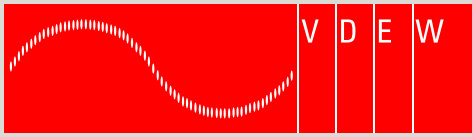
VDEW

MATERIALIEN

M-07/2005

Zehn Schritte zur VEDIS-Sicherheit

Empfehlungen aus Sicht der deutschen Elektrizitätswirtschaft



Verband der
Elektrizitätswirtschaft e.V.

Zehn Schritte zur VEDIS-Sicherheit

Empfehlungen aus der Sicht der deutschen Elektrizitätswirtschaft

Oktober 2005

Beate Becker, Telefon: 030/726147-209, Mail: beate_becker@vdew.net

Ergänzend zu den Gesetzen und Rechtsvorschriften für den Einsatz der elektronischen Signatur und der Verschlüsselung haben die Verbände eine gemeinsame Erklärung zu „Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt" abgegeben. Diese stellt die Basis für die Bildung einer Vertrauensinfrastruktur der Marktteilnehmer beim elektronischen Datenaustausch dar und zeigt Maßnahmen zur Sicherheit auf. Dadurch wird das Sicherheitsniveau auf der technischen und organisatorischen Ebene nachhaltig gehoben.

Public Key Infrastruktur (PKI) in einem Unternehmen zu begründen, einzuführen und im täglichen Betrieb zu leben, hat sich vielfach als mühsames Unterfangen herausgestellt. Viele begrüßen grundsätzlich IT-Sicherheitsmaßnahmen, doch schon die PKI-Terminologien und -Technologien schrecken ab. PKI ist eine infrastrukturelle Maßnahme - wie Telefon oder E-Mail. Eine Anwendung ist meist für einen positiven Business Case zu wenig. Erst mehrere Anwendungen rechnen sich. Ein Unternehmen muss deshalb PKI strategisch wollen und mittelfristig, d. h. über 3 Jahre, budgetieren. Dann wird sich neben dem Sicherheitsgewinn auch der wirtschaftliche Nutzen einstellen.

Das vorliegende Dokument will deutlich machen, dass für alle Marktteilnehmer jeder Größe es wirtschaftlich interessant, gesetzlich opportun und technisch/organisatorisch unproblematisch ist, die im Rahmen von VEDIS empfohlenen PKI-Sicherheitsmaßnahmen von Kommunikationspartnern zu akzeptieren und selbst zu praktizieren. Viele Themenbereiche wurden in bereits vorliegenden VEDIS-Papieren adressiert. Dieses Dokument soll in seinem Leitfadencharakter die Schritte zur „VEDIS-Sicherheit“ darstellen.

VDEW

Verband der
Elektrizitätswirtschaft e.V.

Zehn Schritte zur

VEDIS-Sicherheit

Empfehlungen aus Sicht der deutschen Elektrizitätswirtschaft

VDEW-Projektgruppe Sicherheit beim elektronischen Datenaustausch

Version: 1.0

STAND: 31. OKTOBER 2005

INHALT

1 Sicherheit im Elektronischen Geschäftsverkehr als Gegenstand der Verbandsarbeit

In diesem Dokument sollen im Überblick sinnvolle und notwendige Schritte zum Aufbau einer Public Key Infrastruktur (PKI) aufgezeigt werden. Es wendet sich an Entscheider und an Mitarbeiter von Energieversorgungsunternehmen, die sich mit der Einführung von PKI beschäftigen und Basiswissen und Basisterminologie dazu mitbringen. Dieses Dokument steht im Gesamtzusammenhang mit weiteren Dokumenten, die technisch und organisatorisch tiefer auf die PKI-Thematik eingehen.

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat zur Gewährleistung einer sicheren Kommunikation zwischen den Marktteilnehmern in der deutschen Elektrizitätswirtschaft eine gemeinsame Erklärung zu "Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr im deutschen Strommarkt“ zwischen den beteiligten Verbänden angeregt. Die Erklärung wird von folgenden Verbänden getragen:

- Bundesverband der Deutschen Industrie e. V. - BDI, Berlin
- VIK Verband der Industriellen Energie- und Kraftwirtschaft e. V., Essen
- Verband der Elektrizitätswirtschaft - VDEW - e.V., Berlin
- Verband der Netzbetreiber - VDN - e.V. beim VDEW, Berlin
- Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland - VRE - e. V., Berlin
- Verband kommunaler Unternehmen - VKU - e.V., Köln

Diese Erklärung bildet die gemeinsame Basis, damit die Sicherheitsbelange im Geschäftsverkehr in der Branche angemessen berücksichtigt werden.

Die Erklärung auf der verbandspolitischen Ebene wird durch entsprechende Dokumente im organisatorischen und technischen Umfeld ergänzt und ausgestaltet. Diese Dokumente werden vom VDEW erarbeitet und veröffentlicht.

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.

Die politischen, organisatorischen und technischen Aussagen in der gemeinsamen Erklärung und seinen Folgedokumenten haben Empfehlungscharakter und sollen in der Solidargemeinschaft der Marktteilnehmer eine verlässliche Vertrauensinfrastruktur ermöglichen.

Die Maßnahmen sollen als Leitlinie bei der Umsetzung im eigenen Unternehmen und der nachfolgenden Anwendung an den Marktschnittstellen dienen. Allerdings sollen gegenüber

den Verbandsempfehlungen geänderte Vorgehensweisen begründbar sein und das allgemeine Sicherheitsniveau nicht beeinträchtigen.

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

2 VEDIS - Sicherheit im Elektronischen Geschäftsverkehr

2.1 Ziele von VEDIS - Sicherheit

VEDIS sieht angesichts des Trends, Stammdaten, Zähldaten, Rechnungen oder Avise per Mail über das Internet zu übertragen, konkreten Handlungsbedarf bei der Informationssicherheit. Die Dienstgüte des Internets ist für die Anforderungen der deutschen Elektrizitätswirtschaft in den letzten Jahren ausreichend gut geworden. Die Übertragung muss nur sicher gemacht werden.

Dabei gibt es zu Public-Key-Infrastructure (PKI)-Mechanismen keine Alternative: Alles andere, wie X.400-Boxen, VPN (Virtual Private Network) oder gar symmetrische Branchenschlüssel, wären teurer und umständlicher. Das Argument, es sei bisher nicht viel Schaden entstanden, erscheint nicht akzeptabel. Einzelne Störfälle oder auch Missbrauchsfälle mögen zu verschmerzen sein. Doch wenn zunehmend elektronischer Datenaustausch über Unternehmensgrenzen hinaus automatisiert wird, also branchenweit E-Business-Charakter annimmt, müssen Sicherheitsmaßnahmen für eine weitere Digitalisierung der Geschäftsprozesse allen, am Datenaustausch beteiligten Unternehmen „den Rücken frei halten“. Eine manuelle Überprüfung findet in diesem Fall immer weniger statt. Nur so bleibt weitere Rationalisierung beherrschbar.

VEDIS setzt keine Unternehmens-PKI voraus, sondern lediglich dort, wo elektronischer Datenaustausch zwischen Marktteilnehmern abgewickelt wird, entsprechende organisatorische und technische Maßnahmen.

Regelungen bestehen z. B. bei der elektronischen Rechnung oder formgebundenen Verträgen. VEDIS möchte dort, wo keine gesetzlichen Vorgaben existieren, preiswerte technische Lösungen bei angemessener organisatorischer Sicherheit empfehlen. Bevor Daten per Electronic Data Interchange (EDI) ausgetauscht werden, empfiehlt sich der bilaterale Abschluss eines EDI-Vertrages. Mit der EU-Empfehlung 94/820/EG liegt dazu ein Muster vor. In den Vertragsanhängen können die Marktteilnehmer einfach auf die Verbandsempfehlungen verweisen. Für die Interoperabilität sind dies z.B. die Marktschnittstellen im UN/EDIFACT-Format. Für die Sicherheit sind es die VEDIS-Empfehlungen.

Technischer Bezug ist die ISIS-MTT-Norm mit einigen bewussten Erleichterungen, um eine möglichst breite Anwenderbasis zu erreichen. Die Erleichterungen (z. B. Verzicht auf deutsche Umlaute, UTF-7-Codierung) können dann, wenn normgerechtes Vorgehen und normgerechte Produkte am Markt die Regel sind, aufgehoben werden.

2.2 Ziele dieses Dokumentes

Public Key Infrastruktur (PKI) in einem Unternehmen zu begründen, einzuführen und im täglichen Betrieb zu leben, hat sich vielfach als mühsames Unterfangen herausgestellt. Viele begrüßen grundsätzlich IT-Sicherheitsmaßnahmen, doch schon die PKI-Terminologien und -Technologien schrecken ab. PKI ist eine infrastrukturelle Maßnahme - wie Telefon oder E-Mail. Eine Anwendung ist meist für einen positiven Business Case zu wenig. Erst mehrere Anwendungen rechnen sich. Ein Unternehmen muss deshalb PKI strategisch wollen und mittelfristig, d. h. über 3 Jahre, budgetieren. Dann wird sich neben dem Sicherheitsgewinn auch der wirtschaftliche Nutzen einstellen.

Das vorliegende Dokument will deutlich machen, dass es für alle Marktteilnehmer jeder Größe wirtschaftlich interessant, rechtlich opportun und technisch / organisatorisch unproblematisch ist, die im Rahmen von VEDIS empfohlenen PKI-Sicherheitsmaßnahmen von Kommunikationspartnern zu praktizieren. Viele Themenbereiche wurden in bereits vorliegenden VEDIS-Papieren adressiert. Dieses Dokument soll durch seinen Leitfadencharakter die Schritte zur „VEDIS-Sicherheit“ darstellen.

3 Zehn Schritte zur VEDIS-Sicherheit

3.1 Sicherheitsverständnis entwickeln

Wenn sich das Geschäft weiterentwickelt, muss sich auch das Verständnis weiterentwickeln, wie das Geschäft und damit auch seine effektive Abwicklung abgesichert werden kann. Dies gilt für alle Einflüsse auf das Geschäft und die Geschäftsabwicklung - gleichgültig, ob sie etwa Finanzen, Aufbauorganisation, Ablauforganisation oder Infrastruktur betreffen.

In den angesprochenen Bereichen wird immer zeitnäher auf äußere Einflüsse reagiert: Es wird schneller umorganisiert, Prozesse angepasst, Risikomanagement betrieben und Infrastrukturen den geschäftlichen Anforderungen gemäß technischem Fortschritt angepasst.

Risikomanagementüberlegungen gehen mittlerweile über den engeren Bereich des Finanzwesen und der Kapitalbeschaffung hinaus. Im Rahmen der international in Planung befindlichen, sogenannten „Basel II“-Vorgaben werden erweiterte Risikomanagementmaßnahmen bei der Unternehmensbewertung diskutiert. Diese schlagen sich bei den Mindestkapitalanforderungen der Banken an Unternehmen in den drei Säulen Kreditrisiken, Marktrisiken und operationalen Risiken nieder und sind damit deutlich flexibler, als dies in der Vergangenheit

der Fall war. Mit dem Kunstwort „operationale Risiken“ wird erstmals der Risikobegriff auf Verständnisbereiche ausgedehnt, zu denen auch die Infrastruktur gehört.

Insbesondere bei den operationalen Risiken wird der Tatsache Rechnung getragen, dass IT-Infrastrukturen zunehmend als geschäftskritisch einzustufen sind.

Auch Störungen durch Vorfälle im Bereich der IT-Sicherheit führen zu messbaren Schäden.

Wachsender Automatisierungsgrad kann zudem dazu führen, dass Missstände erst spät erkannt werden. Der Einzelfall mag dabei zu verschmerzen sein; die Summe der Fälle oder die Zeitdauer des Missstandes kann geschäftskritisch werden.

Unternehmen und Behörden begegnen diesen Problemen zunehmend mit organisatorischen Maßnahmen. Dazu gehören

- angemessene Vorgaben und ihre Überwachung („Governance“)
- Verankerung der Informationssicherheit in der Aufbauorganisation
- interne oder externe Dienste, wie Virenkompetenz, Abwehr von Eindringversuchen in die Rechnernetze
- Prävention- und Inventurmaßnahmen in sich rasch verändernden Netzen

Dazu gehört auch, dass alle Mitarbeiter und Führungsverantwortliche, auch die, die lediglich Anwender der IT-Infrastruktur sind, Verständnis für die Risiken gewinnen und Verantwortung für Prävention übernehmen („Awareness“).

Im elektronischen Datenaustausch, also in der externen Kommunikation meist über offene Netze, sollten Anwender wie IT-Verantwortliche das Grundverständnis entwickeln, dass geschäftliche Daten grundsätzlich zu schützen sind. Verschlüsselung sorgt für Vertraulichkeit; die elektronische Signatur sichert die Echtheit der Herkunft und die Unversehrtheit des Inhalts. Das VDEW-Projekt VEDIS möchte Verschlüsselung und elektronische Signatur, wie in der ISIS-MTT-Norm beschrieben, als kryptographische, zertifikatsbasierte Sicherheitsmechanismen einführen.

Das Verständnis für diese Schutzmaßnahmen kann aber nicht „von oben“ verordnet werden. Die Durchsetzung von IT-Sicherheitszielen wird auf nicht absehbare Zeit, trotz nötiger disziplinarischer Vorgaben, auch von der Mitwirkung der Mitarbeiter abhängen. Weiterhin wird IT-Sicherheit immer starke organisatorische Aspekte haben und nicht mit Technik allein zu erreichen sein. Dies gilt in besonderem Maß für die PKI mit ihren Betriebsprozessen.

Rein technikgetriebene Ansätze können deshalb hochproblematisch werden und ursprünglich gewollte Ziele konterkarieren.

Erst das Zusammenwirken von angemessenem Sicherheitsbewusstsein, sinnvoller Organisation und technischer Ausstattung ist Voraussetzung für eine erfolgreiche PKI-Einführung.

3.2 Zertifizierungsdienst definieren

Verschlüsselung und elektronische Signatur im VEDIS-Sinne wenden asymmetrische kryptographische Verfahren an. Asymmetrische Kryptographie beruht auf Schlüsselpaaren, einem öffentlichen und einem privaten Schlüssel.

Ein Zertifikat in diesem Zusammenhang bescheinigt, dass der öffentliche Schlüssel dem Schlüsselinhaber gehört. Es wird durch einen Zertifizierungsdienst ausgestellt (elektronisch signiert), der als vertrauenswürdige dritte Instanz zwischen den Kommunikationspartnern anerkannt werden muss. Ein Zertifikat muss veröffentlicht werden - zumindest in der geschlossenen Benutzergruppe, die sichere Kommunikationsverbindungen damit erreichen will. Obwohl es technisch nicht zwingend erforderlich ist, empfiehlt VEDIS getrennte Schlüsselpaare für Verschlüsselung, Authentisierung und elektronische Signatur. Dadurch kann der Verschlüsselungsschlüssel im Unternehmen vorgehalten werden, um im Bedarfsfall an verschlüsselte Daten zu kommen („Key-Backup“). Authentisierung kann auch ohne PIN-Eingabe erfolgen, während die elektronische Signatur eine persönliche Willenserklärung darstellt und dazu der Schlüssel in der alleinigen Verfügungsgewalt des Signierenden sein sollte. Zumindest sollte deshalb der Signaturschlüssel nicht zu Verschlüsselungszwecken verwendet werden.

Um im bürgerlichen Recht und im Verwaltungsrecht in vielen Fällen elektronische Signaturen den handschriftlichen Unterschriften gleichsetzen zu können, stellt das deutsche Signaturrecht hohe Anforderungen an diesen Gesamtprozess. Es wird damit die gesetzlich elektronische Form bei vielen Urkunden möglich. Anwendungsvoraussetzung ist u. a. ein sogenanntes qualifiziertes Zertifikat und eine sichere Signaturerstellungseinheit.

VEDIS empfiehlt nicht explizit qualifizierte Signaturen, wo sie nicht gesetzlich vorgeschrieben sind, lässt sie aber als höheren Sicherheitsstandard natürlich zu.

3.3 Registrierungsdienst aufbauen oder auswählen

Unter Registrierung wird die zweifelsfreie Identifizierung des Schlüsselinhabers vor dem Zertifizierungsprozess verstanden. Es ist also vor allem ein organisatorisches Thema, um Missbrauch absolut auszuschließen zu können.

Werden nur wenige Zertifikate benötigt, so kann das Standardverfahren des ZDA herangezogen werden. Das Postident-Verfahren, das für eine Reihe von Anwendungsfällen Identifizierung einer Person ohne Anwesenheit vor Ort ermöglicht, kann ebenfalls genutzt werden.

Für größere Unternehmen mit vielen im Rahmen des Verfahrens zu registrierenden Mitarbeitern ist es sinnvoll, sich eine oder mehrere lokale Registrierungsinstanzen (LRA, local registration authority) aufzubauen. Meist werden dazu die Ausweisstellen für den Mitarbeiterausweis genutzt. VEDIS verlangt, dass innerhalb dieses Prozesses eine zweifelsfreie Identifizierung erfolgt, ohne vorzuschreiben, ob dazu ein persönliches Erscheinen bei der Ausweisaushändigung oder der PIN-Zustellung erforderlich ist. Den Unternehmen soll

größtmögliche Flexibilität gewährt werden, ohne das Sicherheitsniveau durch Fehler bei möglichen Doppelvergaben oder gar durch wissentliche Missbrauchsmöglichkeiten einzuschränken.

Auch die Zertifizierungsdiensteanbieter haben mit entsprechenden Angeboten und Standardprozessen reagiert, um diesen organisatorisch wichtigen Sicherheitsschritt flexibel und damit kundenbezogen einbeziehen zu können.

3.4 Directory Service einrichten

Wird ein öffentlicher ZDA in Anspruch genommen, so stellt dieser die Zertifikate mit den öffentlichen Schlüsseln in „sein“ Verzeichnis. Dort können sie öffentlich abgefragt werden.

Dazu haben sich 3 Verfahren etabliert:

a) http-Abfrage:

Mit dem Hypertext Transfer Protocol entstand ein System von Regeln, das im World Wide Web dazu dient, auf Dokumente zuzugreifen. Http ist somit das Protokoll zur Übertragung von HTML -Seiten. In diesem Fall wird im Dialog, also nicht automatisiert, das Zertifikat im http-Modus abgefragt.

Dies kann dort sinnvoll sein, wo aus anderen Sicherheitsüberlegungen heraus nur der Port 80 in der Firewall geöffnet werden soll. Die http-Abfrage ist noch nicht überall verbreitet, stellt aber einen pragmatischen Einstieg dar, um insbesondere externe Zertifikate, z. B. für einen Verschlüsselungsvorgang, zu besorgen. Standardclientanwendungen fragen allerdings heute ausschließlich über LDAP ab. Eine Automatisierung ist deshalb über http nicht möglich.

b) LDAP-Abfrage:

Das Lightweight Directory Access Protocol (Verzeichnisdienst) ist ein TCP/IP-basiertes Directory-Zugangsprotokoll. Es gilt in internetbasierten Netzen heute als Standardlösung für Verzeichnisdienste. LDAP hat ein einheitliches Format, in dem alle Namen darstellbar sind, es bietet unterschiedliche Layouts und eine eindeutige Zuordnung zwischen Namen und ihrer internen Repräsentation. Es ist in den RFC 1777, 1778, 1779 und 1781 spezifiziert. Das Protokoll wurde 1999 durch die IETF (Internet Engineering Taskforce, www.ietf.org) standardisiert.

Die Abfrage mit LDAP kann sowohl Einzelzertifikate als auch Sperrlisten (Certificate Revocation Lists, CRL) umfassen.

Regelmäßige, dezentrale Sperrlistenerneuerung ist der häufigste Einsatzfall der LDAP-Abfrage.

c) OCSP-Abfrage

Eine Online-Abfrage über das Online Certificate Status Protokoll ist noch relativ selten, nimmt aber an Bedeutung zu. Danach wird bei der Validierung nicht auf CRL zugegriffen,

sondern über einen OCSP-Responder der Status abgefragt. Die Antwort über das Protokoll ist signiert und hat im Allgemeinen die Status gültig, ungültig oder unentscheidbar.

Ein Unternehmen, das mit der VEDIS-Umsetzung beginnen will, sollte die gültigen Zertifikate und die wahrscheinlich noch kleine Sperrliste in einem externen Verzeichnis zur Verfügung stellen. Hier bietet sich das LDAP-Zugriffsprotokoll über Port 389 an. Diese Datenbasis liegt in der demilitarisierten Zone (DMZ). Sie ist meist eine Untermenge aus dem Corporate Directory, z. B. einem Active Directory oder DIR.X (X.500), wo die eigentlichen Originaldaten geführt werden. Aus dem Corporate Directory lassen sich über Sprachmittel wie Shadowing oder Chaining diese externe Untermenge erzeugen und aktualisieren, ohne den Datenbestand an mehreren Stellen pflegen zu müssen.

Der Zugriff von außen sollte vollqualifiziert über eine vollständige, korrekte E-Mail-Adresse erfolgen müssen, um Spamming keinen Vorschub zu leisten.

3.5 Datenqualität beachten

Der Aufbau oder teilweise Aufbau einer Public Key Infrastruktur, die im Rahmen von externen Geschäftsbeziehungen zum Einsatz kommt, setzt eine hohe Datenqualität bei den wichtigsten Mitarbeiterdaten voraus. Unter „wichtigen Daten“ werden hier Daten verstanden, die logische und technische Eindeutigkeit über längere Zeiträume erreichen sollen. Dazu gehören Name, E-Mail-Adresse und eine eineindeutige Identifizierungsmöglichkeit. Dies kann eine eindeutige Personalnummer sein. Manche Unternehmen haben dazu einen 8-stelligen Global Identifier (GID) eingeführt.

In der GID garantieren 8 alphanumerische Zeichen einen Zeichenvorrat von 8^{36} Stellen (26 Großbuchstaben und 10 Ziffern) und damit langfristige Eindeutigkeit.

Idealerweise liegt die E-Mail-Adresse innerhalb der Unternehmens-Domäne und wird als „lifetime email address“ vergeben und gerade bei häufigen Namen nicht unmittelbar nach Ausscheiden des Mitarbeiters aus dem Unternehmen neu besetzt.

Die beste Datenqualität haben meist die Systeme, die die „Human Ressources“ verwalten. Diese Daten sollten nach dem „Einbahnstraßen-Prinzip“ verwendet werden und nur im HR-System durch die Personalabteilung gepflegt werden. Im Registrierungsprozess sollten also diese Daten den Nukleus bilden und durch weitere Datenquellen erweitert werden. Dieser Datensatz sollte sich auch im Verzeichnisdienst bzw. externen Verzeichnis finden.

3.6 Betriebsprozesse in einer PKI definieren

Unabhängig von MAKE oder BUY - Entscheidungen beim Marktteilnehmer sind organisatorische Regelungen für bestimmte Praxisfälle zu treffen.

Am Beispiel des wohl häufigsten Falles, nämlich der Kombination von PKI im Rahmen von multifunktionalen Mitarbeiterausweisen sollen hier einige zu behandelnde Fälle genannt werden.

- Neues Zertifikat ausstellen oder
- Defekter Ausweis

Diese Prozesse wurden beispielhaft im Anhang 4.2 als Diagramm dargestellt.

Analog können weitere Standardprozesse definiert werden:

- Neuer Mitarbeiter
- Austritt eines Mitarbeiters aus dem Unternehmen
- Namensänderung
- Übertritt eines einzelnen Mitarbeiters innerhalb des Konzerns
- Vergessen des Ausweises
- Verlust des Ausweises
- Versetzung eines einzelnen Mitarbeiters
- Hausverbot
- Auszubildende, Trainees
- Externe MA

Roll-Out

Um in bestimmten unternehmenspolitischen Situationen nicht auf Prozesse zurückgreifen zu müssen, die für einzelne Mitarbeiter konzipiert sind, können dafür separate Prozesse definiert werden. Beispiele sind die Erstausgabe oder Folgeausgabe an viele Personen.

Wenn sich das Unternehmen entschlossen hat auch Lokal Registration Authorities (LRA) oder zentrale PKI-Komponenten einzurichten, sind weitere Betriebsprozesse zu definieren. Dazu gehören etwa streng kontrollierte Zugriffsmodalitäten auf ein Schlüsselarchiv (für Verschlüsselungsschlüssel), Übernahme von HR-Daten in elektronische Beantragungen oder in ein Kartenmanagement usw.

3.7 Certification Practice Statement und Certificate Policy nach VDEW-CP erstellen

Die VDEW-Certificate Policy (VDEW-CP) definiert Branchenempfehlungen im Sinne von dringend erforderlichen Minimalvorgaben an das Sicherheitsniveau. Auf Basis dieses Dokumentes definiert ein Marktteilnehmer seine eigene CP und veröffentlicht sie als Selbsterklärung für externe Kommunikationspartner und für die Umsetzung in internen Bereichen, Mehrheitsbeteiligungen oder Landesgesellschaften. Die konkrete Umsetzung im jeweiligen Unternehmen oder Unternehmensbereich wird im Certificate Practice Statement (CPS) beschrieben. Diese Dokumente werden im Allgemeinen nicht veröffentlicht.

Die VEDIS-Empfehlungen legen großen Wert auf organisatorische Sicherheit, um bei den technischen Sicherheitskomponenten auf preiswertere Lösungen zurückgreifen zu können.

Die VEDIS-Dokumente, z.B. PKI-Policy und Umgang mit Schlüsselmaterial enthalten deshalb zahlreiche organisatorische Hinweise.

Insbesondere das Dokument „VDEW-Zertifizierungsrichtlinie (CP)“ stellt in strukturierter, nach RFC 3647 aufgebauter Form eine dringende Verbandsempfehlung zu Aufbau und prinzipiellem Inhalt dieser Aussagen dar.

Daran sollten sich die Marktteilnehmer für eigene Dokumente orientieren.

Diese firmenspezifischen Dokumentationen sollten in einer ausführlichen, internen Version der revisionssicheren Beschreibung der einzelnen Verfahrensschritte dienen. Gleichzeitig sollte eine allgemein gehaltene Untermenge der unternehmensinternen Regelungen in Form der Certificate Policy (CP) veröffentlicht werden. Dies dient als vertrauensbildende Maßnahme zwischen den Kommunikationspartnern, um korrekten Umgang mit den vereinbarten Sicherheitsmechanismen zu signalisieren.

Zudem ist es ab 1.1.2004 für Rechnungsaustausch per Electronic Data Interchange (EDI) Pflicht geworden, EDI-Verträge abzuschließen, die vertragliche Regelungen zur IT-Sicherheit enthalten müssen. Diese gesetzliche Forderung nach „Echtheit der Herkunft“ und „Unversehrtheit des Inhaltes“ kann das CP als Vertragsbestandteil beim elektronischen Rechnungsaustausch mittels der entsprechenden EDI-Nachrichtentypen ohne Mehraufwand erfüllen.

3.8 Archivierung

Mit der Einführung von PKI-Mechanismen, besonders bei der elektronischen Unterschrift, vollzieht sich ein Paradigmenwechsel. Der Beweiswert von Daten und Dokumenten wird im Rahmen von elektronischer Kommunikation verkehrsfähig und muss durch geeignete Archivierung dokumentiert und langfristig gesichert werden.

Diese Archivierung muss den Anforderungen an die Revision, an die Klärung von Streitfällen im externen Verhältnis und an die gesetzlichen Vorschriften bei einer Steuerprüfung genügen. Aussagen finden sich in den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ (BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01-) sowie im Nachgang zum Steueränderungsgesetz 2003 - ab 1.1.2004 in Kraft - im BMF-Schreiben vom 29.1.2004 in Bezug auf die elektronische Rechnung.

Diese Regelungen haben durchweg Erleichterungen für die Unternehmen gebracht, weil Ergebnisdokumentation und Verfahrensdokumentation den neuen technischen Möglichkeiten angepasst werden können. Allerdings hat die GDPdU das Prinzip „Gleiche Augenhöhe“ für die prüfende Finanzbehörde eingeführt und das letztgenannte BMF-Schreiben zielt in seinen Regelungen gegen Missbrauchsmöglichkeiten insbesondere beim Vorsteuerabzug.

Die Integrität der Daten und die Signaturberechtigung muss geprüft und das Prüfergebnis muss dokumentiert werden. Weiterhin muss der Signaturprüfschlüssel aufbewahrt werden. Damit sind die signierten Nettodaten, das Validierungsergebnis und das Zertifikat so zu

archivieren, dass diese Daten im Falle einer Steuerprüfung „unverzüglich“ zusammengeführt werden können.

Weitere Anforderungen, etwa die Aufbewahrung von unkonvertierten und konvertierten EDI-Daten und Protokollierungen bleiben davon unberührt.

3.9 VEDIS-Sicherheit im elektronischen Datenaustausch

a) Vertragliche Grundlage

Falls noch nicht geschehen, sollte zwischen den Kommunikationspartnern ein EDI-Vertrag geschlossen werden. Dieser Vertrag nach Artikel 2 der Empfehlung 94/820/EG der Kommission vom 19. Oktober 1994 kann von den Webseiten der Europäischen Union bezogen werden und um die Unternehmensspezifika, wie Name, Adresse etc. ergänzt werden. Grundlage dieser dringenden Empfehlung ist die rechtliche Tatsache, dass ein solcher Vertrag nach §14 Abs. 3 Umsatzsteuergesetz für rechnungsrelevanten Datenaustausch gefordert wird. Da nicht nur Netznutzungsrechnung (INVOIC) und Zahlungsavis (REMADV), sondern auch Zähldaten (MSCONS) und Stammdatenwechsel (UTILMD) wichtige geschäftliche Transaktionen im liberalisierten Energiemarkt darstellen, sollte auch in diesen Fällen eine korrekte Vertragsgrundlage bestehen.

Anlage 1 dieses Vertrages ist der Verweis auf die Marktschnittstellen und ggf. ihre Umsetzung (z. B. Syntaxversion).

Anlage 2 ist der Verweis auf die VEDIS-Dokumente bzw. ihre individuelle Umsetzung, dokumentiert im CP des Unternehmens.

Damit lässt sich ohne großen Aufwand der gesetzlichen Forderung nach vertraglicher Grundlage mit Vereinbarungen zur Gewährleistung der „Echtheit der Herkunft“ und „Unversehrtheit des Inhaltes“ nachkommen.

b) E-Mail-Sicherheit

Das VDEW-Projekt VEDIS wurde initiiert, weil zunehmend elektronischer Datenaustausch über das Internet, speziell über E-Mail (SMTP), abgewickelt wird. Der sogenannte Mail-Body hat nur untergeordnete Bedeutung. Die entscheidenden Informationen werden vor allem in Dateianhängen transportiert. Damit kann die E-Mail-Ebene als Transportebene angesehen werden und die Datei als Informationsebene.

Die E-Mail-Transportebene kann, angelehnt an die Vorgehensweise bei der European Bridge-CA, EB-CA, initialisiert und getestet werden

Siehe dazu: http://www.bridge-ca.de/architektur/pdf/bridgeca_smime_interop.pdf

c) Nutzdatensicherheit

VEDIS möchte zunächst auf E-Mail-Ebene mit zertifikatsbasierten PKI-Mechanismen die Sicherheit im elektronischen Datenaustausch verbessern. Wird nur auf dieser Ebene PKI angewendet, dann sollte verschlüsselt und signiert werden.

Dies ist unabhängig davon, ob eine E-Mail-Gatewaylösung (oft als „virtuelle Poststelle“ bezeichnet) eingesetzt wird oder nicht. Die Empfehlungen gelten allgemein für „Site-to-Site-Sicherheit“, „End-to-End-Sicherheit“ oder Mischformen. Es ist ein pragmatischer Weg, der mit minimalem Aufwand für alle Marktteilnehmer gehbar ist.

Neben Verschlüsselung und Signatur auf E-Mail-Ebene sollte auch das Mittel der Datei-Signatur unterstützt werden. Die S/MIME-Norm hat zwar einige Restriktionen, ist aber schnell, pragmatisch und preiswert einsetzbar und garantiert ein angemessenes Sicherheitsniveau. Diese Einschränkungen sollte man sich aber bewusst machen:

- Bei S/MIME ist Unterzeichner gleich Versender.
- S/MIME unterstützt deshalb auch keine Mehrfach-Signaturen, wie sie z. B. in Geschäftsbriefen nötig sind oder in anderen Anwendungsbereichen mit Mehrfachverantwortung. Auch ein „Durchreichen“ von Daten ohne Verantwortungsnahme kann damit nur schwer ohne sprechende Erläuterung abgebildet werden.
- S/MIME packt Text und Attachment in einen "verplombten" Container. Archivierung und Retrieval inkl. Volltextsuche wird dadurch problematisch.

Aus diesen Gründen und den damit verbundenen wirtschaftlichen Konsequenzen sollte auch die Signatur auf Dateiebene angewendet werden.

Ist diese Stufe erreicht, so genügt es auch, auf E-Mail-Ebene (S/MIME) nur zu verschlüsseln und auf Dateiebene zu signieren.

3.10 Weitere Anwendungsfelder und Anwender

Als Anwendungsfelder für zertifikatsbasierte Sicherheitsmaßnahmen wurden bisher lediglich Mail-Verschlüsselung und -Signatur sowie Dokumenten- bzw. Datei-Signatur angesprochen.

Anwendungen sind im ersten Schritt der Datenaustausch zwischen Marktteilnehmern im liberalisierten Strommarkt. Die VEDIS-Empfehlungen können ausgedehnt werden.

Weitere Anwendungen können sein

- File-Verschlüsselung
- Aufbau von Virtual-Private-Networks (VPN)
- Web-Authentication
- Sichere WWW-Kommunikation

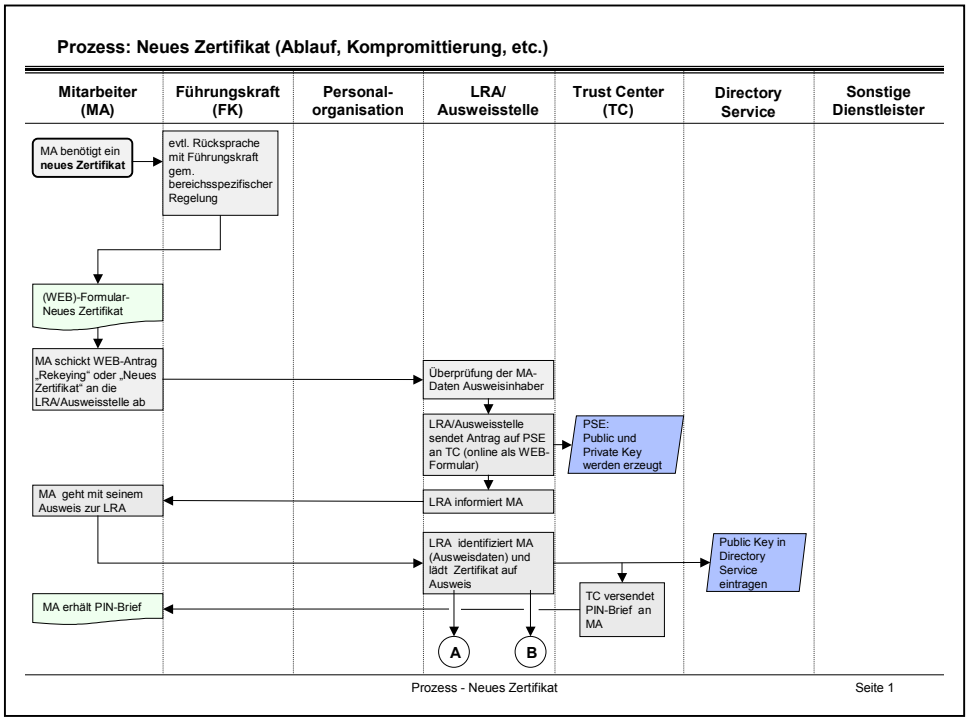
Weitere Anwendungen liegen im Bereich der sicheren Kommunikation mit Geschäftskunden, Behörden oder Lieferanten und Dienstleistern.

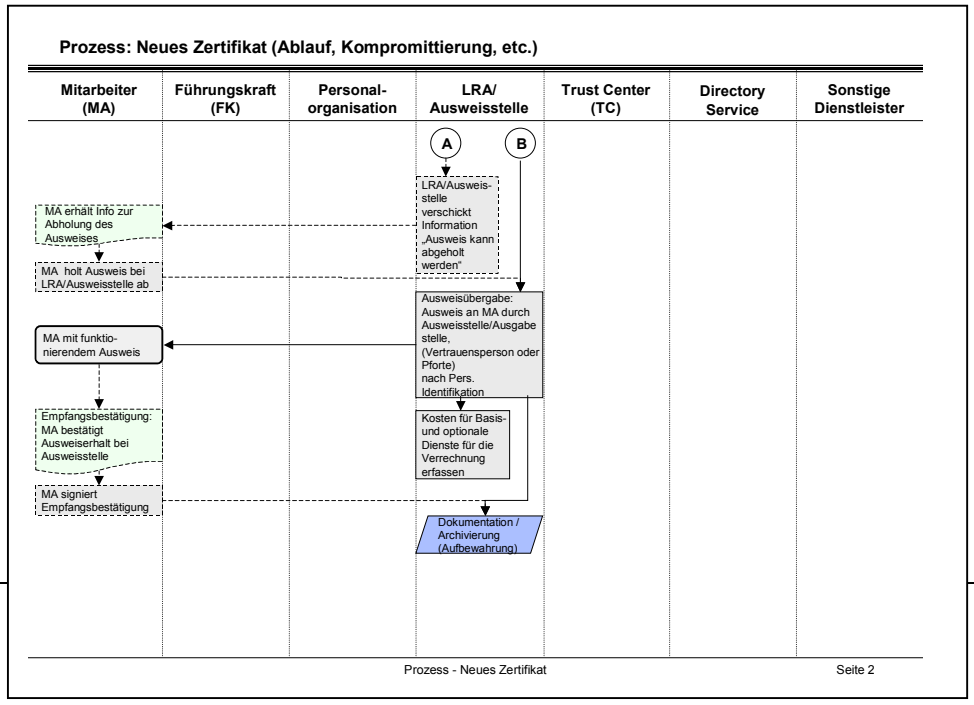
4 Anhang

4.1 Diagramme

4.1.1 Beispiel PKI-spezifischer Prozess beim Mitarbeiterausweis:

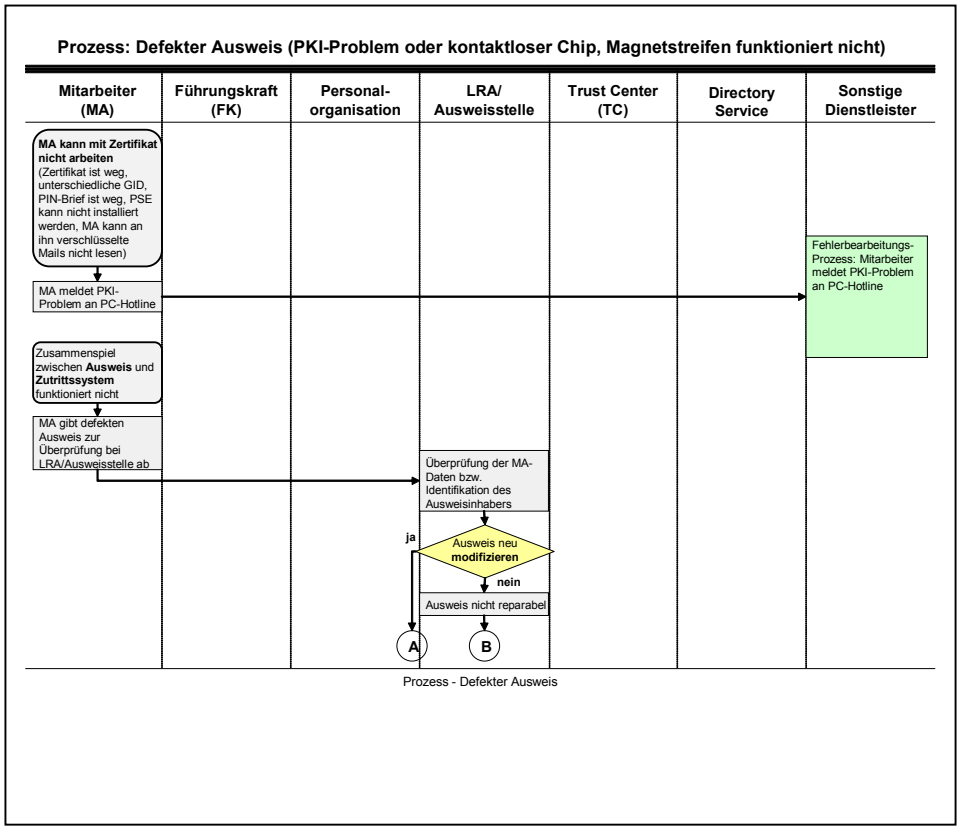
Neues Zertifikat ausstellen

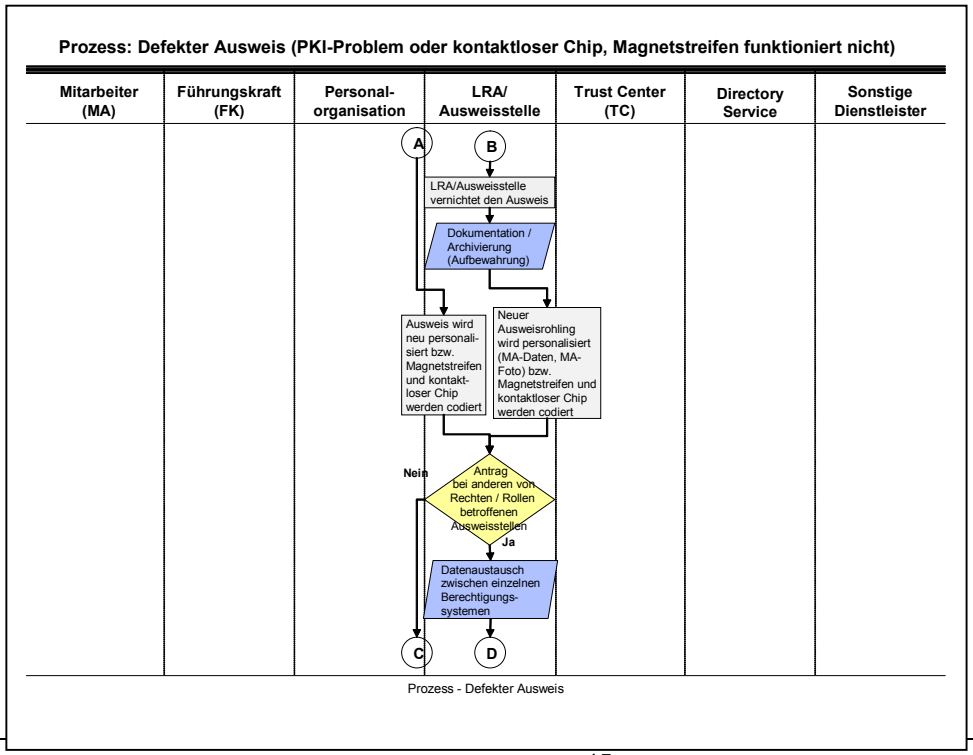




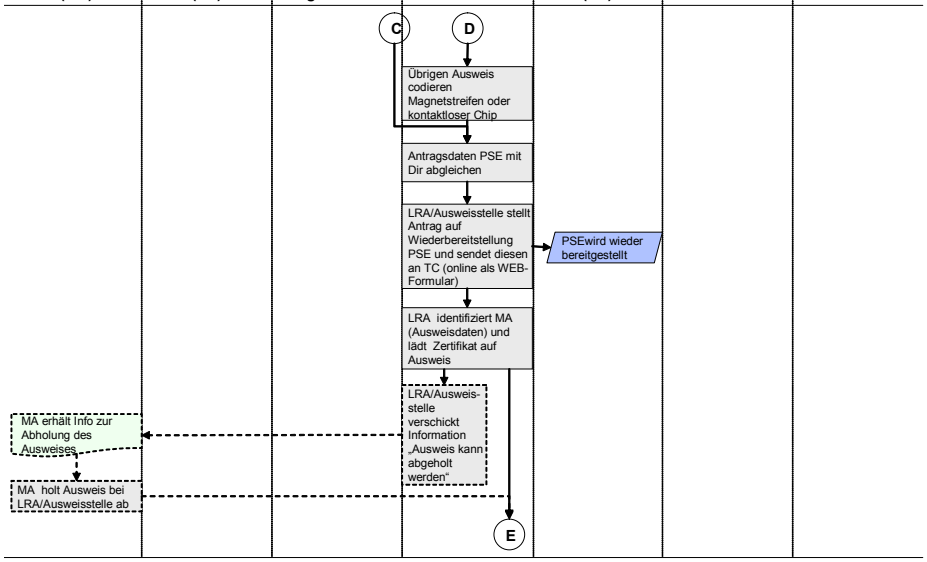
4.1.2 Beispiel allgemeine Funktionen des Mitarbeiterausweises

Defekter Ausweis



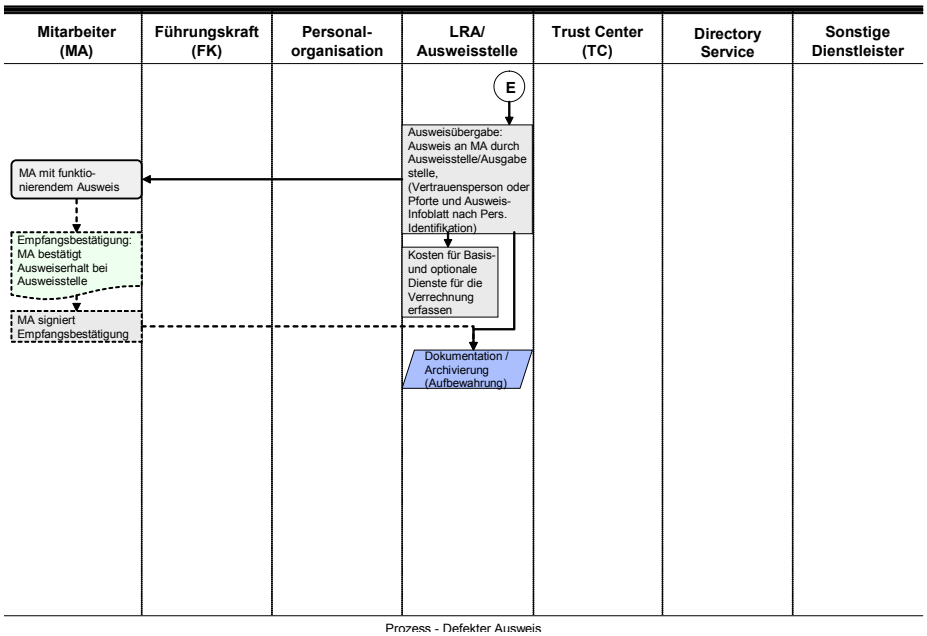


Prozess: Defekter Ausweis (PKI-Problem oder kontaktloser Chip, Magnetstreifen funktioniert nicht)



Prozess - Defekter Ausweis

Prozess: Defekter Ausweis (PKI-Problem oder kontaktloser Chip, Magnetstreifen funktioniert nicht)



Prozess - Defekter Ausweis

4.2 Praxisbeispiele

4.2.1 Beispiel von RWE

Papierlose Rechnung ist Realität

e-Invoicing heißt das Zauberwort, mit dem der RWE-Konzern den Abrechnungsverkehr mit Lieferanten vollständig papierlos abwickeln kann. RWE Systems hat deutschlandweit die Vorreiterrolle.

Gemeinsam mit zwei Partnern ist es der Kreditorenrechnung von RWE Systems erstmals in Deutschland gelungen, die gesamte Prozesskette elektronisch zu organisieren: von der Rechnungserstellung über den -versand bis hin zur Abwicklung in den eigenen Buchhaltungssystemen - authentifizierte elektronische Signatur inklusive.

Das Verfahren funktioniert bereits in der Praxis: Lufthansa Airplus als Pilot-Lieferant stellt RWE seine Leistungen seit Ende Oktober 2003 nur noch elektronisch in Rechnung. Papierrechnungen sind vollständig überflüssig geworden.

Bisher scheiterten die Ansätze zur papierlosen Rechnung an hohen gesetzlichen Anforderungen. Die Echtheit der Rechnungen muss archivfest so sicher dokumentiert werden, dass beim Finanzamt das Recht auf Vorsteuerabzug nicht gefährdet wird. Das ist jetzt erstmals gewährleistet.

Die Vorteile des neuen Systems: Der Rechnungssteller spart Druck- und Portokosten. Der Empfänger muss keine Papierrechnungen mehr scannen und spart neben den Kosten auch noch Zeit. Fehler durch händisches Übertragen von Stamm- und Rechnungsdaten in die elektronischen Systeme entfallen.

Neue Teilnehmer können als Lieferant oder auch als Rechnungsempfänger problemlos dazustoßen: Es sind keinerlei Investitionen in neue Hard- oder Software erforderlich.

Autor: Jürgen Grönke, Dezember 2003, (c) RWE Systems

4.3 Quellen

Common ISIS-MTT Spezifikation for PKI Applications from T7 & TeleTrusT, V1.1,

- http://www.teletrust.de/Dokumente/ISIS-MTT_Core_Specification_v1.1.pdf, 2004-03-16
- ISIS-MTT Testbed Prototype 1.1 (build 5 SP 1, 2003-08-13)

  (Als CD beziehbar von TeleTrusT e.V. Chamissostrasse 11. D-99096 Erfurt)
- ISIS-MTT: Profile for Authentication Certificates, V 1.0, 2004-11-02, in Veröffentlichung

VDEW-Veröffentlichungen

- 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