GS1 Germany

EDIINT AS2 Umsetzungshilfe

GS1 Tech

GS1 Germany-Umsetzungshilfe

zu EDIINT AS2

Hinweis:

Das vorliegende Dokument kann zukünftigen Änderungen unterliegen, um neue internationale technische Spezifikationen zu integrieren, oder um auf neue Geschäftsanforderungen zu reagieren, auf die von Mitgliedern der EDIINT-Anwendergemeinschaft hingewiesen wird.

Ziel der Mitgliedsgesellschaften von GS1 Europe ist es, in Kooperation mit GS1 eine internationale Version dieser Umsetzungshilfe zu entwickeln.

Bitte wenden Sie sich bzgl. der neuesten Version an Ihre nationale GS1-Organisation.

GS1 Germany GmbH

GS1 Germany hilft Unternehmen aller Branchen dabei, moderne Kommunikations- und Prozess-Standards in der Praxis anzuwenden und damit die Effizienz ihrer Geschäftsabläufe zu verbessern. Unter anderem ist das Unternehmen in Deutschland für das weltweit überschneidungsfreie GS1-Artikelnummernsystem zuständig - die Grundlage des Barcodes. Darüber hinaus fördert GS1 Germany die Anwendung neuer Technologien zur vollautomatischen Identifikation von Objekten (EPC/RFID) und bietet Lösungen für mehr Kundenorientierung (ECR - Efficient Consumer Response).

Das privatwirtschaftlich organisierte und kartellrechtlich anerkannte Unternehmen mit Sitz in Köln gehört zum internationalen Netzwerk "Global Standards One" (GS1) und ist die zweitgrößte von mehr als 100 GS1-Länderorganisationen. Paritätische Gesellschafter von GS1 Germany sind der Markenverband und das EHI Retail Institute.

Zu dieser Schrift

Dieses Dokument wurde vom GS1 Europe EDIINT Forum erarbeitet. Der Vorsitzende der Arbeitsgruppe bedankt sich bei den Mitgliedern der Gruppe für ihre Teilnahme und für ihre Unterstützung bei der Entwicklung des vorliegenden Dokuments.

Anders Grangård	GS1 France
Brendan Kernan	GS1 Ireland
Christian Przybilla	GS1 Germany
Stef Spaan	GS1 Netherlands
Jeremy Morton	GS1 Sweden
Gerd Marlovits	GS1 Austria
Rainer Gempp	GS1 Switzerland
Vijay Pindoria	GS1 UK
Pere Rosell	GS1 Spain
João Picoito	GS1 Portugal

Ebenfalls bedankt sich der Vorsitzende bei den folgenden Personen für ihre Beiträge:

John Duker	Procter & Gamble
Gerard Beereport	Albert Heijn
Rienk v.d. Ploeg	InterCommIT
Holger Lubnau	Metro AG

Inhaltsverzeichnis

Abschnitt Seite

Inhaltsverzeichnis

Abbildungsverzeichnis

Abbildung Seite

1 Einleitung

Eines der vorrangigen Ziele von GS1 ist die Standardisierung und Harmonisierung des elektronischen Geschäftsdatenaustauschs.

Das AS2-Projekt wurde im April 2004 gestartet, um Richtlinien für die Einführung und Anwendung der EDIINT-Protokolle (Electronic Data Interchange - Internet Integration) vorzubereiten, die von der IETF (Internet Engineering Task Force) entwickelt worden sind. Diese sehr sicheren Internet-Protokolle gewährleisten den Informationsaustausch zwischen Geschäftspartnern unabhängig von der Art des Übertragungsformats (EANCOM®, XML, etc.).

Eine frühere Projektgruppe von GS1 France stellte fest, dass die IETF-Spezifikationen nicht präzise genug in den Details beschrieben sind, um eine zufriedenstellende Interoperabilität der beteiligten Systeme zu gewährleisten. Vielmehr besteht ein offensichtliches Risiko, dass Implementierungen, die allein auf den AS1- und AS2-Spezifikationen (Applicability Statement) basieren, zu heterogenen Anwendungen mit ungenügender Interoperabilität innerhalb der Anwendergemeinschaft führen können.

Die Mitglieder der Arbeitsgruppe von GS1 France befürworteten daher ausdrücklich die Idee, ein gemeinsames AS2-Profil für die GS1-Anwendergemeinschaft zu entwickeln, das die Interoperabilität beim Datenaustausch gewährleistet. Dies wird als wichtige Voraussetzung für ein zügiges Wachstum des elektronischen Datenaustauschs entlang der gesamten Lieferkette gesehen.

1.1 Zielsetzung dieses Dokuments

Das vorliegende Dokument hat zum Ziel, einen funktionellen Überblick und ein technisches Rahmenwerk für die Implementierung des EDIINT AS2-Protokolls bereitzustellen. Es basiert auf der Arbeit und den Schlussfolgerungen des von GS1 France geleiteten GS1 Europe EDIINT Forums, das für eine Harmonisierung der Implementierungen dieses Standards eingerichtet wurde. Dieses Dokument basiert auf Erfahrungswerten und Best Practice-Empfehlungen, die während der Arbeitsgruppensitzungen zur Verfügung gestellt wurden.

1.2 Zielgruppe

Diese Umsetzungshilfe ist für die GS1-Anwendergemeinschaft - unabhängig von ihrer Branchenausrichtung - in Europa gedacht. Das Dokument ist speziell für alle professionellen Anwender geschrieben worden, die Unterstützung für den Einsatz des AS2-Protokolls benötigen.

1.3 Anwendungsbereich

Die Umsetzungshilfe stellt ein harmonisiertes AS2-Profil zur Verfügung. Sie ersetzt oder überschreibt nicht die von der IETF veröffentlichte AS2-Spezifikation oder die Arbeit von GS1 France. Deren Empfehlungen wurden in dieses Dokument übernommen, jedoch in einigen Teilen detaillierter beschrieben. AS2-Profile anderer Anwendergruppen und Länder wurden ebenfalls in die Diskussionen aufgenommen, die zu dem vorgelegten Dokument geführt haben. Zudem hat die Gruppe Richtlinien für den Gebrauch optionaler und bilateral zu vereinbarender Funktionen bereit gestellt.

1.4 Was ist "EDIINT"?

Das Projekt zu EDIINT wurde von der IETF initiiert, um ein Protokoll zu definieren, das den EDI-Datenaustausch über das Internet ermöglicht, und zwar bei gleichzeitiger Beibehaltung des Verfügbarkeitsgrades bestehender EDI-Austauschprozesse über Breitbandnetze (Value Added Networks - VAN). Das Ziel war, von den Vorteilen der Internet-Technologien zu profitieren, ohne die im Echtbetrieb befindliche EDI-Nutzerbasis negativ zu beeinflussen.

Breitbandnetze garantieren die Vertraulichkeit, Unversehrtheit und Unleugbarkeit der ausgetauschten Informationen ebenso wie die Authentifizierung der Partner. Die Vorgehensweise bei dem EDIINT-Projekt bestand darin, die vielen Technologien, die diese Funktionen für das Internet bereits boten, zu analysieren, zu bewerten und eine integrierte Lösung für die Anwendergemeinschaft bereitzustellen.

Die EDIINT-Protokolle stellen jeweils Umschläge bereit, die es ermöglichen, Daten über das Internet (oder TCP/IP-basierte Netzwerke) zu übermitteln. Dies geschieht entweder mit Hilfe des HTTP-Protokolls HyperText Transfer Protocol, das die Grundlage des World Wide Web bildet, oder mit dem allgemeinen Simple Mail Transfer Protocol - SMTP, oder mit dem File Transfer Protocol - FTP.

1.5 Vorteile von EDIINT

Der elektronische Geschäftsdatenaustausch zwischen Unternehmen (Business-to-Business - B2B) stellt folgende Mindestanforderungen:

- Gemeinsam vereinbarte Nachrichtenformate (derzeit EANCOM® und XML).
- Ein gemeinsames Netzwerk, in diesem Fall das Internet.
- Sicherer Versand von Dokumenten zum vorgesehenen Empfänger.
- Sichere Übertragung von Dokumenten, die gewährleistet, dass die Informationen während des Transports über das Netzwerk nicht gelesen werden können.

- Unleugbarkeit; d.h. Sender und Empfänger von Informationen können nicht abstreiten, ein Dokument gesendet bzw. empfangen zu haben.

- Der genaue Status eines Dokuments; d.h. in der Lage zu sein, Veränderungen seines Inhalts feststellen zu können.

Idealerweise bietet ein B2B-System außerdem:

- Die Verwaltung der Zusammenarbeit zwischen den Handelspartnern, um den Informationsfluss und den Informationstyp zu steuern, der zwischen verschiedenen Partnern ausgetauscht werden kann.

- Software, die Informationen in ein für den Empfänger geeignetes (Daten-)Format übersetzt.

- Telekommunikationsdienstleistungen von traditionellem EDI über private Netzwerke bis hin zu Mehrwertdienstleistungen über das Internet.

Die Mehrzahl dieser technischen Eigenschaften, beispielsweise die Formate und die Unleugbarkeit, wurden durch die Entwicklung von Standards wie UN/EDIFACT, EANCOM®, ANSI X12 und zuletzt durch B2B-Anwendungen auf Basis von XML wie GS1 XML, cXML und OAG adressiert.

1.6 Basisfunktionen von EDIINT

Anstatt neue Lösungen zu entwickeln, nutzt EDIINT existierende Standards, um zuverlässige und abgesicherte Datenaustauschprozesse zu gewährleisten. Beispielsweise garantiert die Nutzung elektronischer Zertifikate, dass die Dokumente ausschließlich an den vorgesehenen Empfänger versandt werden, dass die Übertragung abgesichert und die Identität des Senders authentisch ist. Der EDIINT-Standard ermöglicht die Nutzung der fortschrittlichsten Algorithmen für Verschlüsselung und elektronische Signaturen, die verfügbar sind.

Auf der anderen Seite deckt EDIINT nicht speziell das Problem von Attacken gegen private und öffentliche Netzwerke ab. Die Systemsicherheit beruht auf der Verwendung von Routern und Firewalls, die die Server isolieren und feindlichen Verkehr registrieren.

Um zu garantieren, dass ein Dokument während des Datenaustauschs nicht verändert worden ist, ist es notwendig, die Spur des Datenaustauschs auf verschiedenen Stufen rückverfolgen zu können. Drei dieser Stufen werden normalerweise durch sämtliche Kommunikationsstandards abgedeckt:

- Die Kommunikationsantwort (Communication Response) bestätigt, dass die Datei ordnungsgemäß durch das Kommunikationsprotokoll erhalten wurde.
  Beispiel: Die erwarteten 256 Bytes wurden empfangen.

- Die Funktionsantwort (Functional Response) bestätigt, dass eine gültige Nachricht von einer Geschäftsapplikation empfangen wurde.
  Beispiel: Der EDI-Umschlag wurde geöffnet und der Inhalt des Dokuments war syntaktisch korrekt.

- Geschäftsprozessantwort (Business Level Response) bestätigt, dass der Inhalt der Nachricht gemäß des vereinbarten Geschäftsprozesses strukturiert ist.
  Beispiel: Die empfangene Bestellung beinhaltet alle vereinbarten Datenelemente.

Der EDIINT-Standard fügt eine zusätzliche Stufe hinzu, um die Spur eines Datenaustauschs zu verfolgen: die Meldung über die Verwendung der Nachricht (Message Disposition Notification - MDN). Weil EDIINT die Nachricht während der Übermittlung einkapselt, ist es notwendig zu wissen, ob die Nachricht ordnungsgemäß beim Server des Empfängers angekommen ist. Der EDIINT-Umschlag kann wiederum einen weiteren Umschlag (beispielsweise für ANSI X12 oder UN/EDIFACT) enthalten, der das eigentliche Dokument beinhaltet.

EDIINT-konforme Software packt den Umschlag aus und sendet die Meldung über die Verwendung der Nachricht (MDN) zurück.

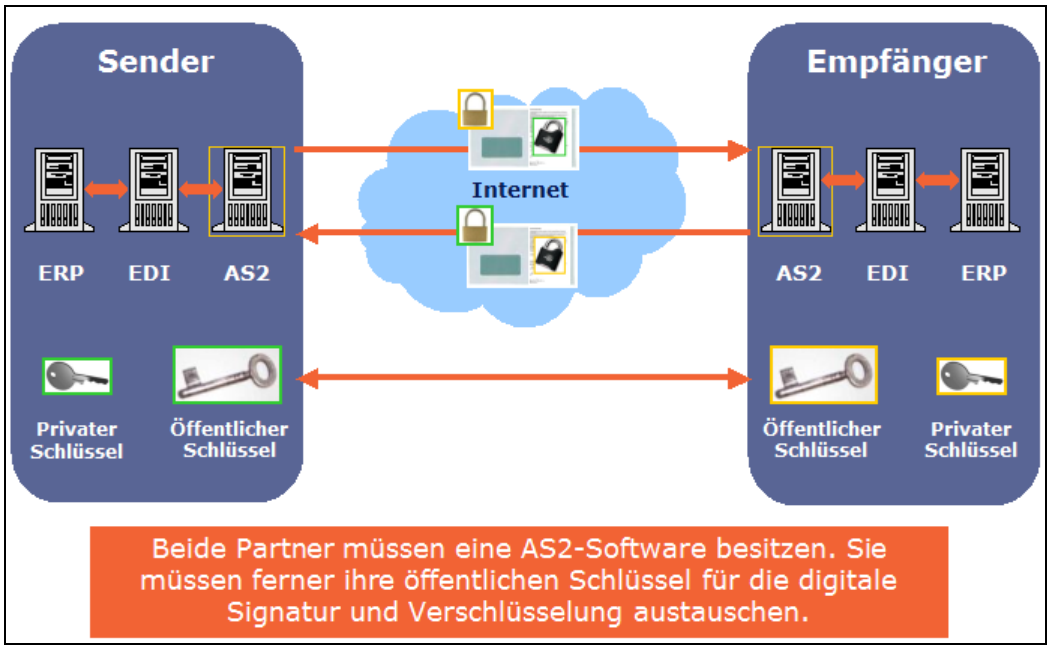

Abb. 1: AS2-Prozessablauf

1.7 Implementierung von EDIINT

Jeder elektronische Datenaustausch benötigt die Angabe eines Senders und eines Empfängers. Der Kommunikationsserver des Empfängers "lauscht" permanent nach Nachrichten im Internet, die an ihn adressiert sind. Der allzeit bereite Austauschprozess ähnelt dem eines Telefons mit Anrufbeantworter. Der Anrufbeantworter "lauscht" nach eintreffenden Anrufen. Falls jedoch der Anrufbeantworter ausgeschaltet ist, kann der Empfänger die Nachricht verpassen.

EDIINT ist so konzipiert, dass alle Arten von Dokumenten übermittelt werden können. In der Praxis wird es jedoch hauptsächlich für Transaktionen in Verbindung mit EDI- und XML-Datenübertragungen eingesetzt.

Zwischen X.400, dem von der ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) definierten, europäischen Standard für die Übertragung von Daten über öffentliche Netzwerke und EDIINT bestehen jedoch zwei wesentliche Unterschiede:

- EDIINT funktioniert ausschließlich in TCP/IP-basierten Netzwerken.
- Bei AS2 muss die Anwendung des Empfängers in dem Moment, in dem das Dokument gesendet wird, mit dem Internet verbunden sein.

Es müssen bestimmte technische und funktionelle Voraussetzungen erfüllt sein, um eine EDIINT-Lösung zu implementieren. Dabei gibt es jedoch eine Reihe von optionalen Anforderungen, die harmonisiert werden müssen.

Der erste Teil des vorliegenden Dokuments erklärt diese Optionen. Der zweite Teil stellt die Empfehlungen des GS1 Europe EDIINT Forums im Detail vor, die zwischen Händlern, Lieferanten und IT-Dienstleistern vereinbart wurden.

1.8 Implementierung des AS2-Protokolls

AS2 setzt eine Reihe von technischen Einstellungen voraus:

- Architektur und Firewalls
- Sicherheit durch die Nutzung digitaler Zertifikate (Anzahl, Typ, Klasse und Gültigkeit, Signaturalgorithmen, Verschlüsselungsalgorithmen)
- Protokolle für den Transport (HTTP und HTTP/S)
- Internetverbindungen (Art und Adressierung)
- AS2-Kopfinformationen (Von- und Zu-Adressierung)
- Empfangsbestätigung (signiert oder unsigniert, synchron oder asynchron)

- Zeitstempel
- Formate (MIME, S/MIME und Komprimierung)
- AS2-Version
- Ports für Ein- und Ausgangsnachrichten

1.9 IT-Architektur und Firewalls für AS2

Einige potenzielle Sicherheitsrisiken, die bei der Nutzung des Internet für den Geschäftsdatenaustausch entstehen, werden durch EDIINT nicht beseitigt. Die am weitesten verbreitete Methode zur Vermeidung oder Minimierung dieser Attacken, ist die Verwendung von Firewalls, die in eingehende Transaktionen "reinlauschen" und die Attacken gemäß vorher festgelegten Regeln herausfiltern.

Drei Vorgehensweisen sind für die Konfiguration von Firewalls möglich:

- Das Platzieren des EDIINT-Servers innerhalb eines Local Area Network (LAN) neben anderen Servern des Unternehmens. Die Server sind ohne Nutzung eines Reverse Proxy Servers durch eine Hardware Firewall vom Internet getrennt. Obwohl diese Konfiguration nicht empfohlen wird, könnte sie von kleinen Unternehmen ausgewählt werden (siehe Abb. 2).

- Eine bessere Konfiguration zeigt Abbildung 3, die den Aufbau einer "demilitarisierten Zone" (DMZ) veranschaulicht. Eingehende Verbindungen aus dem Internet werden in diesem Netzwerk getrennt von den anderen Servern des Unternehmens verarbeitet. Die Server in der DMZ enthalten keinerlei geschäftskritische Informationen wie z. B. EDI-Dateien für eine längere Zeit. Stattdessen werden die Daten zum LAN zur Weiterverarbeitung transportiert.

- Das Netzwerk kann noch sicherer gemacht werden durch die Nutzung eines Reverse Proxy Servers, auf den alle eingehenden Verbindungen aus dem Internet gerichtet sind (siehe Abb. 4). Obwohl diese Konfiguration sehr sicher ist, kann sie manchmal zu Problemen führen, wenn beispielsweise HTTP/S mit Authentifizierung des Client genutzt wird oder in Kombination mit synchroner MDN. Zusätzlich können an der Firewall für IP-Adressen und Ports Filter eingerichtet werden, die den Zugang zur EDIINT-Software reglementieren und nur für jene eingehenden Verbindungen freigeben, die von bekannten IP-Adressen der Geschäftspartner stammen.

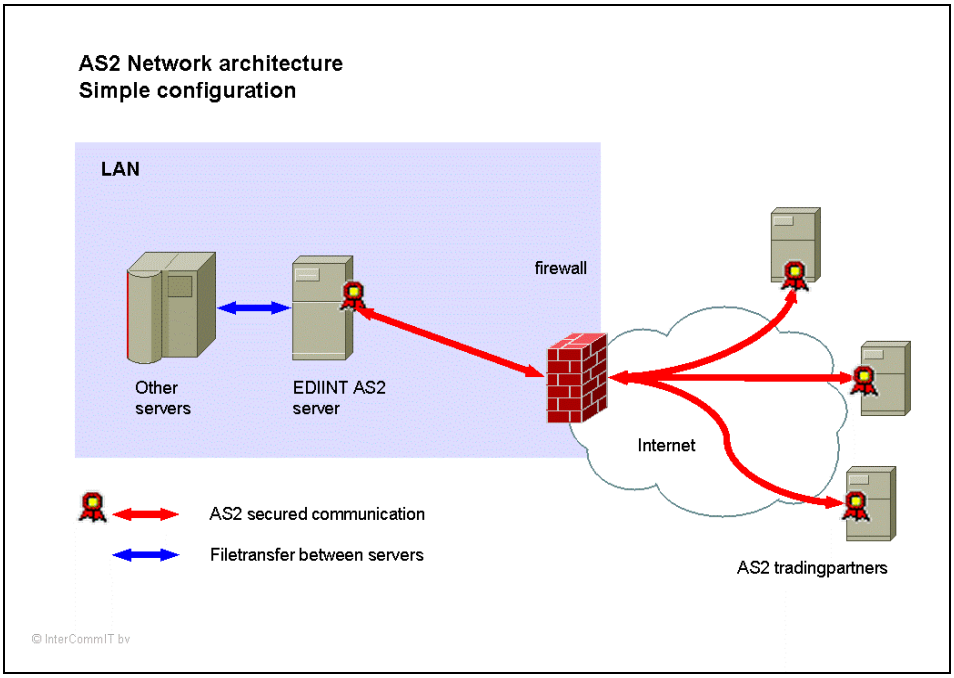

Abb. 2: IT-Architektur ohne DMZ

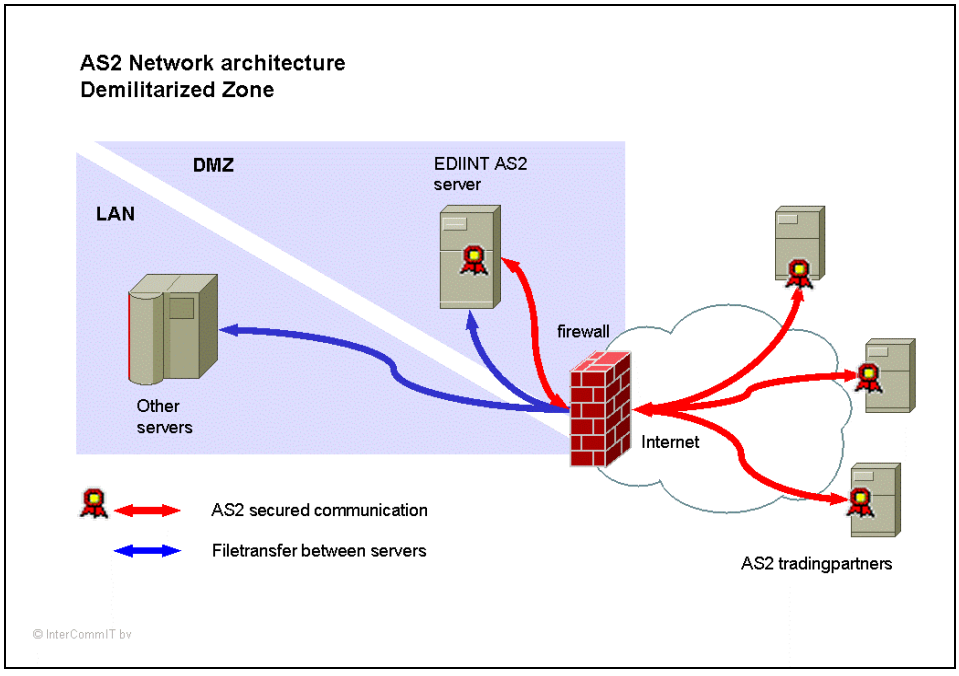

Abb. 3: IT-Architektur mit DMZ

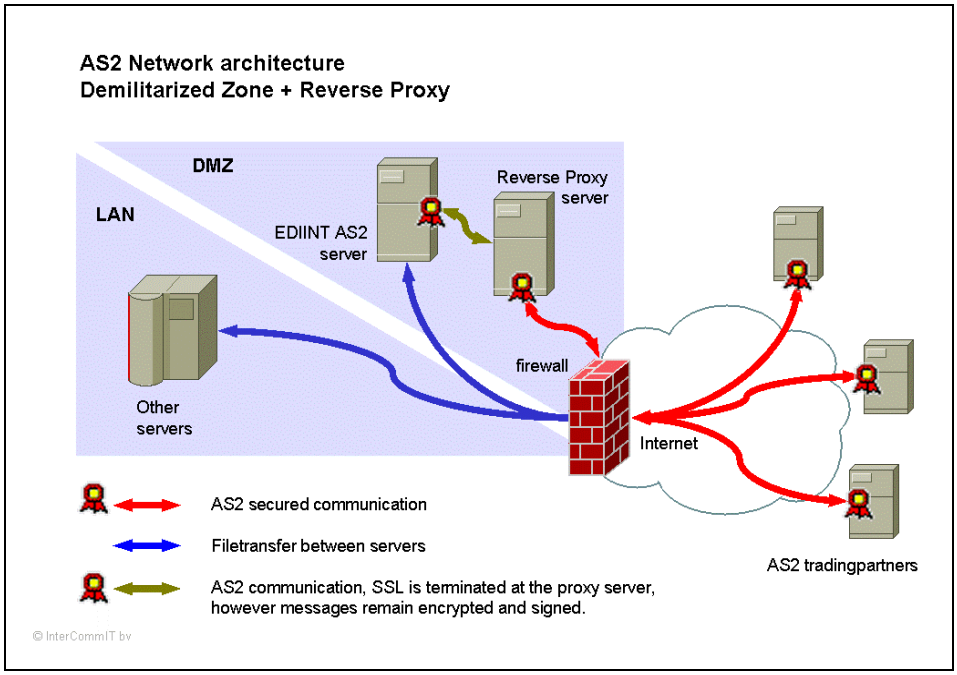

Abb. 4: IT-Architektur mit DMZ und Reverse Proxy Server

1.10 Sicherheit durch die Nutzung digitaler Zertifikate

Digitale Zertifikate können entweder durch das Unternehmen oder die Person, die das Zertifikat nutzen wird, erzeugt werden (selbstsignierte Zertifikate) oder durch eine Zertifizierungsbehörde (Certification Authority - CA) erstellt werden, die die Zertifikate für den Antragsteller verwaltet (beglaubigte Zertifikate).

Die Nutzung von selbstsignierten Zertifikaten (Self-Signed Certificates) vereinfacht anfänglich die Verwaltung von Zertifikaten und Schlüsseln. Die Sicherheitsstufe ist jedoch gering, weil keine neutrale Organisation das System verwaltet und den Ursprung der Zertifikate kontrolliert. Falls ein selbstsigniertes Zertifikat benutzt wird, ist das Verfalldatum bilateral definiert und gespeichert.

Wenn eine Zertifizierungsbehörde (CA) eingeschaltet ist, nutzt das Unternehmen eine vertrauenswürdige Drittpartei (Trusted Third Party). Die Zertifizierungsbehörde verwaltet die Zertifikate und kann ein Zertifikat widerrufen bevor es verfällt, falls seine Nutzung nicht länger als eindeutig oder sicher erachtet wird. Die Zertifizierungsbehörde signalisiert in diesem Fall das Risiko, das mit dem Zertifikat verbunden ist und schlägt vor, dass der Besitzer das Zertifikat ändert. Die Zertifikate einer Zertifizierungsbehörde beinhalten ein Verfalldatum, das die Unternehmen verpflichtet, regelmäßig die Identität ihrer Partner zu überprüfen, wodurch die Sicherheitsstufe erhöht wird. Neben der Verwaltung der Zertifikate garantiert die Zertifizierungsbehörde außerdem, dass der Besitzer des Zertifikats wirklich derjenige ist, der er vorgibt, zu sein. Die Zertifizierungsbehörde stellt ihre Dienstleistungen gegen eine jährliche Gebühr zur Verfügung.

Unabhängig davon, welche Option gewählt wird, ist es unbedingt nötig, den Zugriff auf den privaten Schlüssel (Private Key) beispielsweise durch Vergessen des Passworts nicht zu verlieren. Meist kann weder die Zertifizierungsbehörde noch das eigene System für die Generierung von selbstsignierten Schlüsseln einen verlorenen privaten Schlüssel wiederherstellen. Wenn ein privater Schlüssel verloren wurde, ist es notwendig, ein neues Zertifikat zu generieren und dieses an alle Geschäftspartner zu verteilen.

1.10.1 Rechtliche Aspekte

Das digitale Zertifikat ist die digitale Identität des Unterzeichners. Es ist das Schlüsselelement beim Aufbau eines Sicherheitssystems, weil durch die Zuordnung des Zertifikats und der technischen Gerätschaften, wie beispielsweise eine Smart Card oder ein Software-Modul, der Empfänger eines signierten Dokuments die Transaktion mit vollem Vertrauen akzeptieren kann.

Konsequenterweise ist die Verteilung und Kontrolle von digitalen Zertifikaten ein umfangreicher Prozess, obwohl die meisten Schritte dabei selbstverständlich sind. Das digitale Zertifikat muss auf eine natürliche Person bezogen sein, dessen Identität im beruflichen Zusammenhang überprüft wurde. Es muss im Betrugsfall zügig widerrufbar sein (ähnlich wie EC-Karten) und der Empfänger des Dokuments muss in der Lage sein, es in Echtzeit überprüfen zu können.

1.10.2 Zertifikatstypen

Das Vertrauen in Zertifikate basiert auf der präzisen Kenntnis der Identität der sendenden Partei. Es gibt üblicherweise drei Klassen oder Vertrauensstufen für Zertifikate:

- Klasse 1: Das Zertifikat wird ausgestellt, sobald die Existenz einer Email-Adresse überprüft worden ist.
- Klasse 2: Das Zertifikat wird ausgestellt, nachdem eine Datenbankabfrage erfolgt ist und verwaltungstechnische Dokumente (Personalausweis der verantwortlichen Person und offizielle Registrierungsunterlagen des Unternehmens) erhalten worden sind.
- Klasse 3: Das Zertifikat wird ausgestellt, nachdem eine persönliche Kontrolle durch eine vertrauenswürdige Drittpartei vorgenommen worden ist. Ebenfalls müssen die Anforderungen der Zertifikate der Klasse 2 erfüllt sein.

1.10.3 Selbstsignierte oder beglaubigte Zertifikate

Beide Zertifikatstypen - selbstsigniert und beglaubigt - können durch die EDIINT-Software generiert werden. Festzuhalten ist, dass ein selbstsigniertes Zertifikat nicht mit einer vertrauenswürdigen Drittpartei verbunden ist. Deshalb gibt es in diesem Fall keine unabhängige Überprüfung der Identität.

Die Verantwortungsbereiche und die Struktur der Verwaltung beglaubigter Zertifikate werden in der folgenden Tabelle beschrieben.

	Schlüsselbesitzer (Key Holder - KH)	Registrierungsstelle (Registration Authority - RA)	Zertifizierungsbehörde (Certificate Authority - CA)	Zertifikatsverwalter (Certificate Operator - CO)
Rolle	• Beantragt ein Zertifikat • Generiert den privaten und den öffentlichen Schlüssel	• Bindeglied zwischen KH, CA und CO • Überprüft die Anfragen der Nutzer und übermittelt sie an die CO (Certification Signing Requests - CSR) • Genehmigt oder verweigert die Generierung des Zertifikats	• Legt die Überprüfungsregeln fest. • Auditiert die Registrierungsbehörde	• Generiert das Zertifikat • Speichert und verteilt die Zertifikate • Pflegt die Liste der widerrufenen Zertifikate (Certification Revokation List - CRL)
Widerruf	• Kann den Widerruf eines Zertifikats beantragen (Anfrage an die Registrierungsbehörde) • Beantragt die Erneuerung eines Zertifikats	• Leitet den Widerruf eines Zertifikats an den CO weiter • wie gewünscht		• Widerruft das Zertifikat unter Verantwortung der Zertifikatsbehörde • wie gewünscht
Haftung		• Üblicher Handelsbrauch	• Gesetzliche Haftung	
Grenze		• Die Überprüfungsstufe hängt von der angewandten Sicherheitspolitik ab.		• Sub-Vertragsnehmer der CA

Der Dual-Schlüssel ist ein Schlüsselpaar bestehend aus einem privaten Schlüssel, der sicher und geheim gelagert werden muss, und dem öffentlichen Schlüssel. Die Kombina-

tion dieser privaten und öffentlichen Schlüssel ist notwendig, wenn Verschlüsselungstechniken basierend auf asymmetrischen Algorithmen benutzt werden. Das Zertifikat zertifiziert, dass der öffentliche Schlüssel zu der identifizierten Person oder Firma gehört. Es wird von einer vertrauenswürdigen Drittpartei (Zertifizierungsbehörde) zur Verfügung gestellt. Sobald das Zertifikat signiert wird, ist die Verbindung zwischen dem Zertifikat und dem Dual-Schlüssel überprüft.

Abb. 5: Übersicht Zertifikatsverwaltung

1.10.4 Anwendung von Zertifikaten in der Praxis

Der private Schlüssel, der für die Generierung des Zertifikats genutzt wird, wird nicht ausgetauscht und ist nicht im Zertifikat enthalten. Der private Schlüssel muss sicher gelagert werden und der Zugriff des Schlüsselbesitzers muss eindeutig gewährleistet sein.

Außerdem müssen die Beteiligten folgende Fragen klären und ein gegenseitiges Verständnis für die Anforderungen und funktionellen sowie technischen Beschränkungen zwischen den Geschäftspartnern und Service Providern aufbauen. Diese sind:

- Der Abgleich der Listen von Zertifizierungsbehörden in den AS2-Tools.
- Einrichtung und Pflege von Zertifikatshierarchien der Zertifizierungsbehörden.
- Definition und Pflege der Widerruflisten.

In der Praxis signalisiert die Zertifizierungsbehörde die Notwendigkeit einer Erneuerung eines Zertifikats auf Basis der Gültigkeitsdauer. Die Verantwortung für die eigentliche Er-

neuerung liegt beim Schlüsselbesitzer. Unabhängig davon sollte eine aktuelle Liste der Geschäftspartner, mit denen gültige und beglaubigte Zertifikate ausgetauscht wurden, gepflegt werden.

1.10.5 Algorithmen für elektronische Signaturen

EDIINT bietet einige Optionen für elektronische Signaturen: Keine Signaturen, MD5 oder SHA-1. Wenn ein Dokument elektronisch signiert wurde, ist seine Unversehrtheit und die Sicherheit der enthaltenen Informationen bestätigt. Die elektronische Signatur ermöglicht die Überprüfung, dass der Sender einer Nachricht wirklich derjenige ist, der er vorgibt, zu sein.

MD5 (Message Digest Version 5) ist ein Hash-Algorithmus, der von Prof. Rivest am MIT (Massachusetts Institute of Technology) entwickelt und im April 1993 veröffentlicht wurde. Dieser Algorithmus generiert basierend auf variablen Dokumentenlängen 128 Bit große Quersummen. Die Tatsache, dass es einen Informationsverlust gibt, macht es unmöglich, die Originalnachricht auf Basis der Quersumme wiederherzustellen. Außerdem beinhaltet MD5 einen geringen Kollisionsfaktor; d.h. es ist extrem unwahrscheinlich, dass identische Quersummen für zwei verschiedene Dokumente generiert werden. Der Algorithmus wird häufig für digitale Signaturen speziell in Verbindung mit der RSA-Technologie (Rivest, Shamir and Adleman) genutzt.

SHA1 (Secure Hash Algorithm Version 1) wurde vom National Institute of Standards and Technology (NIST) entwickelt. Die aktuelle Version wurde im April 1995 veröffentlicht. Dieser Algorithmus hat die gleichen Merkmale wie MD5, allerdings generiert er Quersummen von 160 Bit. Er ist aktueller und sicherer als MD5.

1.10.6 Algorithmen für die Datenverschlüsselung

EDIINT erlaubt die Verschlüsselung von Daten, fordert diese Nutzung aber nicht ausdrücklich. Drei Verschlüsselungsalgorithmen werden von EDIINT unterstützt. Zwei davon, 3DES und RC2 128, verwenden 168 Bit-Schlüssel und bieten so ein Höchstmaß an Sicherheit. EDIINT ermöglicht ebenfalls die Nutzung des RC2 40-Algorithmus. AES ist ein weiterer Algorithmus, der mit AS2 genutzt werden kann.

Es ist wichtig, dass die Software des Empfängers den angewandten Algorithmus in der gesendeten Nachricht unterstützen kann. Deshalb müssen die unterstützten Verschlüsselungsalgorithmen vorab geklärt werden.

1.11 Transportebene

1.11.1 AS2-Protokoll für den Transport (HTTP und HTTP/S)

Das Hypertext Transfer Protocol (HTTP) wurde ursprünglich geschaffen, um HTML-Seiten über das Internet zu transportieren. Der Zugriff auf diese auf das Web bezogenen Dienste wird durch die Nutzung von Adressen vom Typ: "http://domain name [/directory]" erreicht.

Das Secure Hypertext Transfer Protocol (HTTP/S) ist eine sichere Version von HTTP und ermöglicht die Absicherung des AS2-Kopfteils. HTTP/S verschlüsselt und entschlüsselt sowohl die Seiten, die vom Nutzer angefragt werden als auch die Seiten, die von den Webservern weitergeleitet werden. HTTP/S fügt einen Secure Socket Layer (SSL) als weitere Schicht zum regulären HTTP hinzu. HTTP/S nutzt normalerweise den Port 443 anstatt des Ports 80, der für HTTP zur Verfügung steht, um mit den unteren Schichten des TCP/IP-Protokolls zu interagieren. Beispiel: Wenn eine elektronische Bestellung generiert wird, kann die Adresse des Webformulars mit "https://" starten. Wenn das Formular überprüft wird, wird die HTTP/S-Schicht durch den Browser verschlüsselt. Die Bestätigung, die vom Server des Empfängers zurückempfangen wird, wird ebenfalls in einem abgesicherten Formular übertragen und kommt beim Partner durch eine Adresse vom Typ "https://" an. Sie wird entschlüsselt durch die HTTP/S-Schicht des Browsers.

Sofern digitale Zertifikate schon für die Verschlüsselung und Signierung der Nachricht benutzt werden, wird HTTP/S normalerweise nicht benötigt. Erstens, weil die Verschlüsselungsschicht keine signifikante Sicherheit hinzufügt und zweitens, weil diese den Austauschprozess verlangsamt. HTTP/S kann dann benutzt werden, wenn die Originalinhalte nicht verschlüsselt sind und es eine Empfehlung gibt, dass diese Inhalte durch digitale Signaturen verschlüsselt werden müssen.

Hinweis: HTTP/S und SSL können die Nutzung von digitalen Zertifikaten vom Typ X.509 für den Server integrieren, um den Sender zu authentifizieren. SSL ist ein offenes, nicht proprietäres Protokoll, das dem W3C (World Wide Web Consortium) von Sun/Netscape bereit gestellt wurde. HTTP/S sollte nicht mit SHTTP, einer sicheren Version von HTTP, verwechselt werden, die von der EIT Corp., CA (USA) entwickelt und als Standard vorgeschlagen worden ist.

1.11.2 Internetverbindung

EDIINT verlangt die Nutzung des TCP/IP-Protokolls und das Internet für die Übermittlung von Nachrichten zwischen den Geschäftspartnern.

Das Prinzip von AS2 ist, dass das Netzwerk permanent nach Nachrichten "lauscht", die für den Empfänger bestimmt sind. Deshalb ist eine ununterbrochene Verbindung zum Internet notwendig. Die Adressierung basiert auf einem vollständig qualifizierten Namen einer Domain (URI) und einer veröffentlichten IP-Adresse für die Konfiguration der Firewall.

1.11.3 Zeitstempel

Ein Zeitstempel (Timestamp) definiert die exakte Zeit, zu der ein rechnerbezogenes Ereignis stattgefunden hat. Durch Nutzung von Tools wie zum Beispiel NTP (Network Time Protocol) ist ein Computer in der Lage, die exakte, aktuelle Zeit zu nutzen. Diese Präzision ermöglicht, dass Computer- und Netzwerkanwendungen effizient kommunizieren können.

Der Zeitstempel-Mechanismus wird genutzt, wenn ein Set von mehreren Anwendungen einen strikt synchronisierten Austausch verlangt. Zum Beispiel kann der Zeitstempel als Mechanismus verwendet werden, der die Reihenfolge für eine Transaktion mit mehreren sequentiellen Ereignissen gewährleistet. Falls die Abfolge scheitert, kann die Transaktion abgebrochen werden.

Eine weitere Anwendung des Zeitstempels ist die Registrierung von Zeitstempeln in speziell temporären Funktionen. Bei der IP-Telefonie teilt das RTP (Real-time Transport Protocol) den Stimmpaketen sequentielle Zeitstempel zu, die es dem Empfängersystem ermöglichen, diese als Speicherstempel zu verwenden und fehlerlos anzuordnen und zu übermitteln.

Für Anwendungen, bei denen die Zeitberechnung vertragliche Auswirkungen hat, ist es möglich, einen beglaubigten Zeitstempel von einem Service Provider zu erhalten.

1.12 Dateiebene

1.12.1 Kopfinformationen

Der Kopf stellt den Teil des EDIINT-Pakets bereit, der den zu übertragenden Daten vorausgeht. Der Kopf enthält sämtliche Basisinformationen (z. B. Sender, Empfänger und Anweisungen für die Fehlerbehandlung), die für die Nachrichtenübermittlung notwendig sind.

Der Hauptteil der Nachricht liegt zwischen dem Kopfteil und der Nachrichtensignatur.

Die folgende Grafik beschreibt die unterschiedlichen Kopfteile bezogen auf die Transportschichten (Verkapselung der Umschläge).

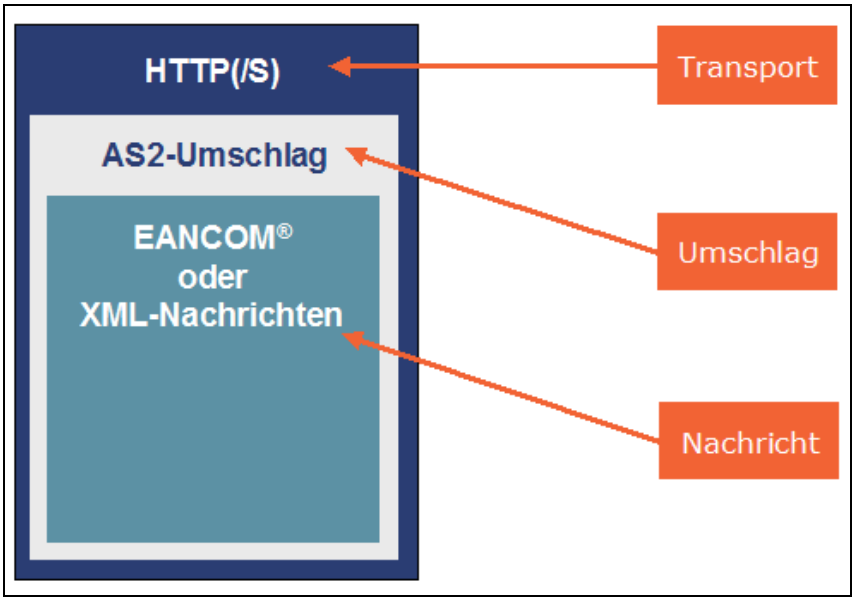

Abb. 6: Struktur EDIINT AS2

Die komplette Liste aller Datenelemente der Kopfteile kann in der internationalen Spezifikation der IETF eingesehen werden.

Gemäß der AS2-Empfehlung der IETF kann die Eindeutigkeit des Präfixes "id-right" beispielsweise durch den Namen der Domain des Senders abgesichert werden. Die Begriffe "AS2-From" und "AS2-To" beinhalten Werte, die eine eindeutige Identifikation der Personen ermöglichen, die Nachrichten austauschen. Die Kernidentifikation dieser Person korrespondiert mit der eindeutigen Identifikation innerhalb der AS2-Anwendergemeinschaft.

Datenelement	Definition
AS2-To	Dieses Datenelement enthält eine Zeichenkette, die den Empfänger der ausgetauschten Informationen identifiziert.
AS2-From	Dieses Datenelement enthält eine Zeichenkette, die den Sender der ausgetauschten Informationen identifiziert.

1.12.2 Empfangsbestätigung

Es gibt fünf potenzielle Wege, die Empfangsbestätigung (Message Disposition Notification-MDN) zu nutzen. Die IETF-Spezifikation erlaubt die Nutzung folgender Wege:

- Keine Empfangsbestätigung: Diese Minimaloption schließt die Prüfung der Übermittlung aus und unterstützt deshalb nicht die Unleugbarkeit (des Empfangs einer Nachricht).
- Einfache synchrone Empfangsbestätigung: Die MDN wird in derselben Kommunikationsverbindung zurückgesendet und signalisiert, dass eine Nachricht empfangen wurde. Die MDN ist jedoch nicht vom Empfänger signiert worden.
- Signierte synchrone Empfangsbestätigung: Die MDN wird in derselben Kommunikationsverbindung signiert zurückgesendet. Diese Option stellt die höchste Prüfungsstufe zur Verfügung, Erstens bestätigt sie, dass die Nachricht empfangen worden ist und zweitens, dass der Empfänger durch den Gebrauch des privaten Schlüssels der vorgesehene Empfänger ist.
- Einfache asynchrone Empfangsbestätigung: Die MDN wird in einer separaten Kommunikationsverbindung zurückgesendet und signalisiert, dass die Nachricht empfangen wurde. Die MDN ist jedoch nicht vom Empfänger signiert worden.
- Signierte asynchrone Empfangsbestätigung: Die MDN wird in einer separaten Kommunikationsverbindung signiert zurückgesendet.

Der Typ der MDN, der vom Sender erwartet wird, ist in der vorab gesendeten Nachricht definiert. Es ist deshalb der Sender der Nachricht, der den Typ der MDN festlegt. Jedoch ist es ohne vorherige Vereinbarung zwischen Sender und Empfänger nicht gewährleistet, dass das Empfängersystem in der Lage ist, mit dem geforderten MDN-Typ zu antworten. Deshalb muss der MDN-Typ zwischen den Partnern vereinbart werden, bevor diese einen EDIINT-Datenaustausch starten.

1.12.3 Formate

MIME (Multipurpose Internet Mail Extensions) ist ein Format zur Übermittlung von nicht-textlichen Dateien per eMail, wie beispielsweise Bilder oder Binärdaten. Der MIME-Typ stellt eine Klassifikation von Dateitypen bereit, die mit MIME über das Internet gesendet werden können. Gemäß der EDIINT-Spezifikationen müssen die folgenden Typen übermittelt werden können:

- Content-Type: application/EDI-X12
- Content-Type: application/EDIFACT
- Content-Type: application/edi-consent
- Content-Type: application/XML

Zudem ist ein einfacher Text (Content-Type: text/plain) ebenfalls akzeptiert wie alle MIME-Typen bezogen auf Binärdateien.

Der genutzte Typ muss mit den Inhalten übereinstimmen, die er qualifiziert. Eine Reihe von Fragen speziell zur Definition und Implementierungsweise in die Protokoll-Software haben die relative Verschwommenheit der internationalen Spezifikationen in Bezug auf den "Content-Type" unterstrichen. Die Schlussfolgerung ist, dass der Empfänger in jedem Fall in der Lage sein muss, sämtliche Inhalte, die übertragen wurden, zu importieren. Praktisch bedeutet dies, dass sämtliche Inhaltstypen von einer AS2-Lösung über das Internet übertragen werden können.

S/MIME (Secure Multipurpose Internet Mail Extensions) ist ein wesentlicher Bestandteil der EDIINT-Empfehlung der IETF. S/MIME ist ein Format und Protokoll, das bei signierten und/oder verschlüsselten Diensten für MIME-Nachrichten genutzt wird, die über das Internet gesendet wurden.

1.12.4 Komprimierung

Die Komprimierung verringert die Größe einer Datei oder einer Gruppe von Dateien. Dies spart Speicherplatz und reduziert Zeit und Kosten bei der Übertragung. Die EDIINT-Arbeitsgruppe innerhalb der IETF stellte fest, dass EDIINT-Implementierungen Komprimierungstechniken auf Basis von ZLIB [RFC1950] unterstützen sollen.

ZLIB ist ein offener, nicht-proprietärer Komprimierungsalgorithmus, der mit praktisch allen Anwendungssystemen kompatibel ist, weil er in einer übergeordneten Sprache geschrieben wurde, die softwareunabhängig ist.

2 Empfehlungen des GS1 Europe EDIINT Forums

Das Akronym "PAIN" kann als treffende Einleitung zu den Sicherheitsüberlegungen verwendet werden, die der AS2-Standard adressiert.

- P - Privacy (Datenschutz); Daten können nur von Sender und Empfänger gelesen werden.
- A - Authentication (Authentizität); Der Sender ist tatsächlich derjenige, der er vorgibt zu sein.
- I - Integrity (Integrität); Die Daten können nicht verändert werden, ohne dass der Empfänger dies erkennt.
- N - Non-repudiation (Unleugbarkeit); Die Kommunikation von Dokumenten kann nach der Übertragung nicht mehr geleugnet werden

Das GS1 Europe EDIINT Forum hat diese Ziele in Bezug auf die aktuell verfügbaren technischen Lösungen berücksichtigt. Basierend auf diesen Überlegungen wurde festgelegt, dass die folgenden Punkte unterstützt werden sollen:

- Das Dokument kann nur von Sender und Empfänger gelesen werden. Die Verschlüsselung des Dokuments sichert diese Integrität.
- Die Identifikation des Senders ist garantiert. Die digitale Signatur des Senders sichert seine Authentifizierung.
- Das Dokument kann nicht modifiziert oder verändert werden. Wenn die Inhalte verändert werden, wird der Empfänger automatisch informiert. Die digitale Signatur des Senders sichert diese Integrität.
- Unleugbarkeit des Ursprungs und des Empfangs. Unleugbarkeit des Ursprungs - Der Sender kann nicht behaupten, dass er die Daten nicht gesendet hat. Unleugbarkeit des Empfangs - Der Empfänger kann nicht behaupten, dass er die Daten nicht empfangen hat. Das erste wird durch die digitale Signatur des Senders und das zweite durch die vom Empfänger signierte Message Disposition Notification (MDN) abgesichert.

2.1 Sicherheit durch die Nutzung digitaler Zertifikate

- **Empfehlung 1**

Die Nutzung eines einzelnen Zertifikats für Signatur und Verschlüsselung ist zulässig und in der Praxis üblich. Im Rahmen von erhöhten Sicherheitsanforderungen wird die Nutzung von zwei verschiedenen Zertifikaten empfohlen.

- **Empfehlung 2**

Die Nutzung von selbstsignierten Zertifikaten ist zulässig und in der Praxis üblich. Im Rahmen von erhöhten Sicherheitsanforderungen wird die Nutzung von beglaubigten Zertifikaten der Klasse 2 empfohlen.

- **Empfehlung 3**

Die folgenden Empfehlungen betreffen den laufenden Einsatz digitaler Zertifikate:

  - Die Gültigkeitsdauer für ein Zertifikat sollte mindestens 2 Jahre betragen.
  - Die Gültigkeitsdauer für ein Zertifikat sollte maximal 5 Jahre betragen.
  - Diese Umsetzungshilfe gibt keine Empfehlung bezüglich der Art und Weise, wie Zertifikate ausgetauscht werden sollen. Dies muss bilateral vereinbart werden. *Hinweis: Sobald die Spezifikation "Certificate Exchange Messaging" von der IETF verfügbar ist, wird diese empfohlen.*
  - Der private Schlüssel wird vom Schlüsselbesitzer gespeichert, der rechtlich verantwortlich ist.
  - Die Erneuerung von beglaubigten Zertifikaten, signalisiert durch die Zertifizierungsbehörde, wird in der Praxis vom Schlüsselbesitzer durchgeführt. Bei selbstsignierten Zertifikaten signalisiert keine Zertifizierungsbehörde die Erneuerung von Zertifikaten. Dies ist vom Zertifikatsinhaber selbst sicherzustellen.

- **Empfehlung 4**

SHA1 ist der bevorzugte Algorithmus für digitale Signaturen.

- **Empfehlung 5**

3DES ist der bevorzugte Algorithmus für die Datenverschlüsselung.

- **Empfehlung 6**

Die Länge des Schlüssels der Sitzung (Session Key) muss 128 Bit oder größer sein. Die Länge des privaten und öffentlichen Schlüssels (X.509) muss 1024 Bit oder größer sein. Im Rahmen von erhöhten Sicherheitsanforderungen kann eine Schlüssellänge von >= 2048 Bit bilateral vereinbart werden.

2.2 Transportebene

- **Empfehlung 7**

Das Transport Protokoll HTTP sollte verwendet werden. Jedoch kann auch HTTP/S verwendet werden, wenn es einen Grund für die Absicherung der Adressfelder "AS2-To", "AS2-From" und weiterer Informationen des Kopfteils gibt.

- **Empfehlung 8**

Als Verbindung zum Internet ist eine permanente Verbindung notwendig, die einen vollständig qualifizierten Namen einer Domain sowie für die Konfiguration der Firewall eine veröffentlichte IP-Adresse nutzt.

2.3 AS2-Kopfinformationen

- **Empfehlung 9**

Das Adressfeld "AS2-From" muss die GLN (Globale Lokationsnummer, ehemals ILN – Internationale Lokationsnummer) des sendenden Servers oder die GLN des Unternehmens, das für den Server verantwortlich ist, beinhalten. Falls ein Hub genutzt wird, kann die GLN des Geschäftspartners verwendet werden, wenn das Adressfeld "AS2-To" für das Routing genutzt wird.

- **Empfehlung 10**

Das Adressfeld "AS2-To" muss die GLN des empfangenden Servers oder die GLN des Unternehmens, das für den Server verantwortlich ist, beinhalten. Falls ein Hub genutzt wird, kann die GLN des Geschäftspartners verwendet werden, wenn das Adressfeld "AS2-To" für das Routing genutzt wird.

2.4 Empfangsbestätigung

- **Empfehlung 11**

Eine signierte MDN ist obligatorisch, weil dies die zentrale Technik ist, um den Empfang der Daten und die Unleugbarkeit der Nachricht sicherzustellen. Die MDN wird nicht verschlüsselt.

- **Empfehlung 12**

Eine asynchrone MDN wird empfohlen.

2.5 Zeitstempel

- **Empfehlung 13**

Der Gebrauch eines Zeitstempels einer dritten Partei ist optional.

2.6 Formate

- **Empfehlung 14**

Der MIME-Typ muss mit dem Inhalt der Nachricht übereinstimmen.

- **Empfehlung 15**

S/MIME ist obligatorisch.

2.7 Komprimierung

- **Empfehlung 16**

Die Komprimierung kann optional genutzt werden. Dies ist bilateral zwischen Sender und Empfänger zu vereinbaren.

2.8 AS2-Version

- **Empfehlung 17**

Die genutzte AS2-Version ist 1.1.

2.9 Eingangs- und Ausgangsport

- **Empfehlung 18**

Die Portvorgaben werden grundsätzlich von jedem Unternehmen selbst festgelegt. Sofern möglich, sollte 4080 für HTTP und 5443 für HTTP/S verwendet werden, um AS2-Transaktionen von Anderen zu unterscheiden, die das gleiche Protokoll nutzen.

3 Checkliste für die Implementierung von EDIINT

Jeder Partner muss:

- entscheiden, ob eine EDIINT-Lösung hinter einer Firewall installiert werden soll oder in einer demilitarisierten Zone, isoliert von den internen Systemen, platziert wird;
- die EDIINT-Software installieren;
- für die Nutzung eines beglaubigten Zertifikats ein digitales Zertifikat erwerben (privater und öffentlicher Schlüssel), das von einer vertrauenswürdigen Drittpartei zur Verfügung gestellt wird. Oder es muss alternativ ein selbstsigniertes Zertifikat selbst generiert werden;
- ein übergeordnetes Transport-Protokoll vereinbaren;
- eine genaue Vorgehensweise für den Nachrichtenempfang vereinbaren;
- einen Algorithmus für die Verschlüsselung auswählen;
- einen Algorithmus für die Signatur auswählen;
- die EDIINT-Software anhand folgender Informationen konfigurieren:
    - URI, die für die Übermittlung von Dokumenten reserviert wird
    - Identifikation des Partners
    - Verfahren für die digitale Signatur
    - Verfahren für die Verschlüsselung
    - Verfahren für den Empfang
    - Verfahren für die Komprimierung
- das Zertifikat des Partners (Öffentlicher Schlüssel) in seine EDIINT-Software laden;
- ein Testdokument senden, um die Konfigurationen der Sende- und Empfangssysteme zu kontrollieren.

Anhang 1: Beispiele für Parameterwerte

user-agent: xxxxx/xx

Method: POST

message-id: <xxx.xxx.xxx@station_xxx>

accept: */*

as2-to: 3027000002022

subject: test.txt

disposition-notification-to: <xxx>

content-transfer-encoding: base64

URI: /b2bhttpdev/inbound/as2test

as2-from: 3027000002008

content-length: 3866

content-disposition: attachment; filename=smime.p7m

Protocol: HTTP/1.1

host: xxx.xxx.xxx.xxx

disposition-notification-options: signed-receipt-protocol=required, pkcs7-signature; signed-receipt-micalg=required, sha1, md5

content-type: application/pkcs7-mime; smime-type=enveloped-data; name="smime.p7"

mime-version: 1.0

date: Fri, 31 Oct 2003 14:47:20 +0100

MIIK9QYJKoZIhvcNAQcDoIIK5jCCCuICAQAxggEaMIIBFgIBADB/MGsxCzAJBgNV

BAYTAkZSMRMwEQYDVQQKEwpDZXJ0aU5vbWlzMSkwJwYDVQQLEyBBQyBJbn-Rlcm1lZGlhaXJlIC0gU3Vic2lkaWFyeSBDQTEcMBoGA1UEAxMTQ2VydGlOb21pc-yBDbGFzc2UgMgIQMDAwMTA2NzU5MTAxNzc1MDANBgkqhkiG9w0BAQEFAASBg FAQfRcQdZVJ…]==

Anhang 2: Referenzen

Auf die folgenden Dokumente wurde in Vorbereitung dieses Dokuments referenziert:

RFC (Request for Comments)	URL Adresse
RFC 2616 - HyperText Transfer Protocol	www.ietf.org/rfc/rfc2045.txt
RFC 822 - ARPA Internet Text Message Standard	www.ietf.org/rfc/rfc2045.txt
RFC 1767 - EDI Content Type	www.ietf.org/rfc/rfc2045.txt
RFC 2376 - XML Media Types	www.ietf.org/rfc/rfc2045.txt
RFC 1847 - Security Multiparts for MIME	www.ietf.org/rfc/rfc2045.txt
RFC 1892 - Multipart/Report	www.ietf.org/rfc/rfc2045.txt
RFC 2045 - MIME Part 1: Format of Internet Message Bodies	www.ietf.org/rfc/rfc2045.txt
RFC 2046 - MIME Part 2: Media Types	www.ietf.org/rfc/rfc2046.txt
RFC 2049 - MIME Part 5: Conformance Criteria and Examples	www.ietf.org/rfc/rfc2049.txt
RFC 2633 - S/MIME Version 3 Message Format	www.ietf.org/rfc/rfc2633.txt
RFC 2630 - Cryptographic Message Syntax	www.ietf.org/rfc/rfc2630.txt
RFC 2298 - Message Disposition Notification	www.ietf.org/rfc/rfc2045.txt

Das technische Basisdokument, das als Entwurf der AS2-Spezifikation von der IETF veröffentlicht und vom GS1 Europe EDIINT Forum genutzt wurde, kann auf folgender Webseite runtergeladen werden: www.ietf.org/internet-drafts/draft-ietf-ediint-as2-16.txt

Anhang 3: Zusammenfassung der Empfehlungen

Der folgende Anhang fasst die AS2-Parameter und Empfehlungen zur Nutzung zusammen:

AS2-Parameter		Empfehlung
Sicherheit	**Zertifikate**	Die Nutzung eines einzelnen Zertifikats für Signatur und Verschlüsselung ist zulässig und in der Praxis üblich. Im Rahmen von erhöhten Sicherheitsanforderungen wird die Nutzung von zwei verschiedenen Zertifikaten empfohlen.
		Best Practice: • Skalierbar • Klasse 1 Typ oder Klasse 2 Typ (im Rahmen von erhöhten Sicherheitsanforderungen) • Selbstsigniert oder beglaubigt (im Rahmen von erhöhten Sicherheitsanforderungen) • Minimale Gültigkeitsdauer: 2 Jahre • Maximale Gültigkeitsdauer: 5 Jahre
	Digitale Signatur	SHA1
	Verschlüsselung	3DES
	Länge des Schlüssels	>= 128 Bit
	Länge des öffentlichen/privaten Schlüssels (X.509)	>= 1024 Bit Länge des öffentlichen/privaten Schlüssels (X.509). Im Rahmen von erhöhten Sicherheitsanforderungen kann eine Schlüssellänge von >= 2048 Bit bilateral vereinbart werden.

Transportebene	**Transport-Protokoll**	HTTP (HTTP/S KANN benutzt werden, um "AS2-To" and "AS2-From" abzusichern.)
	Verbindung zum Internet	Permanente Internet Verbindung; Vollständig qualifizierter Name der Domäne (URI) muss angegeben werden. Für die Konfiguration der Firewall muss eine veröffentlichte IP-Adresse vorhanden sein.
AS2-Kopfinformation	**AS2-From**	GLN des AS2-Servers des Geschäftspartners MUSS verwendet werden. Ausnahme: Sofern ein Hub benutzt wird, kann die GLN des Geschäftspartners verwendet werden, falls das Feld "AS2-To" für das Routing verwendet wird.
	AS2-To	GLN des AS2-Servers des Geschäftspartners MUSS verwendet werden. Ausnahme: Sofern ein Hub benutzt wird, kann die GLN des Geschäftspartners verwendet werden, falls das Feld "AS2-To" für das Routing verwendet wird.
MDN		MUSS
	MDN signiert	MUSS
	MDN verschlüsselt	Nicht erlaubt
	Asynchron / Synchron	Eine asynchrone MDN wird empfohlen.
Zeitstempel		OPTIONAL
Formate	**MIME**	MIME Typ übereinstimmend mit Inhalt
	S/MIME	MUSS
	Komprimierung (Ja/Nein)	Akzeptiert und optional (bilateral zu vereinbaren)
AS2-Version		1.1

Eingangs- und Ausgangsport		Die Portvorgaben werden grundsätzlich von jedem Unternehmen selbst festgelegt. Sofern möglich sollte 4080 für HTTP und 5443 für HTTP/S verwendet werden, um AS2-Transaktionen von anderen zu unterscheiden, die das gleiche Protokoll nutzen.

Anhang 4: Glossar

Begriff	Definition	Quelle
Authentifizierung	Der Prozess, der sicherstellt, dass Personen, Organisationen oder Objekte diejenigen sind, die sie vorgeben zu sein. Im Rahmen einer PKI kann die Authentifizierung der Prozess sein, sicherzustellen, dass eine Person oder eine Organisation, die sich unter einem bestimmten Namen Zugriff auf etwas verschaffen möchte, faktisch die richtige Person oder Organisation ist. Dies korrespondiert mit dem zweiten Prozess, der mit der Identifikation verbunden ist. Authentifizierung kann sich auch auf Sicherheitsdienste beziehen, die garantieren, dass Personen und Organisationen oder Objekte diejenigen sind, die sie vorgeben zu sein, oder dass eine Nachricht oder andere Daten von einer bestimmten Person, Organisation oder Anwendung stammen. Deshalb authentifiziert eine digitale Signatur einer Nachricht den Nachrichtensender.	RFC3647
Benutzeragent (User Agent - UA)	Die Applikation, die die AS2-Anfragen steuert und weiter verarbeitet.	draft-ietf-ediint-as2-16
Empfangsbestätigung (Message Disposition Notification - MDN)	Die Funktionsnachricht, die vom Empfänger an den Sender geschickt wird, um zu bestätigen, dass eine EDI-Datei empfangen wurde. Diese Nachricht kann synchroner oder asynchroner Natur sein.	draft-ietf-ediint-as2-16
Empfangsbestätigung, asynchron	Eine Empfangsbestätigung, die in einer anderen Kommunikation(ssitzung) an den Sender zurückgesendet wird als in der Kommunikation(ssitzung), in der die ursprüngliche Nachricht des Senders geschickt wurde.	draft-ietf-ediint-as2-16
Empfangsbestätigung, signiert	Eine Empfangsbestätigung mit einer digitalen Signatur.	draft-ietf-ediint-as2-16
Empfangsbestätigung, synchron	Eine Empfangsbestätigung, die in der gleichen Kommunikation(ssitzung) an den Sender zurückgesendet wird, in der die ursprüngliche Nachricht des Senders geschickt wurde.	draft-ietf-ediint-as2-16
Handhabungsvorschrift zur Zertifizierung (Certification Practice Statement - CPS)	Die Angabe von Handhabungsvorschriften, die eine Zertifizierungsbehörde (CA) anwendet in Bezug auf: Ausstellung, Verwaltung, Widerruf, Erneuerung oder Änderung von Zertifikaten.	RFC3647

ITU-T (International Tele-communication Union - Telecommunication Standardization Sector)	Die Internationale Fernmeldeunion mit Sitz in Genf ist eine Unterorganisation der UNO und die einzige Organisation, die sich offiziell und weltweit mit technischen Aspekten der Telekommunikation beschäftigt.	
Kryptographische Nachrichtensyntax (Cryptographic Message Syntax - CMS)	Die kryptographische Nachrichtensyntax ist eine Syntax, die beliebige Nachrichten umschliesst, digital signiert, zusammenfasst, authentifiziert oder verschlüsselt.	draft-ietf-ediint-as2-16
MD5	Ein sicherer Einweg-Hash-Algorithmus, der in Verbindung mit der digitalen Signatur verwendet wird. Dieser Algorithmus ist akzepiert in AS2, jedoch wird er wegen seiner kurzen Schlüssellänge nicht empfohlen.	draft-ietf-ediint-as2-16
Nachrichtenprüfung zur Integrität (Message Integrity Check - MIC)	Die Nachrichtenprüfung zur Integrität - auch Kurzfassung der Nachricht genannt - ist das Resultat der Kurzfassung des Hash-Algorithmus, der von der digitalen Signatur verwendet wurde. Die digitale Signatur ist über den MIC berechnet worden.	draft-ietf-ediint-as2-16
PKI Disclosure Statement (PDS)	Ein Instrument, das ein CP oder CPS begleitet und wichtige Informationen über die Politik und Handhabungsvorschriften einer CA/PKI bekannt gibt. Ein PDS ist ein Mittel, um Informationen herauszustellen, die normalerweise detailliert in den zugehörigen CP und/oder CPS-Dokumenten mitgeteilt werden. Ein PDS soll jedoch nicht das CP oder CPS ersetzen.	RFC3647
Pretty Good Privacy (PGP) mit MIME	Digitaler Sicherheitsumschlag basierend auf dem Standard Pretty Good Privacy (PGP), integriert mit MIME Security Multiparts [6].	RFC3335
Registrierungsbehörde (Registration authority - RA)	Eine Organisation, die verantwortlich ist für die folgenden Funktionen: • Identifizierung und Authentifizierung der Zertifikatsanfrager • Bestätigung oder Ablehnung von Zertifikatsanfragen • Veranlassung von Widerrufen und Löschungen von Zertifikaten unter bestimmten Umständen • Weiterverarbeitung von Bezieheranfragen, ihre Zertifikate zu widerrufen oder zu löschen • Bestätigung oder Ablehnung von Bezieheranfragen,	RFC3647

	ihre Zertifikate zu erneuern oder zu ändern RA signieren oder erstellen jedoch keine Zertifikate. Eine RA ist bevollmächtigt, bestimmte Aufgaben einer CA zu übernehmen.	
SHA-1	Ein sicherer Einweg-Hash-Algorithmus, der in Verbindung mir der digitalen Signatur verwendet wird. Es ist der empfohlene Algorithmus für AS2.	draft-ietf-ediint-as2-16
S/MIME	Ein Format und Protokoll für das Hinzufügen von kryptographischen Signaturen und/oder Verschlüsselungen zu Internet MIME-Nachrichten.	draft-ietf-ediint-as2-16
Unleugbarkeit des Empfangs (Non-repudiation of receipt - NRR)	Die Unleugbarkeit des Empfangs ist gesichert, wenn der ursprüngliche Sender der signierten Nachricht die Signatur der Empfangsbestätigung des Nachrichtenempfängers verifiziert hat. Die Unleugbarkeit des Empfangs ist keine funtionelle oder technische Nachricht.	draft-ietf-ediint-as2-16
Zertifizierungsbehörde (Certification Authority - CA)	Eine von einem oder mehreren Nutzern als vertrauenswürdig betrachtete Behörde, die Zertifikate erstellt und ausgibt. Die CA kann auch die Benutzerschlüssel erstellen.	ISO/IEC 9594-8; ITU-T X.509
Zertifizierungsfolge (Certification Path - CP)	Eine bestimmte Reihenfolge von Zertifikaten, die zusammen mit dem öffentlichen Schlüssel des ersten Objekts in der Abfolge zu dem des letzten Objekts weiterverarbeitet werden können.	RFC3647
Zertifikatspolitik (Certificate Policy - CP)	Ein Regularium, das die Anwendung eines Zertifikattyps gegenüber einer bestimmten Gemeinschaft und/oder Anwendungsklassen mit gemeinsamen Sicherheitsanforderungen angibt. Beispielsweise kann ein CP die Anwendung eines Zertifikattyps bezüglich der Authentifizierung von Partnern angeben, die sich im Rahmen von B2B-Szenarien am Austausch von Gütern und Dienstleistungen innerhalb eines bestimmten Preisraums beteiligen.	RFC3647
Zusammenfassung des CPS (CPS Summary or Abstract)	Eine Teilmenge der Bestimmungen eines kompletten CPS, das von einer CA veröffentlicht wird.	RFC3647

Impressum

Herausgeber:
GS1 Germany GmbH, Köln

Geschäftsführer:
Jörg Pretzel

Text:
Christian Przybilla

Redaktion:
Elisabeth Kikidis

GS1 Germany GmbH
Maarweg 133 · D-50825 Köln
Postfach 30 02 51 · D-50772 Köln
Telefon (02 21) 9 47 14-0
Telefax (02 21) 9 47 14-990
eMail: info@gs1-germany.de
www.gs1-germany.de

GTIN 40 00001 01528 3

Markt der Dienstleister A. Auto-ID-Technik, Hard- und Software, B. IT/Kommunikation

A. AUTO-ID

Bluhm Systeme GmbH
Kennzeichnungssysteme
Honnefer Straße 41
53572 Unkel/Rhein
Tel.: (0 22 24) 7 70 80
Fax: (0 22 24) 77 08 20
E-Mail: info@bluhmsysteme.com
www.bluhmsysteme.com

Zertifiziert nach DIN EN ISO 9001:2000

- **Etikettendrucksysteme** (Thermo-/Thermotransfer) für Texte, Grafiken,Logos und alle gängigen Barcodes, z. B. EAN 128, EAN 13 etc. (optional mit RFID-Technologie)
- **Software zur Etikettengestaltung**
- **Etiketten** bedruckt und blanco auf Rolle oder leporello gefalzt, große Auswahl an unterschiedlichen Materialien und Klebern, Spezialetiketten.
- **Druck-/Spendesysteme (mit und ohne RFID-Technologie)** Etiketten drucken und spenden 1:1. Palettenetikettierung ohne Stop nach CCG-Norm/EAN 128
- **Mobile und stationäre Barcodelese-systeme**
- Flächendeckendes **Service-Netz** in D und A mit einer zentralen Service-Hotline.
- Systemgerechte **Verbrauchsmaterialien** und geprüftes Zubehör.
- **Alternative Kennzeichnungsmethoden** mit Großcodierern zum Digitaldruck auf Umverpackungen, Ink-Jet Codierern und Lasercodierern zur Produktkennzeichnung sowie Foliendirektdrucker

B. IT/KOMMUNIKATION

er.com EDI-Systeme & -Beratung
Industriestraße 16-20
33758 Schloß Holte-Stukenbrock
Frau Rutkowski
Tel.: (0 52 07) 95 26-0
Fax: (0 52 07) 95 26-26
E-Mail: info@ercom-edi.de
www.ercom-edi.de

- Software-Haus + Berater für EDI/EC-Lösungen seit 1991
- Produktfamilie EDIAL: branchenneutrale Gesamt-Lösung für den elektronischen Geschäftsverkehr
- auf diversen Plattformen incl. AS/400
- alle Netze und Formate incl. XML
- für alle Geschäftsbereiche
- viele Standard-Integrationen zu Warenwirtschafts- und FIBU-Lösungen
- Vollautomatik
- Seminare, Service, Hotline

er.com-Services GmbH
Industriestraße 16-20
33758 Schloß Holte-Stukenbrock
Herr Eichenbrenner
Tel.: (0 52 07) 95 27-0
Fax: (0 52 07) 95 27-27
E-Mail: info@ercom-edi.de
www.edifact-info.de

- EDI- und E-Commerce-Rechenzentrums-Dienstleistungen
- alle Formate incl. XML und VICS
- alle Netze incl. GXS- und AS2-Dienst
- viele Standard-Integrationen zu Warenwirtschafts- und FIBU-Lösungen
- Partner der SINFOS-GmbH
- Unser Service: schnell und kostengünstig zum SINFOS-Stammdatenpool
- Der Rund-um-sorglos-Service für alle, die nach Alternativen suchen – ob Outsourcing oder Neueinstieg

stratEDI Gesellschaft für Kommunikationskonzepte und -lösungen mbH
Lusebrink 9
58285 Gevelsberg
Herr A. Weng, Herr T. Schmoll
Tel.: (0 23 32) 6 66 00-0
Fax: (0 23 32) 6 66 00-29
E-Mail: info@stratedi.de
www.stratedi.de

GS1 Germany
www.zertifikate.gs1-germany.de
WebEDI System auf Basis GS1 Empfehlung Vers. 2.0 zertifiziert 4000001

- **Classic-EDI:** EDI-Konzepte, -Projekte und Implementierungen
- **CR:** Implementierung der CR-Nachrichten, Optimierung des Warenflusses mit Hilfe des EAN 128
- **BPI:** Business Partner Integration
- **B2B-Services:** WebEDI, EDI via Internet, Clearing, EDI-Outsourcing
- **eInvoicing:** Digitale Signatur von Rechnungsdaten (EDIFACT, EANCOM, PDF, etc.) AUTACK, Verifikation, WebService, Archivierung

Tangram TeleOffice GmbH
Schwarzwaldstraße 99
71083 Herrenberg
Herr Gerd Betz
Tel.: (0 70 32) 320-0
Fax: (0 70 32) 320-321
E-Mail: info@tto.de
www.tto.de

Spezialist für Kommunikation und Realisierung von Lösungen im Bereich der elektronischen Geschäftsprozessintegration (EAI/EDI).
TTO realisiert Geschäftsprozesse. Kernanwendungen wie ERP-Lösungen oder vorhandene Legacy-Anwendungen werden ergänzt. Dabei agiert TTO nach dem Grundsatz „modellieren, integrieren und visualisieren". Von der Beratung, Planung und Realisierung bis hin zum Betrieb durch die TTO Managed Services liefert TTO alle notwendigen Produkte, Lösungen und Dienstleistungen für automatisierte Abläufe zwischen Geschäftspartnern. Das umfassende Know-How der TTO findet Einsatz bei vielen namhaften Kunden.
Leistungsspektrum im Detail:

- Applikationen: Portale (WebEDI), e-procurement und Shop-Anwendungen, Warenhaus und Transport Management, Inventory Management und Replenishment, Lösungen für die Fertigungsindustrie (Produktkonfiguration, Ordermanagement)
- Realisierung von Individual-Anwendungen
- E-Services: Geschäftsprozess-Integration im Outsourcing
- E-Billing: digitale Signatur von Rechnungen, Versand und Archivierung nach GdPdU
- Business Prozess Management: Abbildung von Prozessen entlang der Wertschöpfungskette
- Business Prozess Monitoring: Dashboard, end to end Monitoring
- Outtasking
- Fullfillment: Infrastrukturservices

- Datenkassen, Datenwaagen MDE-Symbol-Lesesysteme
- Filmmaster
- Formulardruck mit Barcode
- Kommunikationssysteme
- Prüfgeräte
- Etiketten/Etikettendrucker
- Software
- Radiofrequenztechnik für Identifikationszwecke (RFID)
- Mitglied EPC/RFID-Umsetzungsnetzwerk

- EDI-Clearing
- EDI-Hotline
- Kommunikationssoftware
- Konverter
- Netzwerk
- Software, andere
- Mitglied EPC/RFID-Umsetzungsnetzwerk

Was können wir für Sie tun?

Haben wir Ihr Interesse geweckt? Erfordert ein konkreter Bedarf schnelles Handeln – oder möchten Sie sich einfach unverbindlich über Themen aus unserem Portfolio informieren? Nehmen Sie Kontakt mit uns auf. Wir freuen uns auf ein persönliches Gespräch mit Ihnen:

T +49 (0)221 9 47 14-0
info@gs1-germany.de

Global Standards – Connecting Business

4 000001 015283

GS1 Germany GmbH

Maarweg 133
50825 Köln
T +49 (0)221 9 47 14-0
F +49 (0)221 9 47 14-990
info@gs1-germany.de

www.gs1-germany.de