
Identity Management

- neue Wege zur Sicherheit -

Claudia Eckert

Fraunhofer-Institut für Sichere Informationstechnologie SIT
eckert@sit.fraunhofer.de

52. Jahrestagung der GMDS, Augsburg 18.9.2007

Gliederung

1. Digitale Identitäten in Unternehmen:

Stand heute

2. Identitäts- und Accessmanagement (IAM)

Ganzheitlicher Ansatz: Technologie + Management

3. IAM-Next: Next Generation IAM

- Identifikation von Geräten
- IAM in Service-orientierten Architekturen (SOA)
- Internet der Dinge

1. Digitale Identitäten heute

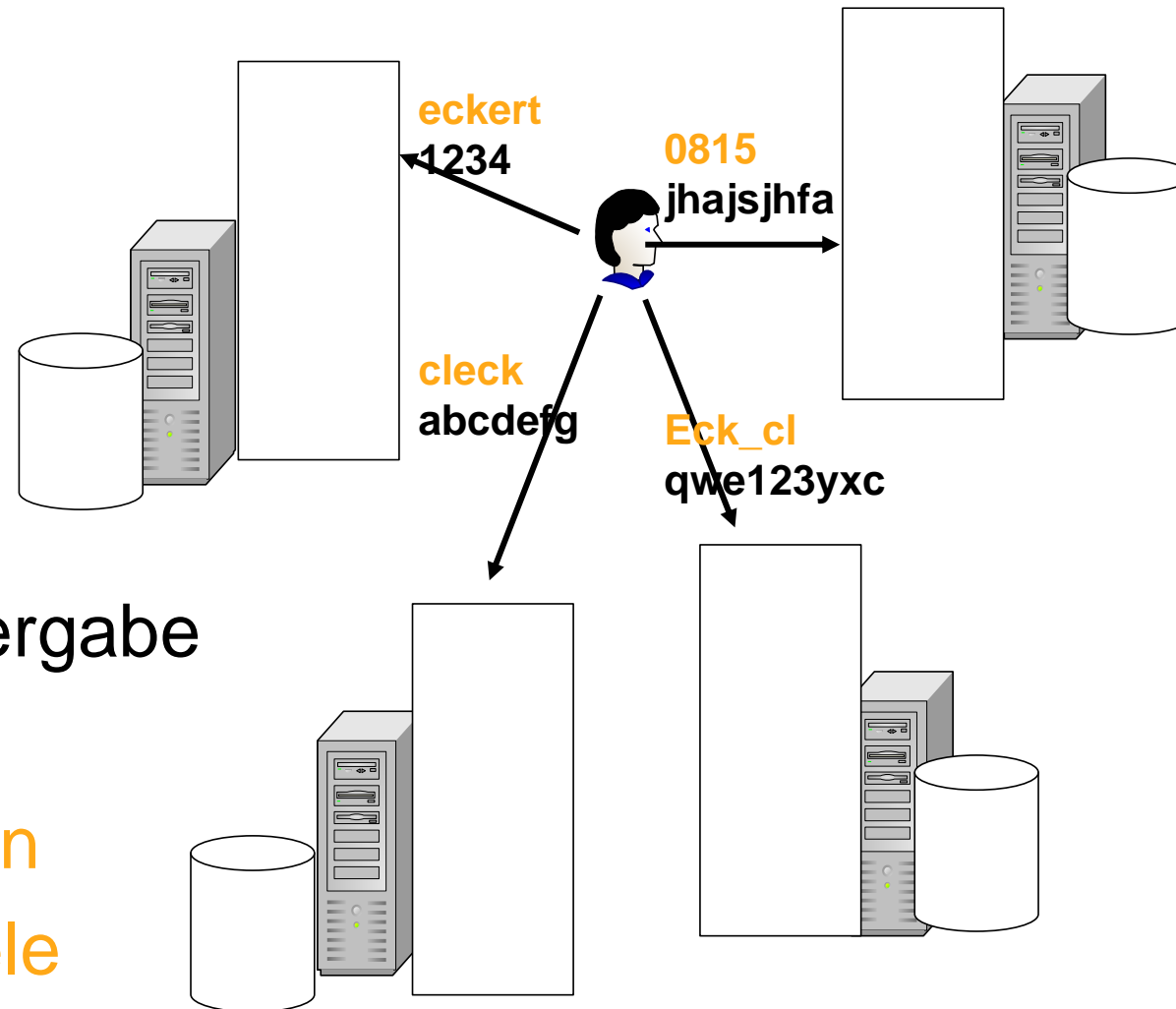
Jedes IT-System besitzt

- eigenes Nutzer-,
- Rechte-, Audit-Mgmt

➔ **Silo-Lösungen!**

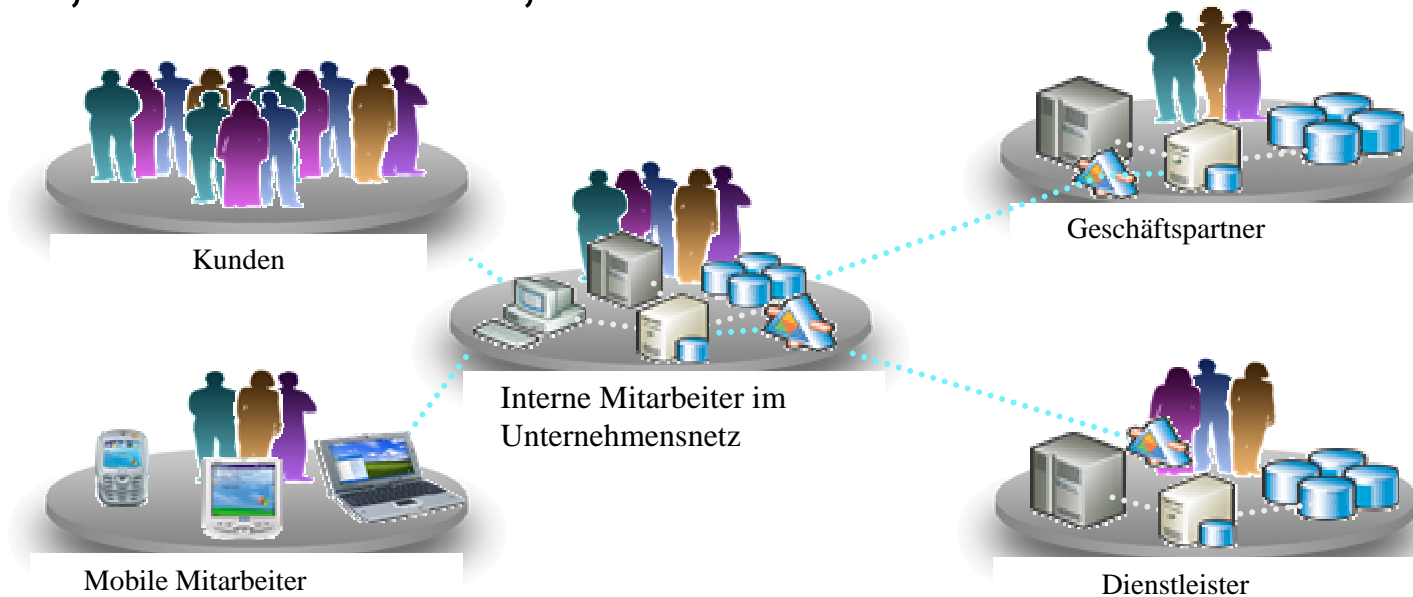
Konsequenzen u.a.

- **Intransparente** Rechtevergabe
- Redundante, häufig manuelle **Administration**
- **verwaiste** Konten, **zu viele** Berechtigungen



Anforderungen an moderne Unternehmens-Infrastrukturen

- **Offene** System- bzw. Unternehmensinfrastrukturen: für Kunden, Dienstleister, externe/interne Mitarbeiter, Partner, ...



- **Flexibilisierung** der Geschäftsprozesse
- **Real-time Enterprise**: aktuelles Wissen: wer darf wann, was

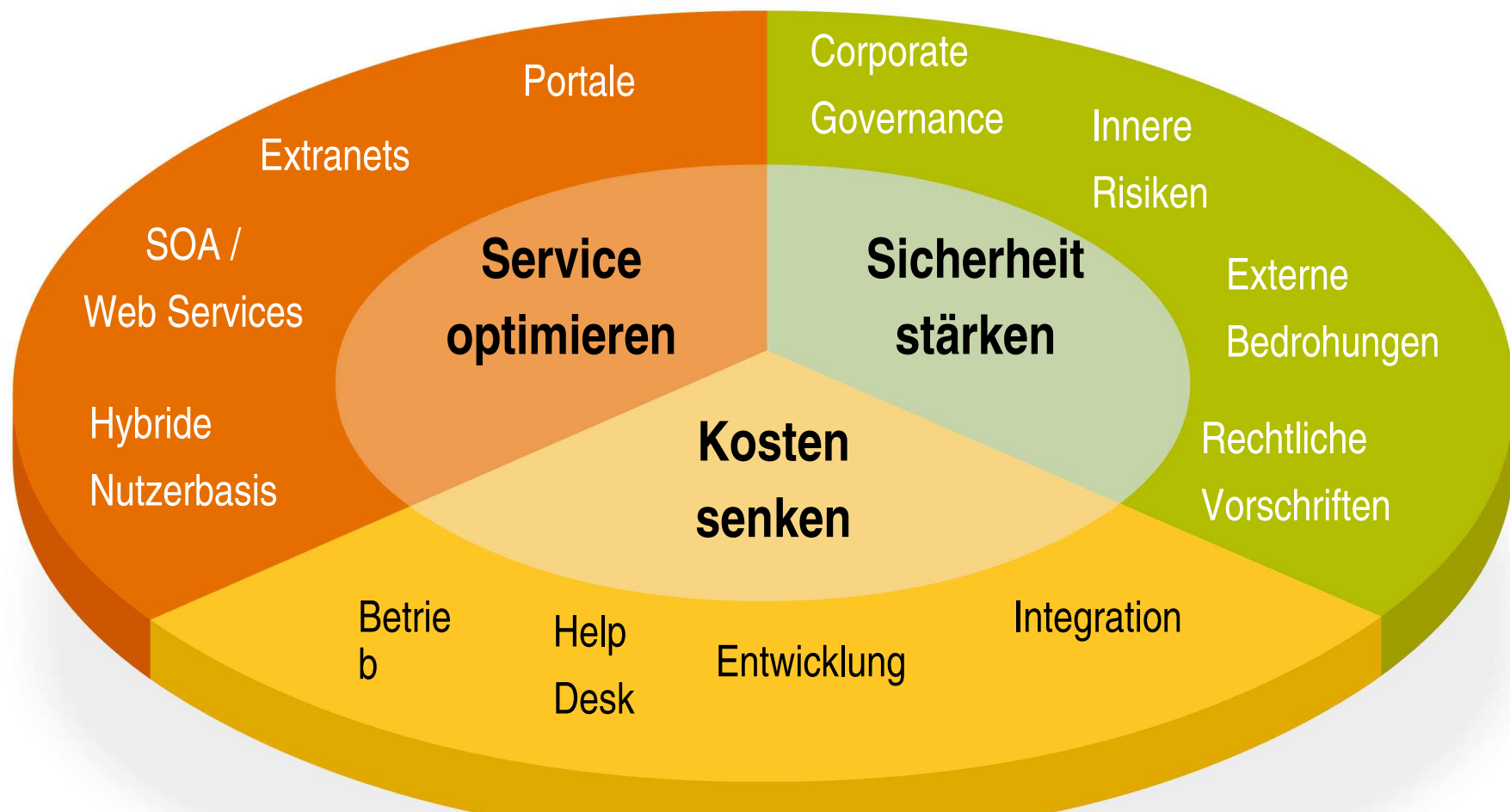
➔ Mit Technik allein sind Anforderungen nicht erfüllbar

2. Identitäts- und Accessmanagement (IAM)

IAM: Dienste, Technologien, Produkte und Standards, die die Nutzung digitaler Identitäten ermöglichen

Neue Wege: Integriertes Vorgehen:

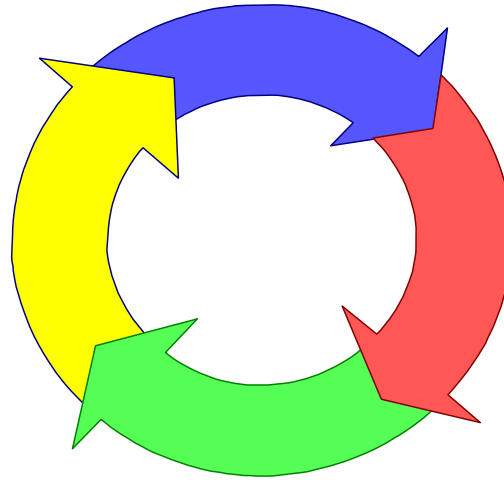
Technik + HR + Management + Mitarbeiter



Management der digitalen IDs über **gesamten Lebenszyklus**

Erfassen der Identität

- Personalsysteme, CRM,
- Kundenportale, ...
- **Identität:** Bezeichner, Attribute, Credentials, ...



Deaktivieren/Löschen

der digitalen Identität

- Deaktivieren der Zugriffsrechte
- Archivierung, ...

Berechtigungsvergabe

- Rollenzugehörigkeit
- Berechtigungen: Zugang zu Anwendungen/Ressourcen
- Ausstellen von Ausweisen

Verwaltung

- Organisatorische Änderungen
- Wechsel der Position
- Rechtedelegation
- Änderung der Rahmenbedingungen (Compliance)

Aufgabenstellung erfordert

- Integriertes, transparentes, ganzheitliches IAM

IAM umfasst Management und Technologie-Integration:

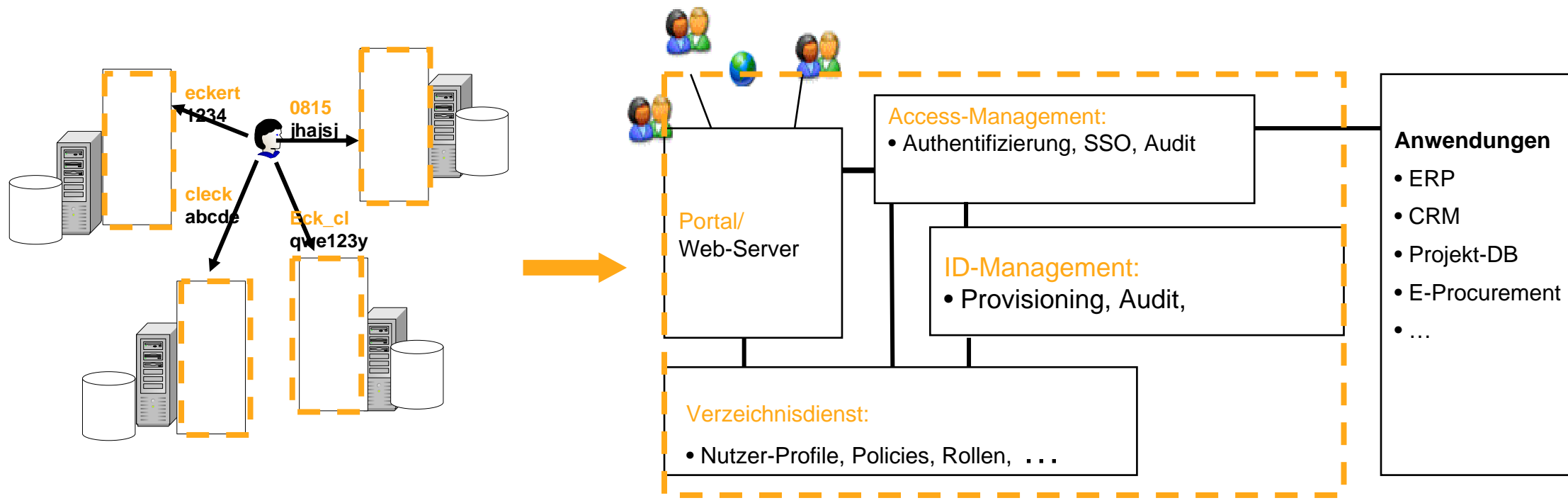
- Technologie folgt den Prozessen!
 - Vereinheitlichung der Abläufe ist notwendig
- Policy-Engineering: Festlegen, Verwalten von
 - Authentifizierungs-, Autorisierungs- und Audit-Regeln
 - (Enterprise) Single-Sign-on (SSO):
 - einheitliche Session für verschiedene Anwendungen
 - Authentifizierung: Smartcard-basiert
- Technologien: SAML, PKI, LDAP, XACML, Cookies, ...



Generische IAM-Architektur

- **Portal-Komponente:** einheitlicher, Web-basierter Zugriff
- **Verzeichnisdienst:** globales Repository
- **Metadirectory:** Vereinheitlichen von IDs zu einer digitalen ID

Integration verschiedener Directories: ERP, CRM, SCM

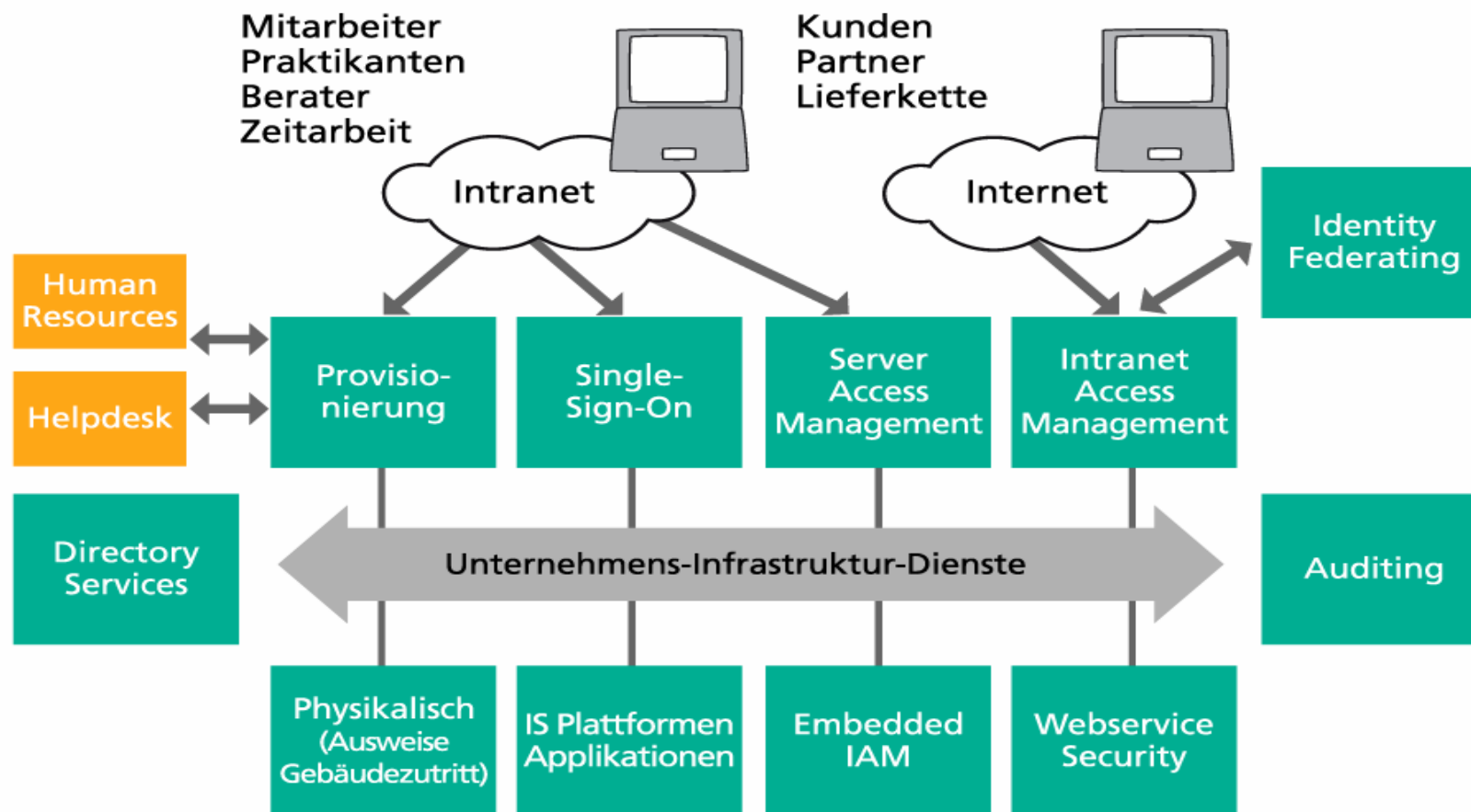


Chancen eines ganzheitlichen IAM

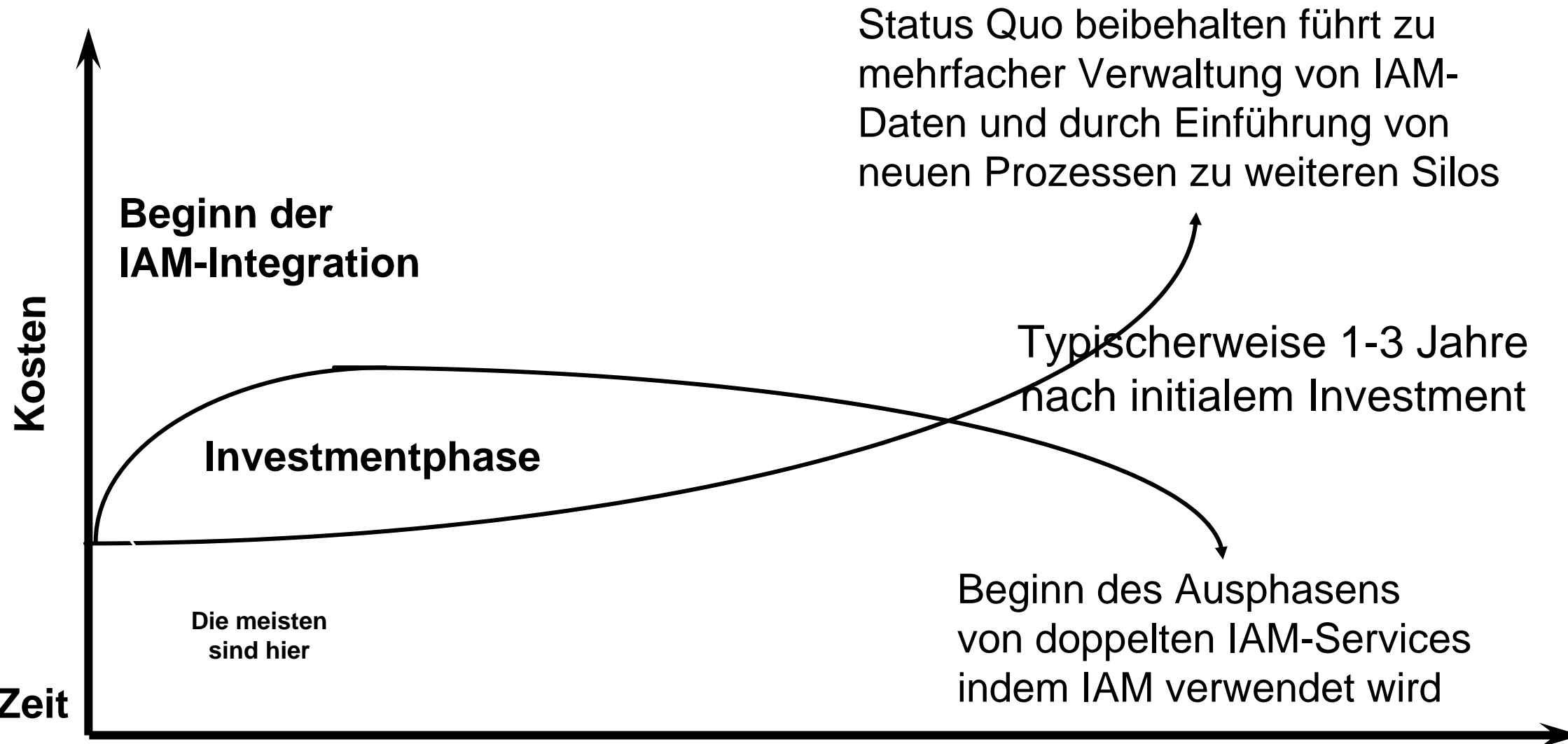
- **Erhöhte Sicherheit** durch **vereinheitlichte** digitale Identität
 - vermeiden von Widersprüchen etc.
 - **Real-time Provisioning**, Reduktion der Delay-Zeiten:
 - automatisierte Rechtevergabe/ -rücknahme
 - höherer Grad an Sicherheit: schnelle Rechteanpassungen
 - **Kosteneinsparungen**:
 - Reduktion der Administrationskosten: Automatisierung,
 - Reduktion der Helpdeskkosten, Lizenzierungskosten,
 - **Usability** und Simplicity aus Nutzersicht: u.a. SSO
 - **aktuelle, vollständige Information**: wer darf wann was, ...
- Prüfung auf Compliance ist automatisierbar

Probleme: IAM **erfordert** die

- **Integration** unterschiedlicher Technologien: aufwändig
- **Definition** unternehmensinterner u. -übergreifender Prozesse
d.h. Einführung eines IAM erfordert sorgfältige **Planung!**



Integrationskosten und Business Case für IAM



Zwischenfazit: Situation heute

- Systeme zur Verwaltung von Identitätsinformation sind gewucherte Eigengewächse
- Berechtigungen werden manuell vergeben
- Anbindung von Anwendungen sind hochgradig proprietär
- Für neue Benutzergruppen werden neue Systeme geschaffen
- Die gleichen Informationen werden in verschiedener Form in verschiedenen Systemen gehalten
- Benutzermanagementprozesse sind Silo-spezifisch

Ganzheitliches IAM

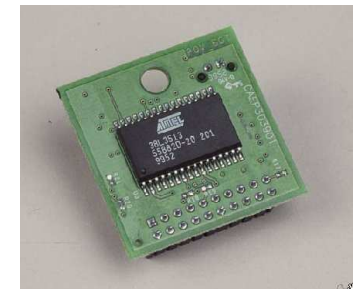
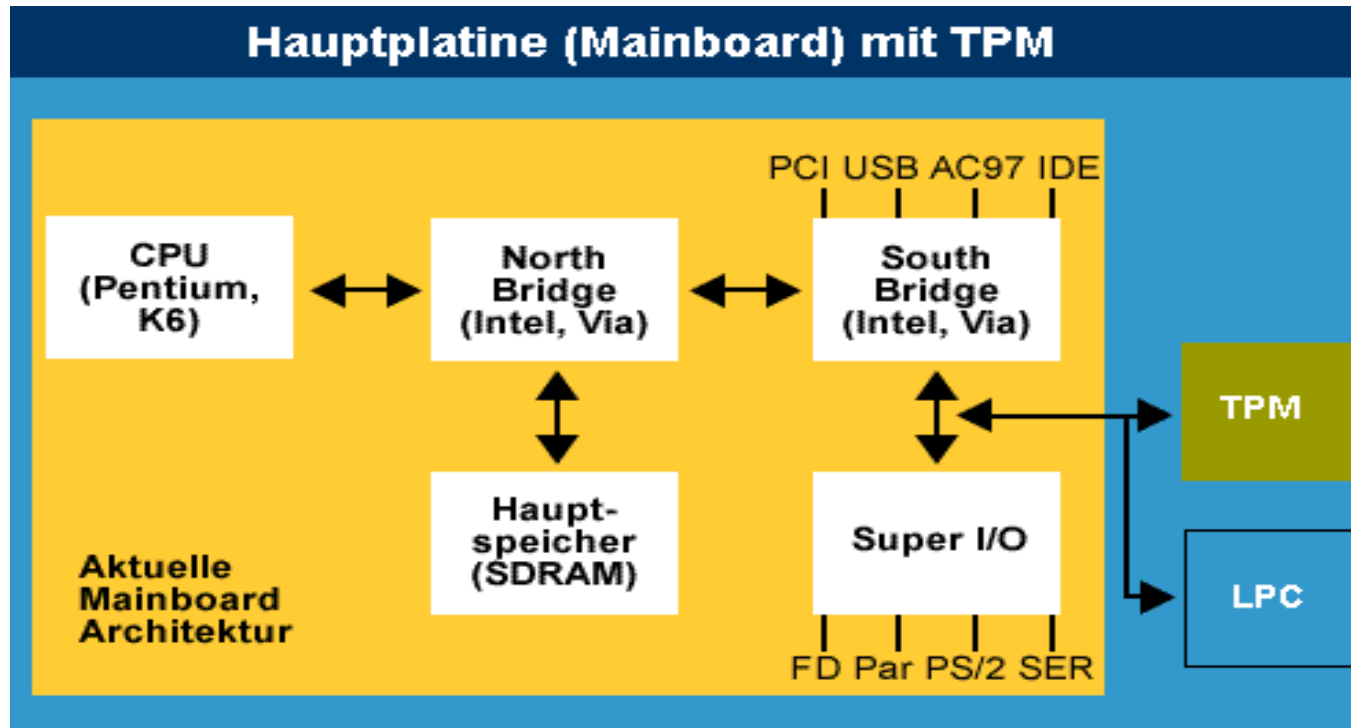
- Standardisierte, zentrale Benutzerdaten werden von allen Anwendungen verwendet
- Rollen/Berechtigungen ergeben sich aus Geschäftsprozessen u. HR
- Neue Anwendungen lassen sich sofort integrieren
- Alle Benutzertypen sind in einem zentralen System
- Einheitliche, korrekte Daten für alle Benutzer ständig aktuell
- Benutzermanagementprozesse sind einheitlich über die Organisation hinweg



3. IAM-Next: Next Generation IAM

3.1 Vertrauenswürdiges Identifizieren von Geräten

- Trusted Platform Module (TPM) („Smartcard“ im Rechner)
- **Endorsement Key (EK)**: RSA-Schlüsselpaar (2048 Bit)
- **eindeutige Identität** des TPM über EK



TPM-Einsatz in

- PCs, PDAs,
- Handy
- Unterhaltungselektronik, ...

Wichtige Dienste des TPM:

- **Attestierung:**

Erstellen signierter Reports über die System-Konfiguration

- **Sicherer Speicher:** Identitätsschlüssel EK, Private Keys,

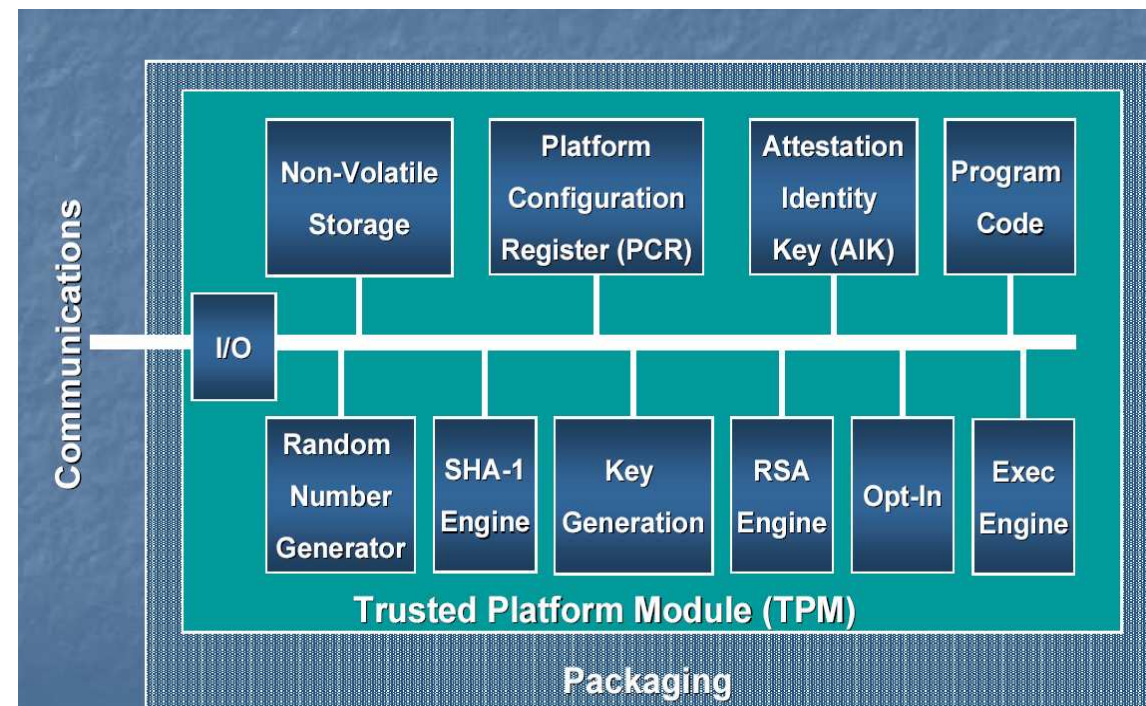
- **Sealing:** Datenverschlüsselung mit Bindung an aktuelle

Systemkonfiguration,
Entschlüsseln nur in
korrekter Konfiguration

- **Signieren**

- **Verschlüsseln**

- ...

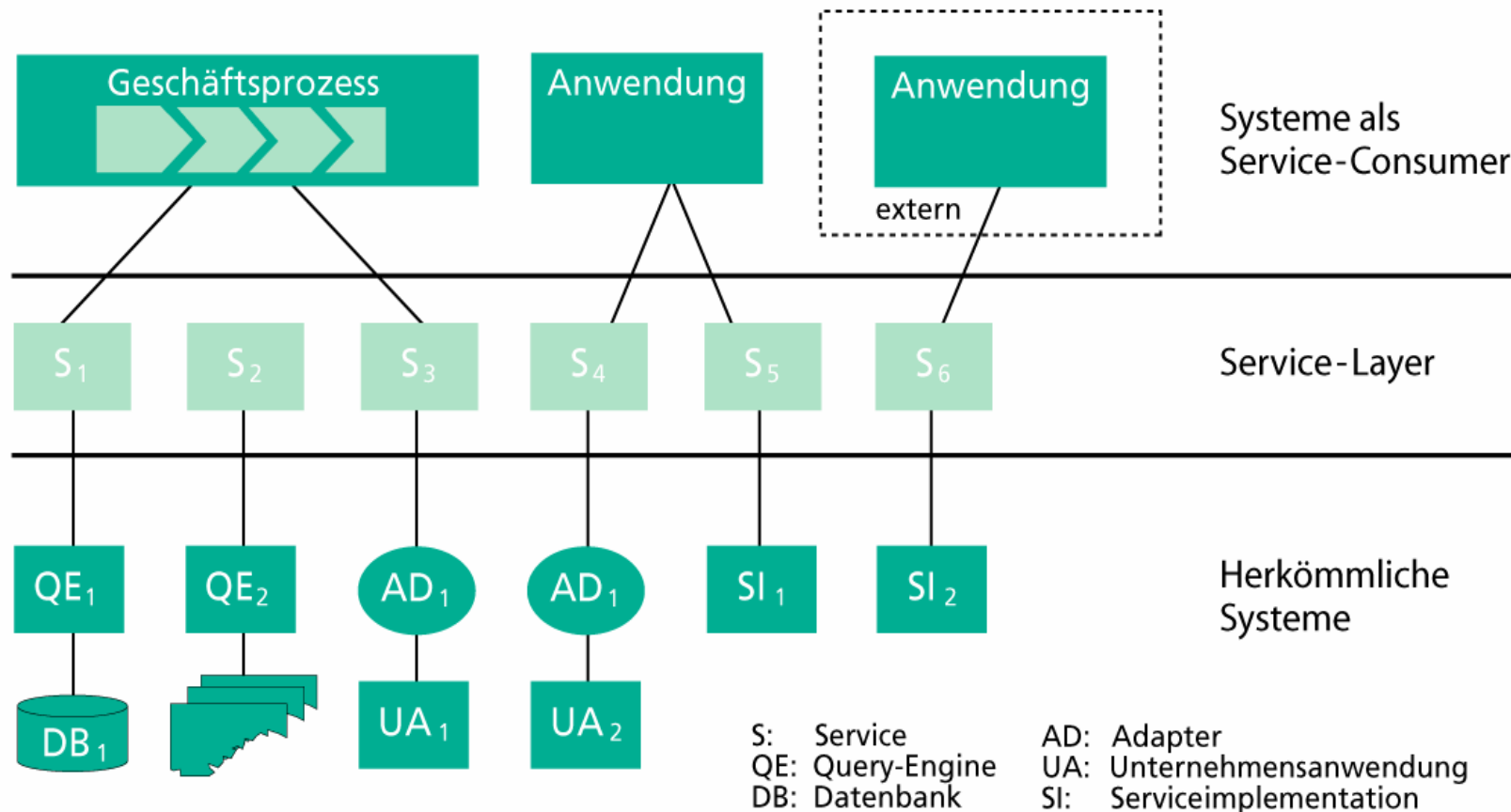


Konsequenzen für IAM der nächsten Generation?

- **vertrauenswürdige M2M-Kommunikation:**
 - Identitätsnachweis nur mit Server-Zertifikat: unzureichend
 - Attestierung von Eigenschaften/Attributen ist notwendig
- Zugriffsberechtigungen an **attestierten Ausführungs-umgebungen** knüpfen (trusted environment)
- TPM als Hilfsmittel **für Compliance-Nachweise:**
 - regelmässige Attestierung der Konfiguration,
 - Aktionen eindeutig mit Geräte-Identität verknüpfbar
- TPM als **sicherer Speicher** für Nutzer- und Dienste-Zertifikate
- **Protection Profile** für IAM-Einsatz notwendig?

3.2 Identität von Diensten in SOA

- Identifizieren von **Services**, deren **Betreiber** und deren **Nutzer**
- flexible **Komposition** von Diensten in Geschäftsprozessen

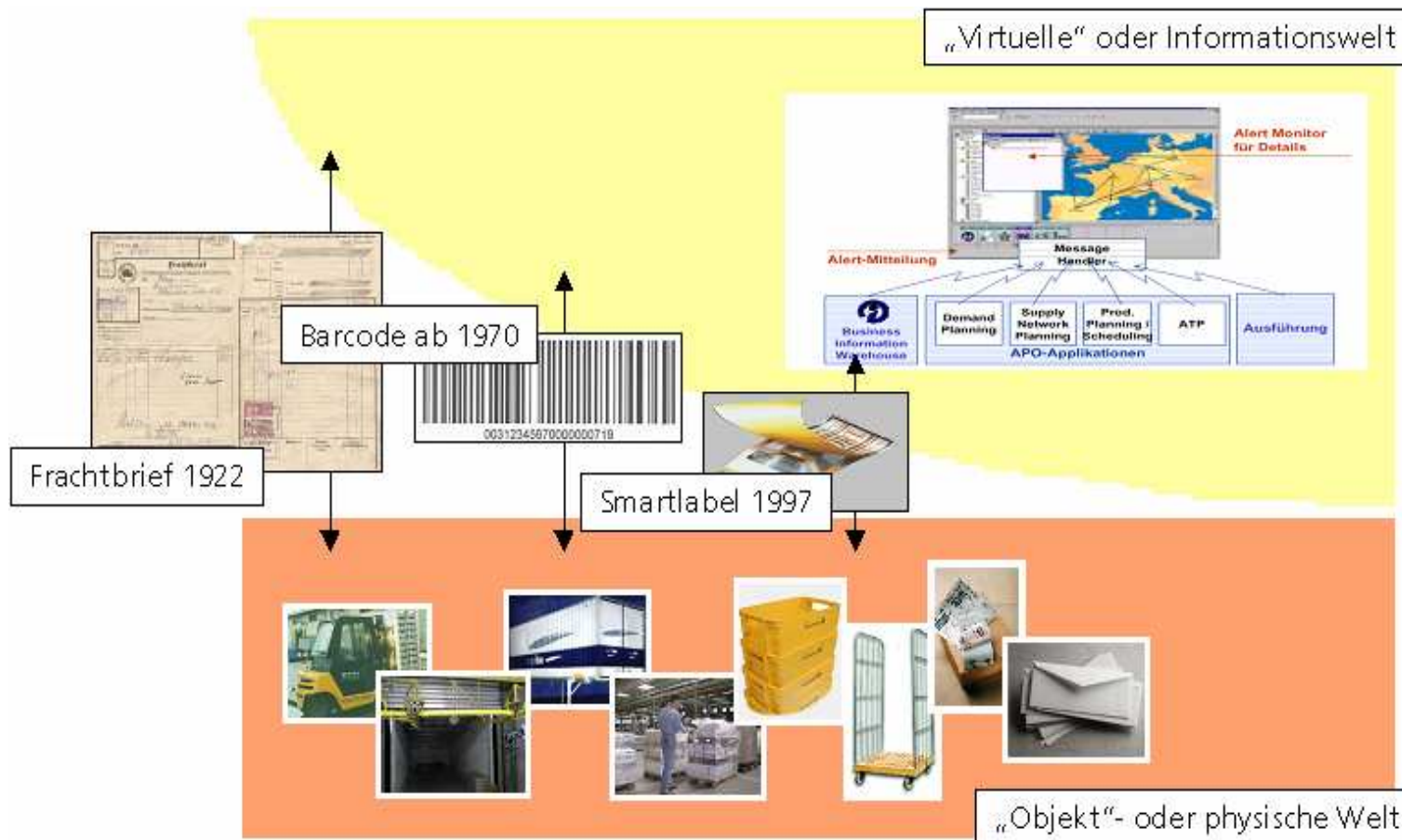


Konsequenzen für IAM der nächsten Generation?

- Orchestrierung von Diensten: ‚Grenzenloses‘ IAM?!
 - Konzern-, Land- , Branchen (z.B. Logistik)- übergreifend
 - Dynamische Anpassung an unterschiedliche Kulturen, rechtliche Vorgaben
 - Kontrollverlagerung beim Wegfall der ‚Grenzen‘:
Security as a Service?
- **Erforderlich:**
 - einheitliche **Bedeutung von Identitäten** in den Domänen!
 - einheitliche **Bedeutung von Berechtigungen**
 - **Identifikation von Services** und dessen Provider:
 - reicht signierter Code? Qualitätssiegel erforderlich? ...

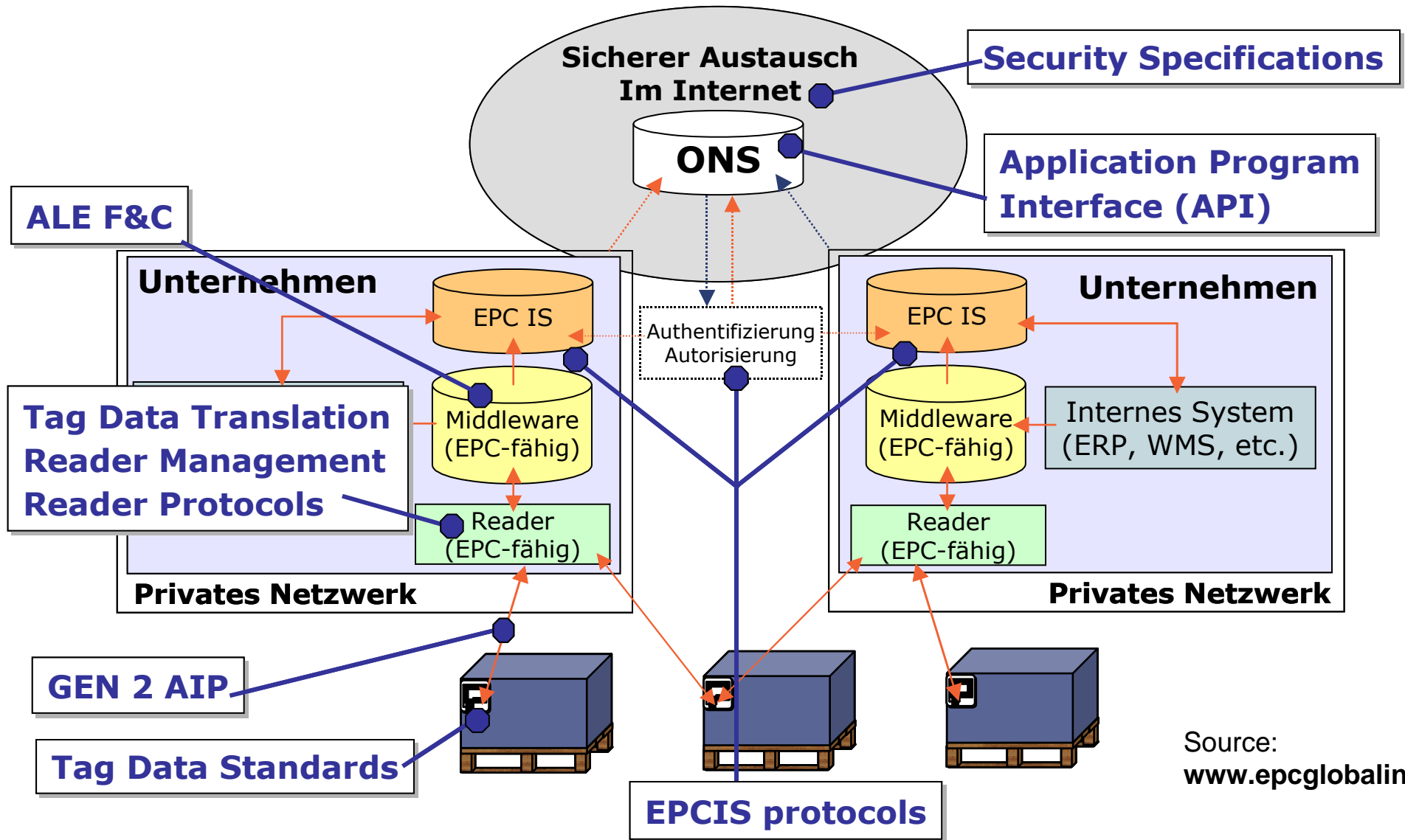
3.3 Internet der Dinge : Identifikation von Objekten

- **Konvergenz** von physischer und virtueller Welt
- Verknüpfung von Gütern und Information: **Tracking, Tracing**



RFID-Tag

Das EPC Modell: Internet der Dinge



Konsequenzen für IAM der nächsten Generation?

- **Fälschungssichere** Verknüpfung von IDs mit Objekten, z.B. für Komponentenidentifikation in Fahrzeugen (Reparatur)
- **Integrität** der Objekte, z.B. manipulierte Preis-, Verfalls-, Lagerdaten in RFID-Chip
- **Interoperation** mit Backend-Systemen: u.a. ERP, SCM, z.B. einschleusen von Viren in Backend-Systeme über Tag
- **Profilbildung**, Verletzen der Privatsphäre, z.B. bei Consumer-Produkten

Neue **Technologische-Verfahren** sind notwendig!

- Energie-sparend, ad-hoc, skalierend,

4. Take home Message

- IAM hat **viele Potentiale**
 - Sicherheit erhöhen, Kosten senken, Prozess-Optimierung
- Nutzen der Potentiale **erfordert neue Wege zur Sicherheit**
 - Prozess-Orientierung, Technologie-Integration, ...
- **Neue Herausforderungen** an IAM durch
 - SOA, Internet der Dinge mit RFID und Sensor-Knoten
- **Neue Wege der Sicherheit:**
 - Technologie (z.B. TPM) als Enabler nutzbar machen
 - Technologie (z.B. SOA) in Management integrieren
 - Technologie (z.B. RFID) gezielt weiterentwickeln



**Technik ist nicht Alles,
aber ohne Technik ist alles Nichts**

Vielen Dank für Ihre Aufmerksamkeit

Fragen?