

Neues von  VEDIS

SELMA-Workshop, Berlin, 23. Juni 2005

SIEMENS

Wer bin ich ?

SIEMENS

**Region Deutschland Rhein-Main
Communication
Consulting Security**

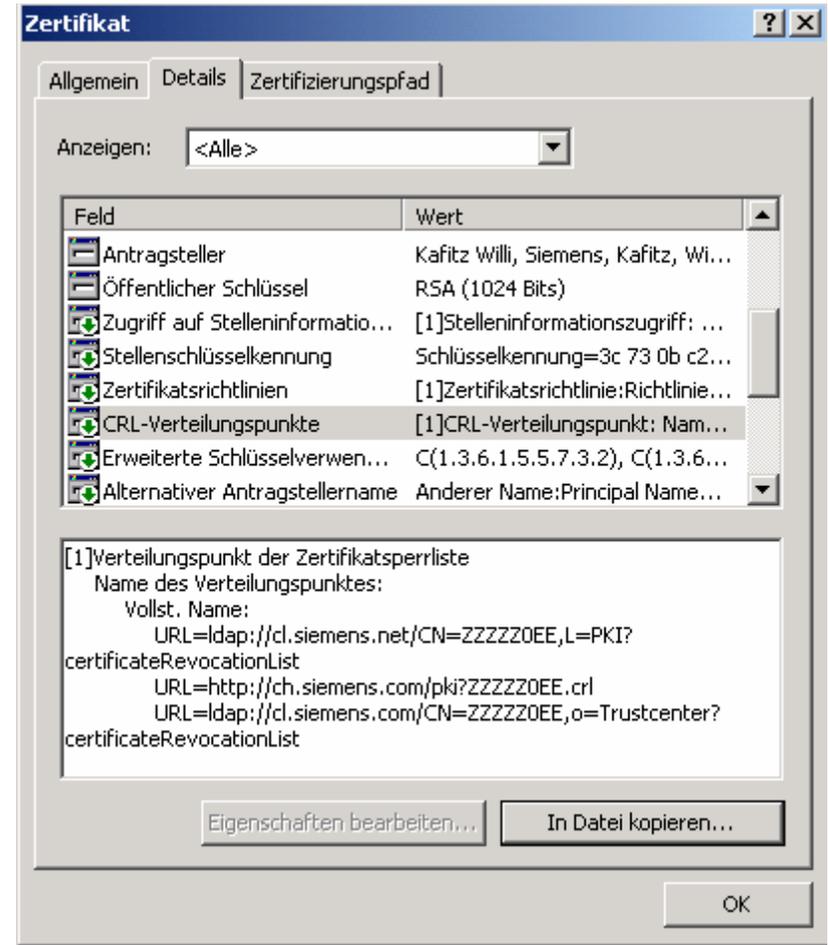
**Postal Address:
P.O.Box 11 17 33
D-60052 Frankfurt/Main**

**Office Address:
Rödelheimer Landstrasse 5-9
D-60487 Frankfurt/Main**

**Dr. rer. nat.
Willi Kafitz**

Senior Consultant

**Phone: +49 69 797 5202
Fax: +49 69 797 4716
E-mail: Willi.Kafitz@siemens.com**



Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ stellt sich vor

Leitung

Beate Becker

VDEW

Mitglieder

Helge-Werner Benke

Vattenfall Europe

Uwe Buntrock

Avacon

Jürgen Dreymann

Überlandwerke Fulda

Ralf Knecht

RWE

Heinz Köhler

E.ON Energie

Carl Major

E.ON Netz

Christoph Matthäus

EnBW

Andreas Mitzkus

T-Systems

Dirk Nolte

Atos Origin CC Informatik

Frank Pooth

STEAG

Günter Schneider

Mannheim (MVV)

Coaching

Dr. Willi Kafitz

Siemens

Agenda



- Was wollen wir ?
- Was haben wir erreicht ?
- Woran arbeiten wir ?

Agenda



- **Was wollen wir ?**
- Was haben wir erreicht ?
- Woran arbeiten wir ?

Das VDEW-Projekt VEDIS

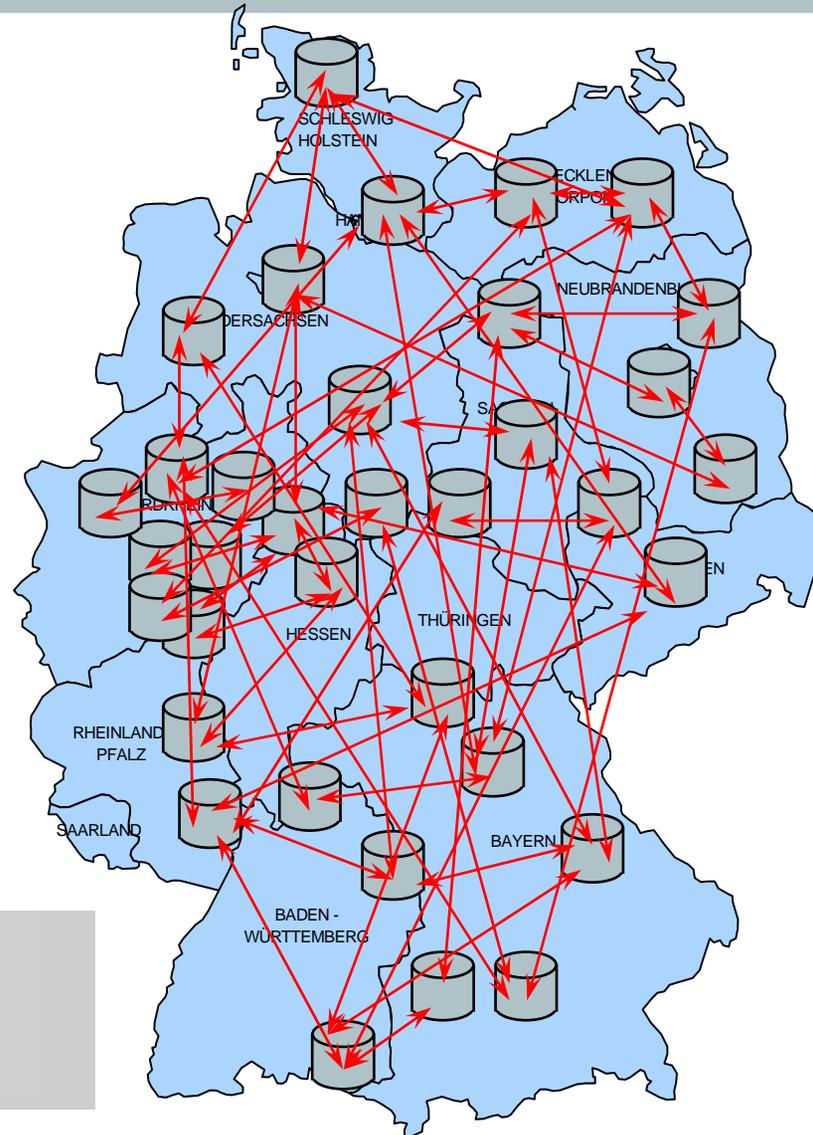


Verbindlichkeit & Sicherheit
im
Electronic Data Interchange

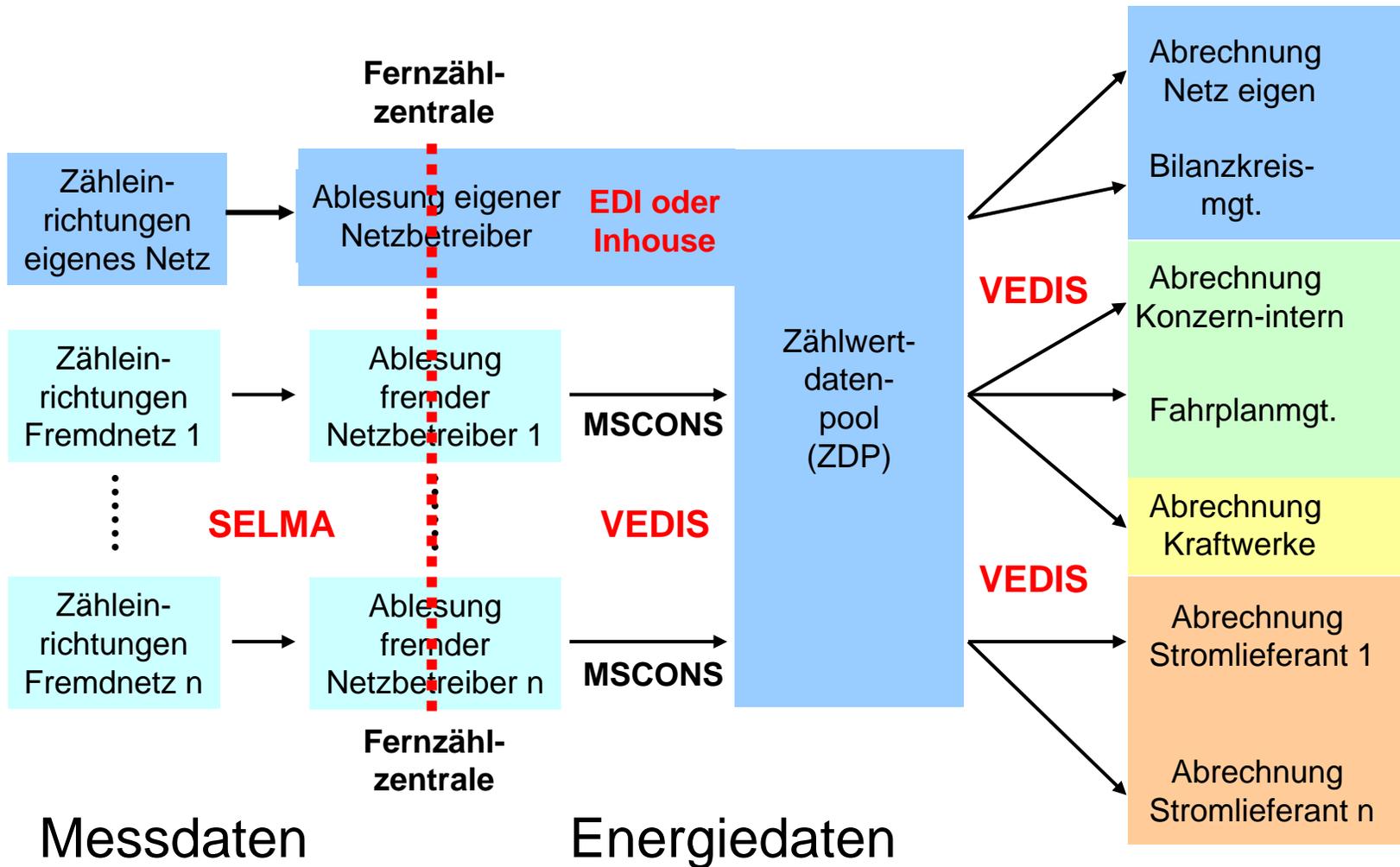
Informationsaustausch im deutschen Strommarkt

- 45 Mio. Kunden
- ca. 950 Netzbetreiber
- ca. 200 Stromlieferanten
- Bilanzkreisverantwortliche
- Übertragungs-Netzbetreiber
- Verteilnetzbetreiber
- National / International ?

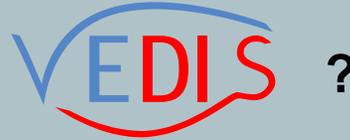
ca. 2,5 Mrd.
Nachrichten / Jahr



Abgrenzung SELMA und



Was möchte



Kurzfristig Side – to – Side Security zwischen den Marktteilnehmern

- Verschlüsselung und Signatur
- Zwischen den Unternehmen
- auf E-Mail-Ebene (S/MIME)
- bei Stammdaten- und Zähl Datenaustausch
- fortgeschrittene Signatur genügt

Später

- Signatur auf Dateiebene (Dateisignatur)
- Erweiterung auf alle EDI-Transaktionen (formatierte Daten)

Mittelfristig End – to – End Security an ausgewählten Arbeitsplätzen

- Elektronischer Geschäftsverkehr (auch unformatierte Daten)
- Verschlüsselung auf E-Mail-Ebene (S/MIME)
- Signatur auf Dateiebene (Dateisignatur)

Vertikale Interoperabilität

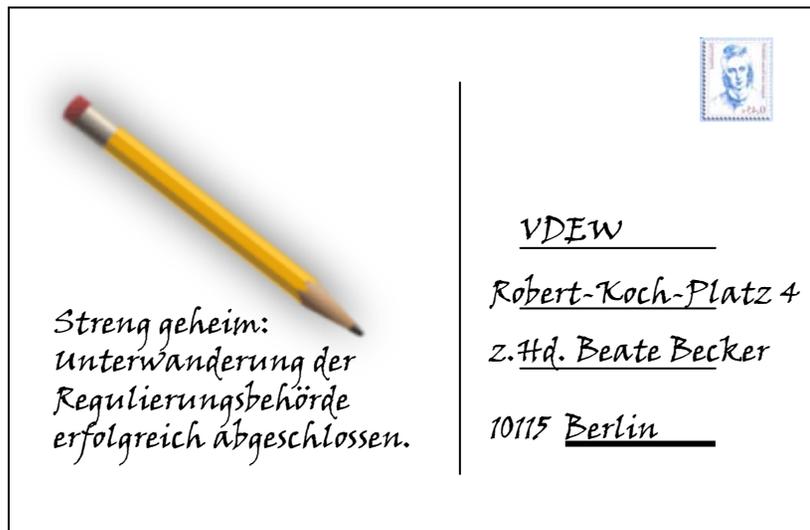
**Gleichstellung von
fortgeschrittenen und qualifizierten Signaturen
durch Branchenkonvention,
wo es der Gesetzgeber zulässt.**



definiert die Branchenkonvention

(Industry Policy Requirements)

Warum Sicherheitsmaßnahmen - Operative Denkweise



Unverschlüsselte und unsignierte Kommunikation im Internet hat vor Gericht den Beweiswert einer mit Bleistift geschriebenen Postkarte.

Warum Sicherheitsmaßnahmen - Strategische Denkweise

Bearbeitung	Anwenderkontrolle	Prozesskontrolle
Manuell	voll	Ergebnisorientiert
Digitalisiert	visuell	Anwendungsorientiert
Automatisiert	indirekt	Systemorientiert

Für weitere Automatisierungsschritte den Rücken frei halten !

Agenda



- Was wollen wir ?
- **Was haben wir erreicht ?**
- Woran arbeiten wir ?

Mit Sicherheit bemerkenswert



An die Geschäftsleiter
der Mitgli...

der Elektrizitätswirtschaft auf Basis von Un...

Allerdings findet heute der Nachweis, dass in einigen Fällen gesicherte Leitungen („Transport-gebundene Sicherheit“) bzw. durch Dokumenten- oder -signatur („Informations-gebundene Sicherheit“) statt.

Die Branche muss aber z. B. beim Lieferantenwechsel selbstverständlich gegen Daten der Kunden gegen widerrechtliches Lesen oder gar missbräuchliches Kopieren schützen. Über die gesetzlichen Anforderungen hinaus, ist Sicherheit aber auch für die Ausschöpfung von Rationalisierungspotential durch den elektronischen Geschäftsverkehr über Unternehmensgrenzen hinweg.

Im Gegensatz zu vielen Bereichen der Kommunikationstechnologie ist Sicherheit nicht 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. Aus diesem Grund legen die Verbände hier eine gemeinsame Erklärung vor, in der Maßnahmen zur Sicherheit im elektronischen Geschäftsverkehr empfohlen werden. Sie haben das Ziel, das Sicherheitsniveau auf der technischen und organisatorischen Ebene nachhaltig zu heben. Diese Sicherheitsrahmenbedingungen sind bewusst allgemein gehalten und sollten mittelfristig Bestand haben. Wir verstehen es als politische Willenserklärung der deutschen

Elektrizitätswirtschaft, geeignete Maßnahmen zu ergreifen, um technisch und organisatorisch die elektronische Kommunikation zu schützen bzw. zu ermöglichen.

Folgende Ziele sollen über die gemeinsame Erklärung der Verbände 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 den Marktteilnehmern, aber auch mit
 - staatlichen Instanzen („E-Government“),
 - Kunden („E-Commerce“) und
 - Zulieferern („E-Procurement“)
 soll bzgl. Risiken, Volumina und Technik beherrschbar bleiben.

Die nötige weitere Ausgestaltung wird dann auf der Ebene von Arbeitsdokumenten erfolgen, die durch zeitnahe Anpassung dem technischen Wandel und kurzfristigen Bedürfnissen in der Branche Rechnung tragen. Diese Dokumente werden durch die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ erarbeitet und durch den VDEW veröffentlicht. Eine erste Version dieser Dokumente wird in Kürze vorgelegt.

Des Weiteren findet am 29.-30. September 2003 ein von allen Verbänden unterstützter VDEW-Infotag „Elektronischer Datenaustausch – aber sicher!“ in Kassel statt.

Mit freundlichen Grüßen

Dr. Eberhard Melker
Hauptgeschäftsführer
Verband der Elektrizitätswirtschaft – VDEW – e. V.

Dr. Konstantin Staschus
Geschäftsführer
Verband der Netzbetreiber – VON – e. V. beim VDEW

RA Wolf-Ingo Kunze
Geschäftsführer
Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland – VRE – e. V.

Michael Schöneich
Geschäftsführer
Verband kommunaler Unternehmen e. V.

Dr. rer. pol. Carsten Kreikau
Mitglied der Hauptgeschäftsführung
Bundesverband der Deutschen Industrie e. V. – BDI

Dr. rer. pol. Alfred Richmann
Geschäftsführer
VIK Verband der Industriellen Energie- und Kraftwirtschaft e. V.

Anlage 1: Gemeinsame Erklärung

91AD709C82AC5D0CC1258D979562340E180

- PKI-Policy
 - Technische PKI-Interoperabilität
 - Umgang mit Schlüsselmaterial
 - Certification Practice Statement
 - Umsetzungsempfehlungen
- ... für die PKI-Selbermacher
 - ... Standards, Standards, Standards – aber keine Nice-to-haves
 - ... Spielregeln für alle Anwender was ist Hui, was ist Pfui
 - ... verbindliche Sicherheit Grundlage für EDI-Verträge
 - ... worauf sollte man achten keine „Stiftung Warentest“

Warum Phase II ?

- VEDIS Phase I

- VEDIS Phase II

- ... legte die politischen, organisatorischen und technischen Grundlagen
- ... definierte die Spielregeln

- ... Herausforderung Topologie
- ... Anwendungsnähe
- ... Praktikabilität
- ... Einsatzpotential

Rahmenbedingungen

PKI-Topologie und Einsatzrahmenbedingungen

Einsatzpotentiale

VEDIS-Einsatzpotentiale in
papierlosen Geschäftsprozessen

Flankierende Maßnahmen

FAQ
Fragebogen
Infotag
Publikationen
Vorträge

Leitfaden

Zehn Schritte zur VEDIS Sicherheit

VEDIS Kerndokumente

Gemeinsame Erklärung
PKI-Policy
CPS nach RFC 2527 wird ersetzt durch CPS nach RFC 3647
PKI-Interoperabilität
Umgang mit Schlüsselmaterial
Umsetzungsempfehlungen



Flankierende Maßnahmen

FAQ
Fragebogen
Infotag
Publikationen
Vorträge

... näher an der Anwendung

- 10 Schritte zur VEDIS-Sicherheit
- Rahmenbedingungen
- Einsatzpotentiale
- Certificate Policy

- ... Leitfaden für Einsteiger
- ... Sichere organisationsübergreifende Geschäftsprozesse mit PKI-Mitteln
- ... VEDIS – für den Strommarkt gemacht, als Business Enabler gedacht
- ... Noch einfacher individuell anpassbar
Sicherheitsgrundlage für EDI-Verträge

Anforderungen

- **Welche Anwendungen und Geschäftsprozesse sollen organisationsübergreifend digitalisiert bzw. automatisiert werden?**
- **Welche Sicherheitsrahmenbedingungen sind erforderlich?**
- **Was wird an eigener Infrastruktur benötigt?**
- **Wie können externe Zertifikate gefunden werden?**
- **Wie verschlüssele ich an externe Partner ?**
- **Wie können externe elektronische Unterschriften überprüft werden?**
- **Wie werden firmeneigene Zertifikate extern bereit gestellt?**
- **Wie kann langfristiger Beweiswert in der Archivierung realisiert werden?**
- **Wie können Vertrauensbeziehungen automatisiert werden ?**

Agenda



- Was wollen wir ?
- Was haben wir erreicht ?
- **Woran arbeiten wir ?**

Generalbebauungsplan VEDIS Phase I, II und III

VEDIS III

**IT-Sicherheit auf der
Transportebene**

**IT-Sicherheit auf der
Informationsebene**

**Flankierende
Maßnahmen**

Fragebogen
Infotag
Publikationen
Vorträge

VEDIS II

Rahmenbedingungen

PKI-Topologie und Einsatzrahmenbedingungen

Einsatzpotentiale

VEDIS-Einsatzpotentiale in
papierlosen Geschäftsprozessen

**Flankierende
Maßnahmen**

FAQ
Fragebogen
Infotag
Publikationen
Vorträge

Leitfaden

Zehn Schritte zur VEDIS Sicherheit

VEDIS I

VEDIS Kerndokumente

Gemeinsame Erklärung
PKI-Policy
CPS nach RFC 2527 wird ersetzt durch CPS nach RFC 3647
PKI-Interoperabilität
Umgang mit Schlüsselmaterial
Umsetzungsempfehlungen

**Flankierende
Maßnahmen**

FAQ
Fragebogen
Infotag
Publikationen
Vorträge



- Kein Datenaustausch ohne Vertrag
- Kein Vertrag ohne vereinbarte Sicherheitsrahmenbedingungen
- Echtheit der Herkunft / Unversehrtheit des Inhaltes garantieren
- Vertragsgestaltung möglichst mit Standardtexten
- Bezug auf die VEDIS-Dokumente im EDI-Vertrag

EDI – mach's mit 

EDI-Vertrag mit konfektionierten Anhängen

EDI-Vertrag

Standard
nach
94/820/EG

Anhang 1
Inter-
operabilität

nach
VDEW-
Empfehlung
Markt-
schnittstellen

Anhang 2
Sicherheit

nach
VDEW-
Empfehlung





im Internet

www.strom.de → Fakten → Themen → Datenmanagement → VEDIS

Noch Fragen ?

