

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 23.05.2012

Die 'Make or Buy'-Frage

Managed Security Services im Smart Grid

Dr. Willi Kafitz

**SIEMENS Enterprise Communications
GmbH & Co. KG**

Die „Make-or-Buy“-Frage Managed Security Services im Smart Grid

Dr. Willi Kafitz

Berlin, 23. Mai 2012

TeleTrusT-Informationstag, IT-Sicherheit im Smart Grid

Wer bin ich?

SIEMENS

SIEMENS

**Siemens Enterprise Communications
GmbH & Co. KG
Consulting & Design – Business Services**

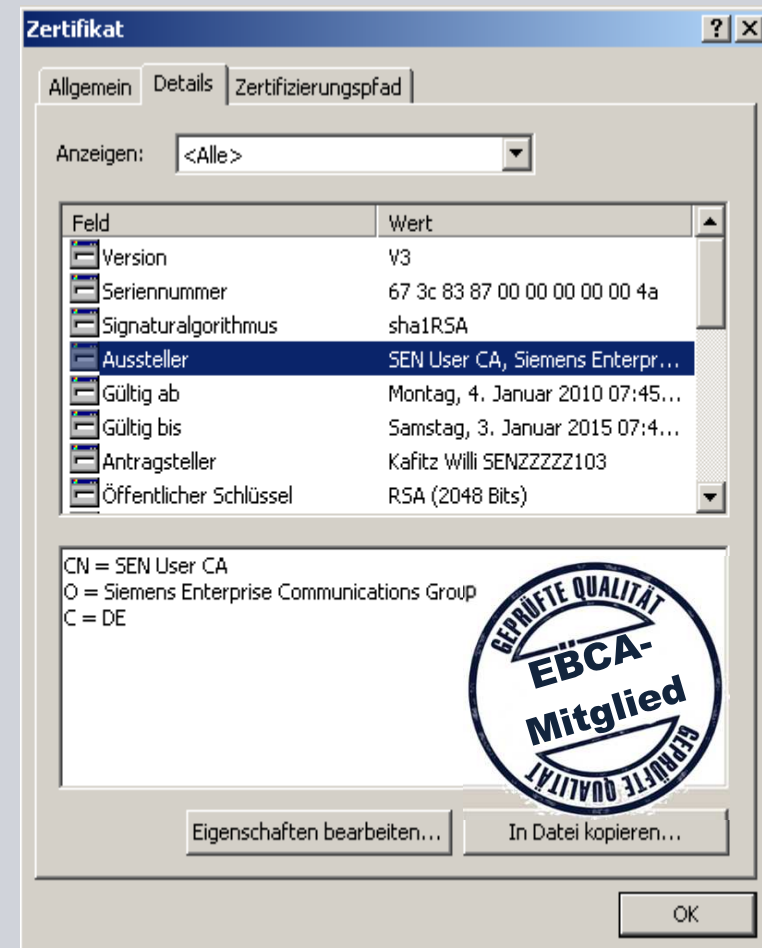
**Office Address:
Lyoner Straße 27
D-60487 Frankfurt/Main
Germany**

**Phone: +49 89 7007 20462
Fax: +49 89 7007 14 20462
Mobile: +49 171 33 59 187
E-Mail: willi.kafitz@
siemens-enterprise.com**

Dr. rer. nat. Willi Kafitz

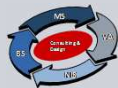
Lead Consultant

Siemens Enterprise Communications GmbH & Co. KG
is a Trademark Licensee of Siemens AG



Unsere Spitzenposition in Zahlen

75 %	aller Global-500-Unternehmen vertrauen unseren Lösungen.
160 Jahre	Lieferant führender Kommunikationstechnologien.
720	offizielle Vertriebspartner rund um die Welt nehmen am preisgekrönten weltweiten Partnerprogramm „Go Forward!“ teil.
1000	Installierte Endgeräte pro Tag.
12.000	Mitarbeiter kümmern sich um direkte und indirekte Kunden in 80 Ländern.
150.000	Anrufe pro Minute gehen von unseren Produkten aus.
> 1 Mio.	Kunden in praktisch allen Branchen nutzen unsere Dienstleistungen.
3.000.000	Sprach- und Datenanschlüsse werden weltweit von uns betreut.



Marktführer

Überragende Marktanteile, überall auf der Welt



Quelle: MZA, Corded PBX-IP PBX (2009, Welt, März 2010)



Agenda



- **Ausgangslage**
- **Neue Anforderungen**
- **Managed Security Services und Cloud Services**
- **Fazit**



Agenda



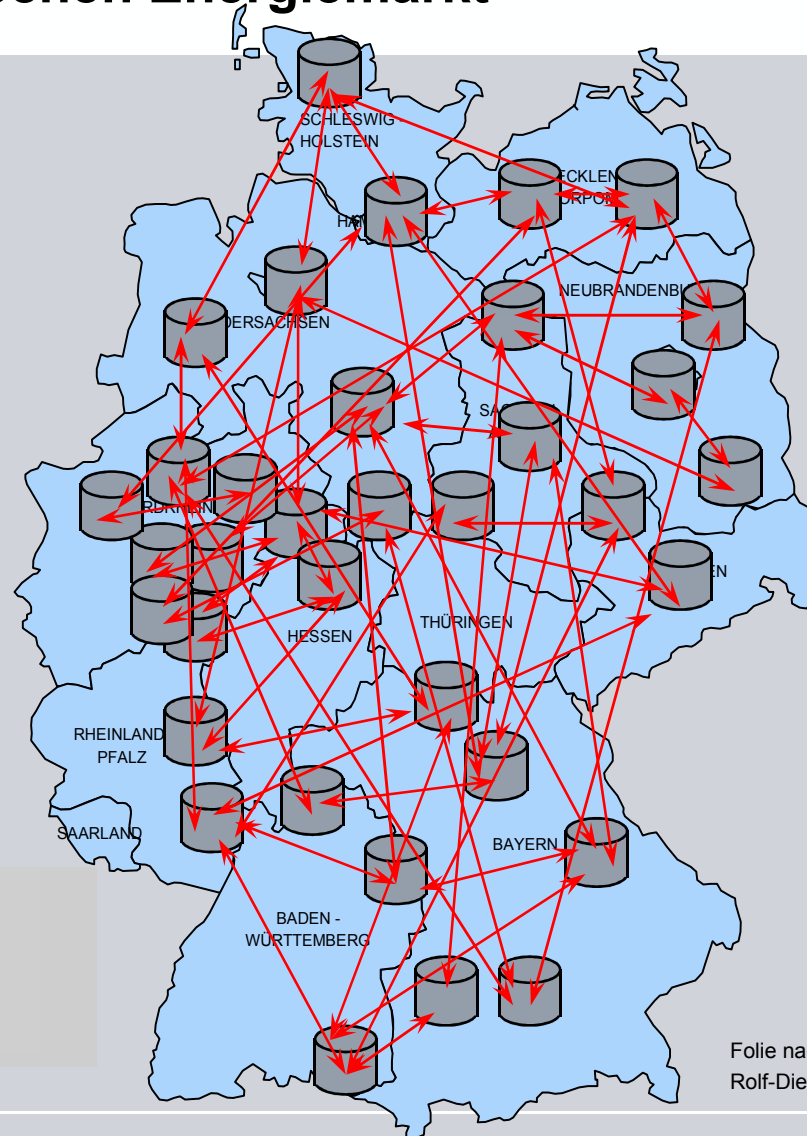
- **Ausgangslage**
- Neue Anforderungen
- Managed Security Services und Cloud Services
- Fazit



Informationsaustausch im deutschen Energiemarkt

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

heute ca. 10 Mrd.
Nachrichten / Jahr



Folie nach
Rolf-Dieter Kasper

Sicherheit beim Datenaustausch in der deutschen Energiewirtschaft: Das BDEW-Projekt VEDIS



**Vertrauen / Verbindlichkeit & Sicherheit / Signatur im
Electronic Data Interchange**

Technik

**S/MIME-Zertifikat, fortgeschrittene elektronische Signatur, verschlüsselter Transport
Asynchron per E-Mail über SMTP oder synchron per AS2 über http (präferiert)**



Veränderung des Rollenmodells im Strommarkt durch Regulierung

Heutige Marktschnittstellen

- Bestehende Rollen werden beibehalten bzw. an Smart Grid Bedürfnisse angepasst
Händler, Lieferant, Bilanzkreis-
verantwortlicher, Messstellenbetreiber,
Messdienstleister, Erzeuger, Verteil-
netzbetreiber, Übertragungsnetzbetreiber
- Der liberalisierte Markt wird heute
mit 5 Nachrichtentypen abgebildet
UTILMD: Stammdaten
DELFOR: Fahrpläne
MSCONS: Zähldaten
REMADV: Zahlungsavise
INVOIC: Netznutzungsrechnung
➔ knapp 10 Mrd. EDI-Transaktionen pro Jahr
- EAN-Codes symbolisieren das vorwiegend
zentral erzeugte Handelsgut Strom
- Daten werden kettenförmig weitergegeben

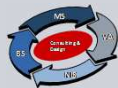
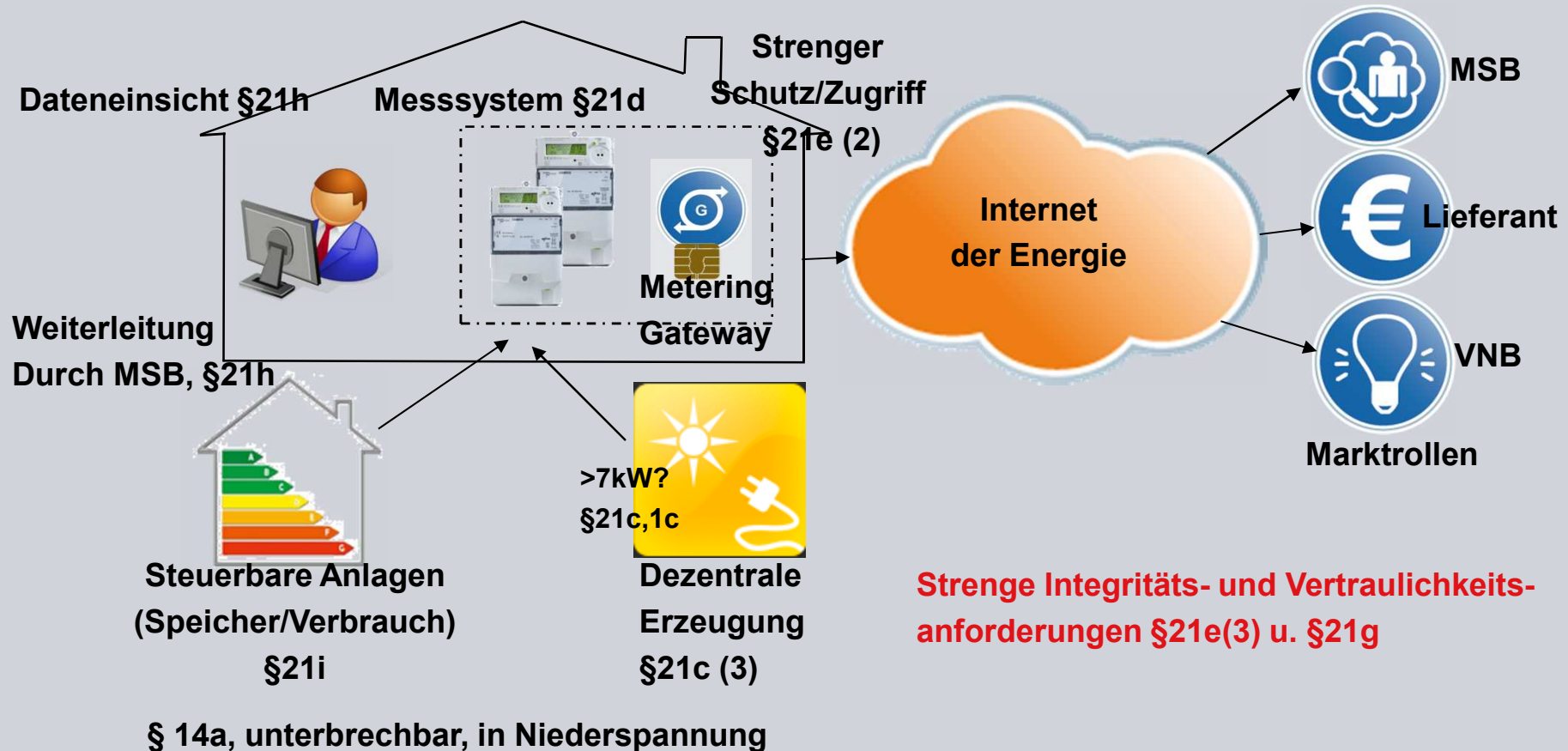
Zukünftige Marktschnittstellen

- §21 EnWG regelt Verantwortung
- Beim IKT-Gateway beginnt Smart Grid:
Datenkommunikation und Schutzprofil
reguliert, Eigentümer offen
- Alle autorisierten Rollen erhalten
unprivilegiert Daten
- Viele offene Fragen (Verifikation der
Netznutzung, Ersatzwertbildung,
Anonymisierungsvorgehen, etc.)
- Datenkommunikation erfolgt sternförmig

Neuer Rechtsrahmen für Messsysteme im Energiemarkt ist sicherheitsgetrieben

SIEMENS

Quelle: EnWG vom 27.07.2011, Konsequenzen aus §21 ff



Agenda



- Ausgangslage
- **Neue Anforderungen**
- Managed Security Services und Cloud Services
- Fazit



Veränderung der Kompetenzfelder durch Smart Grid

Heutige Kompetenzen

- Selbstverständnis noch stark geprägt über Energie als Produktlieferung
- IKT kaum primärer Wertschöpfungsfaktor (Bürokommunikation, Verwaltungsinstrument)
- Elektrotechnische Kernkompetenz dominiert; kaum Digitaltechnik in den Verteilnetzen
- Security vorwiegend als Perimetersicherheit
- Verbrauchsorientierte Erzeugung beherrschen

Zukünftige Kompetenzen

- Wertschöpfung über optimale Distribution von Energie als Dienstleistung
- Digitale Kernkompetenzen werden zunehmend Bestandteil des Kerngeschäftes
- Smart Grid als Digitalisierungsschub für Process IT (PIT) und Commercial IT (CIT)
- Datenschutz / Datensicherheit erzeugen erheblichen Schutzbedarf auch im Netz
- Erzeugungsorientierter Verbrauch beherrschen



Veränderung der Security-Anforderungen durch Smart Grid



Heutige Anforderungen

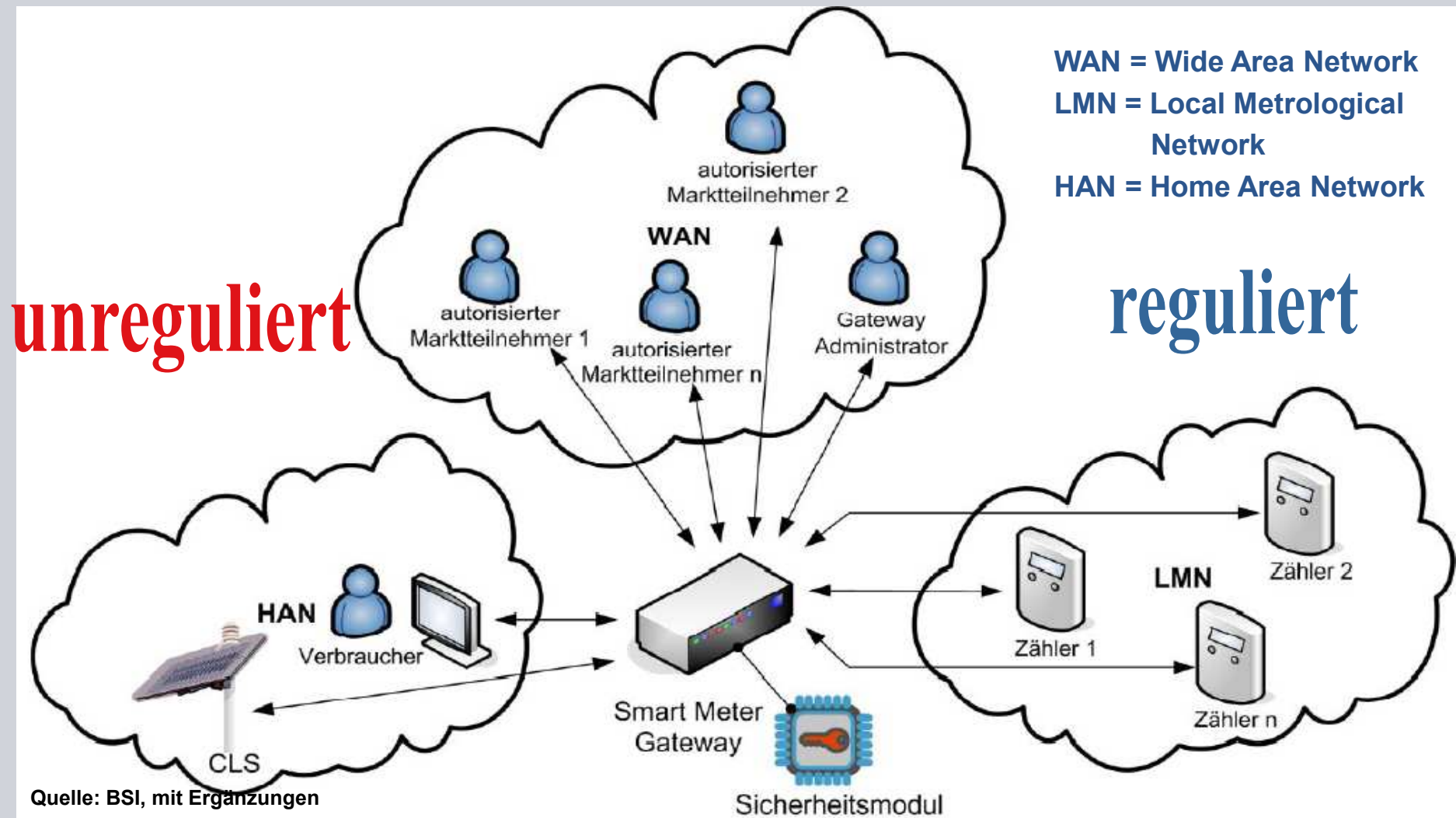
- Marktschnittstellen mit VEDIS-Sicherheit
- Verteilnetze haben heute praktisch keine IT-Security-Anforderungen
- Security in EVU's besteht vorwiegend als Perimetersicherheit
- Durchaus Anforderungen in der Process IT (siehe auch ISO DIN 27009)
- Ein bis wenige PKI-Zertifikate reichen für VEDIS-Sicherheit aus

Zukünftige Anforderungen

- Marktschnittstellen mit Gateway-Sicherheit
- Datenschutz / Datensicherheit erzeugen erheblichen Schutzbedarf auch im Netz
- Cyber War Szenarien müssen im Internet der Energie unbedingt verhindert werden
- Alleine in IKT-Gateways werden Millionen Zertifikate zu managen sein
- Sichere Betriebsprozesse stellen eine organisatorische und wirtschaftliche Herausforderung dar



Positionierung des Smart Meter Gateways



Quelle: BSI, mit Ergänzungen

Sicherheitsbetonte Regulierung als Startschuss für Energiewende

SIEMENS

Politische Anforderungen

- Entflechtung der bestehenden Markttrollen
- IKT-Gateway als Schnittstelle zum “Internet der Energie”
- Differenziertes Rollenmodell und damit verbundener Datenfluss
- IKT-Gateway unterliegt Common Criteria Protection Profile (Sicherheitslevel)
- Technische Richtlinie in Arbeit (Interoperabilität)
- Neues Rollenmodell bestimmt hohe Kryptographieanforderungen bei Authentifizierung und Verschlüsselung (PKI)
- Cyber War Ängste definieren hohes Sicherheitslevel (Chipcard = EAL 4+)

Allgemeine Entwicklungstendenzen

- Neue Markttrollen entstehen
- Akzeptiert von allen westlichen Industrienationen, mind. europaweiter Standard
- Mandantengerechter Datenversand
- Betriebsverantwortung bei Messstellenbetreiber
- Kommunikationsinitiative von innen bedeutet massive Änderungen in Betriebsprozessen
- Neue Marktprozesse bei Zähladataustausch (Verbrauchsdaten)
- Umfassende gesetzliche Verankerung



Status der derzeitigen (Smart) Grid-Security-Diskussion

SIEMENS

Process Information Technology (PIT)

- Safety-Aktionen / Reaktionen $\ll 1$ sec keine performante Verarbeitung einer elektronischen Signatur möglich
- Abschaltvorgänge < 20 millisec
- Keine Kryptographie in der innerstationären Prozesstechnik
- Nur Kommunikation dezentral – zentral wird gesichert
- Autonome Behandlung der Prozessleittechnik notwendig, kein Zugang zu öffentlichen Netzen
- Für nicht-kommerziellen Bereich werden bestehende und zukünftige Standards genutzt (IEC 61850)

Commercial Information Technology (CIT)

- Security-Aktionen / Reaktionen > 1 sec Signatur/Verschlüsselung möglich und sinnvoll
- Metering
- Tarifierung in jeder Form
- Controllable Local Systems
- Remote Grid Control
- Differenzierung über Value Added Functions (demand response, demand side management)



Das Gateway steckt voller moderner Kryptographie

Sicherheitsfunktionen

- Signaturerzeugung
- Asymmetrische Verschlüsselung
- Assistenz bei der Aushandlung von Session-Keys
- Signaturprüfung
- Asymmetrische Entschlüsselung
- Erzeugung von Zufallszahlen
- Sichere Speicherung von privaten Schlüsseln

TLS

- Gegenseitige Authentisierung der Parteien:
 - RSA 2048 oder ECDSA 256 (Brainpool Random Curve)
 - SHA-256
- Schlüsselaushandlung
 - Diffie-Hellmann klassisch
 - Diffie-Hellmann ECDH
- Symmetrische Verschlüsselung
 - AES 128 CBC MAC

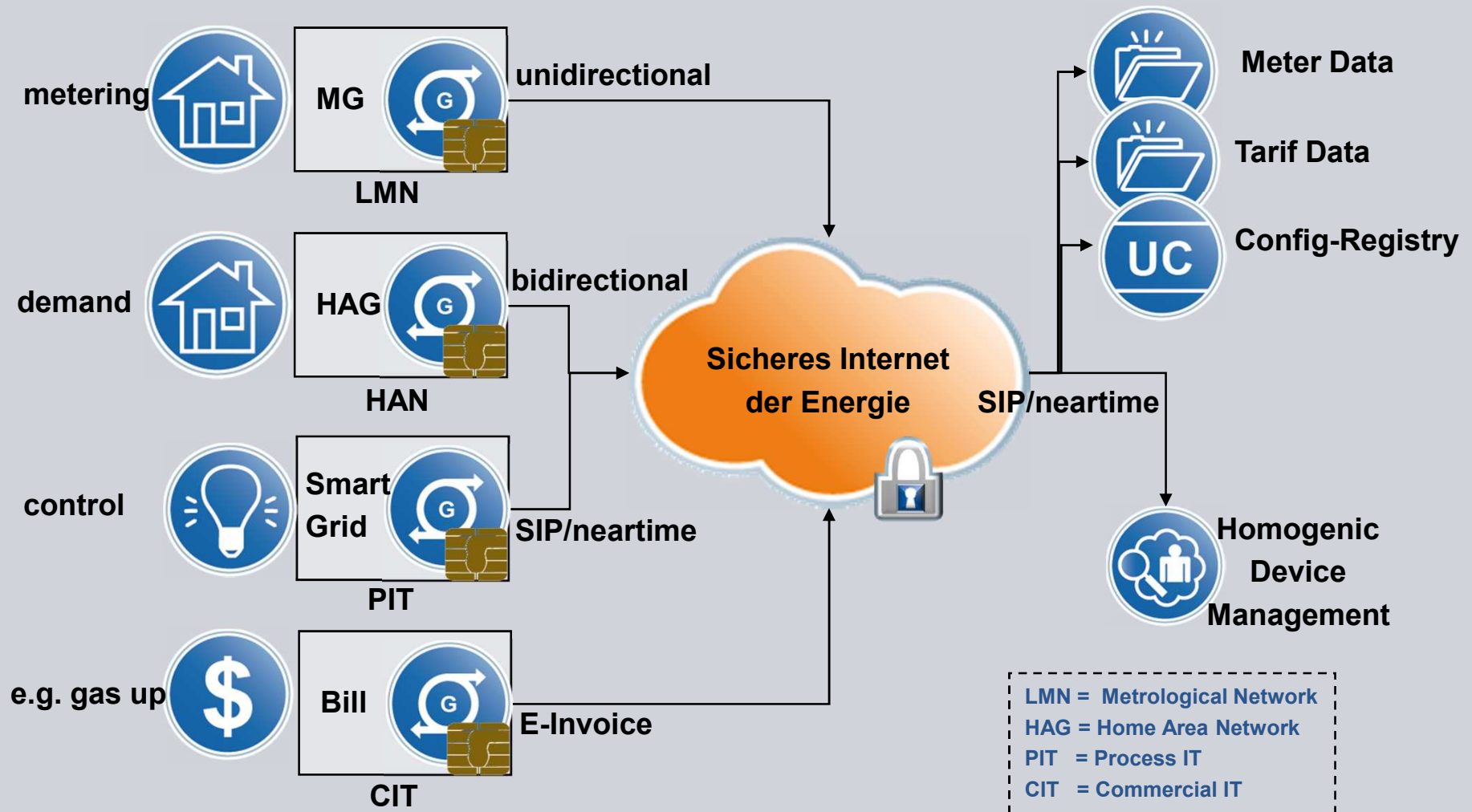
PKCS

- Verschlüsselung und Signatur nach PKCS#7
- Symmetrische Verschlüsselung:
 - AES 128 CBC
- Asymmetrische Verschlüsselung
 - RSA 2048
 - ECC 256
- Signatur
 - RSA 2048 oder ECDSA 256 (Brainpool Random Curve)
 - SHA-256



Sicherheit betrifft nicht nur Metering: Segmentierung der Grid-Kommunikation

SIEMENS



Anforderungen an die Sicherheitsinfrastruktur machen Managed Security Services im Smart Grid sinnvoll

SIEMENS

Klassische Internet Security



- Firewalling**
- Intrusion Prevention**
- Network Access Control**
- Virenschutz**
- Remote Access**

Authentisierung nach Marktrolle



- Messstellenbetreiber als administrative Rolle (Betrieb, Eichung, Feldservice)**
- Lieferant (Zählzeiten als Endrechnungsgrundlage)**
- Verteilnetzbetreiber (Verifizierung der Netznutzungsrechnung)**



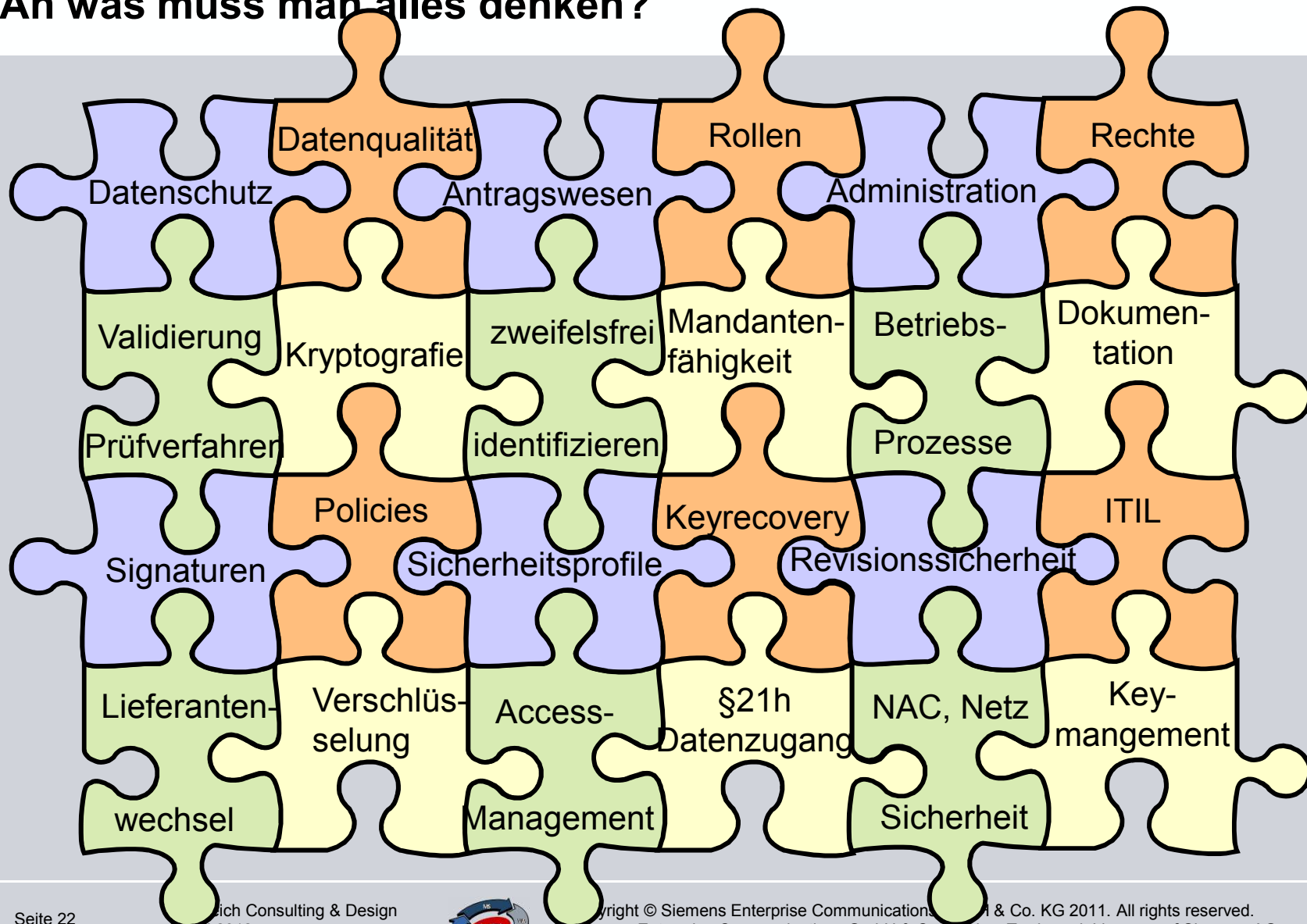
Agenda



- Ausgangslage
- Neue Anforderungen
- **Managed Security Services und Cloud Services**
- Fazit

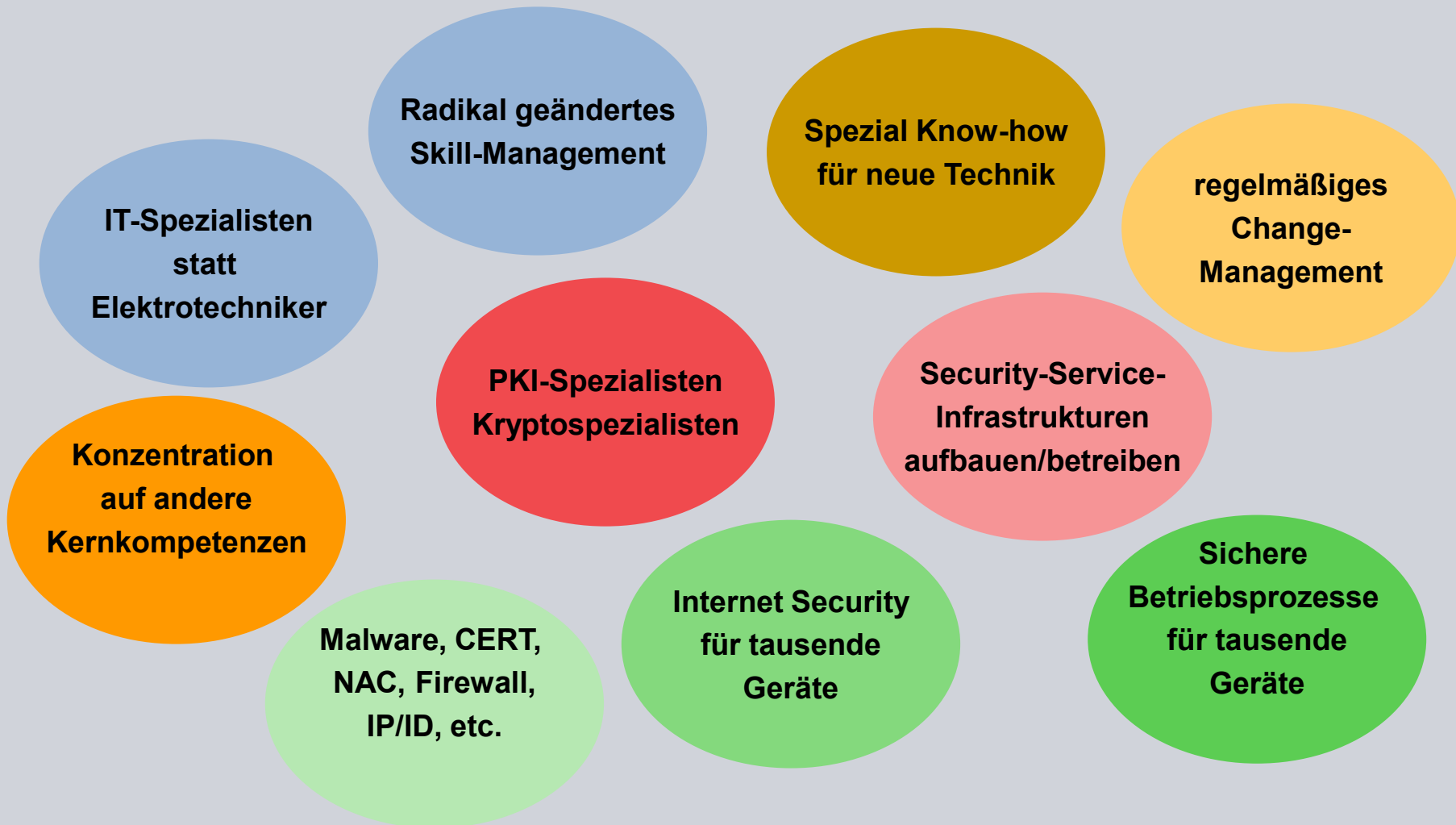


An was muss man alles denken?



Die Make-or-Buy-Frage bei Personal und Infrastruktur

SIEMENS



Smart Grid Managed Security Services

SIEMENS

Anforderungen

- Verwaltung der Sicherheitsfunktionen der eigenen IKT-Gateways und weiterer aktiver Komponenten
- Abwickeln der Geschäftsprozesse / Use cases mit Sicherheitsauswirkungen (Lieferantenwechsel, Umzug, Mieterwechsel, Wechsel Zählerdienstleister, etc.)
- Verwaltung der Rollen / Rechtezugriffe im Rahmen der Marktschnittstellen

Wertbeitrag Siemens Enterprise Communications

- Verwaltung der IKT-Gateways als IP-Devices unter IT-Security Aspekten
- Identity-Management der IKT-GWs (zertifikatsbasiert gemäß CC PP)
- Verwaltung der zertifikatsbasierten Rollen / Rechtezugriffe im Rahmen der Marktschnittstellen (PKI-Funktionen)
- Malware-Schutz
- Firewall-Administration
- Intrusion Prevention / Intrusion Detection
- Wahrnehmen der CERT-Funktionen (Computer Emergency Response Team)

Smart Grid benötigt fundierte Security Services



„You can't manage, what you can't measure.“

Messen, Analysieren, Berichten,
Bewerten, Planen, Handeln

Service Management
liefert jederzeit wichtige
Management Informationen
für schnelle, richtige Entscheidungen

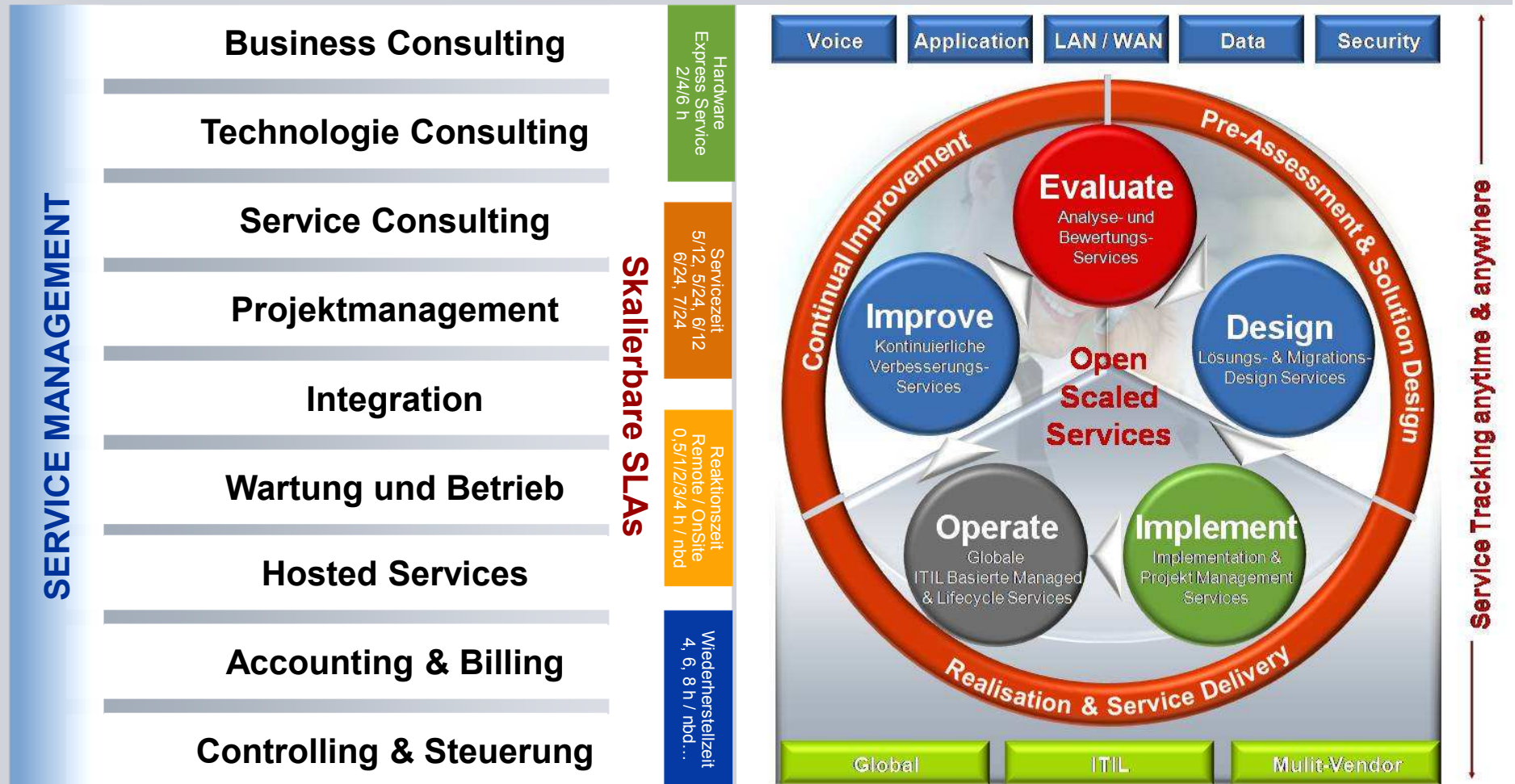
OPTIMIEREN

Permanenter Fokus: Continual Service Improvement



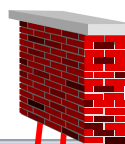
Erfahrungen im Service Management übertragen

Drehscheibe über alle Elemente und Zyklen eines Services



Professionelle Operation Services auf Smart Grid Anforderungen übertragen (Monitoring)

Network Operation Center



„Secure tunneling“



Permanente Systemüberwachung

- Permanente, automatische Datenauswertung
- Sofortige Incidentidentifikation (24/7)
- Direkte Weitergabe mit Priorität an den Service Desk

Automatische Fehlererkennung

- Automatische Ticketgenerierung
- Früherkennung von Ausfällen
- Minimierung der Ausfallzeiten
- Direkte und schnelle Reaktion auf Incidents

Aktive Benachrichtigung bei Incidents

- Sofortige Information bei Incidents
- Minimierung des Störungsmeldeaufwandes

Proaktive Reaktion auf Incidents

- Minimierung der Auswirkung für Mitarbeiter
- Maximierung der Systemverfügbarkeit
- Keine zeitliche Verzögerung zwischen Meldungseingang und Bearbeitung

Agenda



- Ausgangslage
- Neuer Rechtsrahmen
- Managed Security Services und Cloud Services
- **Fazit**



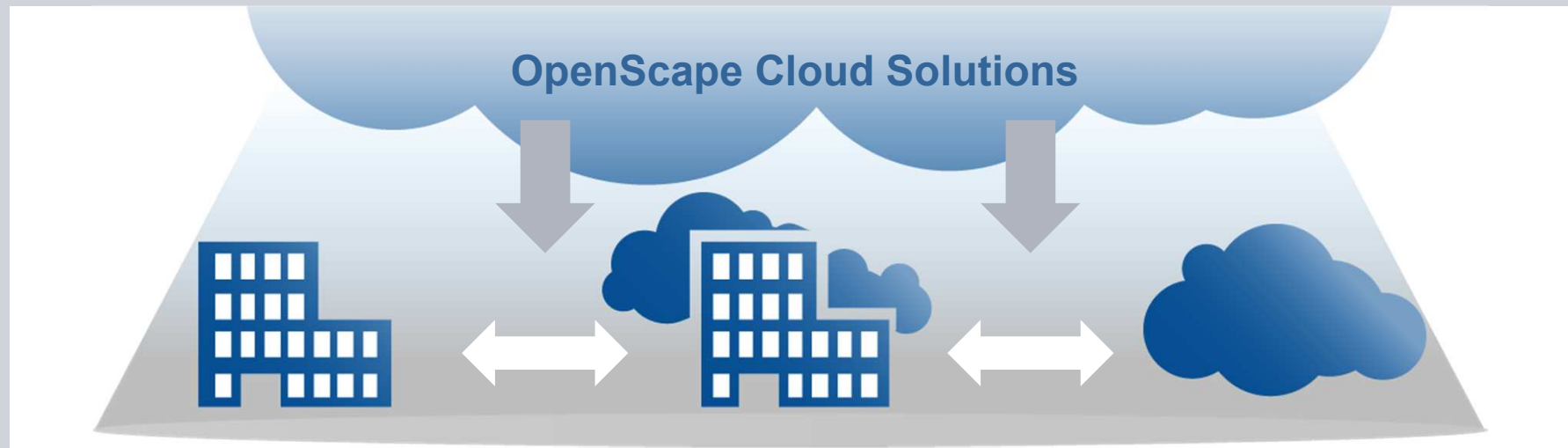


- **Sicherheit treibt den ersten Schritt der Energiewende**
 - **IKT-Sicherheitsinfrastrukturen müssen neu aufgebaut werden**
 - **Die Frage MAKE OR BUY ist nicht allein entscheidend**
 - **Wieviel Kernkompetenz IKT braucht Kernkompetenz Energie?**
 - **Auch Managed Security ist ein Business Enabler**
 - **Entscheidend ist das Kerngeschäft**



Understanding the Vision – Cloud Services im Smart Grid

SIEMENS



Premise-based options

- Ownership Primärnetz
- Große Kapitalbindung
- Kernkompetenz Energiemanagement
- Process IT
- Tiefe Geschäftsprozess-integration und Anpassungs-potential

Hybrid options

- Isolierte Applikationen, wie Registrarfunktionen, können problemlos aus der Public Cloud kommen.
- Private cloud als exzellente Option für mittlere und große Kunden um zu zentralisieren und zu standardisieren.

Cloud options

- 'Pay-as-you-go' Orientierung
- Geringes Kapitalinvestment
- Schnelle Verfügbarkeit
- Einfaches Management
- Zukunftssicher
- Gute Skalierbarkeit
- Packaged offerings



SIEMENS

The End

Thank you!



Fragen ?

SIEMENS

