VDEW

MATERIALIEN

M-06/2004

Aktionsplan WETTBEWERB

Häufig gestellte Fragen - FAQ zu VEDIS
(Version 2.0 - Stand: 03.05.2004)

V D E W

Häufig gestellte Fragen – FAQ zu VEDIS

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat die folgenden Dokumente im letzten Jahr veröffentlicht:

M-14/2003 „Sicherheitspolitik“
M-15/2003 „Technische PKI – Interoperabilität“
M-16/2003 „Umsetzungsempfehlungen“
M-17/2003 „Umgang mit Schlüsselmaterial“
M-18/2003 „Zertifizierungsrichtlinie“

Die Fragen, die aus den Mitgliedsunternehmen aufgrund der Dokumente sowie beim VDEW-Infotag „Elektronischer Datenaustausch – aber sicher!“ häufig gestellt wurden, hat die Projektgruppe zusammengefasst und in diesen Dokumenten beantwortet.

Diese VDEW-Materialien werden stetig weiterentwickelt.

Verband der Elektrizitätswirtschaft – VDEW – e.V.,
Stresemannallee 23, 60596 Frankfurt am Main,
Telefon 069/6304-302

Häufig gestellte Fragen zu VEDIS

Version 2.0

Stand: 3. Mai 2004

Was bedeutet VEDIS?

VEDIS ist das Akronym für Verbindlichkeit und **S**icherheit im **E**lectronic **D**ata **I**nterchange (EDI).

Das „**V**“ kann auch für **V**erschlüsselung und das „**S**“ für (elektronische) **S**ignatur gedeutet werden. Das Projekt VEDIS wurde beim VDEW gegründet. Die Verbandsarbeit leistet die Projektgruppe „Sicherheit beim elektronischen Datenaustausch". VEDIS möchte in den veröffentlichten Dokumenten wirtschaftlich sinnvolle Empfehlungen zu Sicherheitsmaßnahmen geben.

Was bedeutet liberalisierter Strommarkt für den Kommunikationsbedarf?

Die Liberalisierung des deutschen Strommarktes führte automatisch zur Forderung nach einer wirtschaftlich und technisch ausgewogenen Gesamtbilanz im Datenhaushalt der betroffenen Unternehmen. Diese lässt sich nur durch intensiven Datenverkehr zwischen Händlern, Lieferanten, Verteilnetzbetreibern, Übertragungsnetzbetreibern, ‚Bilanzkreisverantwortlichen und den Stromerzeugern erreichen.

Der VDEW schätzt das dazu nötige Nachrichtenvolumen für die wichtigsten, am leichtesten automatisierbaren Transaktionen auf 2,5 Milliarden pro Jahr.

Neben der notwendigen brancheninternen Kommunikation zwischen den Marktteilnehmern unterschiedlicher Rollen sind aber, wie in anderen Branchen auch, eine Fülle von elektronisch abwickelbaren Geschäftsbeziehungen zu Lieferanten, Dienstleistern und nicht zuletzt Kunden entstanden. Auch die in der Energiewirtschaft besonders wichtigen Behördenkontakte sind interessante, digitalisierbare Prozesse.

Mit der Definition von sogenannten „Marktschnittstellen“ auf Basis von UN/EDIFACT- oder auch XML-Sprachmitteln wurde dem standardisierten Kommunikationsbedürfnis im Markt Rechnung getragen.

Da die Kommunikation vielfach über ungesicherte Netze, vor allem auch das Internet, stattfindet, ist es nötig, angemessene, praktikable und interoperable Sicherheitsrahmenbedingungen zu vereinbaren.

Warum mehr Sicherheit beim elektronischen Datenaustausch ?

IT ist schon längst zur kritischen Infrastruktur in praktisch jedem modernen Unternehmen geworden. Im liberalisierten Strommarkt mit seinen Geschäftsprozessen über Firmengrenzen hinaus wird nicht nur die unternehmensinterne Datenverarbeitung, sondern auch der externe Datenaustausch zunehmend wichtiger.

Die Forderung nach mehr Sicherheit kommt einerseits aus gesetzlichen Rahmenbedingungen. Z. B. impliziert das Datenschutzgesetz, dass beim Lieferantenwechsel die personenbezogenen Daten der Kunden gegen widerrechtliches Lesen oder gar missbräuchliches Verändern geschützt werden müssen. Werden diese Daten elektronisch ausgetauscht, kann nur ihre Verschlüsselung diese gesetzliche Anforderung praktikabel abdecken.

Andererseits stellt die Anforderung an Risikominimierung in der normalen, aber zunehmend digitalisierten Geschäftspraxis neue Sicherheitsanforderungen. Die prinzipiellen Grundanforderungen an das geschäftliche Handeln haben sich dabei aber auch in den Zeiten wachsenden Einsatzes von Informations- und Kommunikationstechnologie nicht geändert und sind nicht im geringsten branchentypisch:

- Man möchte sich auf die Inhalte verlassen können.
- Man möchte sicher sein, dass der Absender stimmt.
- Man möchte sicher sein, dass der Absender zu der Geschäftstransaktion „steht“ bzw. dass eine Veränderung „unterwegs“ nicht möglich ist.
- Man möchte sicher sein, dass die Inhalte vertraulich bleiben.

Integrität, Authentizität, Verbindlichkeit und Vertraulichkeit bleiben also unverändert Grundanforderungen an geschäftliche Transaktionen. Ihre Wahrung bekommt aber beim elektronischen Datenaustausch oder gar Massendatenaustausch einen veränderten Stellenwert, weil der Austausch zunehmend automatisiert wird und deshalb auch automatisch kontrolliert werden muss. Dies gilt für die Informationsgesellschaft generell und für den liberalisierten Energiemarkt im Besonderen.

Der liberalisierte Markt bildete also den Anlass für die notwendige Abstimmung im Rahmen der Verbandsarbeit. Die dabei entstehenden Empfehlungen sollten der vielseitig nutzbare Sicherheitsinfrastrukturen initiieren und damit Investitionen schützen.

Warum macht Sicherheit im Strommarkt Geschäftstransaktionen häufig erst möglich ?

Manche Sicherheitsmaßnahmen, wie Gewährleistung der „Echtheit der Herkunft“ und „Unversehrtheit des Inhaltes“, sind Voraussetzungen für die automatisierte Abwicklung von Transaktionen in elektronischer Form vor allem über das Internet. Hier macht Sicherheit beim verstärkten Einsatz von Informationstechnik Geschäftstransaktionen häufig erst möglich.

Erst wenn sich die Unternehmen durch solche Sicherheitsmaßnahmen „den Rücken frei halten“, bleibt zunehmende Automatisierung und Vernetzung beherrschbar.

Bei der elektronischen Rechnung ohne Papierbegleitdokumente (hier Netznutzungsrechnung) verlangt der Gesetzgeber qualifizierte Signaturen.

Im Strommarkt, außer bei der gesetzlich regulierten Rechnung, können einfache Sicherheitsmechanismen vereinbart werden. Hier genügen im allgemeinen fortgeschrittene Signaturen.

Was hat der Verband zur „Sicherheit beim elektronischen Datenaustausch“ getan ?

Im Unterschied zu vielen Bereichen der Kommunikationstechnologie ist Sicherheit und Verbindlichkeit nicht allein durch technische Interoperabilität gekennzeichnet. Vertrauen entsteht erst durch eine Kombination aus sicherer Technologie und sicheren organisatorischen Prozessen.

Das dazu nötige Sicherheitsbewusstsein kann nur in einer gemeinsamen Anstrengung erreicht werden.

Was soll die „Gemeinsame Erklärung“ bezwecken?

In Abstimmung mit den Verbänden, die die aktuelle Verbändevereinbarung zum liberalisierten Strommarkt (VV II plus) mittragen, wurde eine „Gemeinsame Erklärung“ verabschiedet. Dieses politische Dokument, das von sechs Verbänden getragen wird, wird durch Folgedokumente unter der Moderation des VDEW ausgestaltet.

Es hat das Ziel, das Sicherheitsniveau beim elektronischen Datenaustausch auf der technischen und organisatorischen Ebene nachhaltig zu heben. Diese Gemeinsame Erklärung mit Empfehlungscharakter ist bewusst allgemein gehalten und soll mittelfristig Bestand haben. Sie wird als politische Willenserklärung verstanden, geeignete Maßnahmen

zu ergreifen, um technisch und organisatorisch die elektronische Kommunikation zu schützen bzw. im weiteren Ausbau zu ermöglichen.

Folgende Ziele sollen indirekt über die Gemeinsame Erklärung gefördert werden:

- Die heutigen elektronisch abgewickelten Geschäftsbeziehungen sollen besser geschützt werden.
- Die weitere Ausdehnung elektronischer Geschäftsabwicklung soll durch mehr Sicherheit und damit Vertrauen ermöglicht werden.
- Durch optimierte Prozesse soll Rationalisierungspotential (z. B. Wegfall handschriftlicher Unterschriften) erschlossen werden.
- Die erwartete deutlich steigende Nutzung von elektronischer Kommunikation im Geschäftsverkehr zwischen Marktteilnehmern, aber auch mit
  - staatlichen Instanzen („E-Government“),
  - Kunden („E-Commerce“) und
  - Zulieferern („E-Procurement“)

  soll bzgl. Risiken, Volumina und Technik beherrschbar bleiben.

Was soll mit der PKI-Policy erreicht werden?

Die „PKI-Policy“ ist eine Empfehlung zur generellen Sicherheitspolitik bei einer PKI-Einführung. Sie richtet sich an Unternehmen, die eine eigene PKI oder Teildienste aufbauen möchten. Diese Policy beschreibt Terminologie, Dienste und Prozesse, wie sie im PKI-Umfeld üblich sind und auch beim Aufbau einer eigenen PKI durch einen Marktteilnehmer als Leitlinie berücksichtigt werden sollten. Damit soll das adäquate organisatorische Sicherheitsniveau gewährleistet werden, das als Vertrauensgrundlage für sichere Kommunikationsbeziehungen nötig ist. Auch wer lediglich ausgewählte Dienste selbst aufbauen will (z. B. wer den Registrierungsdienst im eigenen Haus installieren, aber den Zertifizierungsdienst bei einem öffentlichen Trustcenter in Anspruch nehmen möchte) sollte sich an die entsprechenden Teile der PKI-Policy halten.

Technische Bedeutung von VEDIS?

VEDIS möchte technische Sicherheitsrahmenbedingungen in der Branche schaffen, in der sicher und interoperabel Daten ausgetauscht werden können.

VEDIS möchte aber auch technischen „Wildwuchs“ verhindern. Unterschiedliche Verfahren verteuern und komplizieren jedoch den elektronischen Datenaustausch unnötig.

Welche VEDIS-Dokumente muss wer lesen?

Grundlektüre sollten die Dokumente „Umgang mit Schlüsselmaterial“ und „Umsetzungsempfehlungen“ sein. „Umgang mit Schlüsselmaterial“ richtet sich dabei auch an Endanwender und Vorgesetzte.

Hauptdifferenzierungspunkt für die Erstellung der Dokumente war

- MAKE – eigene PKI aufbauen und
- BUY – Zertifikate von einem Zertifizierungsdienstleister (ZDA) einkaufen.

Die Hauptarbeit bei VEDIS war, durch entsprechende Regelungen sicherzustellen, dass beim Aufbau einer PKI das organisatorische und technische Sicherheitsniveau eine so angemessene Sicherheitsstufe erreicht, dass dieser Marktteilnehmer am VEDIS-Verfahren ohne Sicherheitseinbußen für die Anderen teilnehmen kann.

Wer eine eigene PKI ganz oder teilweise aufbaut, sollte die Dokumente "PKI-Policy" und "Technische PKI-Interoperabilität" lesen. Deutsche ZDA erfüllen die organisatorischen Kriterien der PKI-Policy und die technischen Interoperabilitäts-Kriterien. Ausländische ZDA, von denen ein Marktteilnehmer Zertifikate beziehen möchte, sollten diesem die Einhaltung der Kriterien schriftlich bestätigen.

Bestandteil des Vertrages zwischen Energieversorgungsunternehmen und ZDA sollte die „Zertifizierungsrichtlinie“ (Certification Practice Statement, CPS) sein, die je nach Eigenanteil an der PKI ergänzt werden sollte. Das CPS ist also noch kein „fertiges“ Dokument, sondern muss an einigen Stellen um Firmenspezifika ergänzt werden.

Was benötigt ein Marktteilnehmer für die Teilnahme am VEDIS-Verfahren?

1) Kompatibilitätskriterium

   Ein Marktteilnehmer benötigt unabhängig von Sicherheitsanforderungen die zu übermittelnden Daten im richtigen Format (EDIFACT, XML, CSV)

2) Publikationskriterium

   Das Zertifikat mit dem öffentlichen Schlüssel des Kommunikationspartners zur Verschlüsselung vor der Kommunikation, um die Datei (bei Dateiverschlüsselung) oder das E-Mail (per S/MIME) damit verschlüsseln zu können.

   Das Zertifikat mit dem öffentlichen Schlüssel des Kommunikationspartners zur elektronischen Signatur nach der Kommunikation, um die Signatur überprüfen zu können (siehe auch Zertifikate veröffentlichen).

   Entsprechende eigene Schlüssel, mindestens getrennt für Verschlüsselung und elektronische Signatur/Authentisierung, und ihre unzweifelhafte Zuordnung zu einer natürlichen Person in Form eines Zertifikates. Diese sind innerhalb der VEDIS-Anwendergruppe öffentlich zu machen.

3) Eine Verifikationssoftware zur Überprüfung der Signatur. Das Prüfergebnis sollte dokumentiert werden.

4) Eine Ver- bzw. Entschlüsselungssoftware (3 und 4 sind in der Regel ein Software-Standardprodukt)

Was soll das VDEW-Dokument PKI-Policy leisten?

Die PKI-Policy ist eine Leitfaden für Marktteilnehmer, die eine eigene PKI ganz oder teilweise aufbauen möchten. Teilweiser Aufbau bezieht sich oft darauf, dass die Registrierung im eigenen Haus durchgeführt wird (PKI-Dienst Registration Authority), während die Zertifizierung, also Zertifikatsausstellung, durch einen Zertifizierungsdienstleister (ZDA) erfolgt.

Die PKI-Policy ist aber auch ein Leitfaden für die Auswahl eines ZDA. Deutsche ZDA, die sich einem freiwilligen Akkreditierungsverfahren bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) unterzogen haben, genügen den Ansprüchen der VDEW-PKI-Policy. Eher unbekanntere ZDA aus dem europäischen oder gar nicht-europäischen Ausland sollten die prinzipielle Einhaltung des Sicherheitsniveaus bestätigen.

Eine firmenübergreifende PKI ist immer eine Gruppe von Certification Authorities (CA) und ihren Diensten, die einer gemeinsamen PKI-Sicherheitspolitik unterliegen. In den VEDIS-Dokumenten wird keine hierarchische Struktur in Form einer Policy-CA (PCA) gefordert, welche die Grundregeln definiert und deren Einhaltung bei den tiefer liegenden CAs überprüft. Allerdings soll die PKI-Policy in einer nicht-hierarchischen Struktur ein gemeinsames Sicherheitsverständnis prägen. Dies wird über die sogenannte Zertifizierungsrichtlinie (Certification Practice Statement, CPS) der einzelnen CAs kontrolliert, in denen die genauen Zertifizierungsabläufe dokumentiert sind (siehe FAQ zum VDEW-Dokument „Zertifizierungsrichtlinie“).

Was soll das Dokument „Technische PKI-Interoperabilität“ leisten?

PKI-Funktionalität ist noch nicht automatisch interoperabel. Das Dokument orientiert sich am Standard PKIX und nicht an weiteren Spielarten wie PGP oder PEM.

Der PKIX-Standard ist sehr mächtig und wird nur in Einzelfällen benötigt. Es war nötig, die Interpretation des Standards zu strukturieren, so dass er interoperabel implementiert werden kann. Dies leistet das anerkannte Profil ISIS-MTT. ISIS-MTT wird als Benchmark für Produkte empfohlen. Wer eine eigene PKI aufbauen möchte, sollte im Zertifikat wenigstens die in diesem Dokument genannten Felder unterstützen. Es wurde das Prinzip „so wenig wie möglich, soviel wie nötig“ angewendet. Besonderer Schwerpunkt wurde auf den Ansatz gelegt, normgerechtes Vorgehen und Industriestandards miteinander zu verbinden.

Was soll das Dokument „Umgang mit Schlüsselmaterial“ leisten?

Der organisatorisch sorgfältige Umgang mit Schlüsselmaterial durch Endanwender und seine Überwachung durch Vorgesetzte soll ein sensibles und bewusstes Sicherheitsempfinden bei allen Anwendern erzeugen. Das Unternehmen sollte für die Einhaltung sorgen, so dass sich die Marktteilnehmer/Kommunikationspartner darauf verlassen können. Besonders sollten die privaten Schlüssel geschützt werden und im Fall einer Korrumpierung zeitnah gesperrt werden sowie die Sperre kommuniziert werden.

Das Dokument „Umgang mit Schlüsselmaterial“ stellt somit einen Vorschlag zur unternehmensinternen Regelung des Umgangs mit kryptographischem Schlüsselmaterial dar. Es richtet sich besonders an Marktteilnehmer, die externe Zertifizierungsdienstleister in Anspruch nehmen. Gerade um den hohen Anteil an organisatorischer Sicherheit zu gewährleisten, wird empfohlen, dieses Dokument sinngemäß in jedem Unternehmen

anzuwenden, so dass deutlich wird, dass unsachgemäßer Umgang mit kryptographischen Schlüsseln und ihrem Trägermaterial in der Unternehmenskultur nicht toleriert wird.

Was soll das Dokument „Umsetzungsempfehlungen“ leisten und was NICHT?

Das Dokument spricht besonders Themenfelder an, die Kriterien für die Umsetzung von Sicherheitsrahmenbedingungen im jeweiligen Unternehmen, im Markt und im rechtlichen Kontext sind. Es wird nach sehr kurzfristig wünschenswerten und mittelfristig sinnvollen Maßnahmen unterschieden. Der erste Schritt, nämlich nicht mehr ohne Verschlüsselung und elektronische Signatur zwischen Marktteilnehmern Geschäftsdaten auszutauschen, wird dabei dringend empfohlen.

Die „Umsetzungsempfehlungen“ sollen einen ersten Leitfaden für die praktische Umsetzung in ihrem betriebswirtschaftlichen Kontext bereitstellen. Es sollen im ersten Umsetzungsschritt die Anforderungen an eine ”Site-to-Site”-Security gewährleistet werden können, d. h. die **Verbindung zwischen korrespondierenden Firmen bzw. Abteilungen** soll abgesichert werden. Dies setzt keine zusätzliche Hard- und kaum Software auf Mitarbeiter- bzw. Arbeitsplatzebene voraus. Es ist ein erster Schritt, der allen zugemutet werden kann und dessen Einführung deshalb kurzfristig empfohlen wird. Für diese Vorgehensweise hat sich der Begriff “Virtuelle Poststelle” eingebürgert. Betroffen sind besonders die Prozesse zum Austausch von

- Stammdaten
- Zählwerten
- Netznutzungsrechnungen

Mittelfristig sollten dann da, wo es aus geschäftlicher Sicht sinnvoll ist, die Absicherung von betroffenem **Mitarbeiterarbeitsplatz zu betroffenem Mitarbeiterarbeitsplatz** erfolgen. In diesem Umsetzungsschritt ist nicht mehr nur der EDI – Austausch, sondern der Austausch von besonders sensiblen Dokumenten (z. B. Verträge, Genehmigungsverfahren und anderer Datenaustausch mit Behörden) im Fokus. Erst dies setzt eine kryptographische Infrastruktur bzw. Content-Security-Infrastruktur an den betroffenen Mitarbeiterarbeitsplätzen voraus. Aber auch diese Maßnahme bedeutet nicht, dass flächendeckend im Unternehmen eine Public Key Infrastruktur erforderlich wird.

Der Kerntext der Umsetzungsempfehlungen enthält weder Hinweise auf Hersteller noch Produkte. Erst in den Anhängen werden Produkthinweise gegeben bzw. hatten Hersteller Gelegenheit zu einer Selbstdarstellung ihrer Kompetenzen in diesem Bereich. Diese Anhänge haben weder den Anspruch auf Vollständigkeit noch wurden Produkte getestet.

Was soll die „Zertifizierungsrichtlinie“ (Certification Practice Statement, CPS) leisten?

Das CPS ist in einer PKI das wichtigste Dokument, wenn es um die Einschätzung des Sicherheitsniveaus geht. Innerhalb eines Unternehmens dokumentiert man im CPS konkrete Aufgaben und Rollen der an den PKI-Diensten beteiligten Instanzen und Personen und besonders auch das Verhalten in Grenz- und Konfliktfällen.

Aus diesem Grund dient das CPS vielfach bei bilateralen oder multilateralen PKI-Beziehungen als Vertragsgrundlage. Der Aufbau eines CPS ist normiert, sodass es als Checkliste für eine vollständige Beantwortung aller relevanten Fragen dienen kann.

Das vorliegende Dokument hat bereits Vorschläge für Themenkomplexe gemacht, die allgemein behandelt werden können. Weiterhin enthält es die Überschriften von Punkten, die firmenspezifisch beantwortet werden sollten.

Die Zertifizierungsrichtlinie, wurde also als Vorlage zur weiteren und konkreten Ausgestaltung in den Unternehmen gestaltet. Die Zertifizierungsrichtlinien stellen vielfach die eigentlichen Vertragsgrundlagen bei sicherheitskritischen Kommunikationsbeziehungen dar. Die VDEW-„Vorlage“ ist dazu angelegt, die bereits ausformulierten allgemeinen Teile einer bilateralen EDI-Vertragsbeziehung zugrunde zu legen und um unternehmensspezifische Aussagen zu ergänzen.

Sieht VEDIS zwingend den Einsatz von SmartCards vor?

VEDIS gibt lediglich Empfehlungen, wie ein „Personel Security Environment“ (PSE), d.h. die Speicherung des „kryptographischen Materials“, den allseits erwünschten Sicherheitsbedingungen und damit dem Vertrauen in die elektronische Kommunikation über Firmengrenzen hinweg genügen kann. Aus wirtschaftlichen Gründen reicht grundsätzlich nach diesen Sicherheitsvorgaben die Nutzung einer auf Software basierenden PSE (mit einem Passwort/PIN zugriffsgeschützte Datei) aus. Die Nutzung einer SmartCard und die damit einhergehende Steigerung der Sicherheit, aber auch Erhöhung der Einrichtungs- und Betriebskosten, ist dem Marktteilnehmer freigestellt.

Einzelplatzlösung oder virtuelle Poststelle?

Im ersten Schritt sollten alle teilnehmenden Unternehmen mindestens den elektronischen Datenverkehr zwischen den Unternehmen, also über offene Netze wie das Internet, absichern.

Bei der Entscheidungsfindung sollten die kurz- und langfristigen Ziele mit den jeweiligen Lösungen verglichen werden. Eine virtuelle Poststelle kann i. d. R. nur für die Absicherung des E-Mail Verkehrs verwendet werden, eine Ende-zu-Ende Lösung bietet zusätzliche Möglichkeiten (HTTPS, Signatur auf Mitarbeiterebene,…)

Verzeichnisdienst

VEDIS ist aus den Anforderungen des Datenaustauschs im liberalisierten Markt entstanden. Das VEDIS-Prinzip kann und soll aber auch für weitere abzusichernde Geschäftsbeziehungen genutzt werden. Deshalb sollte keine „Closed User Group“ entstehen. Es gehört jedoch zu den „VEDIS-Spielregeln“, dass die benötigten Zertifikate extern in einem LDAP-Verzeichnis bereit gestellt werden.

Wer sich die Pflege der LDAP-Beziehungen erleichtern möchte, kann beispielsweise auf die neuen Dienste der European Bridge CA, die der gemeinnützige Verein TeleTrusT e.V. kostendeckend zur Verfügung stellt, zurückgreifen. Alternative Lösungen werden zurzeit von der Projektgruppe geprüft und in Folgedokumenten veröffentlicht.

Qualifizierte oder fortgeschrittene Zertifikate?

Die VEDIS-Dokumente wurden geschrieben, um Marktteilnehmern mit fortgeschrittenen Zertifikaten, gleich ob aus der eigenen PKI oder extern bezogen, die Teilnahme am Verfahren zu ermöglichen. Ihre Erstellung muss lediglich den Sicherheitsanforderungen, wie sie vor allem in der PKI-Policy und in der Zertifizierungsrichtlinie dokumentiert sind, genügen. Ein qualifiziertes Zertifikat, z. B. eines akkreditierten deutschen Zertifizierungsdienste-anbieters (ZDA), erfüllt auch die VEDIS-Anforderungen.

VEDIS möchte im elektronischen Datenaustausch zwischen Marktteilnehmern fortgeschrittene und qualifizierte Zertifikate gleichberechtigt behandeln (Vertikale Interoperabilität). Alle kryptographischen Funktionen mit Hilfe von PKI-Zertifikaten sollen interoperabel ablaufen (horizontale Interoperabilität).

Kann ein Unternehmen jetzt schon beginnen, obwohl die Arbeit an VEDIS weitergeht?

Jedes am elektronischen Datenaustausch interessierte Mitgliedsunternehmen kann und sollte jetzt mit den in den VEDIS-Dokumenten beschriebenen Maßnahmen beginnen.

Der erste Schritt sollte kurzfristig Site-to-Site-Security herstellen, d. h. zwischen den Unternehmensnetzen als ganzes eine gesicherte Kommunikation über das Internet gewährleisten, um Geschäftsdaten nicht mehr ungeschützt austauschen zu müssen.

Die zum Start erforderlichen Dokumente sind alle verfügbar. VEDIS betritt dabei keinesfalls riskantes technisches oder rechtliches Neuland. Die benötigten Produkte und Dienstleistungen sind in ausreichender Qualität und Vielfalt am Markt verfügbar.

Allerdings sind für zukünftige Entwicklungen noch weitere Empfehlungen zu Sicherheitsrahmenbedingungen sinnvoll. Deshalb wird es noch weitere VEDIS-Dokumente geben. Es wird sich dabei jedoch um Erweitungen oder Verfeinerungen handeln, die das grundsätzliche Sicherheitsanliegen von VEDIS und seine grundsätzlichen technischen und organisatorischen Empfehlungen nicht tangieren und damit die Investition schützen.

Wo ist VEDIS ein eigener Weg der deutschen Stromwirtschaft und wo nicht?

Anlass für VEDIS war die notwendige Verbandsarbeit zur Ausgestaltung des Datenaustauschs im liberalisierten Strommarkt. Die Dokumente entstanden also branchenspezifisch. Die Minimalanforderungen an Sicherheit, die dabei in den Dokumenten aufgestellt wurden, sind den Sicherheitsanforderungen im elektronischen Datenaustausch des Strommarktes angepasst worden und insoweit dem Schutzbedürfnis des Werteflusses bzw. der personenbezogenen Daten in der Branche angemessen. Die in der Stromwirtschaft im Rahmen von VEDIS entstehende Sicherheitsinfrastruktur soll aber weit darüber hinaus mit skalierbaren Transaktionszahlen und skalierbarem Sicherheitsniveau eingesetzt werden können. VEDIS orientiert sich deshalb an allseits akzeptierten Standards. Zu nennen sind PKIX in seiner Ausprägung ISIS-MTT. Dieses Profil enthält unveränderte Standards wie X.509, S/MIME, LDAP V3, OCSP und weitere.