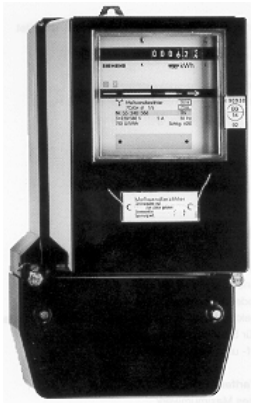
Einsatz von Verschlüsselung und elektronischer Signatur im Geschäftsverkehr der deutschen Elektrizitätswirtschaft

Workshop 5. – 6. Juni 2002

Stand 03.06.02

RWE Net - NT-K
Rolf-Dieter Kasper
rolf.kasper@rwenet.com

Situation vor der Liberalisierung

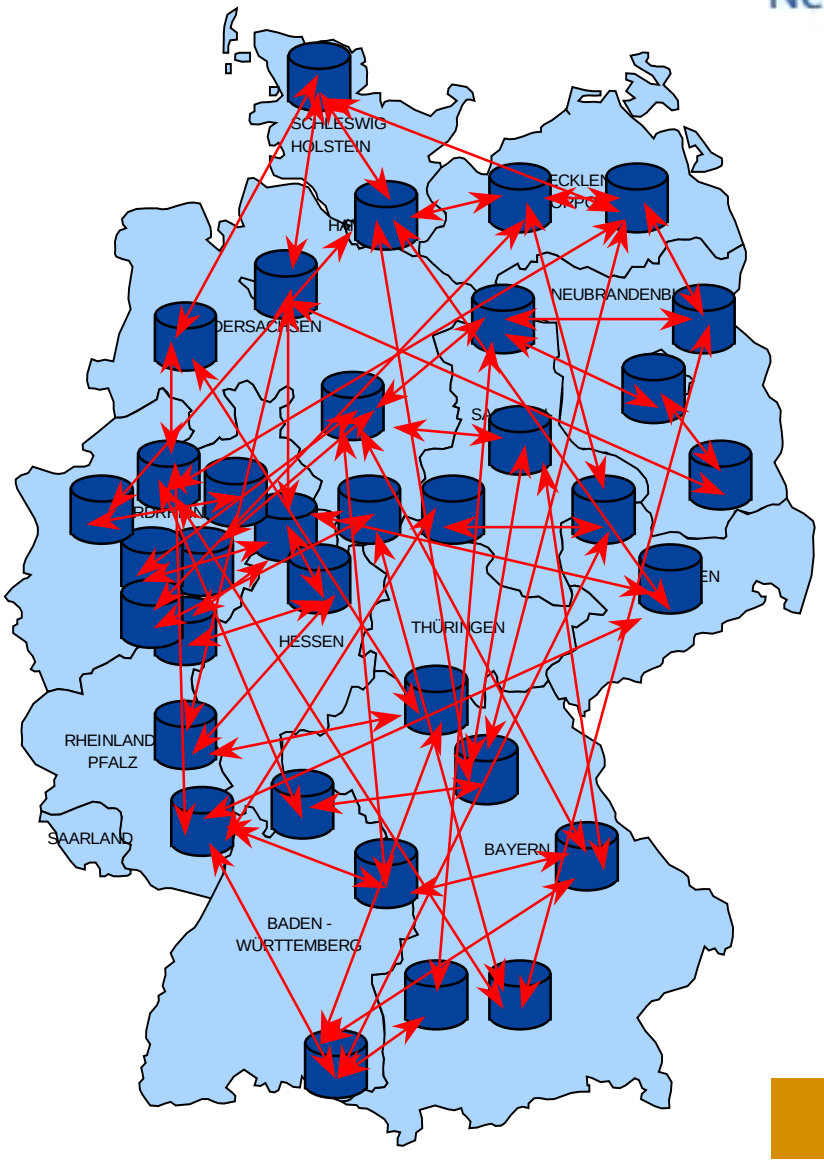


Zähleinrichtung → Ablesung → Energiemengenermittlung → Abrechnung

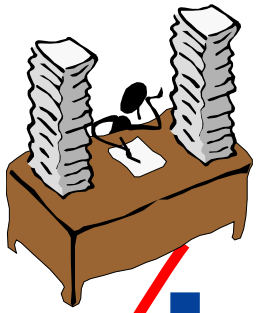
Linearer Prozess in **einem** Unternehmen

Informationsaustausch heute

- 45 Mio. Kunden
- ca. 950 Netzbetreiber
- ca. 200 Stromlieferanten
- Bilanzkreisverantwortliche
- ÜNB, VNB
- National / International ?



Transaktionsaufwand und Deregulierung



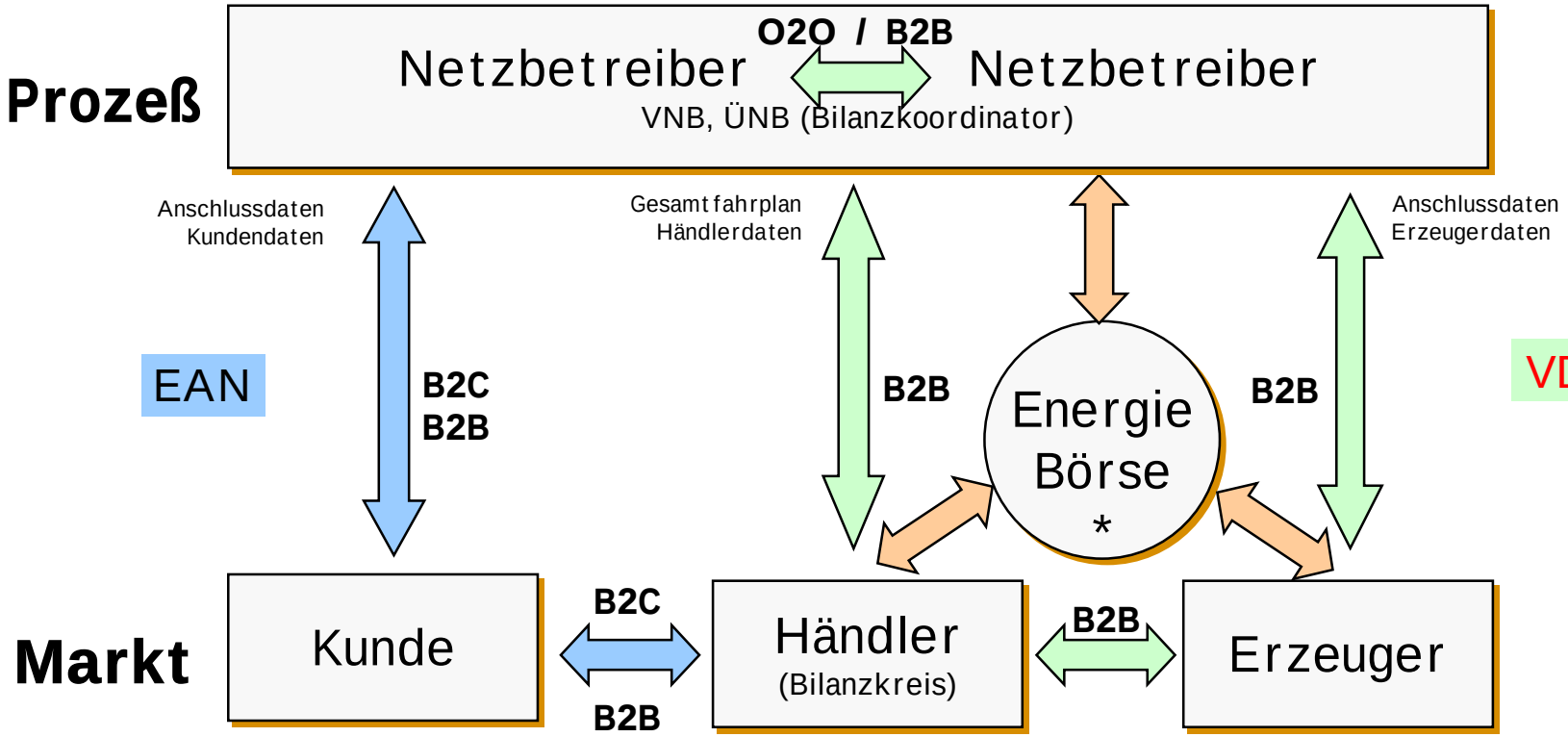
Transaktionsaufwand

erhöht sich mit

Deregulierung

Sichere elektronische Kommunikations-prozesse

Standards für die Kommunikation zwischen Marktteilnehmern

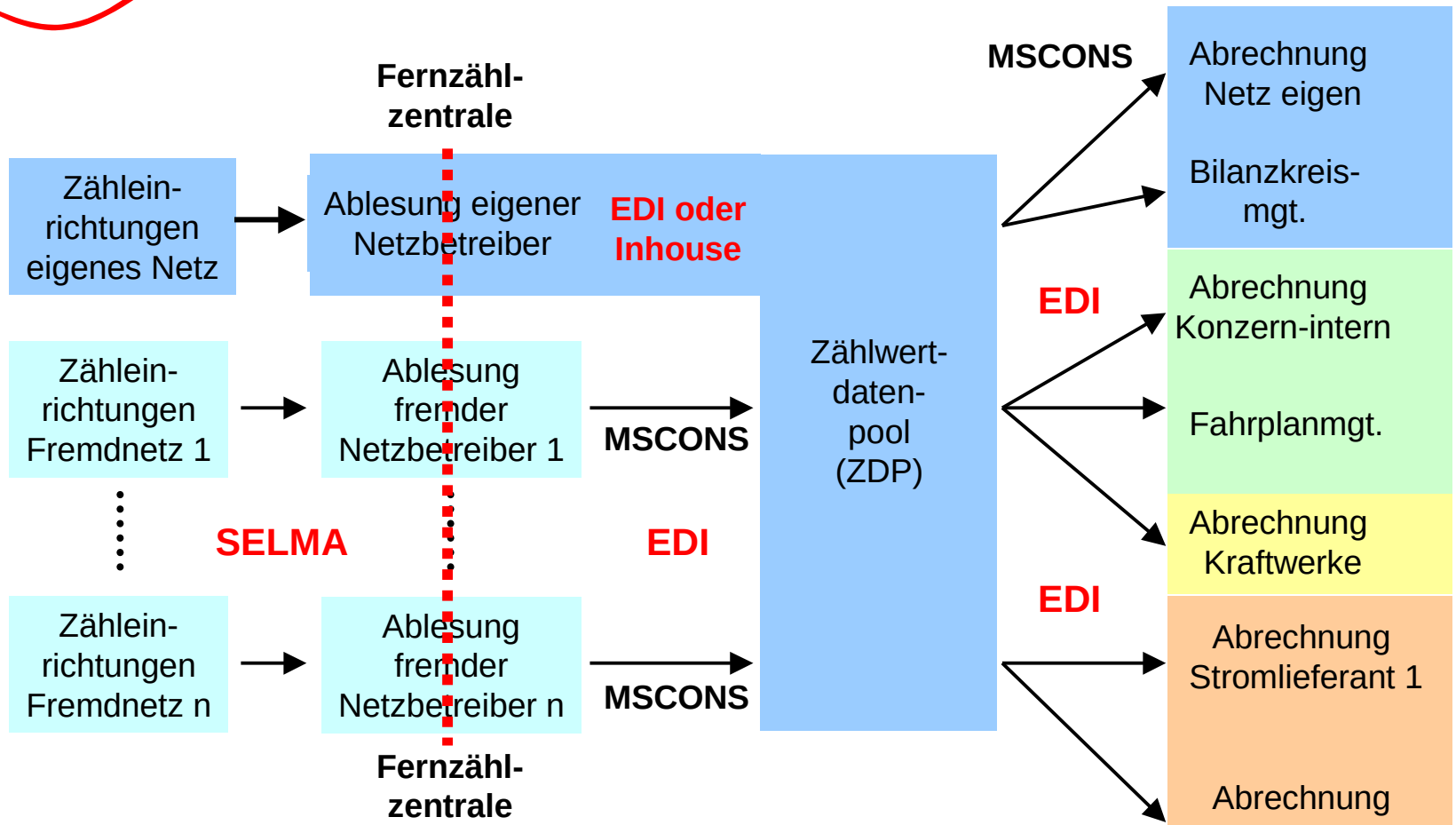


EDIFACT-Nachrichten (VDEW Subset) Datenmodelle und Implementation-Guides für folgende B2B-Kommunikationsprozesse

- **UTILMD** - Stammdaten von Kunden, Verträgen und Zählpunkten
- **DELFOR** - Anmeldung geplanter Energielieferungen, inkl. Bestätigungen und Veränderungen
- **MSCONS** - Bericht über erfolgte Energielieferung bzw. Verbräuchen (+ tech. Daten)
- **REMADV** - Zahlungsavise - detaillierte Abrechnungs-information in Bezug auf eine Zahlung
- **INVOIC** - Netz- und Energiedienstleistungs-abrechnung

XML-Versionen auf Basis der gleichen Datenmodelle sind ebenfalls www.strom.de verfügbar

Schnittstelle zwischen SELMA und VDEW-EDI

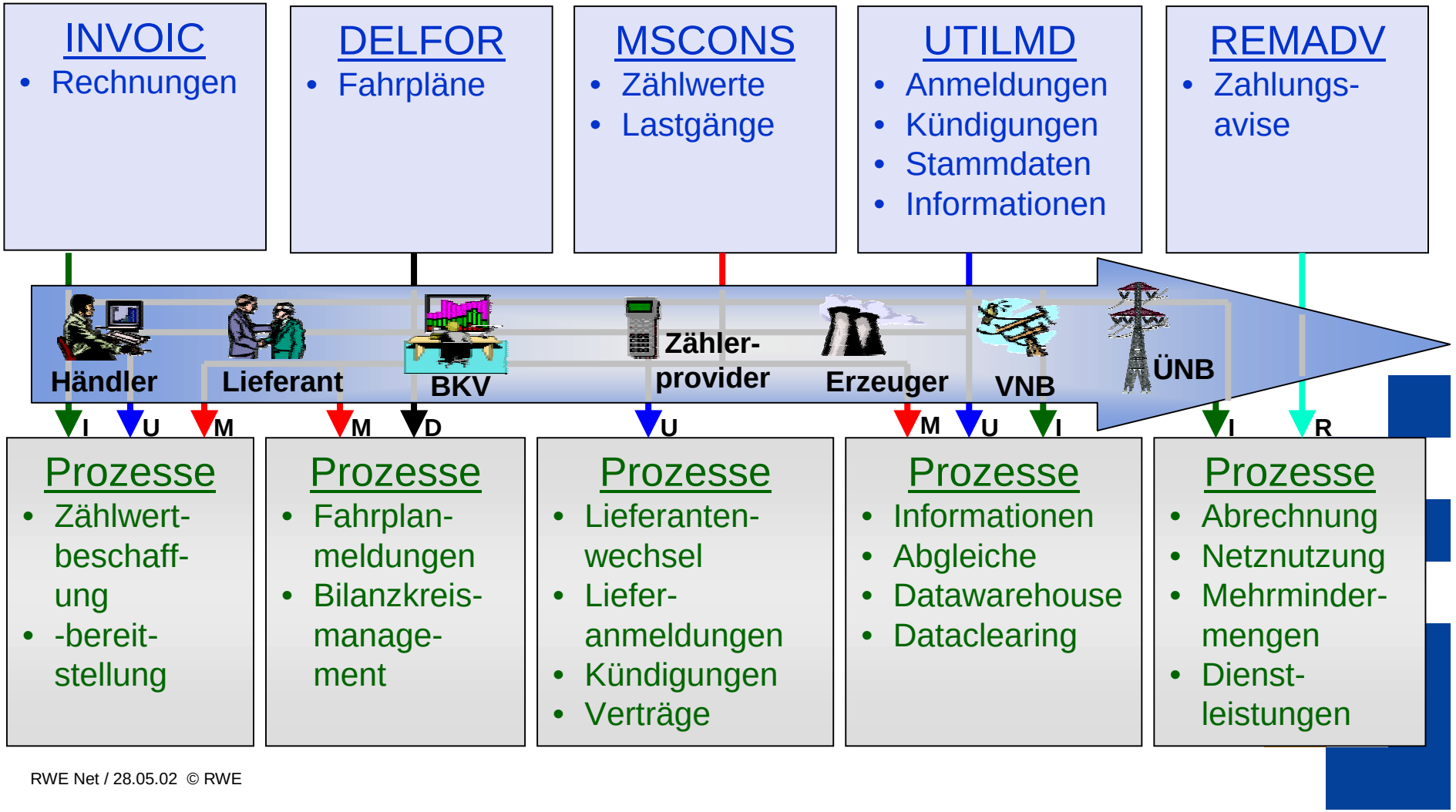


UN/EDIFACT - Dialognachrichten

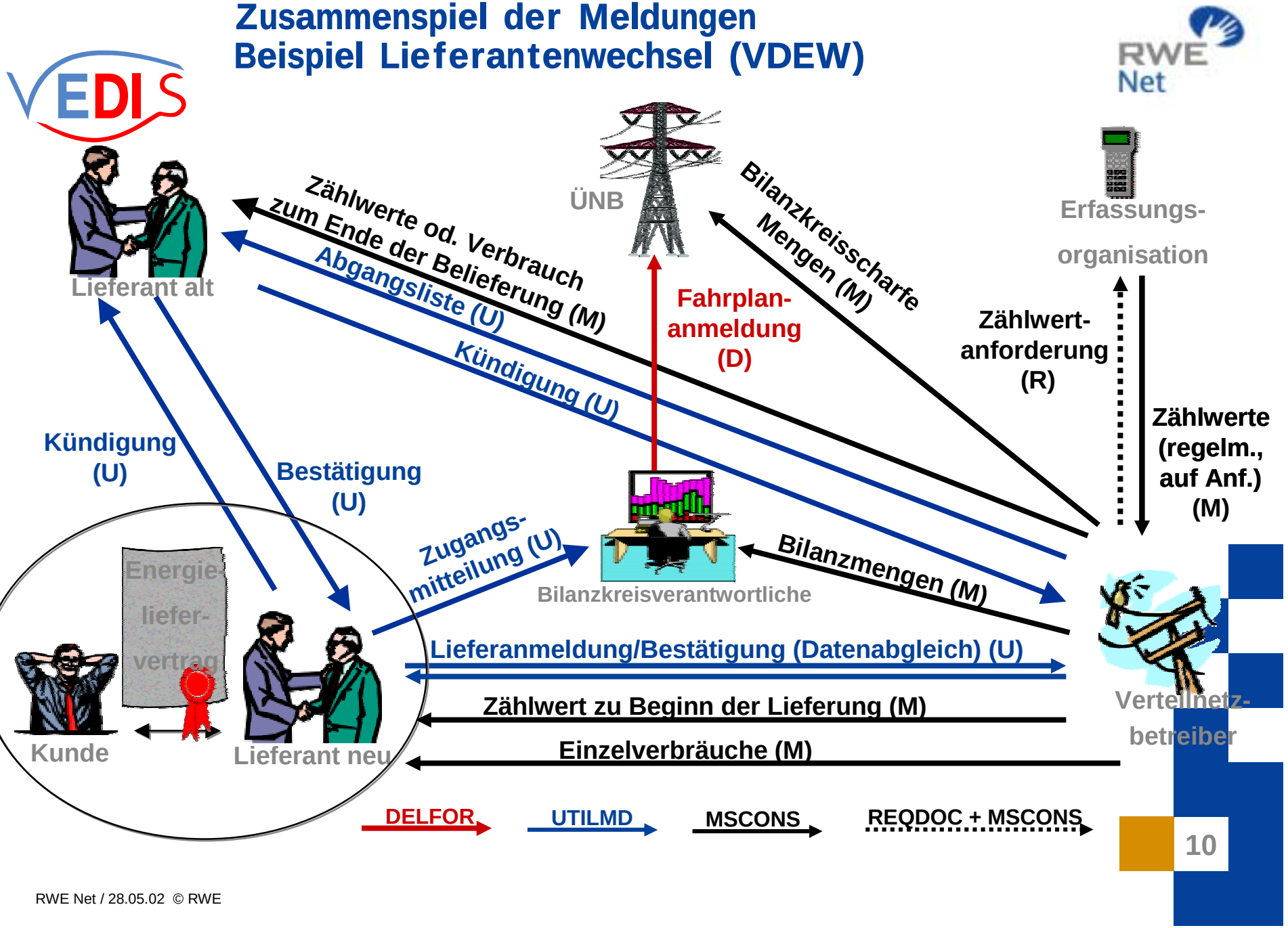
- **Anfragenachricht**
  dient der Anforderung von Informationen mittels weiterer spezieller Nachrichten
  - **REQDOC** Request for document message
    Ausprägung des VDEW für die Anfrage nach Zählwerten Verbräuchen und Lastgängen
- **Antwortnachrichten**
  dienen der Reaktion auf den Eingang von Nachrichten
  - **CONTRL** dient als Empfangsbestätigung von versendeten Nachrichten
  - **APERAK** Application error and acknowledgement message
    dient der Information über Lesbarkeit und einfachen Beantwortung von Anfragen (im Sinne ja/nein)

Prozesse und Standards

- Die Nachrichten unterstützen die unterschiedlichen Prozesse
- Die Nachricht kann von jedem Marktpartner für seine Zwecke genutzt werden.



Zusammenspiel der Meldungen
Beispiel Lieferantenwechsel (VDEW)



Arbeitsziel: Sicheres Business-to-Business-Networking zwischen den Marktteilnehmern




EON AG
Corporate Network

Lieferanten-netze

Sicheres VDEW Business Partner Network

Vertraulichkeit
Verbindlichkeit
Integrität
Autorisierung
Datenschutz
Authentifikation

Kunden-netze

RWE AG
Corporate Network

Partner...
Corporate Network

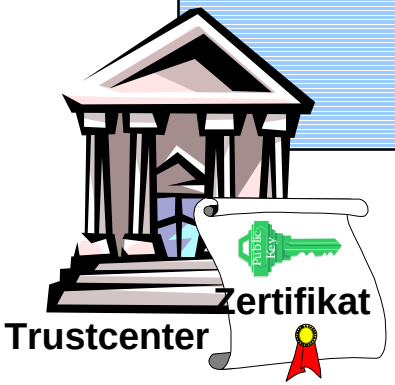
Public Key Infrastructure (PKI)

... ist ein **System** von

- Komponenten,
- Diensten und
- Verfahren,

um **Schlüssel und Zertifikate** für den Einsatz von Kryptographie

- zu generieren,
- zu verteilen und
- zu administrieren.

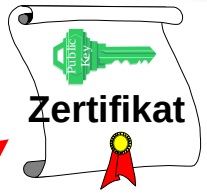


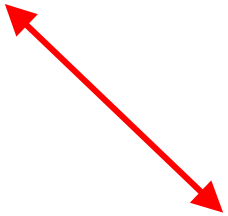
Beispiel: Einsatz einer elektronischen Signatur

- Authentizität
- Integrität
- Vertraulichkeit
- Beweisbarkeit

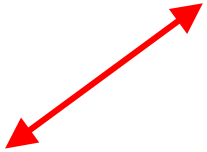
signieren

verifizieren





registrieren



vertrauen

Prozeßeinsparungen am Beispiel „Elektronische Signatur eProcurement (Gutschrift)“

- **Prozeß „Alt“:**
  - Gutschrift ausdrucken
  - vom Drucker holen
  - in Unterschriftenmappe legen
  - 2 Unterschriften aufbringen
  - einscannen
  - archivieren
  - kuvertieren
  - versenden
- **Prozeßkosten:** in GJ 2001
  - 125 Gutschriften p.m.
  - Prozessarbeitszeit 12 Minuten = 300 Stunden (à 85 € p.h.)
  - Kosten f. Drucker, Papier, Porto etc.: 1.000 € pauschal p.a.
- **Gesamtkosten:**
  - **100 %** (= 26.500 € p.a.)

- **Prozeß „Neu“:**
  - eMail Gutschrift elekt. signiere
  - eMail versenden, ar
- **Prozeßkosten:**
  - 2000 € p.a. (PKI anteilig)
  - 125 Gutschriften p.m.
  - Prozeßarbeitszeit 2 Minuten = 50 Stunden (à 85 € p.h.)
- **Gesamtkosten:**
  - **23,6 %** (= 6.250 € p.a.)

Ein Beispiel von vielen !!!

Zeiterfassung

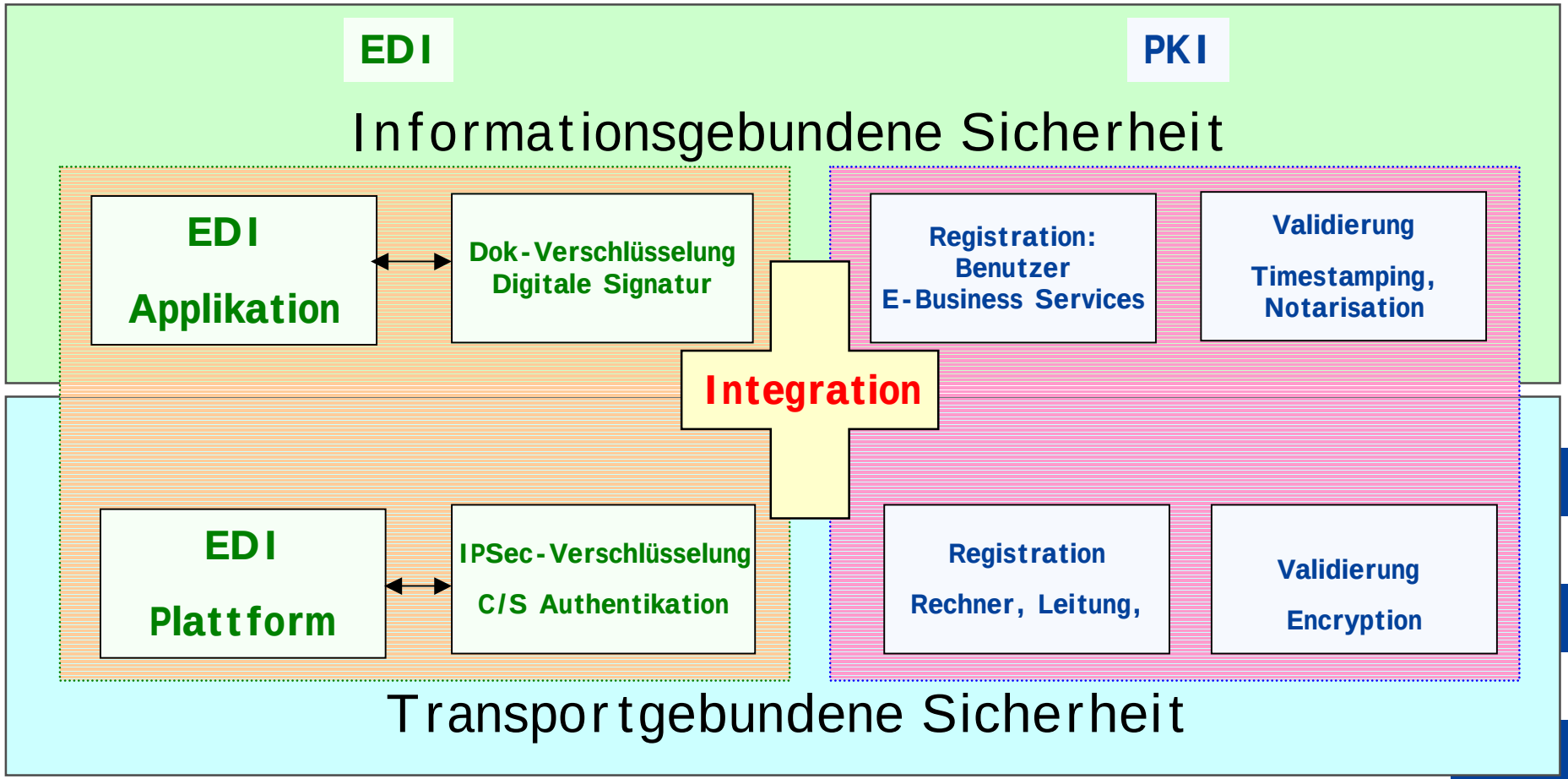
Reisekostenabrechnung

Urlaubsantrag

...

- **Einsparungen „Alt - Neu“:**
  - **76,4%** (= 20.250 € p.a.)
- **Weitere Vorteile:**
  - keine Liegezeiten
  - weniger Archiv-Speicherbedarf
  - kein Medienbruch
  - zukunftssicher

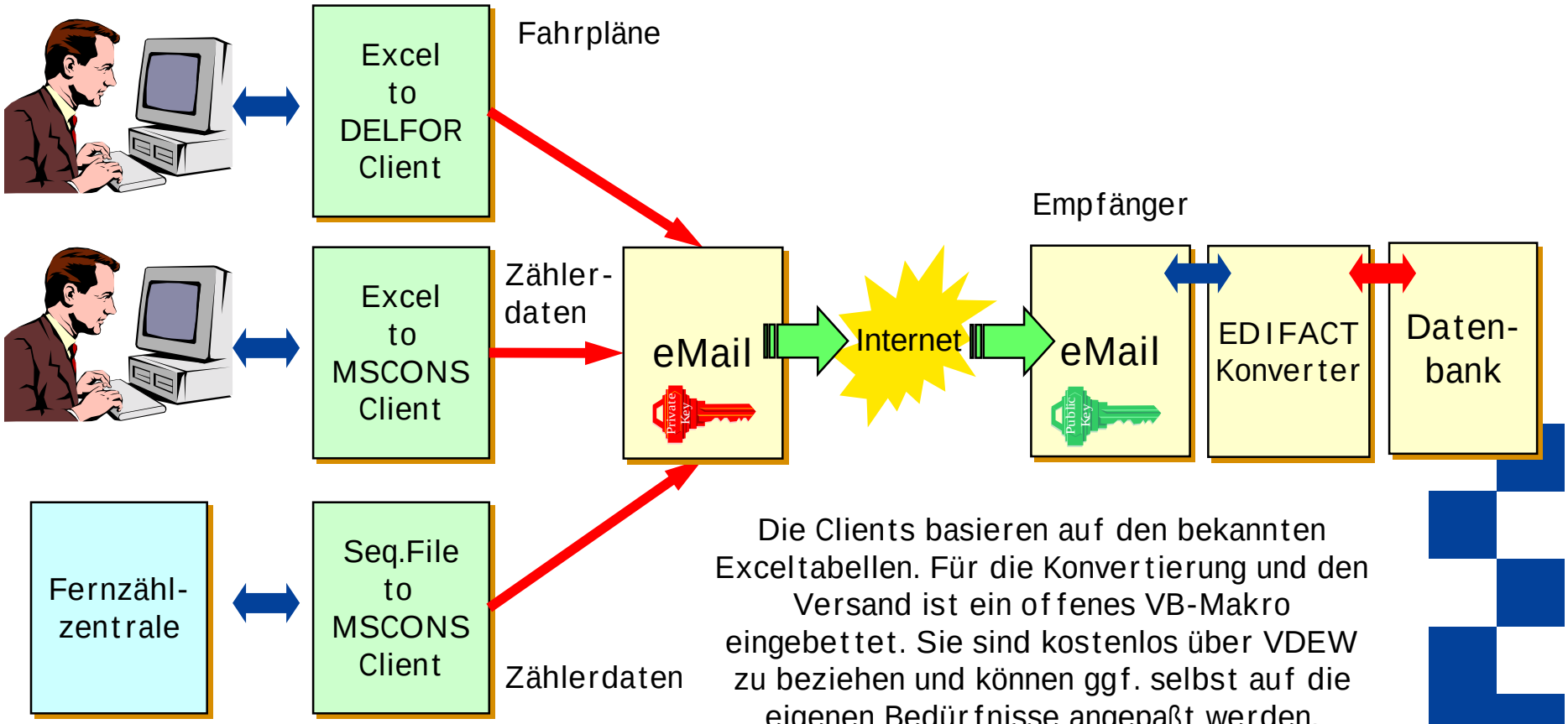
E-Business/PKI Integrationsstrategie



Transportgebundene Sicherheit im Business Partner Network

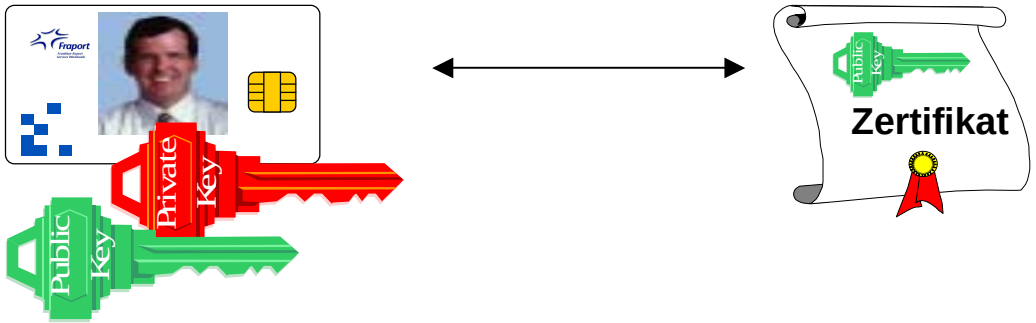
- Verschlüsselung der Leitungen
  - Einsatz von IPSec-Gateways
  - VPN´s im Public Internet bzw.
  - WAN-Verschlüsselung von Standleitungen zwischen Keyplayern
- Mandantentrennung
  - Trennung der Partneradministration
  - ggfs. verbandsmoderierte Zuteilung der IP-Adressen (Routbare Ziele für FW und IPSec-GW)
- Public Key Infrastructure zum Keymanagement auf IPSec-Ebene
  - Digitale Zertifikate für IPSec-Gateways
  - externes Trustcenter

Startup-Prozess: Sichere Übertragung von Marktdaten via S/MIME (ISIS-MTT)



Die Clients basieren auf den bekannten Exceltabellen. Für die Konvertierung und den Versand ist ein offenes VB-Makro eingebettet. Sie sind kostenlos über VDEW zu beziehen und können ggf. selbst auf die eigenen Bedürfnisse angepaßt werden.

Instanzen zur Zertifikatsausgabe



Regeln

PKI-Policy

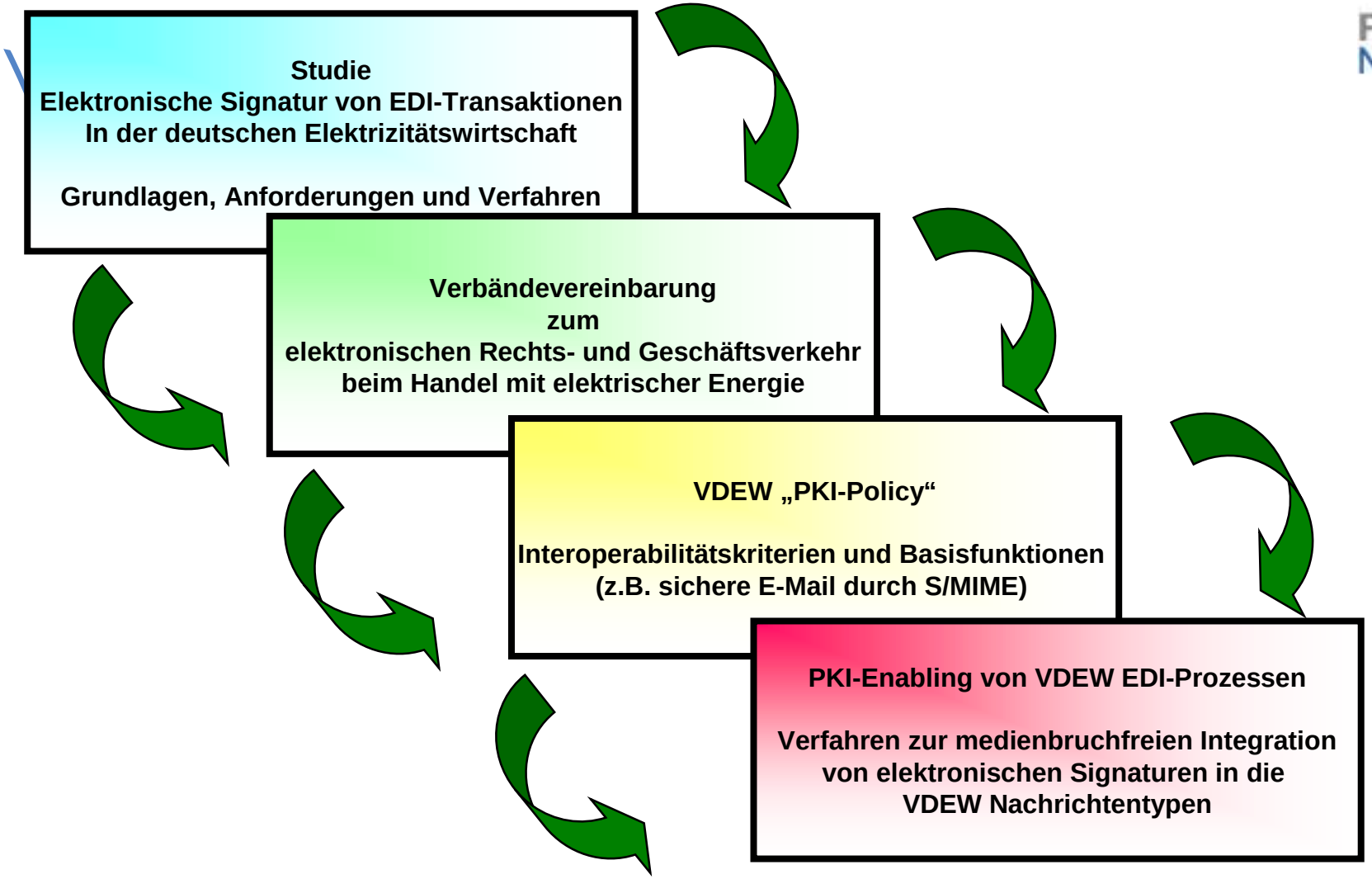
Certification Practice Statement

Certificate Policy

Registrierung
Feststellung der Identität der Anwender,
Ausgabe der Schlüsselpaare, ideal in Verbindung mit Ausweisstelle

Zertifizierung
Erstellung der Schlüsselpaare, Erstellung der Zertifikate
Zuordnung Public Key ⇔ Anwender (el. Signatur der ZS)

Verzeichnis/Directory
Verzeichnis der Anwender und deren Zertifikate/Public Keys
Pflege von Sperrlisten



Vorgehen bei der Einführung von elektronischen Signaturen

Rechtsrahmen und EDIFACT-Nachrichtentypen

Signaturgesetz

- INVOIC, **MSCONS(?), REMADV(?)**

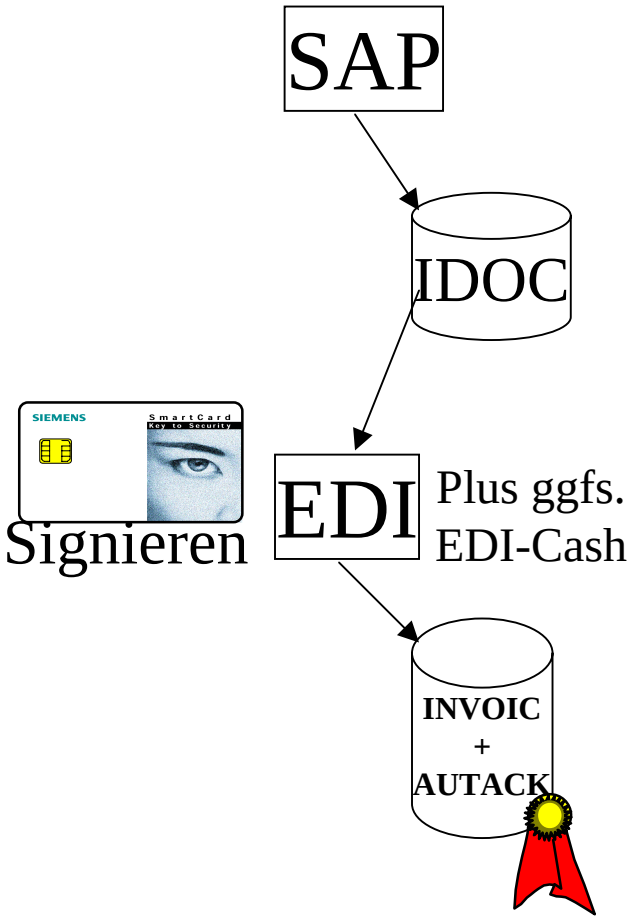
VDEW-Richtlinien

- DELFOR, APERAK, REQDOC, UTILMD

Firmenrichtlinien

- Interne Anwendungen

EDIFACT-immanente elektronische Signatur (AUTACK)

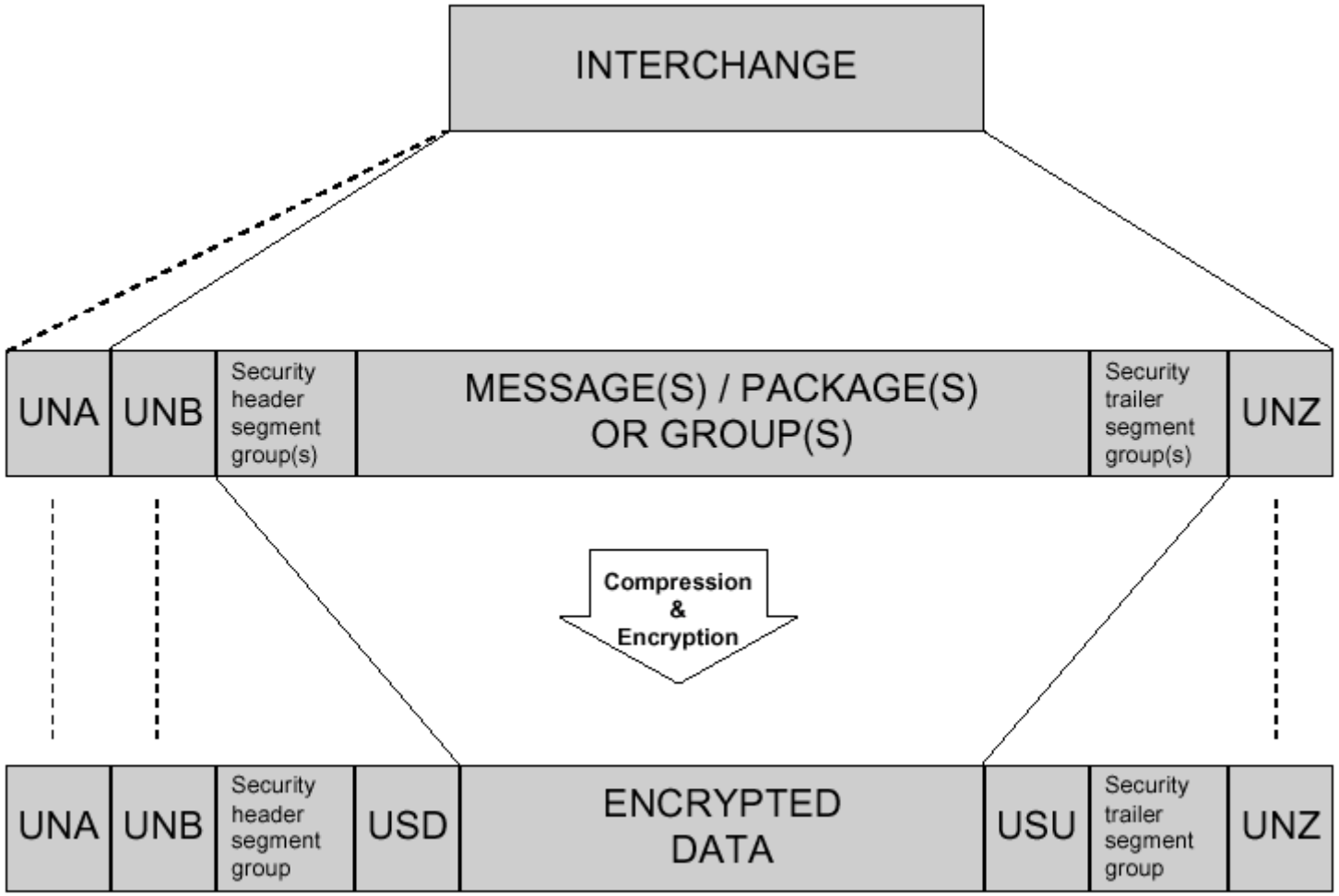


- Die branchenspezifischen EDI-Nachrichtenformate sind bereits normiert
- Mit dem Nachrichtentyp AUTACK liegt eine Nachricht für die EDIFACT-immanente Signatur vor
- Im EDI-System wird mit EDIFACT-Syntax (Authentication_Acknowledge) eine Signatur erzeugt.
- Die AUTACK referenziert die signierten EDIFACT-Nachrichten und wird vom Konverter in den Nachrichtenstrom eingefügt.
- Die Validierung geschieht ebenfalls im Konverter der Empfangsseite, so dass nur minimale Änderungen in den Hostsysteme nötig sind.
- Das Archivsystem muss allerdings auf die neuen Prozessschritte angepasst werden (GDPDU).

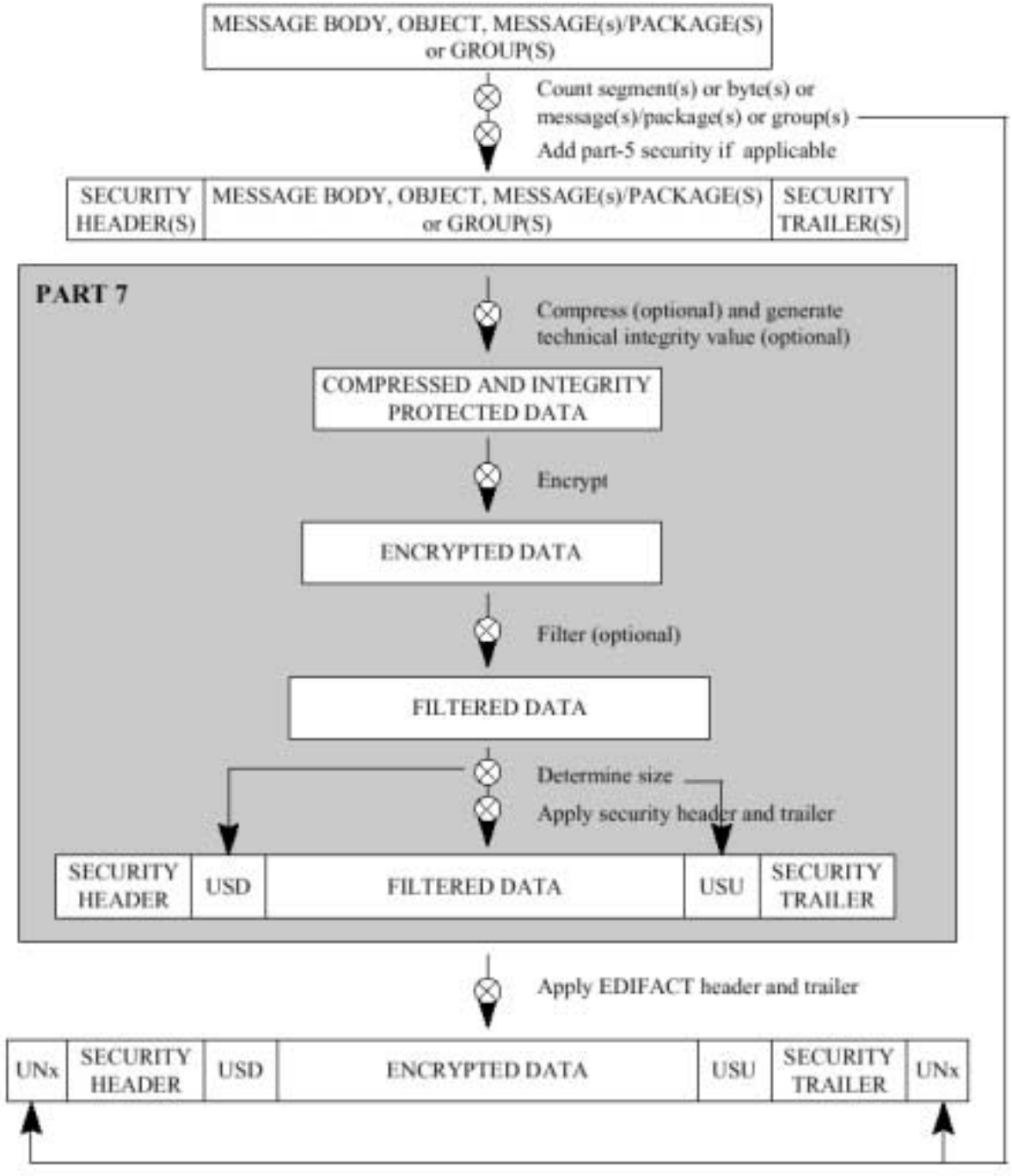
ISO 9735-6 Secure authentication and acknowledgement message (message type - AUTACK)

	POS	TAG	Name	S	R	Notes
Eigensicherung der Nachricht	0010	UNH	Message header	M	1	
	0020	----	Segment group 1 ----------	M	99	-------+
	0030	USH	Security header	M	1	|
	0040	USA	Security algorithm	C	3	|
	0050	-----	Segment group 2 ----------	C	2	----+ |
	0060	USC	Certificate	M	1	| |
	0070	USA	Security algorithm	C	3	| |
	0080	USR	Security result	C	1	----+--+
Payload: Signaturen von anderen Nachrichten	0090	USB	Secured data identification	M	1	
	0100	-----	Segment group 3 ----------	M	9999	----+
	0110	USX	Security references	M	1	|
	0120	USY	Security on references	M	9	----+
Eigensicherung der Nachricht	0130	-----	Segment group 4 ----------	M	99	----+
	0140	UST	Security trailer	M	1	|
	0150	USR	Security result	C	1	----+
	0160	UNT	Message trailer	M	1	

Verschlüsselung von EDIFACT-Nachrichten nach ISO 9735-7



Nachrichten-verschlüsselung nach ISO 9735-7



ebXML: Eine globale XML & EDI Initiative

XML.ORG

The XML Industry Portal
Sponsored by IBM, Sun, Oracle, SAP, ...
A vendor-neutral XML schema clearinghouse.
Info on how to apply XML in industrial and commercial settings.

UN/CEFACT

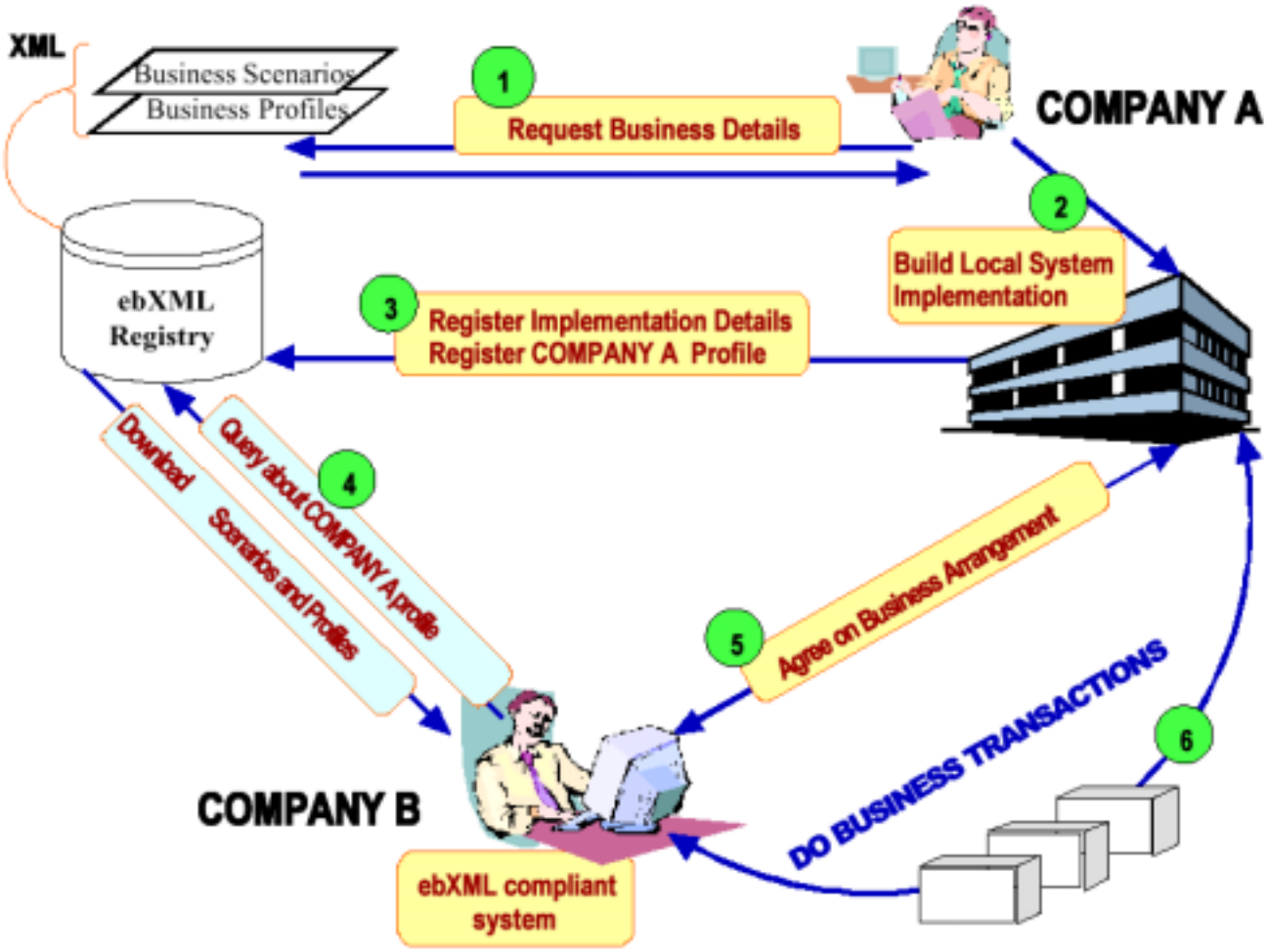
United Nations Centre for the Facilitation of Procedures and Practices for Administration, Commerce and Transport

OASIS
Organization for the Advancement of Structured Information Standards

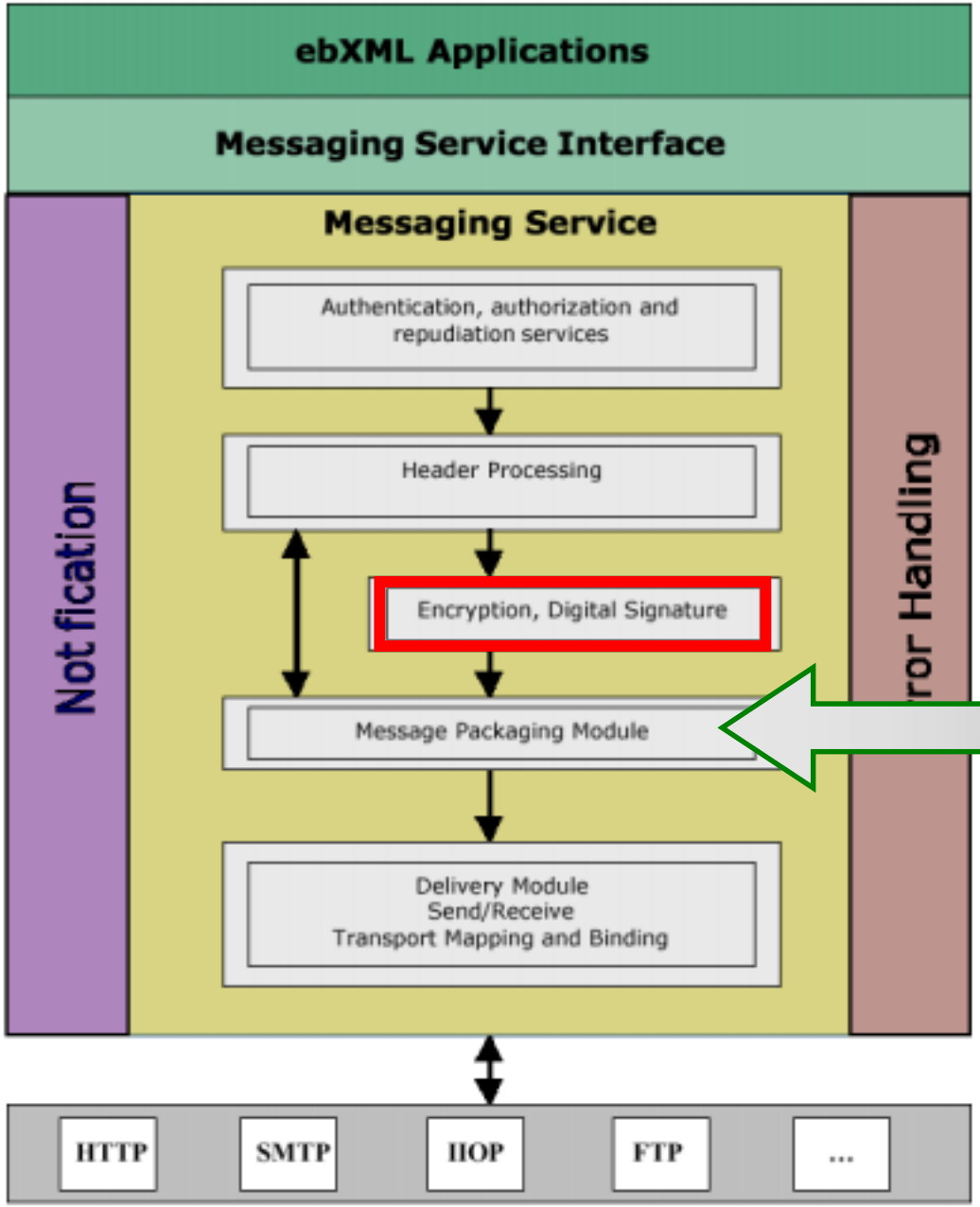
Accelerating the adoption of industry standards
100+ member companies including IBM, Sun, Microsoft, Corel, Software AG, and Oracle.

Aufbau eines e-Geschäftsprozesses nach den ebXML-Regularien

(Schritte 1 bis 6)



ebXML Messaging Services architecture



EDI-Nachrichten in XML-Notation

XML und elektronische Signatur

- Alle branchennotwendigen XML-Formate liegen analog zu EDIFACT vor
- XML-Signaturen sind stabil und genormt
- XML-Signaturen haben möglicherweise gerade in der Stromwirtschaft funktionale und technische Vorteile

Aber:

- Sind die XML-Datenstrukturen bzgl. XMLDSig-Nutzung komplett?

Empfehlungen für elektronische Signaturen:

- Erfahrungshorizont auf signierte XML-Transaktionen ausdehnen
- evtl. Prototyp mit XMLDSig erstellen (Typ 1 und Typ 3)

XML-Signaturen

Der Standard RFC 3075 unterscheidet zwischen 3 Typen von XML-Signaturen:

Nicht-externe Signaturen

externe Signaturen

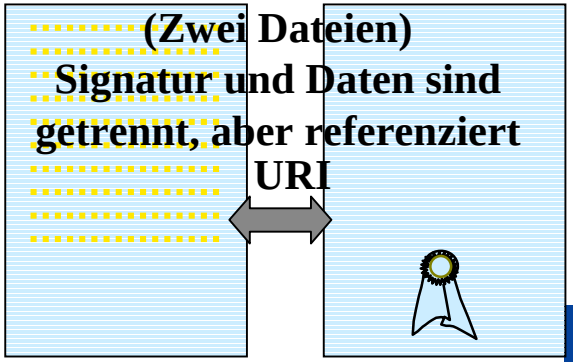
Enveloping signatures

Für neue XML-Anwendungen

Enveloped signatures

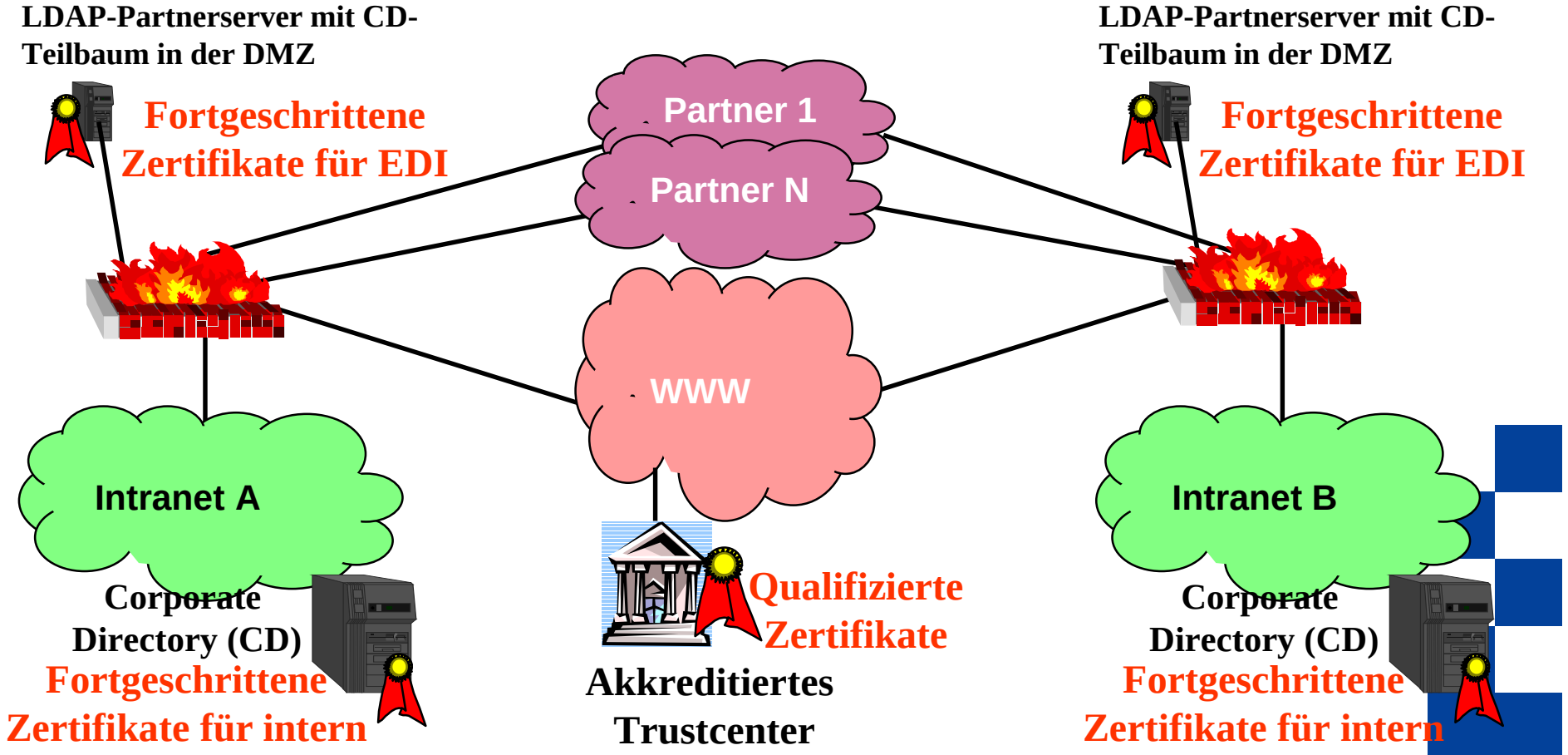
Für Migration-zwecke

Detached signatures



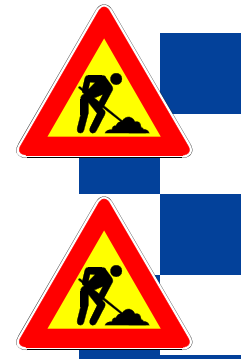
Für Spezial-Fälle (z.B. SW-Verteilung)

Bereitstellung von Directory-Informationen für die Partner



Aktuelle Arbeiten des VDEW AK Sicherheit

- Identifizierung der Themenkomplexe und Handlungsoptionen
- Analyse der Marktanforderungen im Energiemarkt und der politischen, rechtlichen und technischen Situation zur Einführung von Verschlüsselung und elektronischen Signatur als Studie
- Kontakte zu Zertifizierungsdienstleistern und Softwareherstellern
- Verbandsvereinbarung formulieren und Umsetzungsschritte einleiten
- Organisatorische und technische Rahmenbedingungen für die Einführung von informationsgebundener Verschlüsselung und digitaler Signatur bei der Business-to-Business Kommunikation der Marktteilnehmer untereinander definieren



Der VDEW-Arbeitskreis Sicherheit stellt sich vor

Leitung	Beate Becker	VDEW
Mitglieder	Uwe Buntrock	Avacon
	Rolf-Dieter Kasper	RWE Net
	Ralf Knecht	RWE Systems
	Carl Major	EON Energie
	Christoph Matthaeus	EnBW
PKI-Coaching	Dr. Willi Kafitz	Siemens