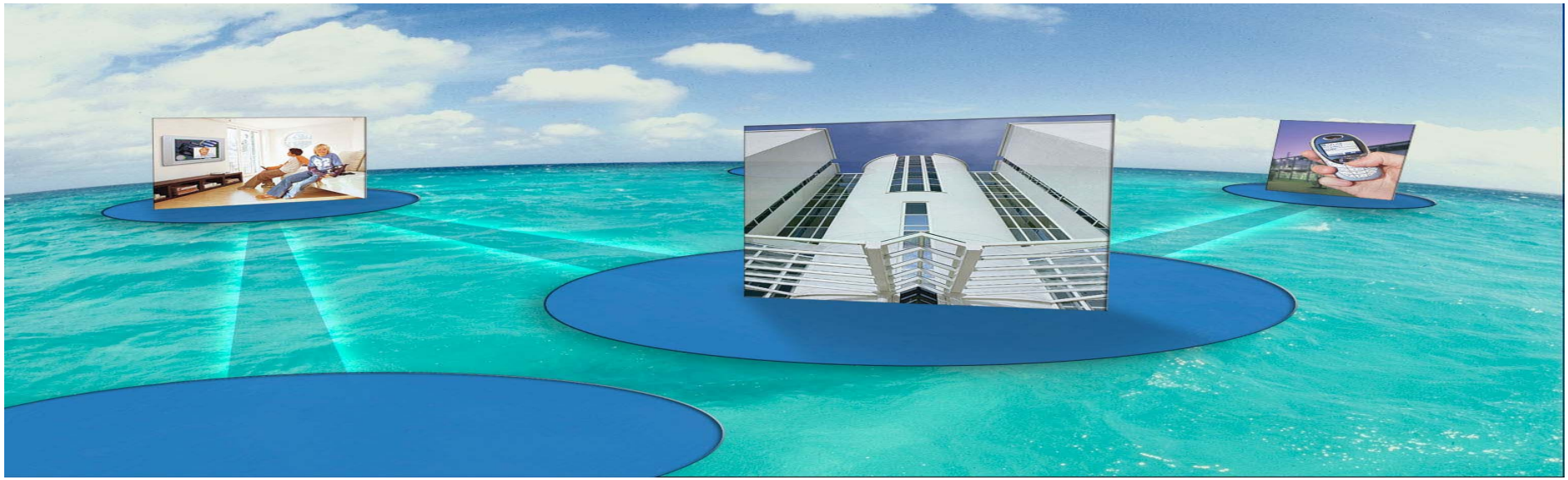


Neues von VEDIS

SELMA-Workshop, Berlin, 23. Juni 2005

SIEMENS

Wer bin ich ?

SIEMENS

Region Deutschland Rhein-Main
Communication
Consulting Security

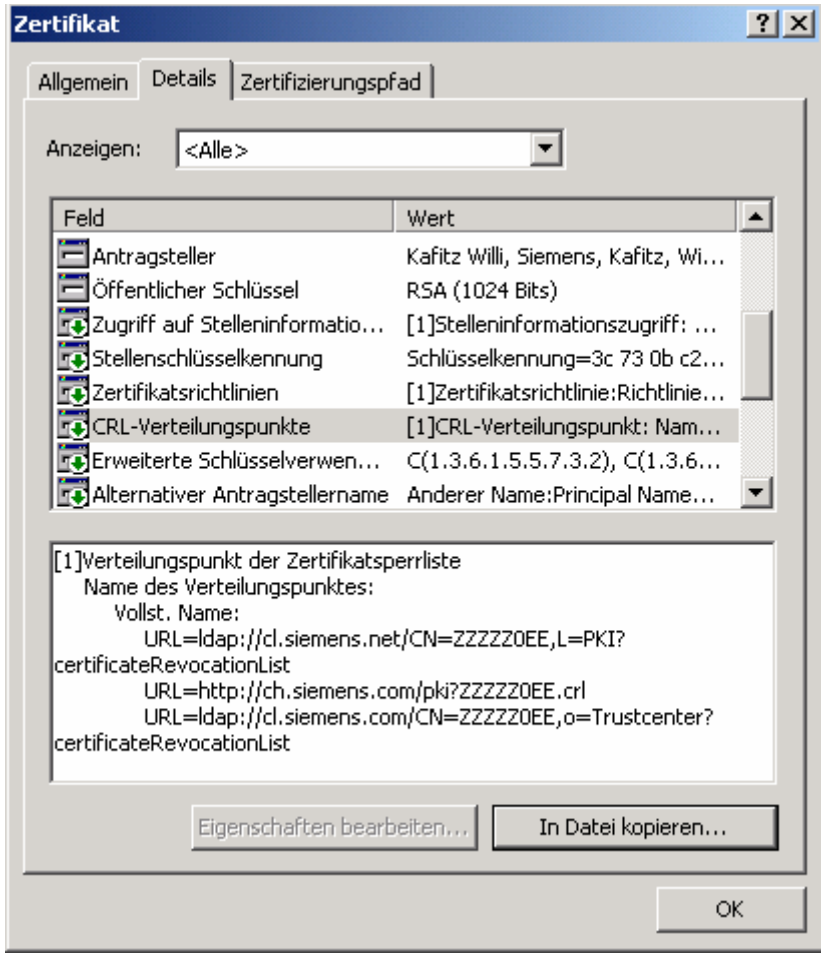
Postal Address:
P.O.Box 11 17 33
D-60052 Frankfurt/Main

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

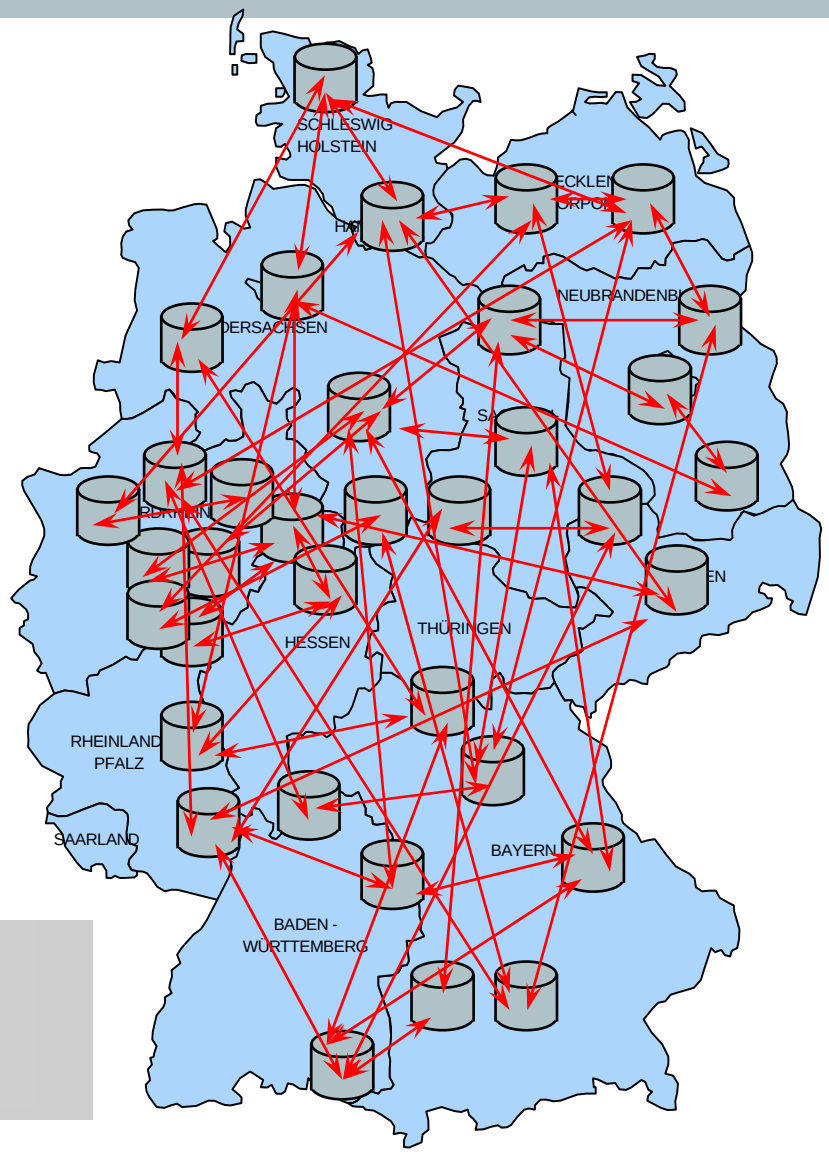
- **Was wollen wir ?**
- Was haben wir erreicht ?
- Woran arbeiten wir ?

Das VDEW-Projekt VEDIS

Verbindlichkeit & Sicherheit
im
Electronic Data Interchange

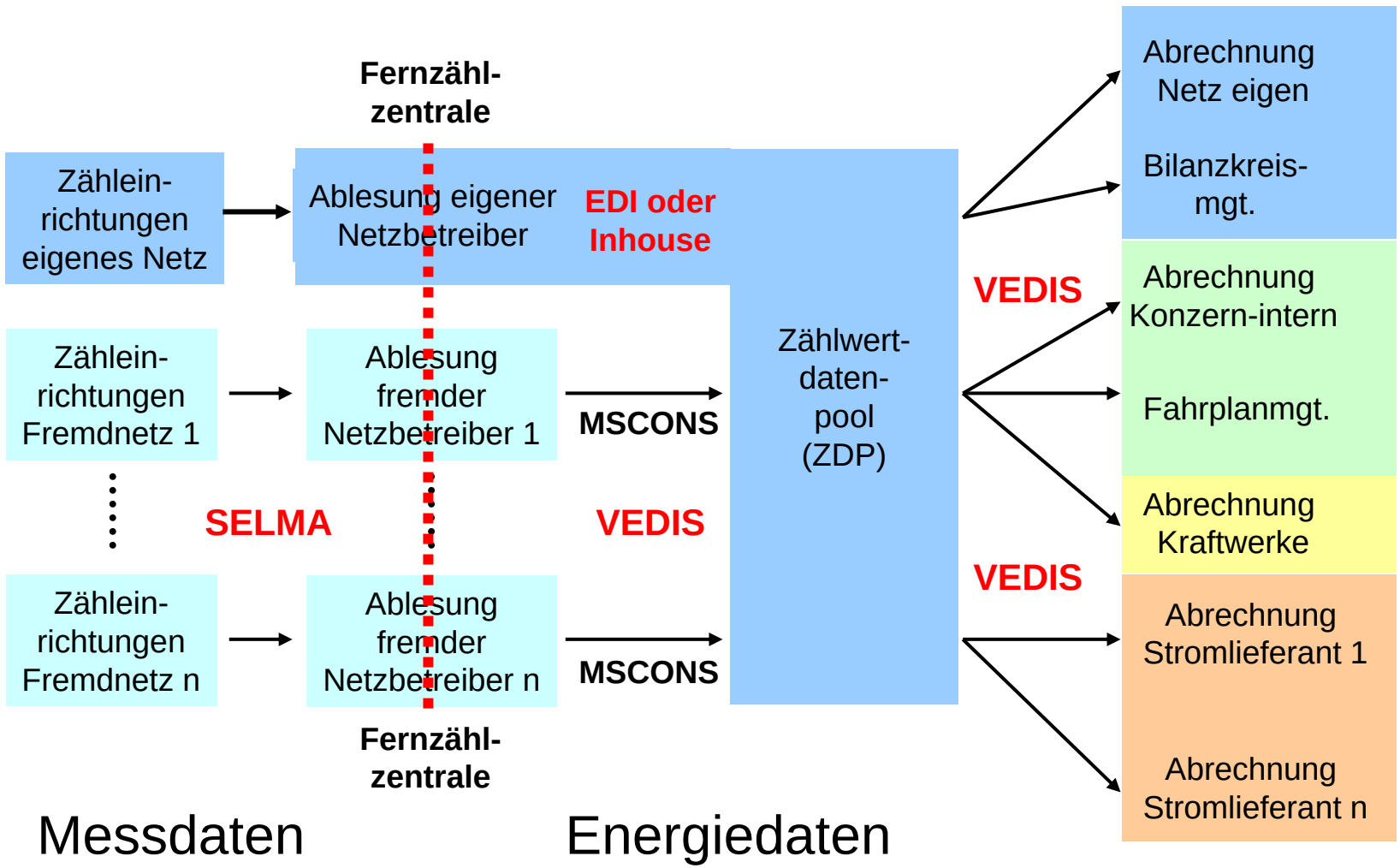
Informationsaustausch im deutschen Strommarkt

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



ca. 2,5 Mrd.
Nachrichten / Jahr

Abgrenzung SELMA und VEDIS



Was möchte VEDIS ?

Kurzfristig Side – to – Side Security zwischen den Marktteilnehmern

- Verschlüsselung und Signatur
- Zwischen den Unternehmen
- auf E-Mail-Ebene (S/MIME)
- bei Stammdaten- und Zähldatenaustausch
- 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

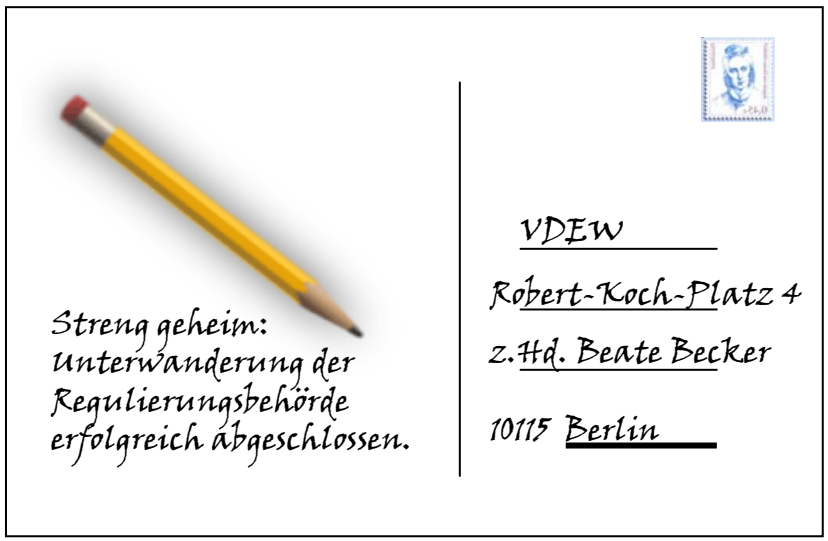
durch Branchenkonvention,

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

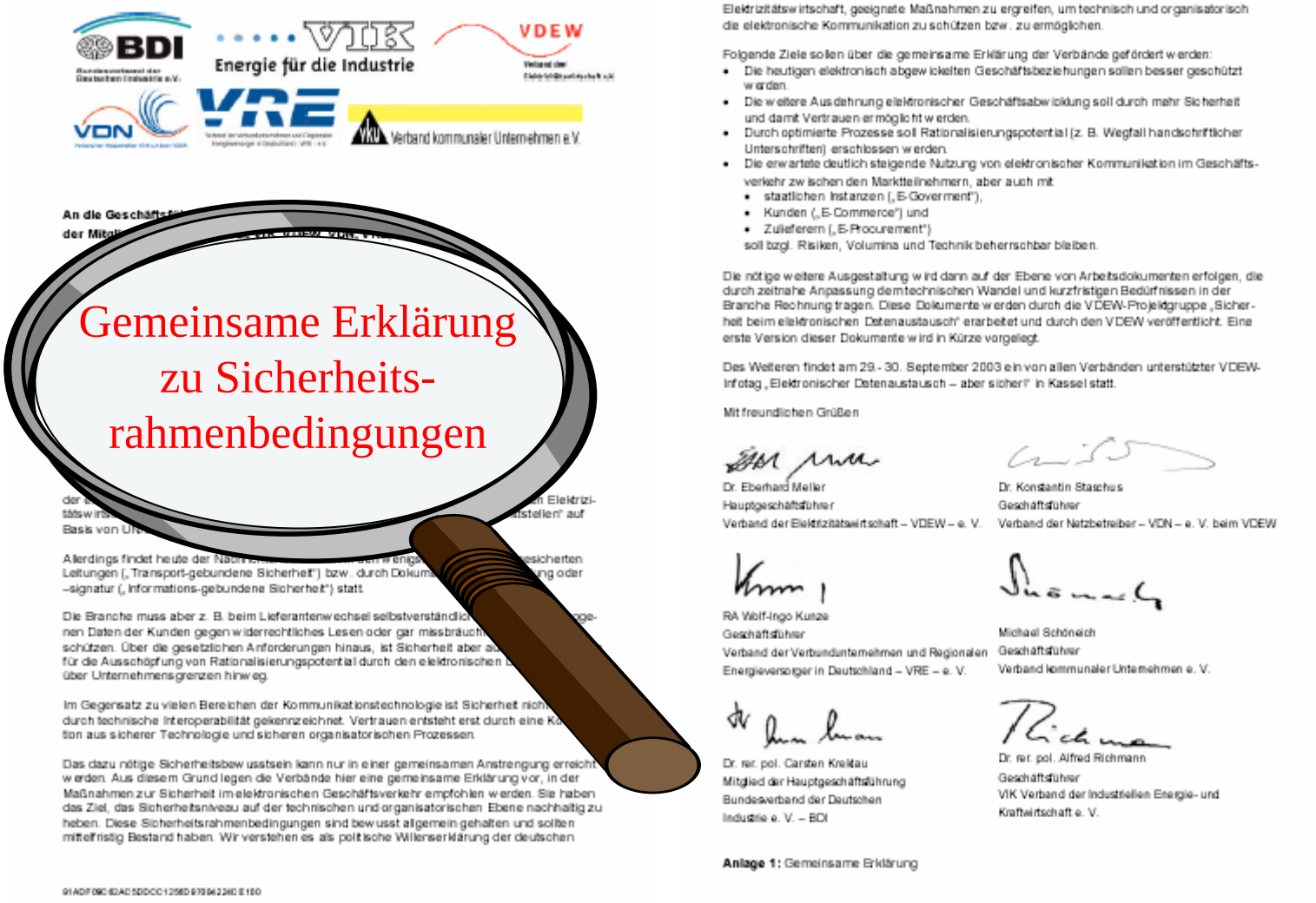
Bearbeitung	Anwenderkontrolle	Prozesskontrolle
Manuell	voll	Ergebnisorientiert
Digitalisiert	visuell	Anwendungsorientiert
Automatisiert	indirekt	Systemorientiert

Für weitere Automatisierungsschritte den Rücken frei halten !

Agenda

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

Mit Sicherheit bemerkenswert



Phase I Folgedokumente

- PKI-Policy
- Technische PKI-Interoperabilität
- Umgang mit Schlüsselmaterial
- Certification Practice Statement
- Umsetzungs-empfehlungen

- ... 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 VEDIS Phase II ?

- VEDIS Phase I
  - ... legte die politischen, organisatorischen und technischen Grundlagen
  - ... definierte die Spielregeln
- VEDIS Phase II
  - ... Herausforderung Topologie
  - ... Anwendungsnähe
  - ... Praktikalität
  - ... Einsatzpotential

Generalbebauungsplan VEDIS Phase I und 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 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

Phase II Folgedokumente

... 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

IT-Sicherheit auf der Transportebene

IT-Sicherheit auf der Informationsebene

Flankierende Maßnahmen
Fragebogen
Infotag
Publikationen
Vorträge

Rahmenbedingungen
PKI-Topologie und Einsatzrahmenbedingungen

Einsatzpotentiale
VEDIS-Einsatzpotentiale in papierlosen Geschäftsprozessen

Leitfaden
Zehn Schritte zur VEDIS Sicherheit

Flankierende Maßnahmen
FAQ
Fragebogen
Infotag
Publikationen
Vorträge

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

Weitere Kernanliegen von VEDIS

- 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 VEDIS

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 ?