BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Energie-Info

Studie über sichere webbasierte Übertragungswege

Sicherheitsempfehlungen bei externen elektronischen Kommunikationsverbindungen über das Internet im Electronic Data Interchange der deutschen Energiewirtschaft

BDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“

Version 2.1

Berlin, 5. November 2009

INHALT

1. Management Summary 3
2. Zielgruppe / Zielsetzung 4
3. Sicherheit im elektronischen Geschäftsverkehr als Gegenstand der Verbandsarbeit 5
4. VEDIS – IT-Sicherheit im elektronischen Geschäftsverkehr 6
   - 4.1 Sicherheit auf der Informationsebene 6
   - 4.2 Synchrone Übertragungsverfahren schaffen Handlungsbedarf für Verbandsempfehlungen 8
   - 4.3 Fokus auf Transport und Information 8
   - 4.4 Was wird nicht behandelt? 9
5. Verbindungsvarianten im Internet 10
   - 5.1 Allgemeine Klassifizierung 10
   - 5.2 Verbindungen auf der Basis von HTTP 10
   - 5.3 Verbindungen auf der Basis von HTTPS 11
   - 5.4 Security-Anforderungen in E-Business-Architekturen 12
   - 5.5 Randbedingungen der EDI-Kommunikation 13
6. Austauschformate, Kommunikationsverfahren und Sicherheitsmechanismen 14
   - 6.1 Übertragungsstandards im Überblick 14
   - 6.2 Asynchrone Kommunikationsverfahren 15
   - 6.3 Das synchrone EDI-Verfahren AS2 15
   - 6.4 Das synchrone EDI-Verfahren Web-EDI 17
7. Fazit 19
8. Literatur 20
   - 8.1 Standards 20
   - 8.2 VDEW-Veröffentlichungen 20
   - 8.3 Abkürzungsregister 21

1 Management Summary

Elektronischer Datenaustausch zwischen Marktteilnehmern oder anderen Partnern gilt als sicher, wenn er über spezielle Services und nichtöffentliche Netze (Value Added Networks, VAN, z. B. X.400-Telebox) abgewickelt wird. Dabei entstehen jedoch mit steigenden Datenvolumen auch linear steigende Service-Kosten. Als Alternativen bieten sich Internet-basierte Dienste an, die meistens in den Unternehmen schon anderweitig genutzt werden und keine zusätzlichen Kosten verursachen. Diese Internet-Lösungen werden heute überwiegend benutzt. Eine Datenübertragung über das offene Internet muss allerdings seriös abgesichert werden, so dass eine Echtheit der Herkunft (Authentizität), eine Unversehrtheit des Inhaltes (Integrität) und die Vertraulichkeit der Inhalte jederzeit gewährleistet sind. Der BDEW[1] hat zu dieser Anforderung bereits eine Reihe von Materialien veröffentlicht (Projekt VEDIS).

Sobald der Datenaustausch über das offene Internet erfolgt, sollten gleichzeitig Verschlüsselung und Signatur eingesetzt werden. Aber selbst abgesicherte E-Mail-Kommunikation kann aufgrund des zeitversetzten Übermittlungsprozesses in einigen Fällen Nachteile haben. Dies gilt besonders bei hohen Anforderungen an die Datenaktualität, an Quittungsmechanismen und bei stark automatisierter Folgeverarbeitung. Diese Anforderungen bestehen z. B. im Bereich der zeitnahen Bereitstellung der täglichen Bilanzierung oder im Fahrplanmanagement.

Die Bundesnetzagentur (BNetzA) gibt durch die Festlegungen u. a. von GPKE und GeLi Gas zu den Geschäftsprozessen in der Energie-Branche die Verwendung von EDIFACT-Nachrichten zum Datenaustausch zwischen den Geschäftspartnern vor. Heute werden hauptsächlich E-Mails zur Übertragung dieser Nachrichten genutzt. Zur effektiveren Prozessgestaltung wird von den Unternehmen jedoch ein Übertragungsverfahren bevorzugt, das auf einer direkten Server-Server-Kopplung basiert und einen impliziten Quittungsmechanismus beinhaltet. Diese Funktion ist integraler Bestandteil des in diesem Dokument näher beschriebenen Übertragungsverfahrens EDIINT AS2 (EDIINT steht dabei für Electronic Data Interchange über das Internet; AS2 für Applicability Statement 2 gem. RFC 4130).

AS2 nutzt die Kerntechnologie des Internets. Betriebswirtschaftliche Funktionen und Sicherheitsparameter sind innerhalb einer Anwendungsumgebung parametrisierbar. Zudem sind Sicherheitsmechanismen integraler Bestandteil des Verfahrens bzw. der Anwendung. Die direkte Server-Server-Kopplung setzt eine ständig verfügbare, durch Firewall geschützte Internetverbindung für die Kommunikation voraus. Es existiert eine Reihe von Standardsoftwareimplementierungen. Die Kommunikation über AS2 kann als hausinterne Lösung oder auch unter Nutzung eines externen Dienstleisters („Datahub“) realisiert werden. AS2 wird als bevorzugtes Übertragungsverfahren für neue EDI-Implementierungen und EDI-Systemmigrationen den BDEW-Mitgliedern als Alternative zur E-Maillösung empfohlen.

[1] Im BDEW Bundesverband der Energie- und Wasserwirtschaft e. V. haben sich die Verbände BGW, VDEW, VRE und VDN zusammengeschlossen. Die bisher vom VDEW veröffentlichten VEDIS-Dokumente haben weiterhin Gültigkeit und sind beim BDEW im Internet zu finden.

2 Zielgruppe / Zielsetzung

Das vorliegende Dokument ist in der Version 2.1 die Fortführung/Überarbeitung der bereits mit Datum vom 15. Juni 2007 (Version 1.0) und mit Datum vom 13. Mai 2009 (Version 2.0) veröffentlichten gleichnamigen Studie. Gegenüber der Version 2.0 wurde insbesondere das Fazit (Kapitel 7) überarbeitet. Darüber hinaus wurde die Studie umfassend redaktionell überarbeitet. Die Ausarbeitung richtet sich im Wesentlichen an Entscheider und IT-Verantwortliche.

Elektronischer Datenaustausch zwischen den Marktteilnehmern wird heute über spezielle Dienste auf Basis X.400 oder internetbasiert über E-Mail und Filetransfer (FTP) realisiert. Diese Verfahren arbeiten ausnahmslos zeitversetzt (asynchron). Auf die Sicherheitsaspekte bei dem internetbasierten Verfahren E-Mail mit Übertragbarkeit der Aussagen auf FTP wurde bereits in veröffentlichten Dokumenten eingegangen. Es wird dringend empfohlen, diese Verfahren zum Datenaustausch nur in verschlüsselter und signierter Form zu nutzen.

Zielsetzung dieses Dokumentes ist es, wichtige webbasierte Verfahren anzusprechen. Dazu soll nach Anforderung der Kommunikation ein geeignetes synchrones Verfahren empfohlen werden. Dieses kann asynchrone Verfahren ersetzen, muss es aber nicht. Wichtig ist dabei, dass sich lediglich der Transportweg ändert und nicht die Anwendungen. Die Verfahren können somit nebeneinander koexistieren. Dazu sind grundsätzlich Lösungen in der Lage, die auf der World Wide Web Technologie und damit dem HTTP-Protokoll beruhen.

Das vorliegende Dokument diskutiert dabei zwei Varianten.

1) AS2-EDI-Lösung (Server-Server-Kopplung):
   Synchrone Kopplung zum Datenaustausch über EDI-Verfahren (EDIFACT) unter Ausnutzung eines bestehenden Standards (AS2). Das vorliegende Dokument diskutiert Motivation und Voraussetzungen zur Einführung dieses Verfahrens. Besonderer Schwerpunkt wird dabei auf die IT-Sicherheitsaspekte gelegt. Dazu wird zunächst der Zusammenhang zu den bisherigen Verbandsempfehlungen in diesem Bereich erläutert.
2) Web-EDI (Client-Server-Lösung):
   Von Web-EDI wird dann gesprochen, wenn einer der Partner kein eigenes EDI-System betreibt oder betreiben lässt. Web-EDI ist stets eine Portalanwendung, die durch einen der Partner bereitgestellt wird, über die mit einfachen Mitteln (manuell über Direkteingabe in einer Webseite; halbautomatisch über Datei-Upload) Daten ausgetauscht werden.

3 Sicherheit im elektronischen Geschäftsverkehr als Gegenstand der Verbandsarbeit

In der Mitteilung Nr. 5 Abs. 2 der BNetzA vom 28. November 2007 „Verwendung von elektr. Signatur und Verschlüsselung“ empfehlen die Beschlusskammern 6 und 7 (Strom und Gas), einvernehmlich zu treffende Entscheidungen über die Verwendung von Verschlüsselungs- und Signaturprodukten an den veröffentlichten VEDIS-Dokumenten auszurichten.

Diese Dokumente bilden die gemeinsame Basis, damit die Sicherheitsbelange im Geschäftsverkehr der Energiewirtschaft angemessen berücksichtigt werden.

Allgemein definiert, haben die organisatorischen Teile den Anspruch, ein einheitliches organisatorisches Sicherheitsniveau bei der Verschlüsselung und Signatur von unternehmensübergreifenden Transaktionen zwischen den Marktteilnehmern zu gewährleisten.

Ebenso allgemein definiert, sollen die technischen Teile der Dokumente auch beim Einsatz unterschiedlicher Produkte oder Dienstleistungen die Interoperabilität auf der technischen Ebene sicherstellen. VEDIS orientiert sich dabei strikt an aktuellen technischen Standards.

Die politischen, organisatorischen und technischen Aussagen in den Dokumenten haben Empfehlungscharakter und sollen in der Solidargemeinschaft der Marktteilnehmer eine verlässliche Vertrauensinfrastruktur ermöglichen.

Die Maßnahmen dienen als Leitlinie bei der Umsetzung im eigenen Unternehmen und der nachfolgenden Anwendung an den Marktschnittstellen. Alternative Vorgehensweisen sollen begründbar sein und das allgemeine Sicherheitsniveau nicht beeinträchtigen.

Die Marktteilnehmer sind aus wirtschaftlichen Gründen daran interessiert, dass die Vertrauensinfrastruktur sich weiter entwickeln kann. Nur dadurch ist die sichere elektronische Abwicklung der Geschäfte gewährleistet und kann so ausgebaut werden, dass auch weitere Automatisierungsschritte beherrschbar bleiben.

4 VEDIS – IT-Sicherheit im elektronischen Geschäftsverkehr

4.1 Sicherheit auf der Informationsebene

VEDIS sieht angesichts des Trends, Stammdaten, Zähldaten, Rechnungen oder Avise über das Internet zu übertragen, konkreten Handlungsbedarf bei der Informationssicherheit. Dabei entspricht die Nutzung des Internets für organisationsübergreifende Kommunikation der heute üblichen Vorgehensweise. Schließlich ist die Dienstgüte des Internets für die Anforderungen der deutschen Energiewirtschaft in den letzten Jahren ausreichend gut geworden, so dass volumenabhängige Kosten für ein Value Added Network (VAN, z. B. X.400) keine wirtschaftliche, organisatorische oder technische bzw. sicherheitstechnische Begründung mehr haben. Die Übertragung über das Internet muss nur so sicher gemacht werden, dass Echtheit der Herkunft (Authentizität des Absenders) und Unversehrtheit des Inhaltes (Integrität der Daten) in jedem Fall gewährleistet bleiben bzw. Manipulationen automatisch erkannt werden können. Dies gilt für asynchrone, also zeitversetzte Übertragungsmethoden, wie E-Mail oder File Transfer oder für zunehmend wichtiger werdende synchrone Methoden.

Die bisherigen VEDIS-Dokumente haben die Voraussetzungen an eine branchenweite Vertrauensinfrastruktur mit PKI-Mitteln definiert.

Die Dokumente orientieren sich an den Grundzielen

- technische Konformität herstellen (bis möglichst zur automatischen Interoperabilität).
- Mindestsicherheitsniveau verbandsseitig definieren.
- Vergleichbarkeit zwischen den Unternehmen über das Selbsterklärungsprinzip veröffentlichter Policy-Dokumente (Certificate Policy, CP) herstellen.

Die so definierte Vertrauensinfrastruktur konnte auf asynchrone Methoden, allen voran E-Mail (SMTP) mit dem dazugehörigen, aber allgemein einsetzbaren Sicherheitsstandard S/MIME, unmittelbar angewendet werden. Diese Übertragungsmethode und der damit verbundene Informationsschutz werden nach wie vor wichtig bleiben.

Für den unformatierten Informationsaustausch von Dokumenten im Rahmen des Geschäftsverkehrs (nicht EDI) wird es zur E-Mail mittelfristig keine wesentliche Alternative geben. Dabei führt bei einer Übertragung über das Internet per SMTP nichts an einer informationsgebundenen Absicherung, also elektronischer Signatur und Verschlüsselung auf Mail- oder Dateiebene vorbei, denn für den gesicherten Mailaustausch zum Partner wird kein VPN aufgebaut. Hier ist asymmetrische Kryptographie und damit Public Key Infrastruktur entweder auf Mailebene in Form von S/MIME oder auf Dateiebene als Dokumentensignatur zwingend erforderlich. Mittelfristig ist dabei aus wirtschaftlichen Gründen Mail-Verschlüsselung als „undurchsichtiger Briefumschlag“ und Dateisignatur als „Unterschrift“ sinnvoll, um nicht auch den „Briefumschlag“ neben der Datei / den Nettodaten zu Beweiszwecken aufbewahren zu müssen. Kurzfristig wird der Einfachheit halber beides zusammen als kombinierte Mail-Verschlüsselung und -Signatur angewendet.

Die ungesicherte Internetkommunikation ist für Unternehmen ein ernstzunehmendes Risiko, weil infolge der zunehmend automatisierten Verarbeitung eine Überprüfung der Kommunikation immer schwieriger wird. Auf jeden Fall nimmt der Energiemarkt branchenweit E-Business-Charakter an. Deshalb müssen Sicherheitsmaßnahmen für diese weitere Digitalisierung und Automatisierung der Geschäftsprozesse allen am Datenaustausch beteiligten Unternehmen „den Rücken frei halten“. Eine manuelle Überprüfung der Übertragungsqualität findet in dieser unaufhaltsamen Entwicklung zukünftig immer weniger statt. Sie muss durch geeignete Sicherheitsmaßnahmen ersetzt werden. Nur so bleibt weitere Rationalisierung beherrschbar.

VEDIS setzt keine Unternehmens-PKI voraus, sondern empfiehlt lediglich dort, wo elektronischer Datenaustausch zwischen Marktteilnehmern abgewickelt wird, entsprechende organisatorische und technische Maßnahmen mit den Mitteln von Public Key Infrastruktur.

Gesetzliche Regelungen bestehen z. B. bei der elektronischen Rechnung oder formgebundenen Verträgen. VEDIS empfiehlt, dort wo keine gesetzlichen Vorgaben existieren, preiswerte technische Lösungen bei angemessener organisatorischer Sicherheit. In bilateralen Vereinbarungen kann auf diese Verbandspapiere referenziert werden. Dadurch kann mit geringem Aufwand ein EDI-Vertrag zwischen den Partnern geschlossen werden.

Wesentliches Dokument ist dabei die Zertifizierungsrichtlinie (englisch Certificate Policy, CP) und erläuternde Dokumente. Sie definiert die drei wesentlichen Branchenziele von VEDIS

- Interoperabilität
- Mindestsicherheitsniveau und
- Vergleichbarkeit bei der Umsetzung von Sicherheitsmaßnahmen

Es soll dadurch branchenweit ein vergleichbares Sicherheitsniveau eingeführt und durch Veröffentlichung der Unternehmens-CP per Selbsterklärung durch den Marktteilnehmer bestätigt werden. Die Unternehmens-CP soll sich an die Zertifizierungsrichtlinie (VDEW-CP) anlehnen; Aufbau und zahlreiche Formulierungen können übernommen werden. Mit dieser Erklärung kann von jedem Marktteilnehmer, der sich zu den VEDIS-Empfehlungen bekennt, ein angemessener sicherer Umgang mit Geschäftsdaten vorausgesetzt werden. Weitergehende Maßnahmen sind nicht vorgesehen.

Zur Gewährleistung von Interoperabilität ist der technische Bezug die ISIS-MTT-Norm mit einigen bewussten Einschränkungen, um eine möglichst breite Anwenderbasis zu erreichen. Die Einschränkungen (z. B. Verzicht auf deutsche Umlaute in den Zertifikaten, UTF-7-Codierung) können dann, wenn normgerechtes Vorgehen und normgerechte Produkte am Markt die Regel sind, aufgehoben werden. Sie werden im Dokument „Technische PKI-Interoperabilität“ beschrieben.

4.2 Synchrone Übertragungsverfahren schaffen Handlungsbedarf für Verbandsempfehlungen

Die BDEW-Projektgruppe „EDI@Energy“ hat für die im Energiemarkt festgelegten Geschäftsprozesse (u. a.GPKE und GeLi Gas) entsprechende Nachrichtenformate definiert und auf Basis von UN/EDIFACT-Formaten normiert (EDI@Energy-Subset). Solange die Austauschformate als Dateien (nicht zusätzlich gesichert) per VAN (z. B. X.400-Box) oder (signiert und verschlüsselt) per E-Mail ausgetauscht werden, besteht auch kein weiterer Handlungsbedarf durch Verbandsempfehlungen. Beim Einsatz von synchronen Verfahren sind Sicherheitsmechanismen, Übertragungsparameter und Übertragungsprotokolle nicht mehr getrennt zu betrachten. Das vorliegende Dokument trägt diesen neuen Anforderungen Rechnung und macht deutlich, weshalb entsprechende Empfehlungen ausgesprochen werden.

Formatierte Daten, also der Austausch mittels EDI, werden zunehmend synchron übertragen, weil ein zeitnahes Quittungsmanagement und eine direkte Folgeverarbeitung benötigt werden oder bei steigender Anzahl von Nachrichten wünschenswert ist. Es gibt zwar schon käufliche Standardsoftware, die den Postkorb regelmäßig nach neuen E-Mails durchsucht und diese einer Folgeverarbeitung zuführt. Das SMTP-Protokoll ist jedoch von seinem Designprinzip „Store-and-Foreward“ so ausgelegt, dass diese Dienstprogramme nur innerhalb begrenzter Möglichkeiten bei E-Mail Effektivitätsgewinne bringen können. Mit asynchronen Methoden werden zwar eine Digitalisierung des Übertragungsprozesses erreicht und somit immerhin Medienbrüche verhindert. Zur besseren Folgeverarbeitung und damit weiteren Automatisierung des Prozesses sind jedoch synchrone, ereignisgetriebene Übertragungsmechanismen zumindest in einigen Anwendungsbereichen sinnvoll. Dies gilt vor allem für zeitkritische Anwendungen, z. B. wo Marktteilnehmer zeitnah ihre Verbrauchsdaten benötigen oder auch im Fahrplanmanagement.

Dies ist mit Verfahren denkbar, die auf dem Standardprotokoll HTTP des Internets beruhen (z. B. AS2 Applicability Statement 2, siehe Kapitel 6.3 oder Web-EDI-Portale, siehe Kapitel 6.4).

Zu zertifikatsbasierten Authentisierungs-Mechanismen gibt es keine sinnvolle Alternative. Andere Lösungen wie Value Added Networks (z. B. X.400, POP3) oder eine Kennung/Passwort pro angeschlossenem Unternehmen sind teurer oder unangemessen unsicher. Es müssen allerdings nicht immer personengebundene Zertifikate benutzt werden, wenn durch Kombination von Maßnahmen ein geeignetes Sicherheitsniveau erreicht wird.

4.3 Fokus auf Transport und Information

Sicherheitsmaßnahmen auf der Informationsebene haben den Vorteil, Sicherheitsmechanismen direkt an die Daten zu binden. Dies wird heute vorwiegend mit Mitteln einer Public Key Infrastruktur (PKI) gemacht. Allerdings scheuen viele Unternehmen den organisatorischen Aufwand, der mit dem Aufbau von PKI verbunden ist und suchen nach Möglichkeiten, allein auf der Leitungsebene zu schützen.

Transportgebundene Sicherheit und informationsgebundene Sicherheit sollten aber nicht als alternative Methoden oder gar als Gegensätze verstanden werden, sondern haben verschiedene Funktionen: Das VPN dient als gesicherter „Tunnel“ und Signaturen als „Plombe“. Bei modernen synchronen Verfahren existiert keine unmittelbar einsichtige und klare Grenze mehr zwischen sicherer Authentisierung, Schutz der Verbindung gegen Manipulation und vertraulicher Übertragung.

In diesem Dokument wird stärker auf Sicherheitsmaßnahmen in Verbindung mit synchronen Übertragungsverfahren eingegangen. Das vorliegende Dokument klammert den Bereich der asynchronen Kommunikation, also vorwiegend E-Mail oder File Transfer, weitgehend aus, weil er in anderen VEDIS-Dokumenten ausführlich behandelt wurde. Es werden keine tieferen Leitungsprotokolle diskutiert, sondern Mechanismen, die vor allem für sichere Datenübertragung über das Internet geeignet sind bzw. dafür konzipiert wurden.

4.4 Was wird nicht behandelt?

Informationsgebundene Sicherheit kann bis zur End-to-End-Security ausgebaut werden. Wird dies nicht gemacht, müssen angrenzende Systeme zumindest im Prinzip mit angesprochen werden, um die Sicherheit der ganzen Transaktionsstrecke beurteilen zu können.

Die Kontrolle externer Verbindungen allein durch Firewall-Systeme an der Netzwerkgrenze bietet in der Mehrzahl der Fälle keine hinreichende Sicherheit für Informationsobjekte bzw. ihre Verarbeitungssysteme. Vielmehr bedarf es einer angemessenen Kombination aus verschiedenen, ineinander greifenden Mechanismen, um ein notwendiges Maß an Sicherheit für interne Systeme zu erzeugen. Zu diesen Mechanismen zählen unter anderem auch fallweise die Überwachung und Härtung des internen Systems selbst. Auch der Einsatz von hostbasierten Intrusion Detection Systemen kann notwendig werden, auf die hier aber nicht näher eingegangen wird. Im Allgemeinen wird bei dem gewählten Ansatz von „Verteidigung in der Tiefe“ gesprochen.

Art und Umfang der als angemessen einzustufenden Schutzmaßnahmen hängen in erheblichem Maße von der Vertrauenswürdigkeit des externen Kommunikationspartners einerseits und der Schutzbedürftigkeit des internen Systems andererseits ab. „Innere Klammer“ ist dabei der Schutzbedarf der Informationsobjekte (Daten), die im Innenverhältnis durch die Verarbeitung und im Außenverhältnis durch die Übertragung betroffen sind. Jedes Unternehmen sollte deshalb Rahmenbedingungen zur Einstufung der Vertrauenswürdigkeit externer Kommunikationspartner und der Schutzbedürftigkeit interner Systeme definiert haben. Eine korrekte Einstufung der beiden Kommunikationsendpunkte und der dazwischen liegenden Verbindung ist eine unabdingbare Voraussetzung für die Auswahl der Zugangstypen. Der Schutzbedarf einer Klasse von Daten/Informationsobjekte (z. B. Adresse, Bankverbindung) wird durch gesetzliche Regelungen oder durch den Dateneigentümer festgelegt.

Diese Aspekte werden in den VDEW-Materialien M-14/2004, Konzept für IT-Sicherheit, näher behandelt.

5 Verbindungsvarianten im Internet

Der Austausch von Geschäftsdaten über das Internet wird im Allgemeinen „E-Business“ genannt. In diesem Kapitel werden die organisatorischen und technischen Aspekte von synchronen Verbindungen diskutiert und daraus Sicherheitsanforderungen für die Geschäftsabwicklung abgeleitet.

5.1 Allgemeine Klassifizierung

Im Internet haben sich zahlreiche Dienste mit ihren spezifischen Protokollen etabliert. Dazu gehören das Simple Mail Transfer Protocol (RFC 2821), das File Transfer Protocol (RFC 959) und das WWW mit dem HTTP-Protokoll. Diese Dienste repräsentieren Anwendungen oberhalb der Transportschicht, die immer IP-basiert ist, aber unterschiedlich ausgeprägt sein kann (TCP, UDP, SSL, etc.).

Aufgrund seiner Bedeutung für die weiteren Ausführungen wird im Folgenden das Hyper Text Transfer Protocol (HTTP) auf Basis des Transportprotokolls TCP und seine gesicherte Variante HTTPS ausführlicher behandelt.

5.2 Verbindungen auf der Basis von HTTP

HTTP-Verbindungen sind mittlerweile eine eigene technische Welt. An dieser Stelle sollen lediglich technische Bezüge zu Sicherheitsmechanismen hergestellt werden, die für externe synchrone Verbindungen zum Zwecke des Datenaustauschs relevant sein können.

Das "HyperText Transfer Protocol" (HTTP; dt: "Hypertext-Übertragungsprotokoll") ist das Datenübertragungsverfahren, auf dem das World Wide Web (WWW) beruht. Es ist in RFC 1945 und RFC 2068 definiert. Das Protokoll dient hauptsächlich zum Transfer von Web-Seiten, die in der "HyperText Markup Language" (HTML) geschrieben sind, kann aber neben reinem Text auch Dateien nach dem Client-Server-Prinzip übertragen.

Die Daten werden dabei in Klartext transportiert, gleiches gilt für eine UserID und ein Passwort für die Anmeldung an fremden Systemen. Zudem kann jeder Internet-Service-Provider die über seine Netzknoten geleiteten Daten-Pakete einsehen (Tool: packet sniffer).

Das HTTP baut auf dem Daten-Transportprotokoll TCP/IP auf. Das HTTP wird als "zustandsloses“ Protokoll bezeichnet, weil jeder Befehl ohne Kenntnis von (und ohne Bezug auf) den zuvor ausgeführten Befehl ausgeführt wird.

Zudem wird HTTP auch als „verbindungsloses“ Protokoll bezeichnet, denn es werden keine dauerhaften Verbindungen aufgebaut. Vielmehr wird für jede Anfrage eines Clients eine Verbindung zum Server eröffnet, auf die Antwort des Servers gewartet und dann die Verbindung wieder abgebrochen. Die Verbindung zwischen Client und Server wird also wieder abgebaut, sobald das angeforderte Dokument geliefert wurde. Dadurch werden die Ports (Netz-Anschlüsse) der HTTP-Server nicht dauerhaft belegt.

5.3 Verbindungen auf der Basis von HTTPS

Mit HTTPS://... beginnen URL (Uniform Resource Locators), bei denen die Datenübertragung zwischen Browser und Webserver über die Verfahren SSL (Secure Socket Layer) oder über TLS (Transport Layer Security) verschlüsselt wird. HTTPS ist deshalb in jeweils unterschiedlichen Normen (RFC) je nach verwendeter Zwischenschicht definiert. Es sichert das im Prinzip zustandslose HTTP-Protokoll mit Hilfe von (zunächst) asymmetrischer und (nach gesichertem Schlüsselaustausch) symmetrischer Kryptographie ab. Der öffentliche Schlüssel des Servers wird dabei durch ein X.509-Zertifikat bestätigt und muss vorher in den Browser installiert werden. Nach dem sicheren Kommunikationsaufbau mit Hilfe asymmetrischer Methoden und dem gegenseitigen Austausch von jeweils unterstützten Algorithmen werden symmetrische Sitzungsschlüssel vereinbart. Der Sitzungsschlüssel wird dann zur performanten, symmetrischen Verschlüsselung genutzt. In sensiblen Bereichen und im Außenverhältnis sollte mit mindestens 128 Bit langen Sitzungsschlüsseln gearbeitet werden.

Die Certification Authority (CA), als vertrauenswürdige dritte Instanz der beiden Kommunikationspartner, bestätigt den öffentlichen Schlüssel per Zertifikat und garantiert so die unverfälschte Übertragung der öffentlichen Schlüssel und die Echtheit des Webservers mit Hilfe von Fingerprint-Vergleichen. Das Zertifikat der CA wird in allen Browsern installiert und erscheint dort als "vertrauenswürdige Stammzertifizierungsstelle". Sollte das Zertifikat nicht installiert sein, erhält der Benutzer beim Öffnen der Webseite eine Fehlermeldung und eine Abfrage, ob er die Verbindung trotzdem herstellen möchte.

Der Benutzer baut die Verbindung auf, indem er entweder auf einen Link (beginnend mit HTTPS://.....) klickt oder die URL im Browser einträgt. Der Browser baut daraufhin eine Verbindung nicht mehr über Port 80 sondern über Port 443 (Default-Wert) zum Webserver auf. Der Webserver überträgt sein Zertifikat, das der Client mit Hilfe des installierten CA-Zertifikats auf Echtheit überprüft. Danach generiert und überträgt der Browser einen nur für den Webserver lesbaren Sitzungsschlüssel (mit dem öffentlichen Schlüssel des Webservers verschlüsselt). Mit dem nun auf beiden Seiten vorhandenen Sitzungsschlüssel kann eine symmetrische Datenverschlüsselung beginnen. Während das HTTP bzw. HTTPS-Protokoll der Anwendungsschicht zugeordnet werden muss, liegt das eigentliche kryptographische Verfahren bei SSL (Secure Socket Layer). SSL setzt auf der Socket-Schicht oberhalb TCP/IP auf und kann auch für andere Anwendungsprotokolle (z. B. FTP) verwendet werden. Wird das SSL-Verfahren auf Webseiten über das Hypertext Transfer Protocol HTTP angewendet, so ändern sich die URL von HTTP zu HTTPS. SSL kennt die Algorithmen, nutzt Serverauthentisierung und optional auch Clientauthentisierung und sorgt für Datenintegrität im Rahmen des paketorientierten Übertragungsverfahrens TCP, d. h. sichert insbesondere die einzelnen Datenpakete in sich ab.[2]

[2] Inzwischen ist in RFC 2246 mit Transport Layer Security (TLS) ein Nachfolger von SSL als offener Standard definiert. Die Unterschiede zu SSL, Version 3, sind minimal.
T. Dierks, C. Allen: RFC 2246: The Transport Layer Security (TLS) Protocol, Version 1.0, Januar 1999
http://www.ietf.org/rfc/rfc2246.txt

Eine bereits hergestellte HTTPS-Verbindung kann von einem der Client-Server-Kommunikation zwischengeschalteten Firewall-System oder Proxy-System nicht überwacht werden. Der Firewall oder dem Proxy ist es lediglich möglich, den Datenverkehr aufgrund von IP-Adressen und Portnummern zu verbieten. Im Datenstrom selbst können, aufgrund der in den TCP-Paketen verschlüsselten Daten, keine weiteren Überprüfungen durchgeführt werden.

Um den Datenverkehr dennoch überwachen zu können, muss ein Reverse-Proxy-System konfiguriert werden. Der Webserver wird nun nicht mehr direkt angesprochen, sondern erhält seine Anfragen vom Reverse-Proxy. Um die Kommunikation von Client zum Reverse-Proxy gesichert ablaufen zu lassen, wird auf dem Reverse-Proxy ein Server-Zertifikat benötigt, so dass eine verschlüsselte Verbindung aufgebaut werden kann. Der Reverse-Proxy seinerseits baut eine Verbindung zum eigentlichen Zielsystem auf. Hierbei besteht grundsätzlich die Möglichkeit, die Verbindung zwischen Reverse-Proxy und dem Zielsystem ebenfalls zu verschlüsseln – aber auch eine unverschlüsselte Weiterführung der Kommunikation ist möglich.

Sobald dem Reverse-Proxy-System der unverschlüsselte Datenstrom vorliegt, ist es möglich, diverse Überprüfungen am Datenstrom vorzunehmen und kontrollierend auf ihn einzuwirken. Beispielsweise können jetzt Normalisierungen oder Viren-Überprüfungen an übertragenen Objekten durchgeführt, Webserver- und Virenattacken erkannt und Zugriffsbeschränkungen bezüglich Kommandos und URL implementiert werden.

5.4 Security-Anforderungen in E-Business-Architekturen

Aus dem Anwendungsszenario „E-Business“ und den genannten technischen Rahmenbedingungen und Protokollebenen im Internet können Security-Anforderungen abgeleitet werden. Die verbreiteten Plattformen für E-Business Anwendungen werden nach analogen Architekturprinzipien eingesetzt. Sie haben zu einer mehrschichtigen Architektur geführt. Im Firewall-geschützten Intranet steht der Application Server als Back-End und hat Zugriff auf etablierte ältere Anwendungen und auf Datenbanken.

Je nach Größe können Varianten mit und ohne Demilitarisierte Zone (DMZ) gewählt werden. Mit der DMZ-Variante sind Backup-Konzepte (z. B. über mehrere Provider) realisierbar, falls die Produktionsverbindung ausfällt.

Variante 1: mit DMZ (siehe Bild 1)

In einer DMZ stehen empfangender Webserver bzw. Portalserver als Front-End und werden durch Firewall gegen das Internet geschützt.

Variante 2: ohne DMZ

Der Webserver empfängt und sendet Daten über einen Provider und ist durch eine entsprechend konfigurierte Firewall geschützt.

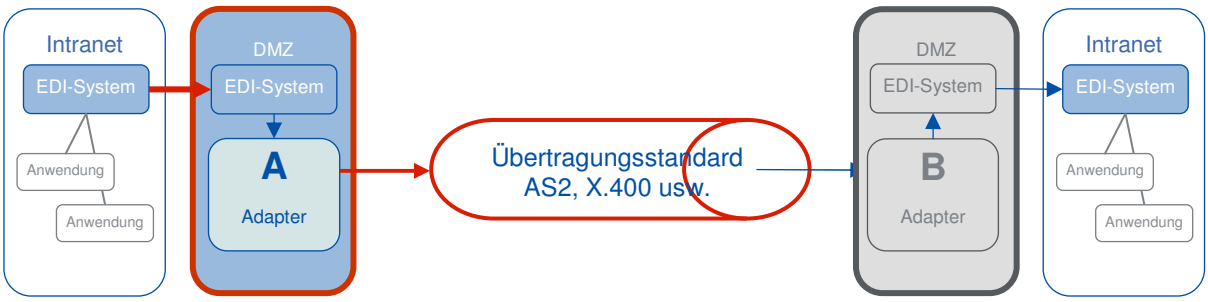

Bild 1: Datenaustausch über AS2 zwischengeschalteter DMZ.

5.5 Randbedingungen der EDI-Kommunikation

Eine EDI-Kommunikation kann über eine synchrone oder asynchrone Verbindung erfolgen. Eine synchrone Verbindung besteht, wenn der Absender mit seiner Nachricht beim Empfänger unmittelbar einen Folgeprozess anstoßen kann. Hingegen erfolgt bei einer asynchronen Verbindung die Reaktion des Empfängers zeitversetzt.

Grundsätzlich kann jeder Geschäftsprozess über eine synchrone oder asynchrone Verbindung abgewickelt werden. Allerdings unterstützen die verschiedenen Kommunikationsstandards (vgl. Kapitel 6) im Regelfall nur eine von beiden Verbindungsarten.

Unter dem Blickwinkel sicherer Übertragungswege sind Zustellzeiten und Zustellbestätigung zu betrachten. Bei einer synchronen Verbindung sind Zustellzeiten und Zustellbestätigung bereits implizit gelöst. Hingegen muss bei Verwendung einer asynchronen Verbindung die Einhaltung von Zustellzeiten und Zustellungsbestätigung gesondert behandelt werden.

6 Austauschformate, Kommunikationsverfahren und Sicherheitsmechanismen

6.1 Übertragungsstandards im Überblick

Zunächst eine Kurzcharakterisierung der marktüblichen Übertragungsstandards die in den Folgekapiteln vertieft werden zusammen mit weiteren Übertragungsstandards.

Übertragungs-standard	Technik	Kosten	Sicherheit
Value Added Network (X.400)	Internetverbindung zu X.400-Provider (Telefon-einwahl unüblich in heutiger Zeit)	Volumen-abhängige Kosten	• asynchrones Verfahren • Quittungsmechanismen • gilt als hinreichend sicher
E-Mail	Internetbasierte Dienste Simple Mail Transfer Protocol (SMTP)	ohne Mehrkosten vorhanden	• asynchrones Verfahren • keine Quittungs-mechanismen • durch Zusatzfunktionen zu sichern
Filetransfer	Internetbasierter Dienst File Transfer Protocol (FTP) bzw. sichere SFTP-Variante	ohne Mehrkosten vorhanden	• asynchrones Verfahren • Quittungsmechanismen über 2. Kanal • durch Zusatzfunktionen zu sichern
Web-EDI	WWW-basiert	Eigene Portalanwendung nötig	• technisch synchrones Verfahren, über Handling de facto zeitversetzt Datenaustausch über ASCII-Schnittstelle (Dialog oder halbautomatisiert) • Sicherheit meist über Username und Passwort
AS2	WWW-basiert	Ständige Internetverbindung erforderlich	• synchrones Verfahren • Quittungsmechanismen sind Bestandteil des Verfahrens • integrierte Sicherheitsmaßnahmen

6.2 Asynchrone Kommunikationsverfahren

Als Marktschnittstellen wurden EDI-Nachrichtenformate in der Vergangenheit zum Datenaustausch im Rahmen des liberalisierten Strommarktes auf Basis von UN/EDIFACT-Nachrichten genormt. Diese Nachrichten wurden anfangs und zum Teil auch heute noch in Kombination mit Übertragungsdiensten, wie der Telebox 400 4400 (X.400-Dienst mit Kurzwahl 4400) der Deutschen Telekom oder anderer Value Added Networks (VAN), genutzt. Durch die externen Postfächer wird eine ständige Erreichbarkeit der Kommunikationspartner gewährleistet. Mittlerweile haben sich hier auch Dienstleister etabliert, die z. B. eine Kombination aus Kommunikations- und Konvertierungsservices anbieten. Dies kann etwa mit Pop3-E-Mail-Einwahl und Konvertierung von Inhouse-Format in EDIFACT und umgekehrt erfolgen.

In jedem Fall entstehen bei VAN weitere, insbesondere volumenabhängige Kosten. Dies ist der Grund, wieso zunehmend eine Übertragung mittels eines VAN durch direkte Nutzung des Internets ersetzt wird. Dieser Trend ist international zu beobachten, seit das Internet eine so verlässliche Dienstgüte erreicht hat, die es erlaubt, geschäftskritische Daten in einem ausreichend kleinen Zeitfenster zu versenden. So sollten in Skandinavien deshalb schon X.400-Boxen abgeschaltet werden und wurden nur nach Protesten von Anwendern weiterbetrieben.

Doch auch der Wechsel zu E-Mail oder Filetransfer als Kommunikationsmethode für EDI-Nachrichten hat seine Nachteile. In vielen Fällen ist eine Benutzereingabe erforderlich. Bei E-Mail ist zwar eine Digitalisierung erreicht worden, die immerhin einen Medienbruch verhindert, aber das Automatisierungspotenzial ist noch nicht ausgeschöpft worden. E-Mail-Transfer kann deshalb nur ein Zwischenschritt in der Entwicklung von organisationsübergreifenden Geschäftsprozessen sein.

6.3 Das synchrone EDI-Verfahren AS2

Die Unternehmen möchten zunehmend direkt das Internet als Transportplattform nutzen und nicht mehr über Value Added Services (VAN), wie X.400, Daten austauschen. VAN gelten zwar als sicherer Transportweg, es entstehen aber volumenabhängige Kosten. Bei E-Mail entstehen kaum volumenabhängige Kosten, es müssen aber Sicherheitsanforderungen, wie Vertraulichkeit, Unversehrtheit und Nichtabstreitbarkeit gewährleistet werden.

Zudem haben SMTP als E-Mail-Standard im Internet oder das Filetransferprotokoll FTP ebenso wie X.400 den Nachteil der Store-and-Foreward Übertragung. Durch die damit verbundene Asynchronität lässt sich eine automatisierte Weiterverarbeitung nur durch indirekte Mechanismen erreichen. Bei E-Mail wird dies heute noch vielfach durch umständliche Auswertung der Betreffzeile erreicht. Oft sind trotzdem noch manuelle Eingriffe erforderlich, um etwa einen Dateianhang einer Folgeverarbeitung zuzuführen. E-Mail-Transfer kann deshalb nur ein Zwischenschritt in der Entwicklung von organisationsübergreifenden Geschäftsprozessen sein. In den Anwendungsfällen, wo es um zeitnahe Datenübermittlung geht, werden deshalb synchrone Verfahren gefordert.

Auch für synchrone Verfahren muss die Sicherheit gewährleistet und in Form von Vereinbarungen definiert werden.

Der Standard EDIINT AS2 (Applicability Statement 2, RFC 4130) soll in seiner wichtigsten Intension ein Protokoll bereitstellen, das den synchronen EDI-Datenaustausch über das Internet mit minimalen Umstellungskosten und bei weicher Migration ermöglicht. Dies bedeutet, dass der Datenaustausch bei gleichzeitiger Beibehaltung bestehender EDI-Austauschprozesse und unter Beibehaltung von netzspezifischen Nutzergruppen erfolgen muss. Die Daten werden immer über die gängigen Austauschformate, also Marktschnittstellen, ausgetauscht. Die EDI-Schnittstellen arbeiten heute vor allem auf dem für die Energiewirtschaft wichtigen auf UN/EDIFACT basierenden Nachrichtenformaten. Diese können bei AS2 beibehalten werden und müssen nicht auf XML umgestellt werden. Bestehende Wege (z. B. X.400, E-Mail) werden lediglich um einen weiteren Weg (HTTP) ergänzt. Auf dem zusätzlichen, synchronen „Weg“ ist lediglich das Transportprotokoll anders, wie es auch beim Übergang von X.400-Boxen zu E-Mail sich geändert hat. Somit kann man von Internet-Technologien profitieren, ohne die bestehenden Prozesse und Verarbeitungsschnittstellen negativ zu beeinflussen. Dies wird mittels standardisierter Signatur- und Verschlüsselungsmechanismen auf der Transportebene erreicht. Es wird quasi ein sicherer Briefumschlag um jedes beliebige Datenaustauschformat gebildet. AS2 verlangt zwingend ein TCP/IP-basiertes Netz und erfordert eine ständige Erreichbarkeit der Kommunikationspartner über das Internet. Nach dem Verbindungsaufbau erfolgt eine Authentifizierung und erst dann ein vertraulicher Datenaustausch.

Das Verfahren AS2 hat folgende Vorteile:

- Etablierte Nachrichtenformate können beibehalten werden
- Bestehende Anwendungen und Prozesse bleiben unberührt
- Nur das Transportnetzwerk wird geändert
- Internet-basiert (TCP/IP)
- Kerntechnologie des World Wide Web (HTTP)
- Statusinformationen des Dokumentes / Erkennen von Veränderungen
- Vertraulicher Versand von Dokumenten für den adressierten Empfänger
- Quittungsmechanismen
- Sichere Übertragung ohne Mitlesemöglichkeit
- Unleugbarkeit (Nicht-Abstreitbarkeit)
- Konsequente Verwendung und Integration bestehender Standards

Vor allem bei Anforderungen an ein konsistentes Quittungsmanagement haben synchrone Verfahren herausragende Bedeutung, weil nur ein Request-Response-Verfahren zeitnah und unter Bezug auf die einzelnen Verarbeitungsebenen quittieren kann.

Logisch getrennte Ebenen sind anhand folgender Fragen zu unterscheiden:

1. Physikalische Übertragung korrekt? (Kommunikationsantwort, Communication Response)
2. Syntaktisch korrekt? (Funktionsantwort, Functional Response)
3. In der Anwendung verarbeitbar? (Geschäftsstufenantwort, Business Level Response)
4. Vertraglich korrekt?

Wenigstens bei den Punkten 1 bis 3 ist eine synchrone Quittungsbehandlung wünschenswert, Punkt 4 kann in letzter Konsequenz nur durch Menschen entschieden werden.

Bei AS2 kann neben den Punkten 1 bis 3 aus dem Bild 2 ein weiterer synchroner Empfangsbestätigungsmechanismus eingestellt werden, der als Message Disposition Notification (MDN) bekannt ist und den Verwendungszweck charakterisiert. Die Parameter des Verfahrens für den Einsatz im deutschen Energiemarkt werden in einem zusätzlichen VEDIS-Dokument (Leitfaden) veröffentlicht.

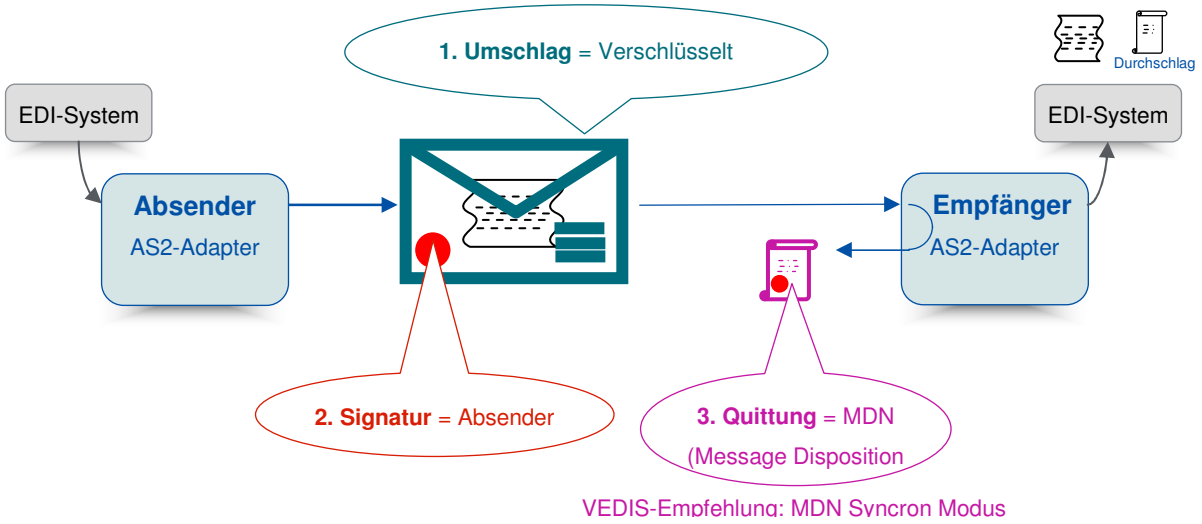

Bild 2: Prinzip der AS2-Übertragung; Darstellung der wesentlichen Merkmale des Verfahrens

6.4 Das synchrone EDI-Verfahren Web-EDI

Von Web-EDI wird dann gesprochen, wenn einer der Partner kein eigenes EDI-System betreibt oder betreiben lässt. Web-EDI ist stets eine Portalanwendung, die durch den einen Partner bereitgestellt wird, über die mit einfachen Mitteln (manuell über Browser, halbautomatisch über ASCII-Schnittstellen) Daten ausgetauscht werden.

Web-EDI wird benutzt, um manuell oder teilautomatisiert Daten in ein Portal des Marktpartners einzustellen. Bei Web-EDI sind praktisch keine EDI-Vorkenntnisse beim Benutzer erforderlich, weil die EDI-Infrastruktur vom Marktpartner bereitgestellt wird. Zur manuellen Erfassung werden HTML-Formulare bereitgestellt oder zur Teilautomatisierung lediglich eine AS-

CII-Schnittstelle. Diese Varianten haben sich in der deutschen Energiewirtschaft bereits etabliert, wie z. B. beim Einzelkundenwechsel oder bei der Eingabe von Jahreszählerständen.

Soll der Datenaustausch im Energiemarkt Web-EDI-basiert bzw. Portal-basiert erfolgen, so entspricht das Vorgehensmodell einem Download oder Upload der Daten aus oder in das Portal bzw. die Web-Anwendung des anderen Marktteilnehmers. Unter IT-Sicherheitsgesichtspunkten sind hier besonders Autorisierung und Authentifizierung interessant. Autorisierung mittels Kennung/Passwort ist zwar noch weit verbreitet, wird aber zunehmend durch zertifikatsbasierte Verfahren ersetzt, weil eine Unternehmenskennung kaum geheim zu halten ist.

7 Fazit

Elektronischer Datenversand stellt hohe Anforderungen an Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit. Aus diesem Grunde sind vertrauliche Daten über verschlüsselte Wege zu senden und per Signatur zu authentifizieren.

Die Einhaltung von Fristen in den Geschäftsprozessen fordert in stark zunehmendem Umfang eine Einstufung als zeitkritischer Prozess und erfordert somit die Wahl eines synchronen Übertragungsverfahrens.

AS2 wird als synchrones Standardaustauschverfahren über das Internet empfohlen. Es verlangt wenige Änderungen am EDI-Geschäftsprozess, ist lediglich eine andere Transportvariante auf hoher Protokollebene und gewährleistet die Unleugbarkeit der fristgerechten Zustellung.

Diese Empfehlung entspricht auch der EASEE Gas Empfehlung für den Europäischen Gasmarkt (CBP 2007-01-01).

Das im Energiemarkt zur Zeit eingesetzte Verfahren basierend auf E-Mail (SMTP) mit S/MIME kann dort weiterhin genutzt werden. Grundsätzlich sollte die E-Mail-basierende Kommunikation weder im Strom- noch im Gasmarkt für Neuimplementierungen verwendet werden. Um die Kommunikationsaufwände in der Branche zu reduzieren, empfiehlt der BDEW, auch die bestehenden E-Mail-Lösungen durch AS2 abzulösen.

Weitere Veröffentlichungen zum Übertragungsverfahren AS2

Wegen der Bedeutung des Übertragungsverfahrens AS2 für die Branche veröffentlicht der BDEW zur weiteren Unterstützung seiner Mitgliedsunternehmen und ergänzend zu dieser überarbeiteten Studienversion 2.1 gleichzeitig folgende weiteren Dokumente:

- Leitfaden "Implementierung von AS2 in Unternehmen der Energiewirtschaft"
- Marktüberblick zu existierenden AS2-Lösungen für die Energiewirtschaft

8 Literatur

8.1 Standards

- Common ISIS-MTT Spezification for PKI Applications from T7 & TeleTrusT, V1.1, März 2004
- EDIINT AS2 Umsetzungshilfe, GS1 Germany, Köln 2005
- AS2 Beschreibung und Parameter, EDI Anwenderkreis Handel, vom 10.10.2004

8.2 VDEW-Veröffentlichungen (siehe Fußnote 1 auf Seite 3)

- Einsatz von Verschlüsselung und Elektronischer Signatur im elektronischen Geschäftsverkehr der deutschen Elektrizitätswirtschaft, Studie
  VDEW-Materialie M-14/2002
- Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt, Gemeinsame Erklärung der Verbände
- Sicherheitspolitik (PKI-Policy), Version 1.0
  VDEW-Materialie M-14/2003
- Umgang mit Schlüsselmaterial, Version 1.0
  VDEW-Materialie M-17/2003
- Technische PKI-Interoperabilität, Version 1.0
  VDEW-Materialie M-15/2003
- Umsetzungsempfehlungen, Version 1.0
  VDEW-Materialie M-16/2003
- Zertifizierungsrichtlinie (Certification Practice Statement), Version 1.0
  VDEW-Materialie M-18/2003
- Zehn Schritte zur VEDIS-Sicherheit
  VDEW-Materialie M-07/2005
- Unternehmensübergreifende PKI-Topologien, PKI-Dienste und Einsatzrahmenbedingungen
  VDEW-Materialie M-08/2005
- Weitere VEDIS-Einsatzpotenziale in papierlosen Geschäftsprozessen
  Energie Spezial 2006
- PKI-Zertifikatsrichtlinie (Certificate Policy) des VDEW
  Energie-Info 01/2007
- Studie: Sicherer elektronischer Geschäftverkehr
  Energie-Info 02/2007
- Kommunikationsrichtline (aktuelle Fassung siehe www.edi-energy.de)

8.3 Abkürzungsregister

AS2	EDIINT AS2 (EDI over Internet applicability statement 2) Internet-basiertes Datenaustauschverfahren auf Basis des HTTP-Protokolls
BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
CA	Certification Authority
DMZ	Demilitarisierte Zone Die DMZ wird durch eine Firewall (außen) und eine Firewall (innen) gegen das Internet abgeschirmt. Durch diese Trennung besteht die Möglichkeit Zugriff auf öffentliche Dienste (z. B. E-Mail, WWW) anzubieten und gleichzeitig das interne Netz LAN vor ungerechtfertigten Zugriffen zu schützen.
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EDIINT	Electronic Data Interchange Internet Integration
FTP	File Transfer Protocol Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke
HTTP	Hyper Text Transfer Protocol Das Protokoll im World Wide Web
HTTPS	Hypertext Transfer Protocol Secure Mittels SSL/TLS gesicherte HTTP-Verbindung
IP	Internet Protocol
IPSEC	IP Security Ergänzungen zur Behebung von Sicherheitsschwächen von → IP in der Version 4 und Entwicklungsbasis für IPv6
MIME	Multipurpose Internet Mail Extensions Informationen über den Typ der übermittelten Daten (Content-Type) und Festlegung der sicheren Kodierung gemäß Übertragungsweg (Content-Transfer-Encoding)
ISIS-MTT	Industrial Signature Interoperability and Mailtrust Specification
PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3 Kommando-orientiertes ASCII Übertragungsprotokoll, über das ein Client E-Mails von einem E-Mail-Server abholen kann.
RFC	Requests for Comments
S/MIME	Secure MIME Verschlüsseln und digitales Signieren von Nachrichten mittels asymmetrischer Kryptographie

SFTP	Secure File Transfer Protocol Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke, das eine File-Transfer-Protocol-Verbindung (FTP) teilweise über Secure Shell (SSH) tunnelt.
SMTP	Simple Mail Transfer Protocol Protokoll der TCP/IP-Protokollfamilie zum Versand von E-Mails
SSH	Secure Shell Entferntes, authentisiertes und verschlüsseltes Einloggen und Programme über Port 22 ausführen
SSL	Secure Sockets Layer bzw. Transport Layer Security (TLS) Verschlüsselungsprotokoll für Datenübertragungen im Internet. TLS ist die standardisierte Weiterentwicklung von SSL 3.0.
TCP	Transmission Control Protocol Zuverlässiges, verbindungsorientiertes Transportprotokoll; Teil der TCP/IP-Protokollfamilie
TLS	Transport Layer Security
UDP	User Datagram Protocol Minimales, unzuverlässiges, verbindungsloses Netzprotokoll
URL	Uniform Resource Locator Identifizieren eine Ressource über ihren primären Zugriffsmechanismus (häufig HTTP oder FTP) und den Ort (engl. location) der Ressource
UTF-7	Unicode-Transformation-Format. UTF-7 erlaubt die Verwendung von Unicode in nicht 8-bit-festen Umgebungen
VAN	Value Added Network
VDEW	Verband der Elektrizitätswirtschaft e.V. (siehe Fußnote 1 auf Seite 3))
VEDIS	Vertraulichkeit und Datensicherheit Eine verbandsübergreifende Projektgruppe der Energiewirtschaft
VPN	Virtual Private Network Computernetz zum Transport privater Daten über ein öffentliches Netz (zum Beispiel das Internet), Absicherung über → IPsec oder → SSL/TLS
XML	Extensible Markup Language
X.400	Ein Übertragungsstandard nach ISO 10021 Nicht auf das Internet bezogene elektronische Mail-Verfahren mit aufwendigen Protokoll- und Quittungsmechanismen

Ansprechpartner:

Rainer Lautenbacher
Telefon: +49 30 300199-1661
rainer.lautenbacher@bdew.de

Beate Becker
Telefon: +49 30 300199-1666
beate.becker@bdew.de