Fraunhofer FOKUS

Coud Computing und eGovernment

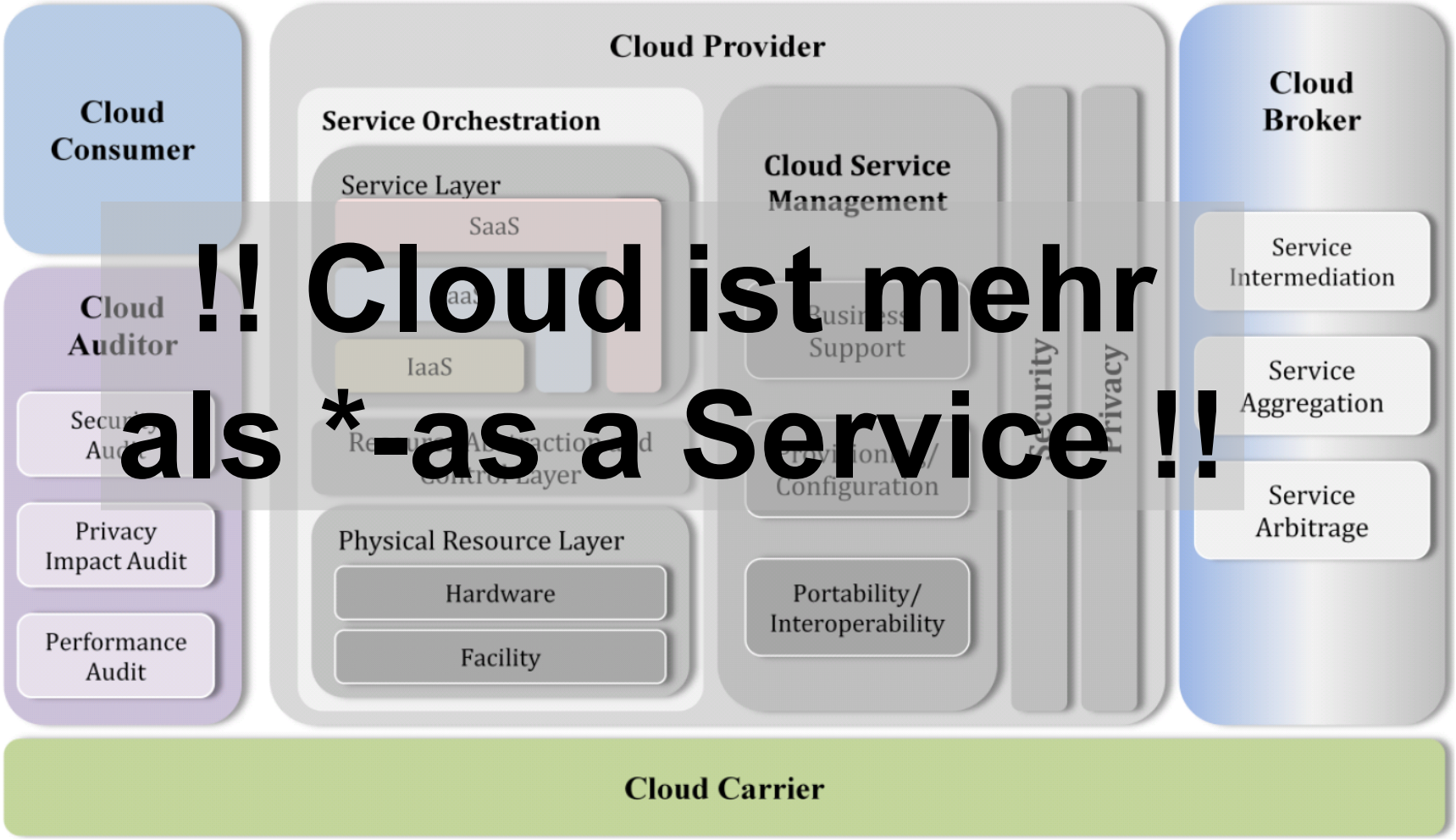
Linda Strick
Fraunhofer-Institut für Offene Kommunikationssysteme

Fraunhofer FOKUS

Was ist Cloud Computing?

Technische Rahmenbedingungen

Cloud Referenzarchitektur von NIST (6-2011)



!! Cloud ist mehr als *-as a Service !!

Cloud Computing Komplexität

Eigenschaften

Validation der Dienstgüte durch den Kunden; Optimierung durch den Betreiber

Mandantenfähiger Bedarfsbetrieb auf Anforderung / pay-as-you-go

Überall verfügbar (auch von mobilen Endgeräten)

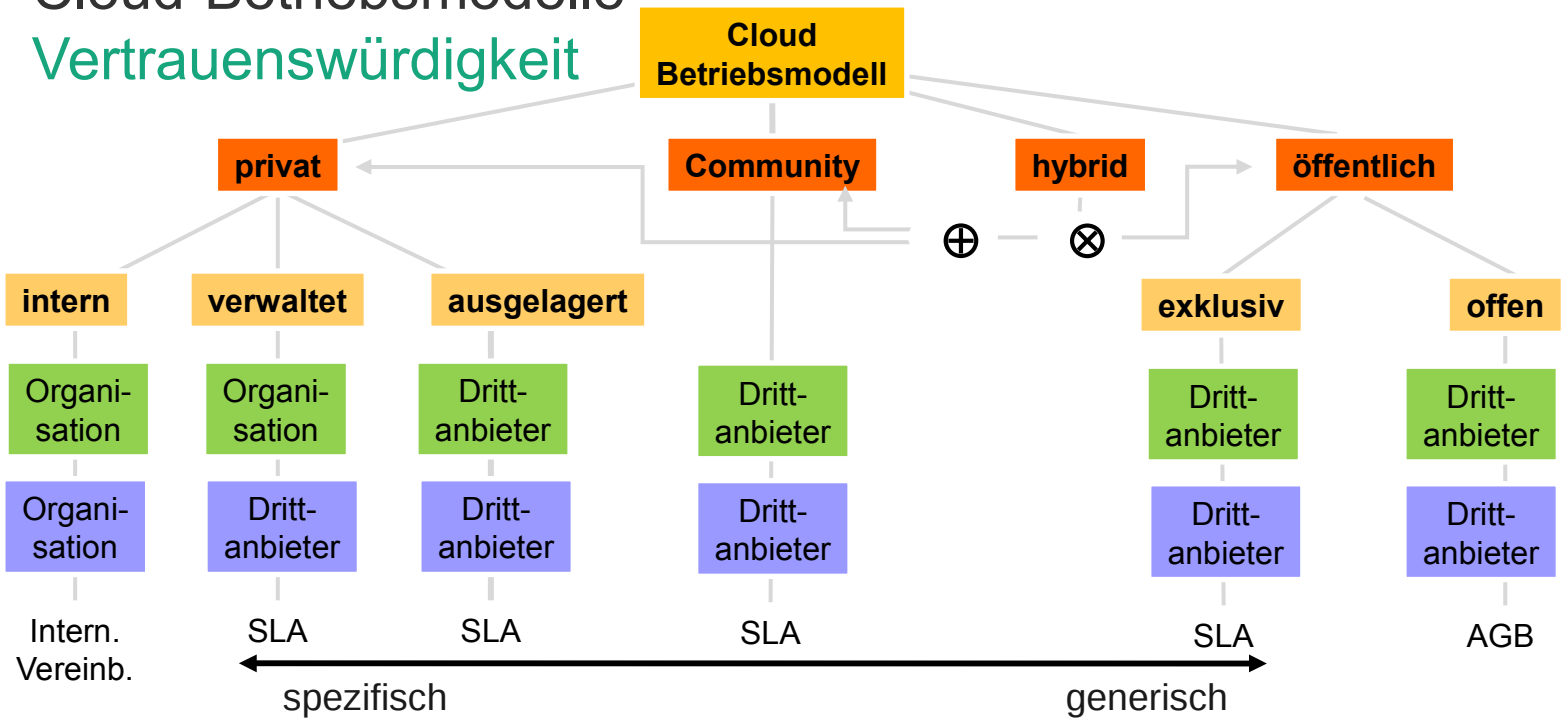
Im Kern: Umfassende Automatisierung

- **Homogenisiertes Systemmanagement**
- **Automatisiertes Dienstmanagement**
  - Provisioning & Deprovisioning
  - Monitoring
  - Lifecycle Management
  - Event- & Failure-Management, etc.
  - Ressourcenallokation
- **Weitreichende Protokollierungsmechanismen**

Bedarfsgerechter Verbrauch mit dynamischer Skalierung

Ortsunabhäng
Ressourcenve
(Virtualisierun

Cloud-Betriebsmodelle
Vertrauenswürdigkeit



	vertrauenswürdig		**nicht vertrauenswürdig**	
Technische Details	- eigene Infrastruktur - Selbt oder durch Dritten betrieben - „klassisches“ Outsourcing	- Infrastruktur und Betrieb bei Provider - Zentralisierte Architektur	- Infrastruktur und Betrieb gemeinsam genutzter Resourcen bei Provider (Multi-Client.Plattform)	- Öffentliches Internet - dezentralisierte weltweite Architektur auf Infrastruktur des Providers
Kontrolle der Daten	- Daten bleiben unter physischer Kontrolle des Auftraggebers - Aber: Provider hat evtl. Zugriff (z.B. Remote)	- Daten unter Kontrolle des Providers - Aber: Daten auf abgegrenzten Ressourcen	- Daten unter Kontrolle des Providers - Aber: Daten auf abgegrenzten Resourcen	- Infrastruktur und Betrieb bei Provider - Zentralisierte Architektur

Cloud Computing – Kontrolle

Cloud Kunde – Cloud Anbieter Verhältnis

Steuerung und Entwicklung beim Cloud-Kunden

Software as a Service (SaaS)

e.g. Google-Apps for Business, Microsoft CRM , Salesforce.com,

Platform as a Service (PaaS)

e.g. Force.com, Google-App Engine, Microsoft Azure, ORACLE

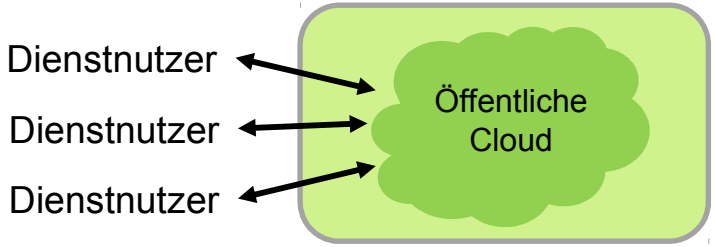
Infrastructure as a Service(IaaS)

e.g. Amazon EC2 + S3, AppNexus, HP Cloud Enabling Computing, ORACLE, IBM, SUN, Hadoop

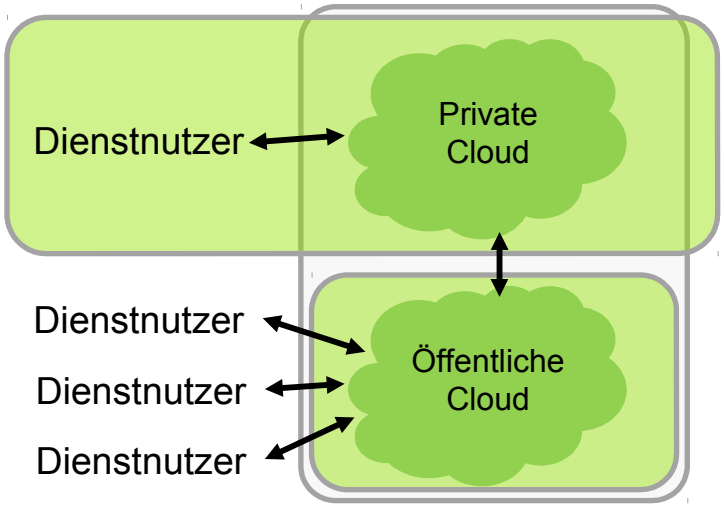
Steuerung und Entwicklung beim Cloud Anbieter

Cloud-Betriebsmodelle

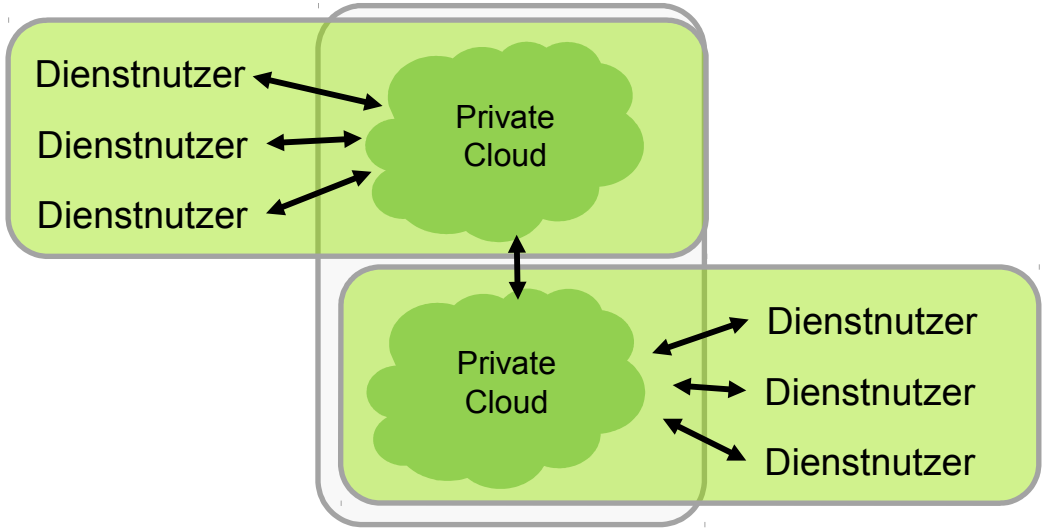
Private Cloud: Hauseigenes RZ oder dedizierter Dienstleister



Öffentliche Cloud: Standardisierte Dienstleistungen für Jedermann



Hybride Cloud: Private Cloud mit öffentlichem Anteil



Community-Cloud: Zusammenschluss/Kooperation privater Clouds

Fraunhofer FOKUS

Welche Anforderungen hat der öffentliche Sektor Sicherheit, Datenschutz, Compliance, Governance

Hindernisse für den Einstieg in die Cloud

Sicherheit in der Cloud

- Für den **öffentliche Sektor** gelten besondere Anforderungen
  - Kontrolle über die Aufgabenwahrnehmung und -durchführung
  - Datenschutz, etc.
- Wirtschaftliche Überlegungen kommen erst an zweiter Stelle

Organisation

- Multiple Standorte
  - Redundante Daten und Prozesse
- Verteilte Datenhaltung
  - Absicherungsmechanismen auf Netzwerkebene
- Einheitliches Sicherheitskonzept
  - Zeitnahe Aufdeckung von Schwachstellen und Durchsetzung von Gegenmaßnahmen
- Dediziertes Expertenteam
  - Konsolidiertes und effektives Bedrohungsmanagement
  - Verkürzte Reaktionszeiten

Cloud-Technologie

Einheitliche Sicherheitsmechanismen
- Failover Mechanismen
- Desaster Recovery
- Redundante Ressourcen

Adaptive Ressourcenskalierung

Standardisierte Schnittstellen für Sicherheitsmanagement

Anforderungen
Datenschutz

- Beachtung rechtlicher Aspekte und Regularien
  - Gültige nationale Rechtsprechung bei der Verarbeitung personenbezogener Daten
- Trennung von Personendaten und Systemverwaltung
- Nachvollziehbare Mandantentrennung
  - Sichere Ressourcenteilung
  - Maßnahmen zur Datenlöschung
- Effektive Zugriffsmechanismen (Self-Service)
  - Rechte- und Rollenmodel

Anforderungen
Governance

- Wirtschaftliche Vorteilhaftigkeit
  - Leistungsadäquanz
  - Kosteneffizienz
- Steuerbarkeit
  - Service Level Agreements
  - Durchgängiges Rollenmodell (definiert Rechte und Pflichten)
  - Vergaberecht
- Risikobeherrschbarkeit
  - Transparenz von Prozessen
  - Etablierung von Kontrollmechanismen
    - Audits
    - Reporting (z.B. Datenschutzbeauftragte)
    - Steuerung über SLAs

Anforderungen
Compliance

- Berücksichtigung der gültigen Rechtsprechung (regional, national, EU), z.B.
  - Gerichtsstandort des Cloud-Anbieters innerhalb der EU
- Einhaltung von Regularien
  - BDSG / LDSG
  - Spezialgesetze (Gesundheit, Arbeitsrecht, Vergaberecht. . .)
  - . . .
- Durchführung von Audits
- Beachtung von Lizenzbestimmungen und –verträgen
- Berücksichtigung von Haftungsfragen
- Einhaltung von SLAs

Fraunhofer FOKUS

Risikoanalyse

Wie sicher ist die Cloud nun wirklich?

Sicherheitsanforderungen aus heutiger Sicht
BSI-Grundschutz als „Benchmark-Test“ für Cloud-Computing

Grundschutz

- Katalog konkreter Gefährdungen und Maßnahmen
- Gegliedert in thematische Bausteine
- Grundlage für ISO 27001 Zertifizierung

Bausteine „Outsourcing“ und „Datenschutz“

- Bewertung von Cloud-Computing bzgl. zentraler Aspekte
- Notwendige (nicht hinreichende!) Anforderungen
  - Ergänzt durch ein „Eckpunktpapier“ des BSI

Gefahrenlage Outsourcing
Öffentliche Cloud

- Situation im wesentlichen vergleichbar mit Auslagerung von IT-Dienstleistungen an einen herkömmlichen Dienstleister
- Virtualisierung und konsolidiertes, homogenes Management mindern viele Gefahren und machen Maßnahmen leichter implementierbar, z.B.
  - Änderungsmanagement
  - Kontrolle/Qualitätssicherung
- Definition geeigneter Sicherheitslevel
  - Nicht alles muss geschützt werden
- Standards erleichtern den Anbieterwechsel
  - Vermeidung von lock-ins durch Standard Bausteine basieren auf offenen Schnittstellen
- Standardisierte Föderationskonzepte
  - z.B Sicherheit-Gateways
- Dedizierte SLAs

Gefahrenlage Datenschutz
Öffentliche Cloud

- Ortsbindung
  - Alle Anbieter erlauben eine Beschränkung auf die EU
  - Gerichtsstandort EU?
  - Wie steht es aber mit der Kontrolle?
- Kontrolle
  - Einhaltung der Rechtsgrundlage und der Zweckbestimmung
  - Die Sicherstellung der Rechte des Betroffenen (Auskunft, Berichtigung, Sperrung, . . .)
  - Verpflichtung der Mitarbeiter bzgl. Datenschutz
  - Zugang
    - Zugangskontrolle, Zugriffskontrolle,
    - Einrichten von Benutzern
    - Erstellung von Rechteprofilen
  - Zuständig sind Landesdatenschutzbeauftragte: Ortsbindung?

Anforderungen an Cloud-Anbeiter
Ergänzungen des BSI

- ITIL/COBIT (Erweiterungen erforderlich)
- Technische und organisatorische Maßnahmen, z.B.
  - Gesicherte Netze (Firewalls, IDS, IPS, DDoS-Abwehr, . . .)
  - Spezielle Anforderungen bzgl. Virtualisierung (z.B. Umgang mit Images, Absicherung von Hypervisoren)
  - Anforderung an Verschlüsselung
  - Identitäts- und Rechtemanagement
  - Multifaktor-Authentifizierung
- Transparenz
  - Standorte müssen bekannt sein
    - Subunternehmer (Vertragsgestaltung!)
  - Klienten-seitige Konfiguration durch den Cloud-Betreiber bedarf Zustimmung
- Vermeidung von lock-in Situationen
  - Interoperable und portierbare Anwendungen und Daten (offenen Schnittstellen)

Fraunhofer FOKUS

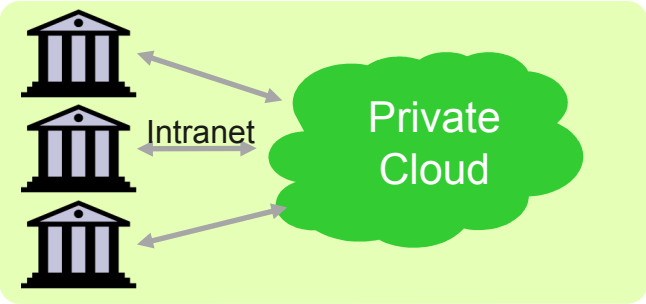
Migration in die Cloud

Ausgestaltungsoptionen und Road Map

Private Clouds
Technologischer Upgrade für behördliche Rechenzentren

Vorteile
- konsolidierte IT-Expertise, reduziere Hardware, reduzierte/keine Betriebskosten
- einfache Bereitstellung von SaaS wie Email, CRM, ERP - ohne Administration
- einheitliche und aktuelle Sicherheitsmechanismen

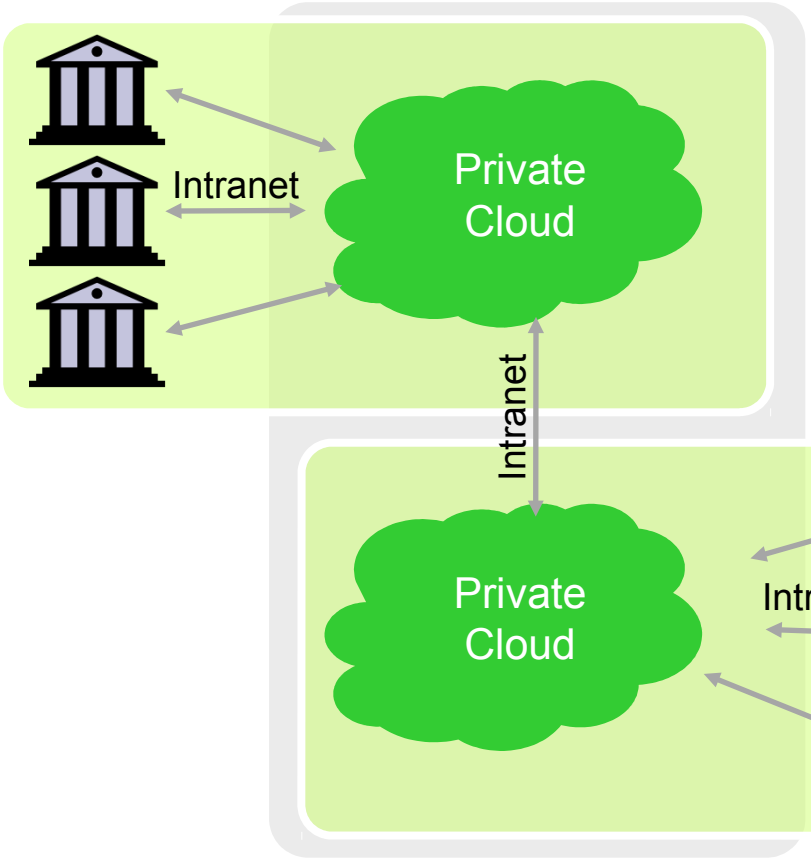
Probleme
- Umfassende Modernisierung verursacht Kosten jenseits Bugettierung
- Wirtschaftlichkeit



Cloud-basiertes Datenzentrum für eine oder mehrere Behörden

Umsetzungen werden bereits vollzogen
- IaaS (allerdings ohne Elastitizität):
  - wird von vielen Shared-Service Centern angeboten („Services anstelle von Servern“)
- PaaS:
  - Verzeichnisdienste z.B. für Geodaten (Vermessungsämter, Behörden für Stadtentwiclung, etc.)
- SaaS:
  - „Thin Clients“
  - Fachverfahren (ERP, CRM, Finanzen, etc.)

Community-Clouds
Shared Service Center



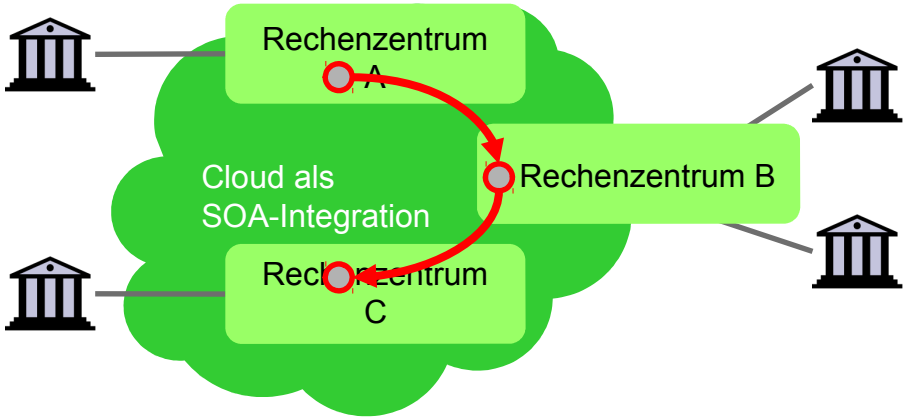
- Vorteil
- Skalierbare DLZ übergreifende Nutzung von Ressourcen (transparent für den Kunden)
- konsolidierte IT-Expertise, reduziere Hardware, Sicherheit, etc…

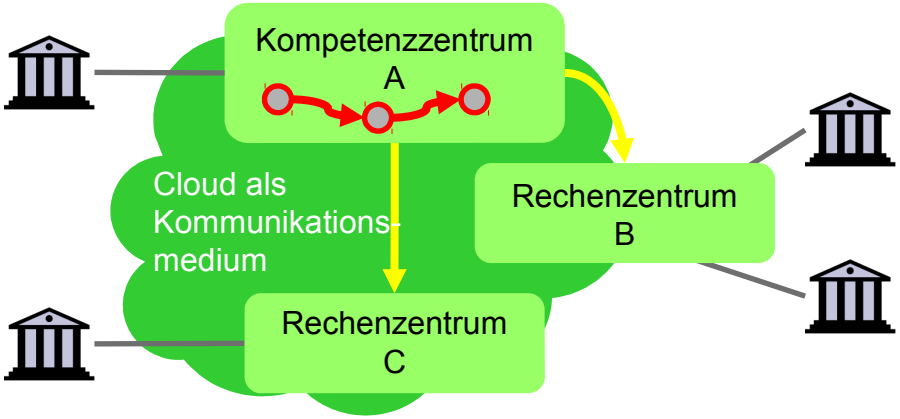
- Probleme
- Back-up in anderer Lokalität
- Bereitstellung von (wiederverwendbaren) Shared Services
  - Prozessketten

Bereitstellung einer föderierten Cloud durch den Zusammenschluss mehrerer DLZ

Community-Clouds
Ausgestaltungsoptionen (I)

- Übergreifende Kooperation
  - Kollaboratives Bereitstellen von Dienstleistungen
  - Prozesse durchlaufen verschiedene Rechenzentren

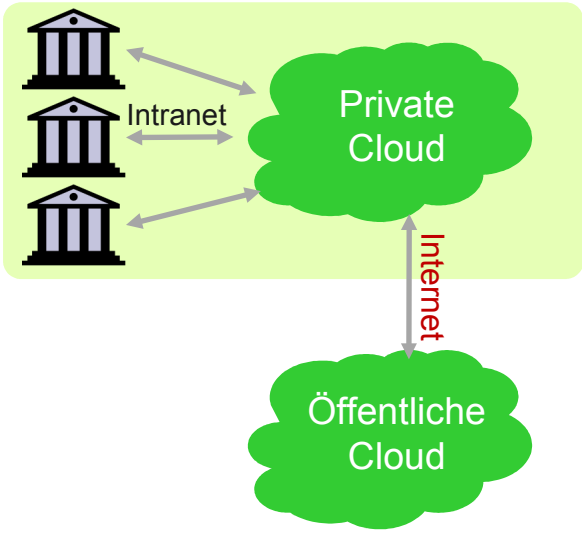




- Kompetenzbasierte Kooperation
  - Einzelne Rechenzentren treten als Kompetenzzentren gegenüber anderen Partnern im Verbund auf

Öffentliche bzw. hybride Clouds
Modell für ÖPP

- Dienst-Auslagerung in öffentliche Clouds ist kritisch zu bewerten (Datenschutz, Transparenz, etc.)
- Allerdings offeriert der privatwirtschaftliche Sektor ein großes Potential an Ressourcen und Know-how
- Optionen
  - Auslagerung öffentlicher Daten in die Cloud
    - Verkehrsinformationen, Wetterdaten, Wirtschaftsdaten, Finanzdaten, digitale Karten, etc.
  - Entwicklung „sicherer Dienste“
    - Elektronische Safes für Daten & Dokumente (verschlüsselt, fragmentiert)
- Anforderungen
  - externe IT-Audits und Kontrollen durch den Auftraggeber
  - Protokollierungs- und Zusammenarbeit
  - Portabilität zwischen verschiedenen Clouds (Vermeidung von »*lock-ins«-)*
  - transparentes, standardkonformes Dienst- und Systemmanagement
  - Transparenz bezüglich der Standorte
  - Offenlegung von Subunternehmern und Verträgen



Cloud-basiertes Datenzentrum mit temporärer Nutzung einer öffentlichen Cloud

Technische Voraussetzungen für die Anwendung von Cloud-Computing

?? Compliance ??

?? Interoperabilität ??

?? Adoption ??

Migration
Road Map

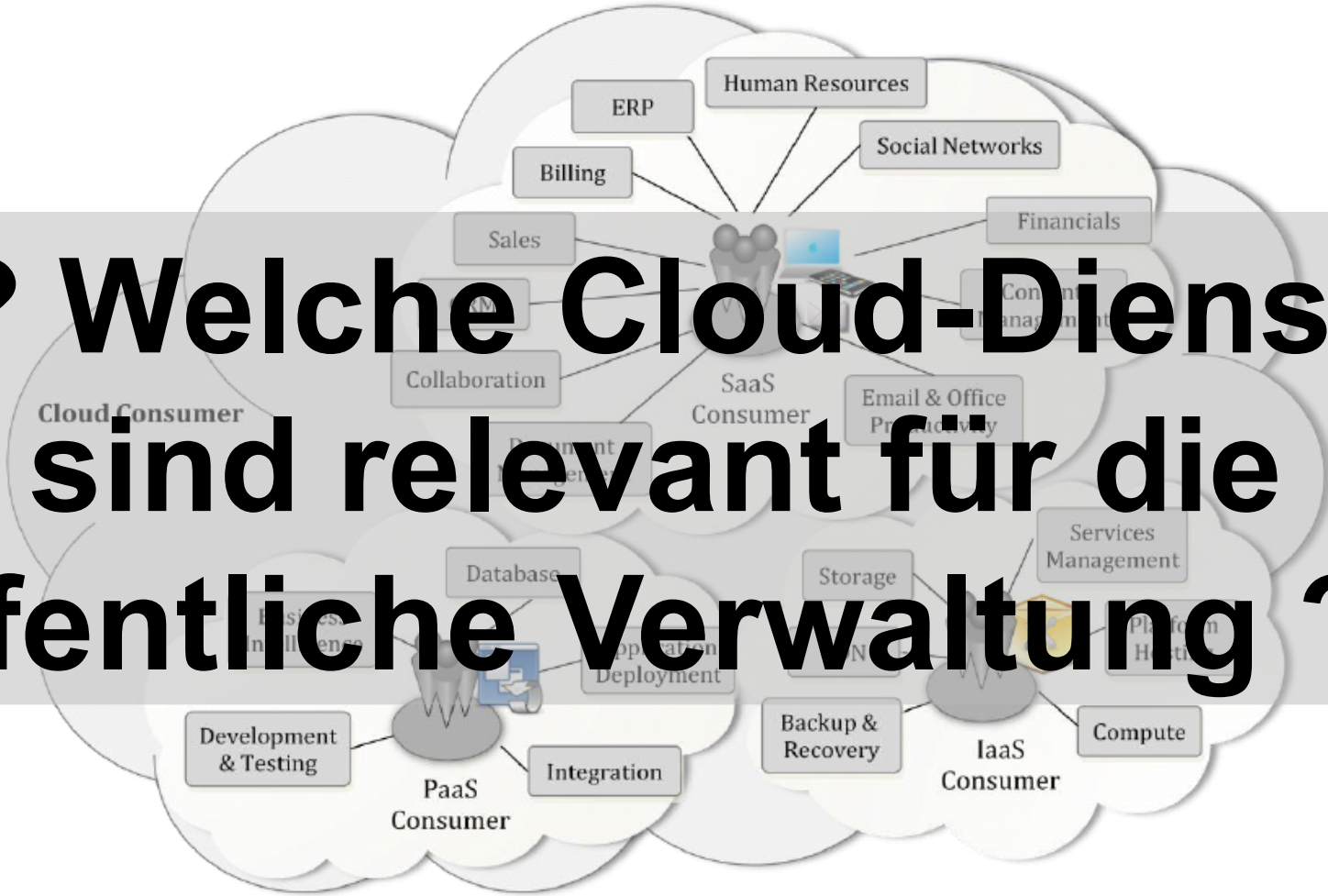
- Erstellung eine Cloud-Strategie
  - Welche Dienste aus der Cloud kommen in Frage
  - Definition geeigneter Sicherheitslevel
  - Bewertung der Cloud-Angebote und SLAs
  - Bewertung der eigenen Compliance und Sicherheits-Anforderungen
  - Risk-Assessment, ROI Analyse und Business-Case
  - Auswahl der ersten Szenarios
  - Auswahl geeigneter Provider
- Vorbereitung der eigenen IT-Organisation
  - Etablierung eines Provider-Managements
  - Automatisierung der Prozesse / Aufbau eines Cloud-Lifecycles
  - Ggf. Erweiterung des IT Service-Katalogs und –Managements

Migration
Road Map

- Start mit einer isolierten Cloud-Installation bzw. einer externen privaten Cloud
  - Low-risk Szenarios
  - Standardisierung von IT-Infrastrukturen
  - Bereitstellung eines Self-service Portals
- Behördenweite Einführung – Shared Services
  - Erweiterung der Cloud-Kapazitäten
  - Überführung vorhandener Dienste in die Cloud
  - Definition von „wiederverwendbaren“ Anwendungen
    - Konolidierung der Anwendungen

Technische und organisatorische Rahmenbedingungen

Cloud Taxonomie - Cloud Dienste nach NIST



?? Welche Cloud-Dienste sind relevant für die öffentliche Verwaltung ??

Fraunhofer FOKUS

Fallbeispiele

Wo stehen wir heute?
Überblick

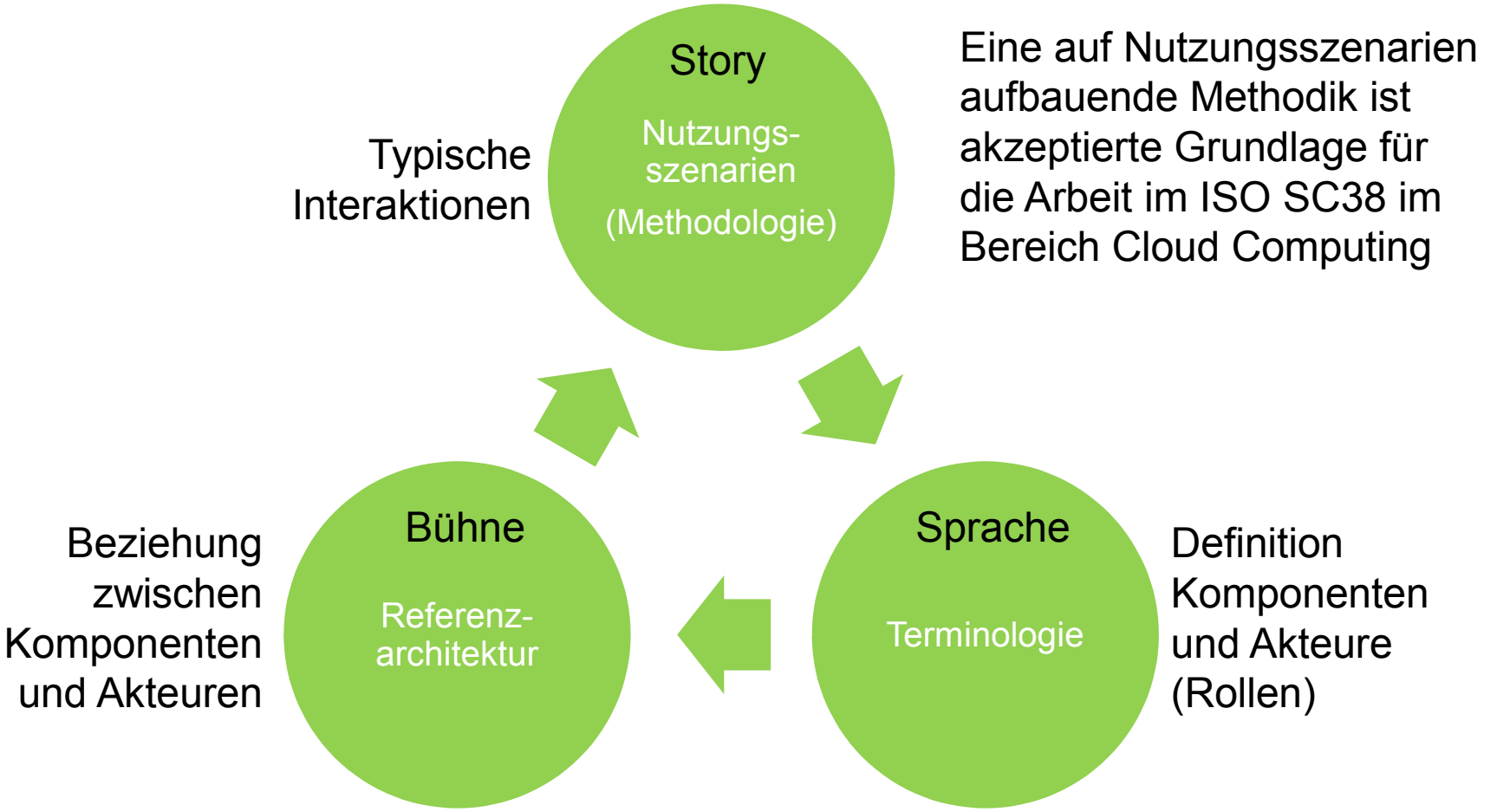
- Arbeitsergebnisse von Fraunhofer FOKUS
  - Zusammenstellung und Vergleich von Definition im Umfeld von Cloud Computing
  - Zusammenstellung und Vergleich von Anwendungsfällen (use case) und zugehörigen Akteuren
  - Entwicklung einer Taxonomie für Anwendungsfälle und Akteure im Cloud Computing
  - Identifikation von für den öffentlichen Sektor in Deutschland wichtiger Anwendungsszenarien
  - Implementierung von Fallbeispielen mit Laborpartnern
  - Einbringen der Ergebnisse in die nationale (DIN) und internationale Standardisierung (ISO JTC 1/SC38)

Nutzungsszenarien als Standardisierungsinstrument

- Methodik zur Identifikation von Standardisierungsanforderungen
  - Wo ist noch etwas zu tun?
- Evaluation von vorhandenen Standards
  - Wie gut regelt ein Standard ein bestimmtes Szenario
  - Welche Nutzungsfälle sind berücksichtigt?
- Treiber zur Entwicklung von Standards
  - Interaktion und Diskussion mit Stakeholdern anhand konkreter Beispiele
- Berücksichtigung nationaler Anforderungen
  - Welche Anforderungen ergeben sich aus nationalen Kontexten?
  - Sind nationale Standards und rechtliche Rahmenbedingungen zu berücksichtigen?

Nutzungsszenarien als Standardisierungsinstrument

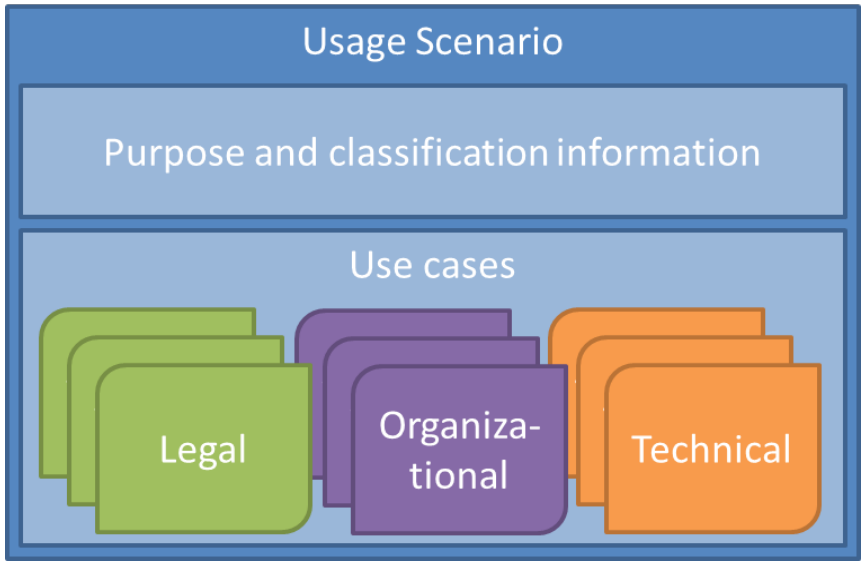
Aktivitäten im ISO JTC 1 SC 38 (WG 3: Cloud Computing)



Eine auf Nutzungsszenarien aufbauende Methodik ist akzeptierte Grundlage für die Arbeit im ISO SC38 im Bereich Cloud Computing

Szenarien und Anwendungsfälle

Aktivitäten im ISO JTC 1 SC 38 (WG 3: Cloud Computing)



- Nutzungsszenarien
  - „High-level“: Beschreibt eine Anwendung, Geschäftsidee, etc.
  - Definiert Kontext
  - Identifiziert die generelle „Botschaft“: Was soll erklärt werden?
- Nutzungsfälle
  - Spezifische Interaktionen zwischen den verschiedenen Akteuren
  - Konzentration auf legale, organisatorische, technische, ... Aspekte

Usage scenario	
US01	Electronic Document Safe (EDS)
Description	Bob and Clair, proud parents for the first time, face the next challenge in their life, namely to manage applying for parenting benefit . . .
Category	Technical, organizational, legal
Domain	Public sector, public private partnership
Goals and purpose	Purpose of the usage scenario is to demonstrate how personal documents can be stored in public/hybrid Clouds while preserving evidence using cryptographic signatures.
Actors and Roles	Document & EDS owner (citizen), Document/data provider or consumer (public administration), Safe provider, Certificate provider, PKI provider
Software layers	PaaS, SaaS
Deployment models	Public, hybrid
Components and services required for execution	. . .
New specifications required between the actors	■ UC-Organizational: Specifications for “dynamic” Cloud bursts ■ UC-Technical: Data migration protocol
Related use cases	UC-Legal, UC-Organizational, UC-Technical

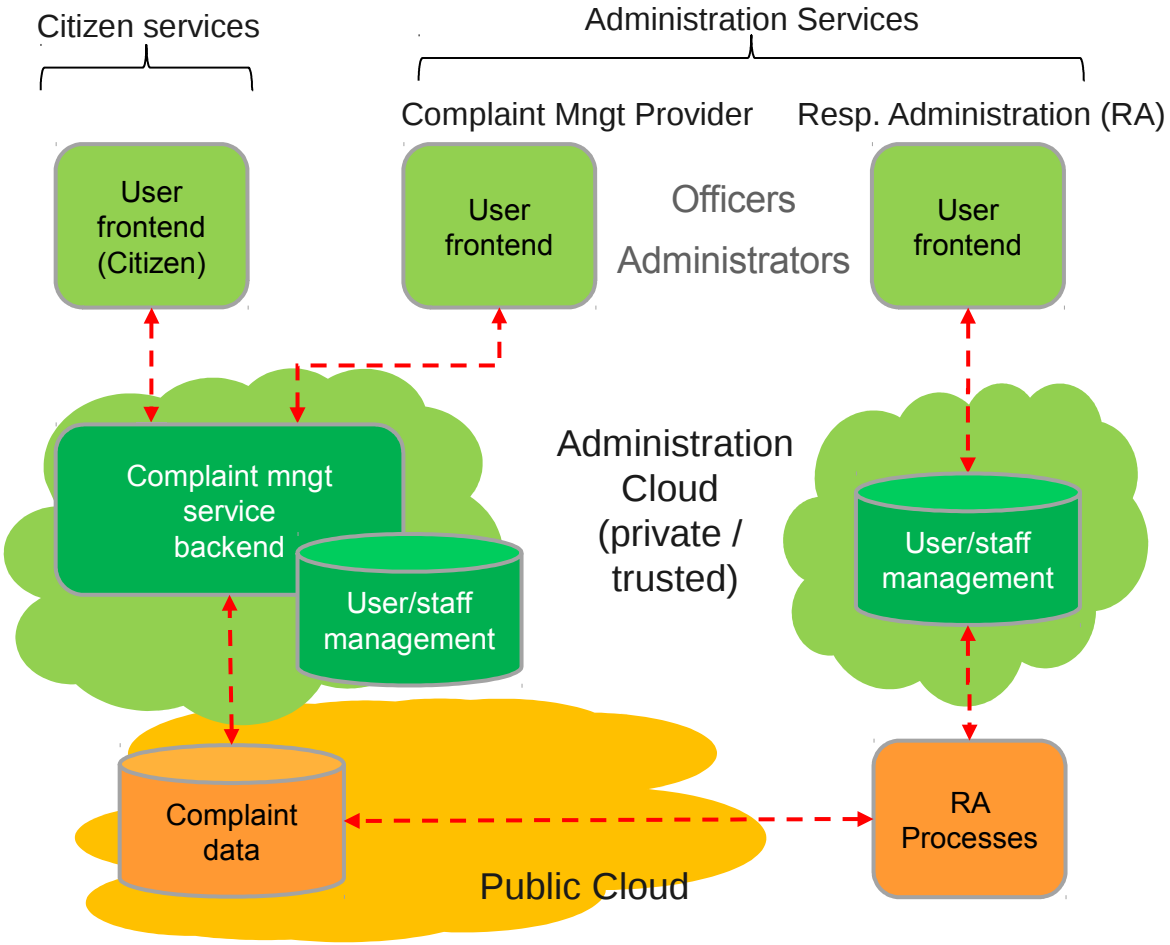
Szenario 1
Trennung von offenen und geschützen Daten

- Viele administrative Prozesse involvieren keine sensiblen Daten
  - Stassenbau
  - Stassenreinigung und öffentliche Abfallentsorgung
  - Transportlogistik
  - Öffentliche Bauvorhaben

Beispiel

- Anliegenmanagement
  - Bürger reicht eine Beschwerde oder ein Anliegen ein (z.B. Stassenschäden)
  - Bürgerdaten sind notwendig, um die Bearbeitung von Anliegen (Status) zu verfolgen
  - Werden jedoch nicht zur Behebung der Anliegen/Beschwerdeursachen benötigt
  - ⇨ Beschwerdedaten (nicht personenbezogen) und administrative Prozesse der verantwortlichen Behörden können ausgelagert werden (auch in die öffentliche Cloud)
  - ⇨ Bürger- (und Bearbeiter-)Daten verbleiben in der privaten Cloud

Szenario 1
Trennung von offenen und geschützen Daten



Beispiele für ähnliche Dienste:

- FreedomSpeaks
- Märker Brandenburg
- Unortkataster Köln
- Wer denkt was
- AbgeordnetenWatch

- Rechtssichere Ablage personenbezogener Daten
  -
  - Löschung nach Auftragsbearbeitung
  - Sensible Daten nur in Privater Cloud

Schlußfolgerungen

- Offene Daten sind nicht nur Bürgerbeschwerden, sondern auch
  - Statistiken
  - Demographische Informationen
  - Informationen über geplante Bauvorhaben
  - . . .
- Eine Aufbereitung dieser Daten kann durch privatwirtschaftliche Unternehmen erfolgen
- Standardisierung
  - Schnittstellen und Protokolle
  - Datenformate, Metainformation
  - Compliance-Anforderungen an Cloud-Anbieter:
    - Welches Sicherheitsniveau ist für offene Daten anzusetzen?
    - Welche Anforderungen ergeben sich

Szenario 2
Unterstützungsdienste für den Bürger

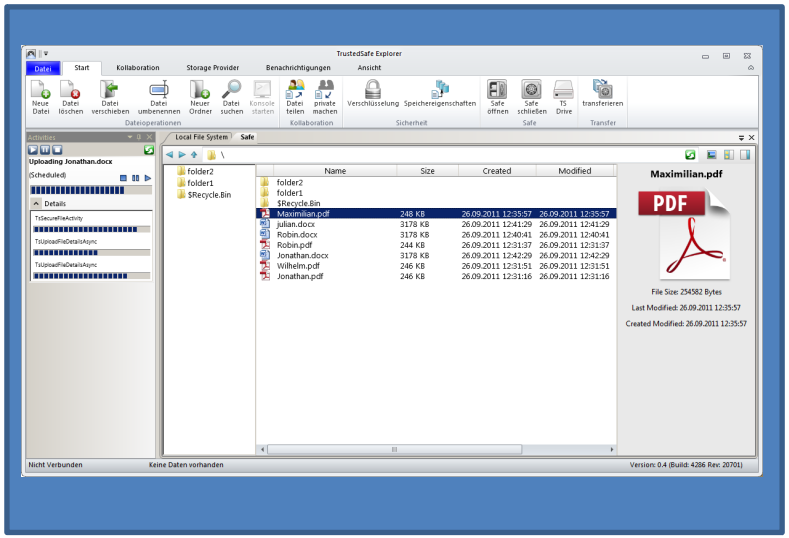
Elektronischer Datensafe

- Sicherer Langzeitspeicher für persönliche Daten und Dokumente
  - Cryptographisch signiert
  - Beweiswerterhaltung
- Erlaubt den elektronischen Geschäftsverkehr zwischen Bürgern, Unternehmen und Behörden
- Definition von Zugriffsrechten abhängig von konkreten behördlichen Prozessen
  - Keine proaktive Datenerheben
  - Bürger gibt Zugriff in Zusammenhang mit dem jeweiligen Antrag frei

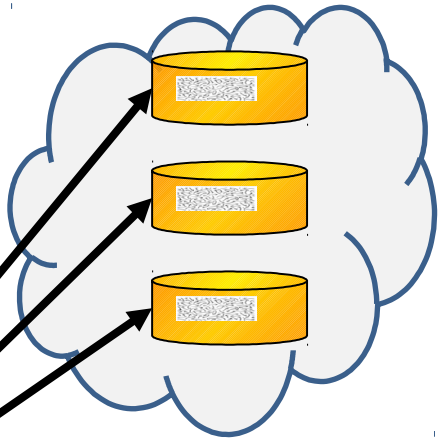
trustedSafe
Privacy for the cloud

Fraunhofer FOKUS Spin-Off trustedSafe GmbH

User PC



Cloud Storage Provider
e.g., Microsoft, Amazon, Eurohost



Highly secure encrypetion/fragmentation algorithm developed by Fraunhofer FOKUS **)

Safe Manager
nPA
authentication

trustedSafe Client

Safe Key
e.g. Memory Stick

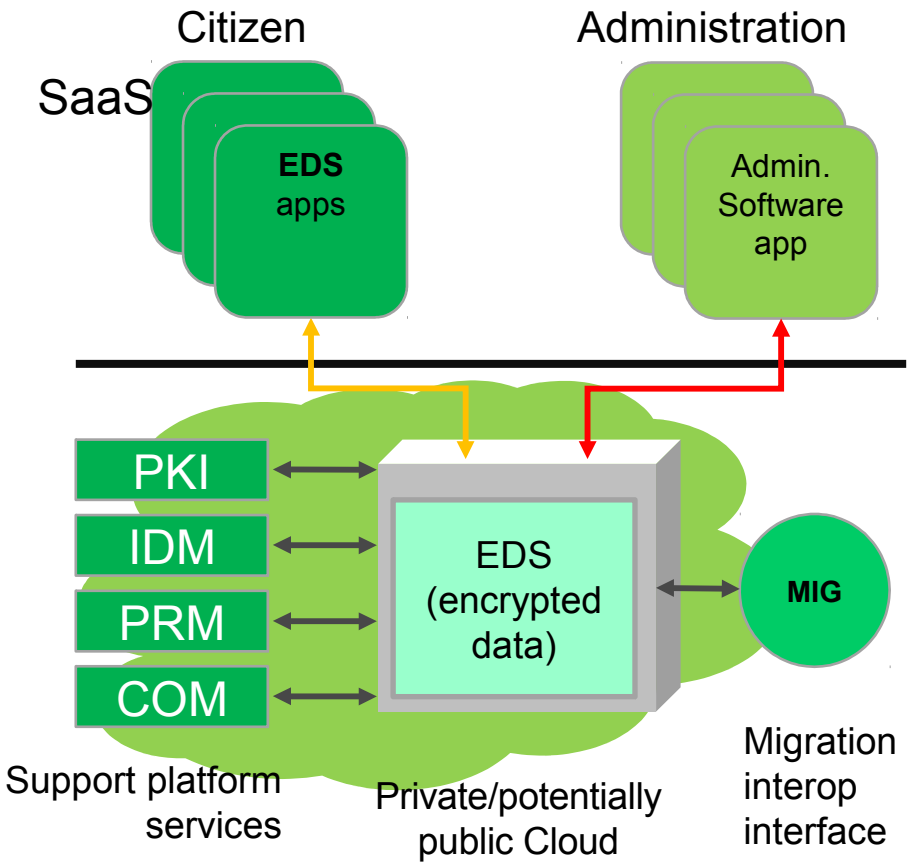
Szenario 3
Unterstützungsdienste für den Bürger: Beispiel Elterngeldantrag

- Unterlagen (Auszug):
  - Geburtsurkunde. Schulbescheinigung, Ausbildungsnachweis, Studiennachweis, Verdienstbescheinigung, Meldebescheinigung, Mietvertrag, . . .
  - Max. 27 verschiedene Dokumente

- Bearbeitungsstatistik Meklenburg-Vorpommen 2010
  - 15.955 Anträge

- **Elektronische Bereitstellung relevanter**
  Bearbeitung von Anträgen signifikant b
- **Interaktionen zwischen Bürger und Beh**

Szenario 3
Unterstützungsdienste für den Bürger



- **Anbieterunabhängige Verschlüsselung**
  - Verwaltung des Safes durch eine privatwirtschaftlichen Anbieter (öffentliche Cloud) ist denkbar
  - Voraussetzung: Sichere Verschlüsselung (mit “upgrade” entsprechend “state of the art”), extrem hohe Verfügbarkeit
- **Daten-Interoperabilität** (via MIG)
  - Notwenig, um lock-ins zu vermeiden
  - Standardisierte Formate für signierte Dokumente

Schlußfolgerungen

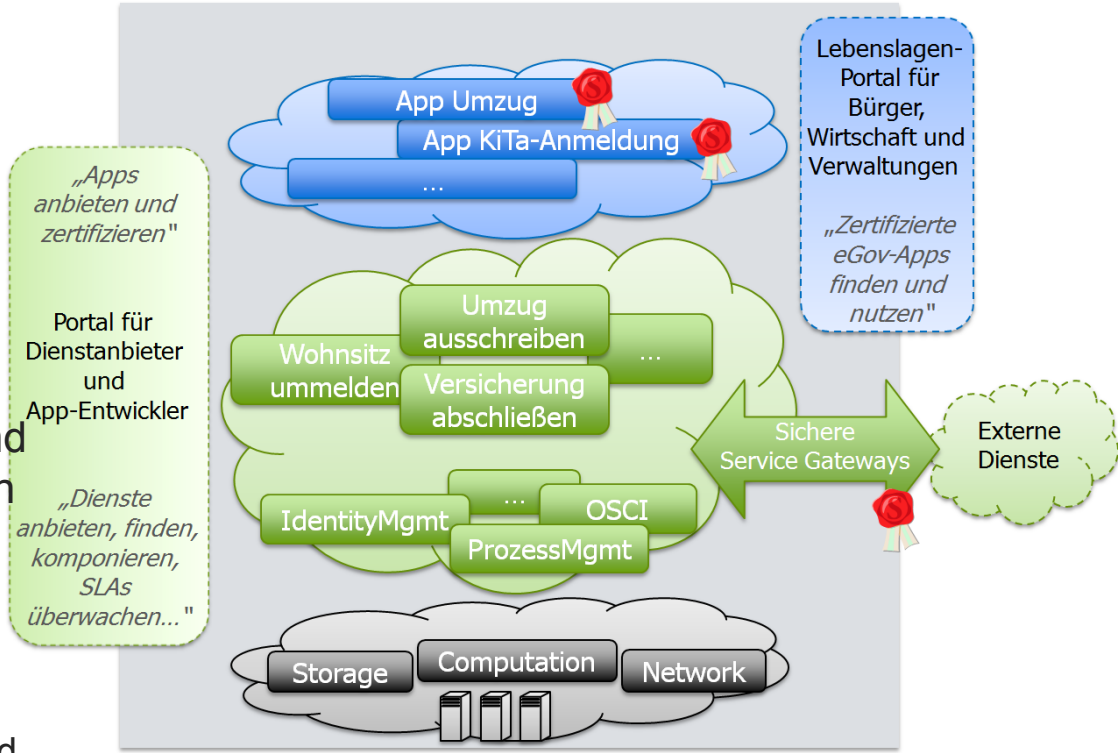
- Standardisierung
  - Sicherheit, auch gegenüber dem Dienstleister!
    - Cloud-Dienstleister unabhängige Verschlüsselung/Verteilung von Dokumenten
    - Compliance: Zertifizierung von Schlüssel/Identitäts-Anbietern
  - Nationale Regelwerke
    - Signaturgesetze
    - Technische Richtlinie TRESOR (BSI) zur beweiswerterhaltenden Langzeitarchivierung
  - Migrations-Schnittstelle notwendig um behördliche Diensterbringung zu garantieren
    - Gewährleistungspflichten
    - Dateninteroperabilität
    - Protokolle zur sicheren Datenmigration

Cloud-basierte eGovernment Dienstemarktplätze

goBerlin - „Business incubator“

Trusted Cloud

- Viele Verwaltungsprozesse werden durch privatwirtschaftliche Geschäftsprozesse ergänzt
  - Z.B. „Lebenslage“ Wohnungswechsel:
    - Ummeldung beim Einwohnermeldeamt
    - Makler, Umzugsunternehmen, Handwerker
- „Lebenslagen-App“
  - Integration von behördlichen und privatwirtschaftlichen Prozessen
  - Notwendige Infrastruktur wird geteilt (Hybrid Cloud)
    - Private Cloud für öffentliche Aufgaben
    - Öffentliche Cloud für KMUs und Kleinstunternehmen ohne eigene Infrastruktur



Entwicklungsbeispiel goBerlin – Marktplatz & Trusted Cloud für Vertrauenswürdige Dienste aus Verwaltung und Wirtschaft

- Integration von eGovernment und eBusiness für Bürger, Wirtschaft und Verwaltung
  - Eröffnung eines kooperativen Dienste-Markts mit hohem wirtschaftlichen Potenzial für Unternehmen und Verwaltungen mit neuen Wertschöpfungsmodellen durch kooperative Leistungserbringung
- Nachfrageorientierte Bereitstellung und verbrauchsabhängige Abrechnung von Diensten und Basiskomponenten
  - Gewährleistung einer sicheren Betriebsumgebung durch öffentlichen Dienstleister: Schaffung eines vertrauenswürdigen Rahmens, Nachvollziehbarkeit und Rechtssicherheit
- Schaffung wieder verwendbarer Basistechnologien für Entwicklung, Authentisierung, Integration und Bezahlung Gesicherter Zugang durch entkoppelte Sicherheitsdienste
  - Zertifizierung von Diensten und Applikationen
  - Definition von Rahmenbedingungen, Standards und Schnittstellen
- Pilotierung und dynamische Erweiterung des Marktplatzes und bundesweite Übertragung

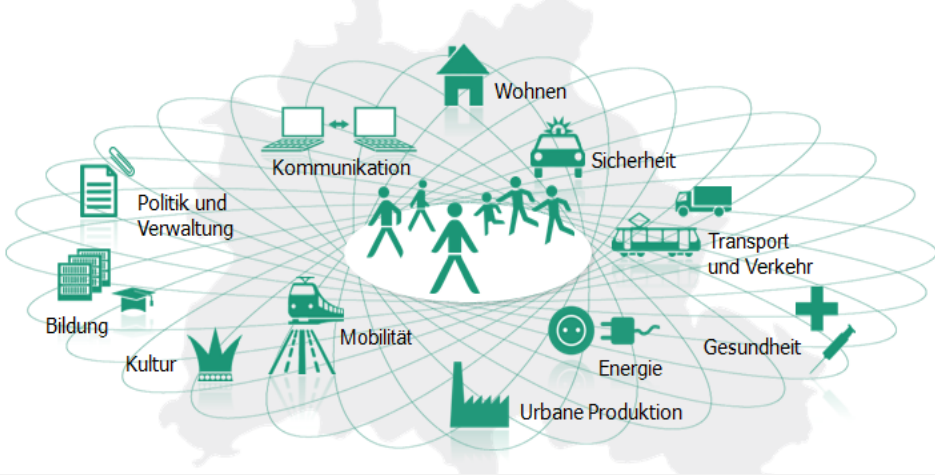
Fallbeispiel - Szenario 4

Daten-Infrastrukturen als Rückgrat einer Smart City

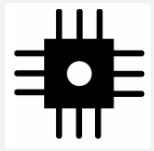
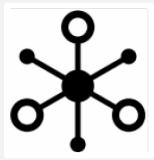
Die Stadt als System von Systemen

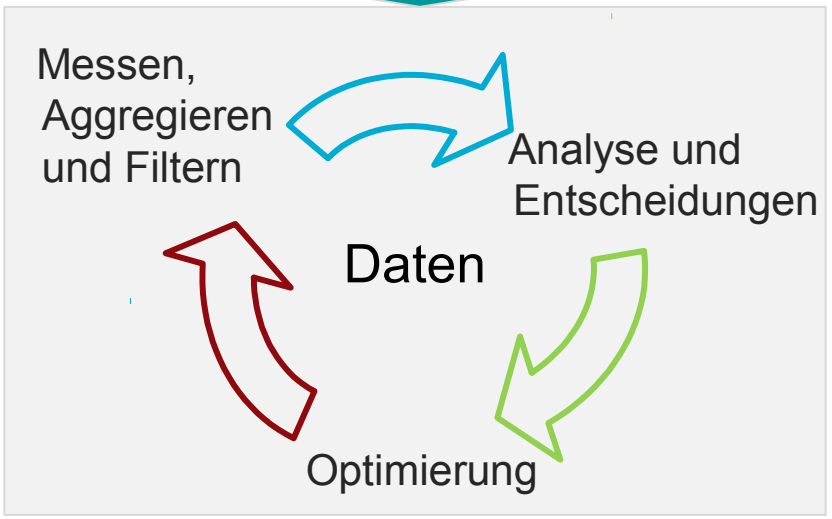
Einzelsysteme → Gesamtsystem

Die Effektivität und Effizienz des Gesamtsystems resultiert aus dem möglichst optimierten Zusammenwirken der Einzelsysteme



Instrumented Interconnected Intelligent

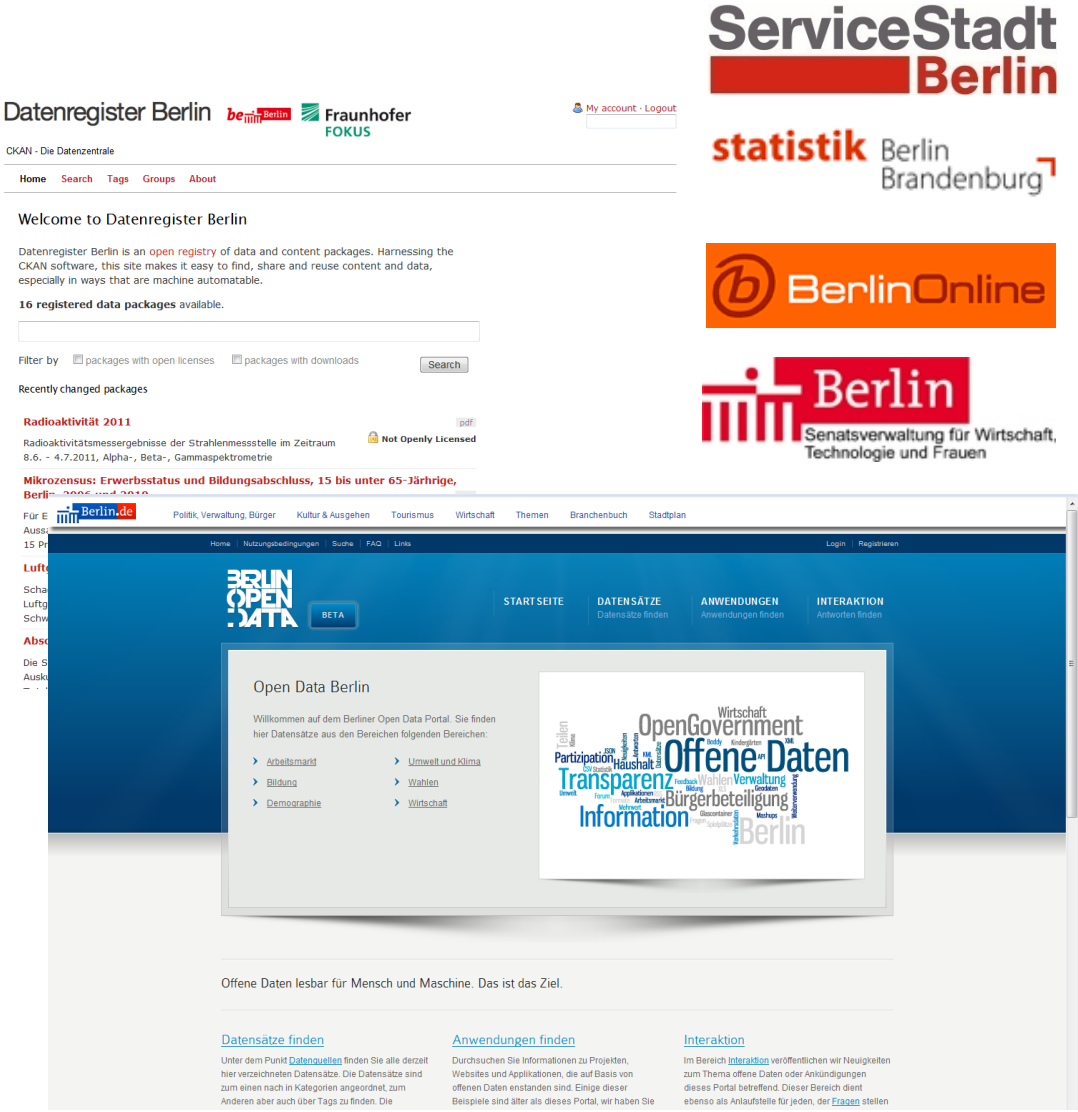



Berlin Open Data Portal

Making Open Data Real

- http://daten.berlin.de
  Launched Sept. 14, 2011
- Initiated by Senate of Berlin: Department for Economy, Technology and Women
- Planned by FOKUS
- Realized by BerlinOnline and FOKUS
- Data sets on statistics, environment, business, etc.
- Using free licenses (CC-BY and ODC-BY)



"It was much nicer before people started storing all their personal information in the cloud."

Danke für Ihre Aufmerksamkeit

Fragen?

Linda Strick

Fraunhofer Institut für offene Kommunikationssysteme (FOKUS)

linda.strick@fokus.fraunhofer.de