anzahl der ungültigen Versuche ist zwischen 1 und 99 einstellbar. Anmeldeversuche, die darüberhinaus gehen, führen zur automatischen Sperrung des Benutzers.

**Passwortlänge**

Außerdem kann die Mindestlänge des Paßwortes zwischen 3 und 8 Zeichen gewählt werden. Die drei ersten Zeichen dürfen nicht mit der Benutzerkennung übereinstimmen.

**Passwortwiederholung**

Die letzten fünf in der Vergangenheit benutzten Passwörter dürfen nicht benutzt werden, und generell zu verbietende Passwörter sind in die Tabelle USR40 einzutragen. Damit die voreingestellten Passwörter dem Admini-

1. Vgl. [Hornberger/Schneider2000] Seite 39.

strator nicht bekannt sind, müssen sie bei der ersten Anmeldung durch ein individuelles ersetzt werden.[1] Die Gültigkeit der Passwörter ist bei ECOM auf 90 Tage beschränkt. Daraus folgt, dass das Passwort spätestens alle 90 Tage geändert werde muss, wobei nur einmal pro Tag eine Änderung zulässig ist.[2] Dies gilt jedoch nicht für Benutzer mit einer SAP_ALL-Berechtigung.

### 6.4.2 Autorisierung

Nach erfolgreicher Authentifizierung des Benutzers erlangt dieser Zugang zum System. Welche Anwendungen und Datenbestände ihm dann zur Verfügung stehen, hängt von seinen Berechtigungen, die er im SAP-System besitzt, ab (Autorisierung).

**Berechtigungsinstanzen**

Diese Berechtigungen stellen Instanzen der generischen Berechtigungsobjekte dar, welche in Berechtigungsprofilen hinterlegt sind. Dem Benutzer werden die Berechtigungen erteilt, indem die Berechtigungsprofile im Benutzerstamm eingetragen werden.

**Berechtigungsprüfung**

Grundlegende Berechtigungsprüfungen, wie das Starten von Transaktionen oder das Ausführen von Reports, finden bereits in der SAP-Laufzeitumgebund statt. Ob der Anwender alle Berechtigungen der Objekte besitzt, die ein Programm zur Ausführung benötigt, wird in den jeweiligen Programmteilen, an den entscheidenden Stellen geprüft. Dazu wird das Konstrukt "AUTHORITY-CHECK" der SAP-Programmiersprache ABAP/4 verwandt.[3]

**SAP-Profilgenerator**

Der SAP-Profilgenerators vereinfacht über Aktivitätsgruppen das Anlegen von Berechtigungen, da nicht für jedes Objekt einzeln dem Anwender eine Berechtigung erteilt werden muss. Es werden auf Ebene der, im SAP-System angebotenen, betriebswirtschaftlichen Transaktionen die entsprechenden Profile erzeugt.

### 6.4.3 Transaktionssicherheit/Datenintegrität

**LUW**

Durch das SAP-Transaktions- und Verbuchungskonzept wird der Schutz der Datenintegrität erreicht. SAP-Transaktionen sind in eine oder mehrere Abschnitte unterteilt, die Logical Units of Work (LUW) genannt werden.[4]

Da eine LUW eine Transaktion auf Datenbankebene darstellt, ist sie mit der üblichen Datenbanktechnik gesichert. Das heißt, sie bildet eine Einheit, wird also ganz, oder gar nicht ausgeführt und überführt die Datenbank in einen Konsistenten, dauerhaften Zustand.

### 6.4.4 Aufzeichnung, Protokollierung und Prüfung

Zu einem vollständigen Sicherheitskonzept gehört die Aufzeichnung und Protokollierung sicherheitsrelevanter Ereignisse in einem System.

---

1. Vgl. SAP Sicherheitsleitfaden Band I Version 2.0a vom 6. Juli 1999 Seite 3-2.
2. Vgl. OSS-Hinweis 2467, Thema: Kennwortregeln und fehlerhafte Anmeldungen.
3. Vgl. [Hornberger/Schneider2000] Seite 56.
4. Vgl. [Hornberger/Schneider2000] Seite 65.

**Änderungshistorie**

SAP-Anwendungen und zentrale Verwaltungsanwendungen, wie beispielsweise die Benutzerverwaltung, schreiben Belege, die in der Datenbank gespeichert werden. So entsteht eine Änderungshistorie.

Zudem gibt es eine allgemeine Protokollierung von Customizing-Tabellenänderungen, in der jeweils der alte und der neue Wert notiert werden.[1]

**Security Audit Log u. System Log**

Der Security Audit Log[2], welcher erfolgreiche und nicht erfolgreiche Aufrufe und Anmeldungen aufzeichnet, sowie das Audit-Informationssystem[3] (extra Installation nötig OSS-Hinweis angeben) (TC: SECR), welches einen Überblick über detaillierte Informationen einzelner Sicherheitsaspekte verschafft, liefern dem Administrator wichtige Informationen.[4] Das Computing Center Management System (CCMS) zeigt allgemeine Fehlersituationen des Systems an, die im System Log aufgezeichnet werden. Zudem stehen dort die protokollierten Daten des Security-Audit-Logs abrufbereit.

## 6.5 SAP-Schnittstellen für externe Sicherheitsprodukte

Um nicht gegen das deutsche Exportrecht oder länderspezifische Gesetze für den Import irgendwo in der Welt zu verstoßen, hat sich die SAP AG entschieden, in der SAP-Standardauslieferung keine Verschlüsselung zu unterstützen.[5]

Da das SAP R/3-System in einem Client/Server-Umfeld betrieben wird, wodurch die Kommunikation und der Datentransport über das Netztwerk erfolgt, sind zwei offene Schnittstellen für die Integration externer Sicherheitsprodukte in das SAP-System bereitgestellt.

**„C“-Schnittstelle**

Beide Sicherheitsschnittstellen sind als "C"-Programmierschnittstellen entworfen und unmittelbar in die Basisschicht integriert.

### 6.5.1 Secure Network Communications

Die Secure Network Communications-Schnittstelle (SNC-Schnittstelle) verwendet das Gerneric Security Services API Version 2 (GSS API Version 2), welches von der IETF[6], unter Mitwirkung von SAP, standardisiert wurde.[7] Mittels SNC lassen sich Benutzer-Authentifizierung und der Schutz der, über die Netzwerkverbindungen übertragenen, Daten in einem SAP-System mit den kryptographischen Mitteln eines externen Sicherheitsproduktes realisieren. Der Schutz der Daten bezieht sich auf die Dauer und den Kontext von Kommunikationsbeziehungen zwischen den verschiedenen Komponenten des SAP-Systems (z.B. SAP Frontend, Anwendungsserver, RFC, SAPlpd, SAProuter, etc.). Die Daten werden in der

1. Vgl. [Hantusch1997] Seite 67.
2. Der Security Audit Log ist über die Transaktionen SM19 zu konfigurieren. Die Auswertungen sind über die Transaktion SM20 zu erreichen und werden über SM18 reorganisiert. Aufgezeichnet werden Vorgänge, wie Start und Stop von Anwendungsserver, erfolgreiche und nicht erfolgreiche Dialoganwendungen, RFC-Aufrufe, Transaktionsaufrufe Reportaufrufe, Upload/Download-Vorgänge etc.
3. Das Auditinformationssystem (AIS) ist als Add-On zu installieren und erreichbar über die Transaktion SECR.
4. Vgl. [Hornberger/Schneider2000] Seite 69.
5. Vgl. [Hornberger/Schneider2000] Seite 80.
6. IETF steht für Internet Engineering Task Force (http://www.ietf.org) (Zugriff: 23-Mai-2002).
7. Vgl. [Hornberger/Schneider2000] Seite 91.

Basisschicht "verpackt" und "entpackt", wodurch den Anwendungen in der ABAP-Laufzeitumgebung die Daten in gewohnter Form zur Verfügung stehen und eine sichere Verbindung unabhängig vom Transportmedium garantiert ist. Je nach Sicherheitsprodukt ist es möglich, Smartcards, Hardware-Token, Software-Token und/oder biometrische Authentifizierung (z.B. Fingerabdruck, Iriserkennung) zu verwenden.

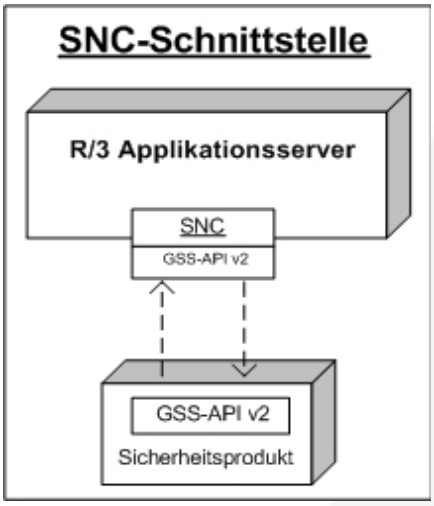


Abbildung 6.2: SNC-Schnittstelle

## 6.5.2 Secure Store & Forward (SSF)

Zum Schutz von Daten und Dokumenten, die in der Datenbank oder im Dateisystem gespeichert oder auf beliebige Medien exportiert wurden, existiert die Schnittstell SSF ergänzend zu SNC.[1]

**digitale Signatur u. digitaler Umschlag**

Es gilt sicherzustellen, dass die Daten nicht verändert wurden, dass der Ersteller der Daten eindeutig identifiziert werden kann und dass die Daten nicht unbefugt eingesehen werden können. Zum Einsatz kommen hier die digitale Signatur zum Schutz der Integrität und Authentizität eines Dokuments, sowie der digitale Umschlag, der, mittels Verschlüsselung, Schutz vor unbefugtem Lesen bietet.[2] Beide basieren auf der Public-Key-Technologie.

Es besteht die Möglichkeit, die Daten, bzw. das Dokument, mit mehreren öffentlichen Keys zu verschlüsseln, so dass die entsprechenden Anwender mit ihrem jeweiligen privaten Schlüsseln an den Inhalt gelangen. Da symmetrische Verfahren schneller sind als asymmetrische Verfahren, wird bei dem digitalen Umschlag ein hybrides Verfahren verwendet. Verschlüsselt werden die Daten mit einem zufällig erzeugten und pro Nachricht, bzw. Dokument, neuen symmetrischen Schlüssel. Dieser wird dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, so dass nur der Empfänger, mit seinem privaten Key, den geheimen symmetrischen Nachrichtenschlüssel ermitteln und die Nachricht wieder gewinnen kann.

1. Vgl. [Hornberger/Schneider2000] Seite 82.
2. Vgl.SAP Sicherheitsleitfaden Band I Version 2.0a vom 6. Juli 1999 Seite 3-11.

Zur Speicherung des privaten und öffentlichen Schlüssels wird im SAP-Standard eine verschlüsselte Datei erzeugt, die mit einem Paßwort versehen ist. Durch den Einsatz von Partnerprodukten an der SSF-Schnittstelle sind aber je nach Hersteller, auch Hardware-Lösungen möglich.

Über ABAP-Funktionsbausteine können SSF-Funktionen direkt von den Anwendungen aus aufgerufen werden. Da der private Schlüssel nur auf dem Frontend-PC vorhanden ist, erfolgt nach Aufruf der Signierfunktion von einer Anwendung ein RFC-Aufruf zum Frontend, auf dem daraufhin das SSF-Serverprogramm gestartet wird. Zudem werden die zu signierenden Daten übertragen. Das Serverprogramm lädt die Programmbibliothek des Sicherheitsproduktes zur Erzeugung der Signatur über die SSF-Schnittstelle und gibt als Ergebnis die digitale Signatur zurück. Der Ablauf für die Entschlüsselung von Daten ist entsprechend gleich. Statt der Signatur werden die verschlüsselten Daten zurückgegeben.

### 6.5.3 Spezielle Sicherheitslösungen für das R/3-System

Die SAP AG und die SECUDE GmbH haben zusammen ab der SAP-Version 3.1G eine spezielle Sicherheitslösung für das R/3-System entwickelt, die nicht nur die Datenübertragung chiffriert, sondern eine Benutzerauthentifikation zwischen Benutzern, Druckern, SAPRoutern und R/3-Applikationsservern ermöglicht. Dabei werden digitale Signaturen ausgetauscht, die durch sogenannte Zertifizierungsstellen ausgegeben werden.

Die asymmetrische Verschlüsselung geschieht hierbei mit RSA, bei den symmetrischen Algorithmen kommen DES, Triple DES oder IDEA zum Einsatz.[1]

**Single Sign-On**

Zu Beginn der Sitzung wird die sichere Verbindung mit dem Secure Single Sign-On[2] mittels eines Zertifikates einmalig etabliert.

Mittlerweile gibt es eine Vielzahl von Herstellern, die Sicherheitsprodukte für die SNC-Schnittstelle anbieten. Beispiele dafür sind Impress Software, Entrust Technologies oder Safelayer Secure.

## 6.6 Sicherheitsbetrachtung von ECOM

Ein steigendes Datenaustauschvolumen beim elektronischen Datenverkehr und der Zugang zum Internet von jedem Arbeitsplatzrechner, haben ECOM vor einiger Zeit zu neuem Denken im Bereich der Datensicherheit bewegt.

---

1. Vgl. [Hantusch1997] Seite 157.
2. Mittels Single Sign-On ist nur eine einmalige Anmeldung für alle Anwendungen, die zuvor in der Sicherheitssoftware registriert worden, notwendig. Der Benutzer meldet sich zu Beginn beim externen Sicherheitsprodukt an. Das Sicherheits-Tool versorgt dann die Anwendungen (z-B. SAP-Systeme, OSS, etc.) mit den Authentifizierungsdaten.

### 6.6.1 Netzwerk- und Ausfallsicherheit

**örtliche Sicherheit**

Örtlich gesehen sind die Server in einem speziellen Raum untergebracht, der über eine Alarmanlage gegen Einbruch und eine Klimaanlage gegen Unter-/Über-Temperaturen geschützt ist.

**Datensicherungskonzept**

Damit keine Daten verloren gehen, existiert ein Datensicherungskonzept, das vorschreibt, wann welche Sicherungen (partielle Sicherung, Vollsicherung), auf welchen Datenbändern einzuplanen sind. Die beschriebenen Datensicherungsbänder werden in einem feuersicherem Safe aufbewahrt.

**RAID-Level 5**

Die Festplatten der SAP-Applikationsserver werden in RAID-Level 5[1] abgesichert, wodurch beim Ausfall einer Platte die Daten wiederhergestellt werden können.

**eingeschränkte Benutzerrechte**

Die Arbeitsplatzrechner, die zum SAP-Zugang dienen, arbeiten größtenteils mit den Betriebssystemen Win NT und Win 2000 mit eingeschränkten Benutzerrechten, so dass keine zusätzlichen Installationen ohne weiteres ausgeführt werden können. Darüber hinaus ist der Zugriff auf Netzlaufwerke über das Active Directory von Microsoft gesichert, in dem eine komplexe Ressourcenberechtigung für jeden einzelnen User aufgebaut wurde.

**Firewall, ITS-Absicherung u. DMZ**

Eine moderne Firewall[2] trennt das interne ECOM-Netzwerk vom Internet. Zudem wurde eine demilitarized Zone (DMZ) eingerichtet, die den Internet Transaction Server (ITS) und den Webserver isoliert, da dieser vom Internet aus erreichbar sein muss. Der ITS besteht aus zwei Teilen (A-Gate und W-Gate), siehe auch Kapitel 4.7, wobei das W-Gate in Form einer DLL an den Webserver gebunden ist. ECOM sollte überlegen, das Gate zum Applikationsserver (A-Gate) hinter der Firewall auf einem gesonderten Rechner zu betreiben. Dadurch besteht die Möglichkeit zwischen dem W- und A-Gate eine gesicherte SNC Verbindung aufzubauen. Zudem werden dann die DIAG- bzw. RFC-Aufrufe aus der DMZ zum R/3-System durch TCP/IP-Aufrufe zum A-Gate ersetzt. Die Firewall sollte so konfiguriert sein, dass sie nur noch TCP/IP-Anfragen vom W-Gate auf bestimmte Ports zuläßt. Liegt das A-Gate im lokalen Netzwerk und nicht in der DMZ sind die HTML-Templates und Servicedateien, die unter anderem Anmeldeinformationen für anonyme oder automatisierte Zugriffe enthalten, vom Internet abgeschirmt. Desweiteren ist es sinnvoll eine sichere HTTPS-Verbindung zwischen Webbrowser und dem Webserver, der mit dem W-Gate verbunden ist, zu betreiben, damit nicht der gesamte Datenverkehr „mitgehört“ werden kann.

**Parimetercheck**

Eine vom Matsushita Konzern beauftragte Firma, die sich auf Internet-Sicherheit spezialisiert hat, führt in gewissen Abständen sogenannte Parimeterchecks durch, um die Sicherheit der Firewall zu testen. Werden Sicherheitslücken erkannt, sind diese umgehend zu beseitigen.

**VPN-Tunnel**

Die Firewall ist zusätzlich in der Lage eine sichere VPN-Verbindung über IPsec-Clients (lizenzpflichtig) oder über PPTP aufzubauen, worüber eine

---

1. RAID ist die Abkürzung für Redundant Array of Inexpensive Disks. Bei dem RAID-Level 5 werden die Parity-Daten auf allen Laufwerken des Arrays verteilt. Beschreibung dazu im Internet: http://www.glossar.de/glossar/z_raid.htm (Zugriff: 24-Mai-2002).
2. Die Modell-Bezeichnung der Firewall lautet: Watchgurad Firebox 1000.

sichere Verbindung zum internen Netzwerk (E-Mail und Netzlaufwerke) über das Internet hergestellt werden kann.

### 6.6.2 SAP-Sicherheit

**SAProuter**

Zur Absicherung des SAP-Systems im lokalen Netzwerk setzt ECOM einen SAProuter ein, wodurch eine zusätzliche Kontrolle der Zugriffe auf das System geboten ist. Dieser SAProuter ist direkt auf der AS400 installiert und dem SAP-System vorgeschaltet.

**Berechtigungskonzept**

Innerhalb des Systems nutzt ECOM das, von der Firma Orange Five GmbH erarbeitete, Berechtigungskonzept. Dadurch sind die einzelnen Transaktionen vor unberechtigten Zugriffen geschützt.

**Passwort-Schutz**

Die Parameter zum Passwort-Schutz, bei dem SAP durchaus einigen Spielraum einräumt, sind seitens ECOM sicherheitsbewusst eingestellt. Beispielsweise sind die Optionen so gewählt, dass nach dreimaligem Eingeben des falschen Passwortes der Benutzer gesperrt und erst durch den Administrator wieder freigeschaltet werden kann.

**sichere Datenübertragung**

Bei der Datenübertragung von elektronischen Dokumenten mit anderen Geschäftspartnern wurde über das Thema Sicherheit noch nicht weiter nachgedacht. Die Nachrichten, die über das Pananet, respektive über die Telebox 400 der Deutschen Telekom gesendet werden, sind nur durch dessen Sicherheitsvorkehrungen geschützt. Eine Verschlüsselung der Daten seitens ECOM oder eines Geschäftspartners findet derzeit noch nicht statt. Deshalb ist es sinnvoll, den Einsatz eines externen Sicherheitsproduktes, über die von SAP zur Verfügung gestellten Schnittstellen, zur Ver- und Entschlüsselung von Daten, in Erwägung zu ziehen.

In absehbarer Zukunft wird ECOM allerdings auf ein neues „Format-Paket“ mit dem Namen Panasonic e-Procurement umsteigen, das zur Absicherung eine asynchrone Verschlüsselung mit zusätzlichem digitalen Zertifikat benutzt. Dadurch wird die Authentizität und Integrität gewährleistet und die Dokumente erlangen einen verbindlichen Character.

# 7

# B2B Connection bei ECOM

ERP-Systeme werden miteinander verbunden, um Geschäftsprozesse über Systemgrenzen hinaus abbilden zu können. So wird eine enge Kooperation mit den Geschäftspartnern ermöglicht. Dieser Aspekt ist um so erstrebenswerter, je kostengünstiger die Installation, je geringer der Aufwand und je höher der Return on Investment (RoI) sich darstellen.

**Komfort der Schnittstelle**

Der Komfort der Schnittstelle hat entscheidenden Einfluss auf die Realisierung. Leicht einzurichtende Schnittstellen führen zu einer schnellen Umsetzung derartiger Projekte, wodurch erhebliche Implementierungskosten eingespart werden.

**gute Voraussetzungen**

Gute Voraussetzungen sind gegeben, wenn beide Geschäftspartner die gleiche Software einsetzen, da die Schnittstellen optimal aufeinander abgestimmmt sind. Bei Partnern mit unterschiedlichen ERP-Systemen ist eine direkte Verbindung, aufgrund der Kosten und Strukturen, nicht unbedingt sinnvoll. Deshalb wurde im Rahmen dieser Diplomarbeit untersucht, welche Möglichkeiten für ECOM durch die SAP-Schnittstellen gegeben sind und welchen Einfluss dies für die Geschäftspartner hat.

## 7.1 Ist-Situation

In Kapitel 5.4 wurde bereits beschrieben, wie der elektronische Nachrichteneingang und Nachrichtenausgang bei ECOM realisiert ist. Die Tabelle 7.1 gibt einen Überblick über die Nachrichtenarten, die mit den Geschäftspartnern elektronisch ausgetauscht werden.

Gegenüber der Weitergabe von Nachrichten per Fax oder per Post, ergeben sich eine Reihe von Vorteilen, die im folgenden Unterkapitel erläutert sind. Aufgrund der besonderen Beziehung zu der Panasonic Industrial Europe GmbH erfolgt eine getrennte Beschreibung der Ist-Situation.

| EDI Partner | Message type | Message format | Übertragungsweg |
|---|---|---|---|
| Purchase ECOM | | | |
| Murata | ORDERS | EDIFACT | X.400 |
| Singapore Components (SINCOM) | ORDERS, INVOIC, ORDRSP, DESADV | EDIFACT | GIS |
| Matsushita Electronic Components (MECOM) | ORDERS, DESADV | EDIFACT | GIS |
| Matsushita Electric International Business Operation (MEI IBO) | ORDERS, ORDRSP, DESADV, INVOIC | EDIFACT | GIS |
| Sales ECOM | | | |
| Matsushita Audio Video Devices (MAVD) | ORDERS | EDIFACT | GIS |
| Panasonic Industial Europe (PIE) | ORDERS | EDIFACT | GIS |
| Matsushita Television Europe (MTE) | ORDERS | EDIFACT | GIS |
| Matsushita Electronic UK (MELUK) | ORDERS, ORDCHG | EDIFACT | GIS |

Tabelle 7.1: EDI-Partner von ECOM

### 7.1.1 Benefit durch EDI

**Kürzere Bearbeitungszeit u. schnellere Abwicklung**

Die Übermittlung der Daten in vereinbarten Austauschformaten führt dazu, dass ECOM beim Empfang auf eine Neuerfassung verzichten kann. Das führt zu wesentlich kürzeren Bearbeitungszeiten und einer schnelleren Abwicklung von Geschäftsvorgängen.

**geringere Personalkosten**

Dies wiederum generiert positive Kosteneffekte aufgrund der Einsparung von Personal für die Erfassung und des geringeren Zeitaufwandes zur Bearbeitung eines gesamten Geschäftsvorganges. Dazu kommt ein geringerer Lagerbestand, sowie die daraus resultierenden Einsparungen im Bereich der Lagerhaltung und des gebundenen Kapitals. Zudem steigt die Datenqualität, da ohne manuelle Neuerfassung keine Erfassungsfehler gemacht werden.

**frühere Disposition**

Schneller übermittelte Rechnungen ermöglichen ECOM eine frühe Disposition, wodurch sich auch die Zeit zwischen Rechnungserstellung und Bezahlung verkürzt, insbesondere wenn die Bezahlung vom Rechnungseingangsdatum abhängt.

**geringere Übertragungskosten**

Die Einsparungen im Bereich Papier, Formular, Druck und Porto sind abhängig von dem Weg der Datenübertragung. Werden die Daten über VANs ausgetauscht, wie es auch bei ECOM der Fall ist, sind die Einsparungen eher gering, da relativ hohe Kosten für die Datenübertragung aufzubringen sind.

Wird dagegen das Internet als Übertragungsmedium genutzt, so sind die Einsparungen, da keine zusätzlichen Kosten anfallen, entsprechend höher.

**stärkere Kundenbindung**

Insgesamt wird durch EDI eine stärkere Kundenbindung durch intensivere Kontakte und höherer Liefertermintreue erreicht.

### 7.1.2 Geschäftsbeziehungen mit der Panasonic Industrial Europe GmbH

Wie aus der Tabelle 7.1 hervorgeht, werden zwischen ECOM und der Panasonic Industrial Europe GmbH derzeit nur Bestellungen elektronisch ausgetauscht. Darüberhinaus findet keine Informationsweitergabe statt.

Da die Systeme nicht direkt miteinander verbunden sind, wird für den Austausch von beiden Seiten das sogenannte Mapping der Felder und eine Umsetzung der SAP-internen IDocs in das EDIFACT-Format durch Subsysteme vorgenommen. Dieser Ablauf ist in Abbildung 7.1 dargestellt.

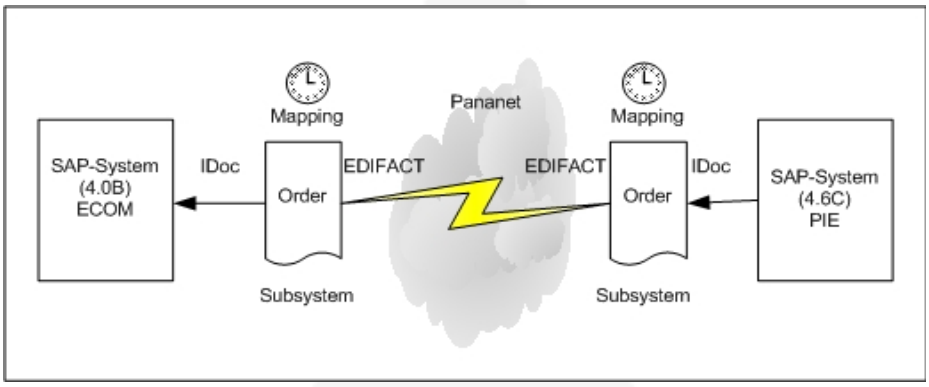


Abbildung 7.1: Indirekte Verbindung ECOM - PIE

**SAP bei PIE**

Da PIE seit dem 1. Februar 2002 ebenfalls SAP einsetzt und sich ein Teil der Mitarbeiter im Hause von ECOM befindet, wird analysiert, welcher Mehrwert durch die direkte Verbindung der SAP-Systeme möglich ist, was an der Ist-Situation verbessert werden kann und wie eine mögliche Umsetzung aussieht.

**Kosten der Datenübertragung**

Derzeit empfängt ECOM monatlich ca. 150 Bestellungen von PIE über das Pananet. Die Kosten pro übertragener Nachricht betragen ca. 68 Cent. Daraus ergeben sich Kosten von € 102. Rechnungen werden per Fax an PIE weitergeleitet. Aufgrund von Teillieferungen kommen monatlich ca. 250 Rechnungen zusammen. Zudem besteht der Wunsch mit Bestellbestätigungen zu arbeiten.

**zwischengespeicherte Daenübertragung**

Der Datenaustausch läuft über eine zwischengespeicherte Übertragung. Das heißt, die Bestellungen werden bei PIE in einem Verzeichnis gesammelt und mittels eines Schedulers zu bestimmten Zeiten übertragen. Das gleiche geschieht seitens ECOM. Die eingehenden Bestellungen werden ebenfalls gesammelt und nach einem festen Zeitplan an das SAP-System übermittelt. Das Übermitteln, bzw. Einspielen der Daten erfolgt pro Tag zwei Mal (9:00 Uhr und 14:00 Uhr).

### 7.1.3Geschäftsbeziehungen zu anderen Partnern[1]

Die Ist-Situation stellt sich so dar, dass teilweise ein Datenaustausch über EDI mit den Geschäftspartnern erfolgt (siehe Tabelle 7.1), mit anderen

wiederum noch keine elektronische Geschäftsbeziehung besteht. Die Übertragung der EDI-Daten findet, genau wie mit PIE, durch Zwischenspeicherung statt und wird zu festen Zeitpunkten ausgeführt.

Darüber hinaus findet ebenfalls kein Austausch aktueller Informationen oder Nachrichten statt.

**heterogene Systemlandschaft**

Aufgrund der heterogenen Systemlandschaften besteht keine Möglichkeit - ohne hohe Investitionen - der direkten Verbindung der Systeme, da ein Return on Investment (RoI) sehr spät oder vielleicht gar nicht erzielt wird.

Deshalb wird untersucht, welche Möglichkeiten SAP und das Internet bieten, um diesen Kunden und Lieferanten aktuelle Informationen zur Verfügung zu stellen.

## 7.2 Motivation of Changes

**SAP global**

Da der Matsushita-Konzern entschieden hat, weltweit, nach und nach die SAP-Software als ERP-System in den einzelnen Unternehmen einzusetzen, soll untersucht werden, welchen Nutzen die direkte Verbindung der SAP-Systeme mitsichbringt.

**Pilotprojekt mit Referenzmodell**

Einen Anfang zur konzernweiten Einführung von SAP machte ECOM im Februar1999. Damals hatte sich der Konzern allerdings noch nicht für eine übergreifende Nutzung von SAP ausgesprochen. Dies erfolgte erst im Jahre 2000 und wurde mit der Implementierung von SAP bei der Panasonic Industrial Europe GmbH initiiert. Aus diesem Projekt resultiert ein Referenzmodell, dass für eine einfache Verbreitung von SAP im Konzern genutzt werden soll.

**Kundenbefragung**

Ein weiterer Motivationsgrund ist eine, im ersten Quartal 2002 durchgeführte, Kundenbefragung. Daraus geht hervor, dass die Kunden Zugriff auf aktuelle Informationen bezüglich Auftragsstatus, Lieferstatus, sowie eine Bestandsübersicht als wichtig einstufen. Diese Kundenwünsche zu erfüllen, hat für ECOM hohe Priorität.

## 7.3 Ergebnisse der Untersuchung

Bei der Untersuchung wurde, wie bei der Ist-Analyse, zwischen den Geschäftsbeziehungen zu PIE und zu anderen Partnern unterschieden. Im folgenden werden die Untersuchungsergebnisse, zuzüglich dem erweiterten Benefit, beschrieben.

### 7.3.1 Ergebnisse bezüglich PIE

**Umgestaltung der Geschäftsprozesse**

Die Untersuchung hat ergeben, dass die Geschäftsbeziehung zwischen ECOM und PIE neu gestaltet werden kann. Durch eine direkte Verbindung der Systeme besteht keine Notwendigkeit der Umwandlung des Übertragungsformates von IDoc zu EDIFACT und umgekehrt. Die Abbildung 7.2

1. Mit anderen Geschäftspartnern sind die Beziehungen zu allen Unternehmen, ausser PIE, gemeint.

zeigt, dass lediglich ein Mapping seitens des Empfängers, aufgrund der verschiedenen Bezeichnungen bei Lieferbedingungen, Zahlungsbedingungen, etc. in den Systemen erforderlich ist.

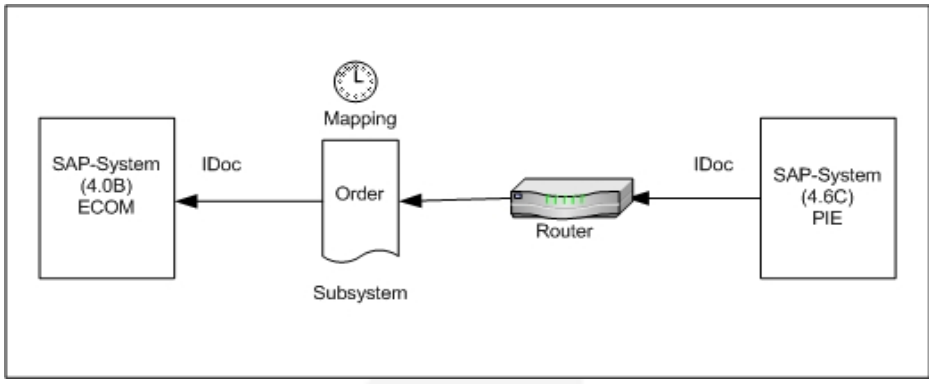


Abbildung 7.2: Direkte Verbindung PIE - ECOM

**Verbindungsszenarien**

Zur Installation der Verbindung sind unterschiedliche Szenarien vorstellbar. Mit einem Hardware-Router oder durch einen Applikation-Gateway ist eine direkte Verbindung der separaten Netzwerke, der beiden Firmen, möglich. Es besteht die Möglichkeit die Router so zu parametrisieren, dass nur auf die SAP-Maschinen zugegriffen werden kann. Alle weiteren Dateien und Verzeichnisse bleiben geschützt, ohne dass eine zusätzliche Rechtevergabe notwendig ist.

Da SAP den SAProuter kostenlos zur Verfügung stellt, fallen bei diesem Weg nur Kosten für einen zusätzlichen PC an. Die Realisierung mit den Hardware-Router ist nicht wesentlich teurer und erfordert keine zusätzlichen Programme. Vorteile einer Hardware-Lösung sind höhere Betriebs- und Ausfallsicherheit, sowie eine bessere Performance.

**sofortige Verarbeitung**

Die direkte Verbindung läßt eine unmittelbare Übertragung von Daten zu. Die Nachrichten ruhen nicht Stunden in Verzeichnissen, wodurch die Aktualität der Daten im System wesentlich zunimmt.

**Automatisierung ohne Medienbrüche**

Weiterhin ergibt sich aus der Untersuchung, dass neben Bestellungen auch Bestellbestätigungen und Rechnungen von SAP-System zu SAP-System ausgetauscht werden können. Im Bereich Bestellbestätigungen werden derzeit hin und wieder Excel-Dateien ausgetauscht, die aufgrund von Verfügbarkeitsprüfungen die möglichen Liefermengen bestätigen. Die Realisierung über SAP bringt daher auf beiden Seiten die Möglichkeit einer weitgehenden Automatisierung ohne Medienbrüche. Durch die Umstellung der Rechnungen von Telefax auf EDI fällt der Medienbruch ebenfalls weg.

Dies führt zu Kosteneinsparungen, da eine Übertragung über das VAN nicht weiter erforderlich ist. In Zahlen: Zum einen können € 102 für die Bestellungen eingespart werden. Zum anderen kommt die Einsparung der Kosten, die anfielen, wenn Bestellbestätigungen (ca. 150 Stück/Monat = € 102) und Rechnungen (ca. 250 Stück/Monat = € 170) ebenfalls über das VAN übertragen würden. Das führt zu einem Gesamtersparnis von monat-

lich € 374, sowohl für ECOM als auch für PIE, da auch beim Empfang von Daten Kosten verursacht werden.

**One-Step-Business**

Wichtig ist auch der Erstellungszeitpunkt der Nachrichten. Durch die direkte Verbindung der SAP-Systeme ist die Einrichtung eines sogenannten One-Step-Businesses möglich. Dabei werden Realtime-Geschäftsvorgänge unter Beteiligung der beiden Geschäftspartner vollständig automatisiert und mit einem einzigen Mausklick abgewickelt.

Das heißt, sobald PIE durch eine Kundenbestellung einen Verkaufsauftrag anlegt, löst dieser unmittelbar einen Beschaffungsauftrag aus, der wiederum unmittelbar einen Verkaufsauftrag in dem System von ECOM zur Folge hat.

**SCP-Interface**

Eine weitere Möglichkeit ALE zu nutzen ist das Supply Chain Planning-Interface (SCP-Interface).[1] Dadurch können folgende Szenarien realisiert werden:

**Verteilung der Absatz- u. Produktionsgrobplanung**

Neben dem direkten Austauschen von Bestellungen, Bestellbestätigungen und Rechnungen besteht auch die Möglichkeit, die Absatz- und Produktionsgrobplanung für bestimmte Produkte zu verteilen. Da solche Daten derzeit zwischen ECOM und PIE nicht ausgetauscht werden, kann dadurch die Aktualität und Genauigkeit im Forecast-Bereich wesentlich erhöht und verbessert werden. Voraussetzung ist das Anlegen der Informationsstrukturen für Sales & Operations Planning (SOP).[2]

**unternehmensübergreifendes Controlling**

Darüber hinaus ist ein Austausch kumulierter Informationsdaten möglich. Dafür muss im Logistikinformationssystem eine Informationsstruktur festgelegt werden, in der auch das logische System aufgenommen ist. Zudem muss die Informationsstruktur in den beteiligten Systemen jeweils gleich sein. Dies erlaubt ein unternehmensübergreifendes Bestands-, Einkaufs- und Vertriebscontrolling.[3]

**schnelle Reaktion durch aktuelle Daten**

Aus der aktuellen Bedarfs- und Bestandsliste können IDocs erzeugt und über das SCP-Interface auszutauschen. Dazu kommen weitere Bewegungsdaten die übertragen werden können: Fertigungsaufträge, Serienaufträge und Planaufträge. Genau zu wissen, welche Aufträge und Bestände PIE in Bezug auf ECOM aktuell im System hält, vermeidet zum einen Deadstock, erlaubt anderen aber auch schnelle Reaktionen auf erhöhte Bedarfe zu.[4]

**einsehen von Daten im Partnersystem**

Zudem bietet ALE noch einen ganz anderen Ansatz. Vorstellbar ist ein Szenario, bei dem für ECOM oder PIE im jeweiligen Partnersystem ein Benutzer berechtigt wird nur Daten einzusehen, die sein Unternehmen betreffen. Dadurch können aktuelle Informationen, bezogen auf den Kundenauftragsstatus, Lieferstatus und auf Bestandsinformationen, direkt abgefragt werden.

---

1. Das Supply Chain Planning-Interface wird über den Pfad: Logistik > Zentrale Funktionen > SCP-Interfaces aufgerufen.
2. [SAPDOKU1999] Thema: Supply Chain Planning.Interface.
3. [SAPDOKU1999] Thema: Logistikinformationssystem.
4. [SAPDOKU1999] Thema: aktuelle Bedarfs- und Bestandsliste.

### 7.3.2 Ergebnisse bezüglich anderer Geschäftspartner

Die Geschäftsbeziehungen zu Partnern, die kein SAP-System einsetzen, bzw. zu denen keine EDI-Verbindung besteht, kann auf zwei Arten verbessert werden.

**Austausch zusätzlicher Nachrichtenarten**

Zum einen sollte darüber nachgedacht werden, ob nicht zusätzliche Nachrichtenarten, als die in der Tabelle 7.1 aufgezählten, per EDI ausgetauscht werden können. Zum anderen ist für jeden Kunden und Lieferanten, mit denen die Geschäftsdaten per Telefax oder Post ausgetauscht werden, zu prüfen, inwiefern eine elektronische Verbindung hergestellt werden kann. Wichtig dabei sind Fragen, wie: Welche ERP-Software wird eingesetzt? Wie sieht die Verbindung zum Internet aus? Besteht ein Vertrag mit einem VAN-Diensteleistungsanbieter? Welche Übertragungsformate kommen in Frage?

Ziel sollte es sein, mit möglichst vielen Kunden und Lieferanten Bestellungen, Bestellbestätigungen, Bestelländerungen, Rechnungen, sowie Lieferabrufe auf elektronischem Weg auszutauschen. Die in der Tabelle 7.1 genannten Unternehmen haben die Voraussetzungen zum elektronischen Datenaustausch bereits geschaffen. Eine Erweiterung der bestehenden Nachrichtenarten ist deshalb nicht mit zusätzlichen Hardwarekosten verbunden.

**Herausforderungen**

Die Herausforderungen bestehen zum einen in der Unterzeichnung und der Einigung des EDI-Vertrages, zum anderen in der Notwendigkeit, in den Systemen die EDI-Stammdaten und Konvertierungsregeln zu erweitern und anzupassen.

**Internet-Schnittstelle**

SAP bietet mit dem Internet Transaction Server eine Schnittstelle für das SAP-System zum Internet. ECOM kann diese Schnittstelle nutzen, um den Geschäftspartnern aktuelle Informationen aus dem SAP-System zur Verfügung zu stellen. Eine Prüfung des Kundenauftragsstatus und der Verfügbarkeit von Beständen ist genau so möglich, wie die Abfrage des Kontostandes.

### 7.3.3 Erweiterter Benefit

**ALE**

Eine beschleunigte Informationsweitergabe ist eine Voraussetzung zur Bestandsreduzierung. Dies geschieht durch eine weitere Verringerung der Übermittlungszeiten gegenüber EDI, wodurch die gehaltenen Daten an Aktualität gewinnen.

Dazu kommt eine Vereinfachung des Mappings, da keine Umwandlung in das EDIFACT-Format notwendig ist und nur der Empfänger Inhaltsumwandlungen der Felder vorzunehmen braucht.

**geschlossener Datenkreislauf**

Der geschlossene Datenkreislauf kann sukzessive für die Übermittlung weiterer Informationen genutzt werden und somit die Geschäftsbeziehungen stärkt.

**One-Step-Business**

Aus dem One-Step-Business ergeben sich besondere Vorteile in Form von Erleichterung und Beschleunigung des gesamten Kauf- und Verkaufsprozesses.

**ITS**

Durch den Einsatz des Internet Transaction Servers werden die Geschäftspartner jederzeit mit exakten Informationen versorgt. Das hinterläßt einen positiven Einfluß auf die Geschäftsbeziehung und verschafft Wettbewerbsvorteile.

Die selbständige Abfrage von Beständen, Kontoinformationen und des Lieferstati erhöhen das Einsparungspotential durch die Entlastung der eigenen Mitarbeiter.

Über den ITS kann somit ein intelligenter Kundensupport gestaltet werden, der eine umfassende Pre- und Aftersales-Betreuung ermöglicht.

## 7.4 Lösungsansätze

Die Lösungsansätze beschreiben, wie die ermittelten Untersuchungsergebnisse in die Praxis umgesetzt werden. Zum einen wird die Einrichtung und Anpassung des Internet Transaction Servers erläutert, zum anderen die direkte Verbindung zweier SAP-Systeme über ALE.

### 7.4.1 ITS-Projekt

Im Rahmen der Diplomarbeit wurde der Internet Transaction Server auf einem dedizierten Rechner mit dem Betriebssystem Windows 2000 Server eingerichtet.

**Installationsparameter**

Im weiteren Verlauf erfolgte die Installation der Administrator-Instanz, sowie des A- und W-Gates. Dabei wurden die notwendigen Informationen (IP-Adresse des SAP-Anwendungsserver [192.168.0.200], die Systemnummer [01] und die Systembezeichnung), welche für die Verbindung zum SAP-System notwendig sind, eingegeben.

Damit der ITS aus dem Internet zugreifbar ist, wurde eine offizielle IP-Adresse 193.99.35.30) mit entsprechendem Port (81) vergeben. Allerdings verhindern die meisten Firewalls eine Kommunikation über Port 81. Deshalb wird darüber nachgedacht, den ITS über Port 80 freizuschalten.

Aufgerufen werden kann der ITS somit über das Internet mit der URL: http://193.99.35.30:81.

**Benutzerpflege**

Im SAP-System sind unterschiedliche Benutzer anzulegen. Ein SAP-User mit den Berechtigungen zum Ausführen von ABAP-Programmen, RFC-Zugriff und für die aus dem Internet aufzurufenden Transaktionen. Dazu sind weitere Internetbenutzer zu registrieren, welche mit der Kundennummer übereinstimmen, so dass jeder Kunde nur die Informationen einsehen kann, die ihn betreffen.

**Realisierung des Kundenauftragsstatus**

Zunächst steht nur das Abrufen des Kundenauftragsstatus zur Verfügung. Dieser ist über den Service VW10 realisiert.[1] Dahinter steht ein ABAP-Programm im SAP-System, sowie Service-Dateien und HTML-Templates auf dem ITS. Die URL zum direkten Aufrufen des Service lautet: http://193.99.35.30:81/scripts/wgate/vw10/!

1. Damit der von SAP ausgelieferte Service VW10 auch für die Kunden von ECOM benutzt werden kann, war eine Anpassung zur Ausgabe der Materialnummern notwendig, die die hausinternen Suffixe unterdrückt.

**Übergabeparameter**

Mittels Fragezeichen (?) und Tilde (~) können noch weitere Parameter über die URL mitgegeben werden.

Beispielsweise:
http://193.99.35.30:81/scripts/wgate/vw10/!?~language=de, führt zu einem Anmeldebildschirm in deutscher Sprache.

http://193.99.35.30:81/scripts/wgate/vw10/!?~language=en, liefert den gleichen Anmeldebildschirm in englischer Sprache.

Die folgende Abbildung zeigt beispielhaft den Auftragsstatus eines Kunden im ITS:

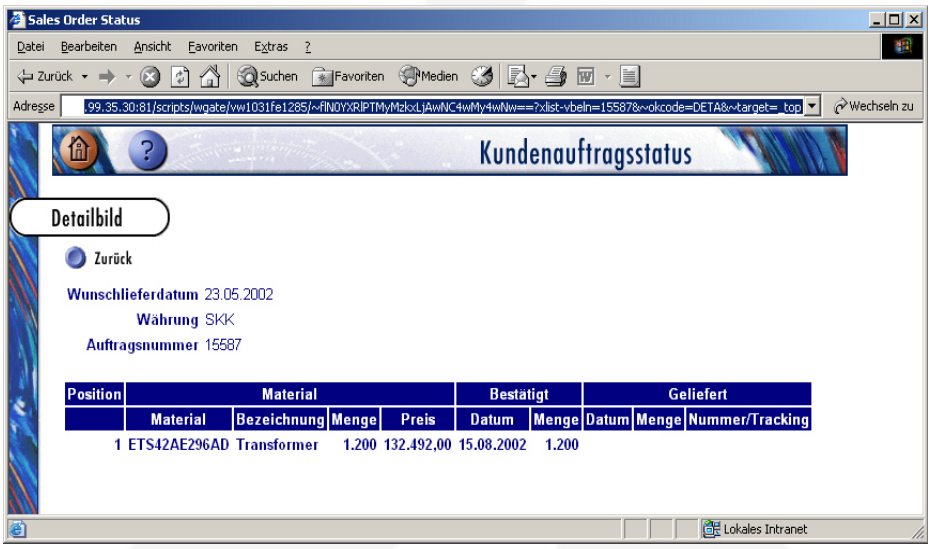


Abbildung 7.3: ITS Kundenauftragsstatus

Diese Parameter können auch in der Konfigurationsdatei des entsprechenden Service voreingestellt werden. Dazu ist die Administrator-Instanz besser geeignet als das SAP@Web Studio, da viele Parameter in Formularfeldern bereits zur Verfügung stehen.

## 7.4.2 ALE-Projekt

Im ALE-Projekt wurde eine Verbindung zwischen zwei SAP-Systemen hergestellt, um Bestellungen, Bestelländerungen und Rechnungen direkt mit PIE austauschen zu können. Es folgt die Beschreibung zur Konfigurations des SAP Systems von ECOM über die Transaktion SALE.

**logisches System einrichten**

Als erstes besteht die Notwendigkeit, ein logisches System einzurichten. Das logische System bildet den Namen eines Partners in der Verteilung ab. Angelegt wurde das logische System „LÜNE“, das im zweiten Schritt dem Mandanten 100 des Produktivsystems zugeordnet wurde.

**Nummernkreise pflegen**

Es folgt das Anlegen der Nummernkreise für die IDocs, damit zwischen internen und externen Belegen unterschieden werden kann und es keine Überlappung der Belegnummern zwischen den Systemen gibt.

**ISO-Code-Umsetzung**

Die Einstellung der ISO-Codes definiert die Umsetzung zwischen ISO-Code und Maßeinheiten. Dies ist erforderlich, da bei der Übertragung in einem IDoc nie die direkte Maßeinheit verwendet wird, sondern immer der jeweilige Code. Da auch eigene Codes angelegt und vorhandene geändert werden können, ist darauf zu achten, dass in beiden Systemen die Umsetzung des ISO-Codes identisch definiert ist.

**WF-Grundeinstellungen**

Wie bereits in Kapitel 4.6 beschrieben, steht ALE im direkten Zusammenhang mit dem Workflow Management. Deshalb müssen die Grundeinstellungen dafür ebenfalls vorgenommen werden. Dies geschieht durch das Starten mehrerer Programme zur Aktivierung von Objekten und Ereignissen.

**Verteilungsmodell**

Im Verteilungsmodell wird der Datenfluss in der Systemlandschaft festgelegt. Durch die Angabe des sendenden und empfangenden logischen Systems und der Datenart, erfolgt die Definition für, beispielsweise, Bestelländerungen und Rechnungen. Damit wird festgelegt, dass alle Bestelländerungen und Rechnungen, beim Anlegen an das andere System, übertragen werden. Über einzustellende Filter erfolgt eine Beschränkung auf Bestelländerungen und Rechnungen, die für PIE bestimmt sind.

**Datenkonvertierung**

Für den Fall, dass das Customizing zwischen den Systemen im Verteilungsmodell voneinander abweicht, sind Datenkonvertierungen zu definieren. Beispielsweise, wenn die Codes für Liefer- und Zahlungsbedingungen in beiden Systemen nicht übereinstimmen.

**Eingabe- u. Ausgabeparameter**

Sind alle Einstellungen im Verteilungsmodell vorhanden, ist eine Partnervereinbarung zu generieren. Für die Ausgabeparameter ist festzulegen, ob die IDocs sofort übergeben oder gesammelt werden. Dahingegen sind für die Eingabeparameter die Optionen sofortige Verarbeitung oder Verarbeitung im Hintergrund möglich. Bei ECOM werden die IDocs sofort ausgegeben und an das EDI-Subsystem übermittelt, wo sie gesammelt und zu bestimmten Zeiten verteilt werden. Eingehende IDocs werden dagegen sofort verarbeitet.

**RFC-Verbindung**

Unabhängig von den anwendungstechnischen Einstellungen, muss die Kommunikation zwischen den Partnern des Verteilungsmodells definiert werden. Wie in Kapitel 4.6.2 erwähnt, basiert die Kommunikation auf der RFC-Technik. Dazu müssen die Daten für die RFC-Verbindung eingegeben werden. Diese Daten bestehen aus dem Verbindungstyp (3 = R/3-Verbindung), der Zielmaschine (IP-Adresse), der Systemnummer (zweistellig), sowie den Anmeldedaten (Sprache, Mandant, Benutzername und Passwort). Danach erfolgt die Zuordnung der RFC-Destination zum logischen System.

Alle Einstellungen zur Verteilung können beiden Partnersystemen bekannt gemacht werden (Funktionstaste F8). Für den Empfang ist es allerdings nicht notwendig.

**Nachrichtensteuerung**

Damit die Bestelländerungen und Rechnungen auch beim Anlegen über ALE versendet, bzw. gesammelt werden, ist die Nachrichtensteuerung in den SAP-Programmen so zu ergänzen, dass die Erzeugung der IDocs und die Weiterleitung an die ALE-Schicht erfolgt.

Dadurch wurde eine Möglichkeit geschaffen Rechnungen und Bestelländerungen zwischen SAP-Systemen auszutauschen. Die gleiche Konfiguration ist für das entfernte System ebenfalls vorzunehmen.

### 7.4.3 Alternative

Als Alternative kann der Business Connector zur Verbindung von SAP-Systemen eingesetzt werden. Dieser bietet den Vorteil der direkten Verbindung von SAP-Systemen über das Internet.

Da der Business Connector XML und HTML als Datenformat einsetzt, ist es nicht unbedingt erforderlich, dass beide Geschäftspartner mit dem SAP-System arbeiten. Das heißt, das der Business Connector eine Möglichkeit darstellt, Geschäftsprozesse verschiedener Partner unabhängig vom eingesetzten System zu integrieren.

In der Regel einigen sich beide Partner auf ein XML-Format für die auszutauschenden Dokumente. Es besteht aber auch die Möglichkeit, durch sogenannte Module, die SAP kostenlos zur Verfügung stellt, eine Konvertierung vorzunehmen. So kann beispielsweise eine eingehende Bestellung im EDIFACT-Format durch den Business Connector in ein IData Object umgewandelt werden. Dabei erfolgt die Validierung gegen ein Record, das aus einem XML-Schema erzeugt wird. Da der Business Connector die XML-Schnittstelle von SAP darstellt, wird das erzeugte IData Object in ein anderes IData Object, dass das SAP-System repräsentiert, gemappt. Erst danach erfolgt die Übergabe an das SAP-System über einen RFC- bzw. tRFC-Aufruf unter der Nutzung von BAPIs.

Beim Nachrichtenausgang wird der umgekehrte Weg genommen. Allerdings erfolgt keine Validierung, sondern die Daten werden in IData Objectes geschrieben, die auf XML-Templates basieren.

Da der Business Connector ebenfalls kostenlos zur Verfügung gestellt wird und eine Verbindung von Systemen über das Internet die Kooperation mit jeden System und jeden Partner erlaubt und zudem noch, in Kapitel 4.8 genannte, Funktionalität bietet, ist eine Weiterführung dieses Themas sehr vielversprechend.

# 8

# Schlussbetrachtung

Ziel der Arbeit war eine Betrachtung der B2B-Connection am Beispiel von SAP R/3 in einem Unternehmen. Dabei wurde das SAP-System mit seinen Schnittstellen untersucht und Lösungsansätze zur Verbesserung der Beziehungen zwischen Geschäftspartnern aufgezeigt. Es erfolgte ebenfalls eine Betrachtung aus betriebswirtschaftlicher Sicht, die es erlaubt den resultierenden Nutzen aufzuzeigen.

Im Rahmen dieser Diplomarbeit wurde ein "C"-Programm und ein ABAP-Programm zur Lösung firmeninterner Probleme beim Datenaustausch geschrieben.

Darüberhinaus wurde der SAP Internet Transaction Server, sowie der Business Connector, als Alternative gegenüber dem ITS und der direkten Verbindung von SAP-Systemen über ALE, eingerichtet und analysiert.

Aufgrund der Gefahr des Missbrauchs innerhalb des elektronischen Geschäftsverkehrs, z.B. durch Datenmanipulation, verlangt der Einsatz ein integriertes Sicherheitskonzept, welches auf den Schutz der gesamten elektronischen Datenverarbeitung eines Unternehmens abzielt.

Noch für das Jahr 2002 hat die SAP AG eine neue Version ihrer ERP-Software, mit dem Namen SAP R/3 Enterprise, angekündigt, die sowohl den Internet Transaction Server, als auch den Business Connector integriert. Dadurch ist eine einheitliche Entwicklung aus dem SAP-System heraus möglich und zudem wird das System im Rahmen von XML internetfähig ausgeliefert.

Dies macht es "offen" für jede Business-to-Business-Connection und forciert somit den Paradigmawechsel von "ein Unternehmen, ein System, ein Geschäftsvorgang" hin zu "viele Unternehmen kooperieren über Systemgrenzen hinaus".