



Identitätsmanagement in der Zukunft – Anwendungsszenarien & Blick in andere Länder

BITKOM Forum „Digitale Identitäten – Basis einer vernetzten Welt“

5. Oktober 2006

Frank Zimmermann, HP Consulting & Integration EMEA



Inhalt

- Einführung ins Thema Identitätsmanagement
 - Begriffskontext
- Identitätsmanagement in Unternehmen
 - Treibende Faktoren und Anwendungsszenarien
 - RFID - ID for everything
- eID-Karten
 - Ganzheitlicher Ansatz mit Beispielen aus anderen Ländern
 - Grundsatzfragen & Erfolgsfaktoren

In welchem Kontext können digitale Identitäten („Web-IDs“) eingesetzt werden?

e-citizen:

Passkontrolle

e-health:

Elektronisches Rezept

e-education:

Schulgeld bezahlen

e-democracy:

e-voting

e-tax:

Steuererklärung

e-police:

Bußgeldbescheid

e-car:

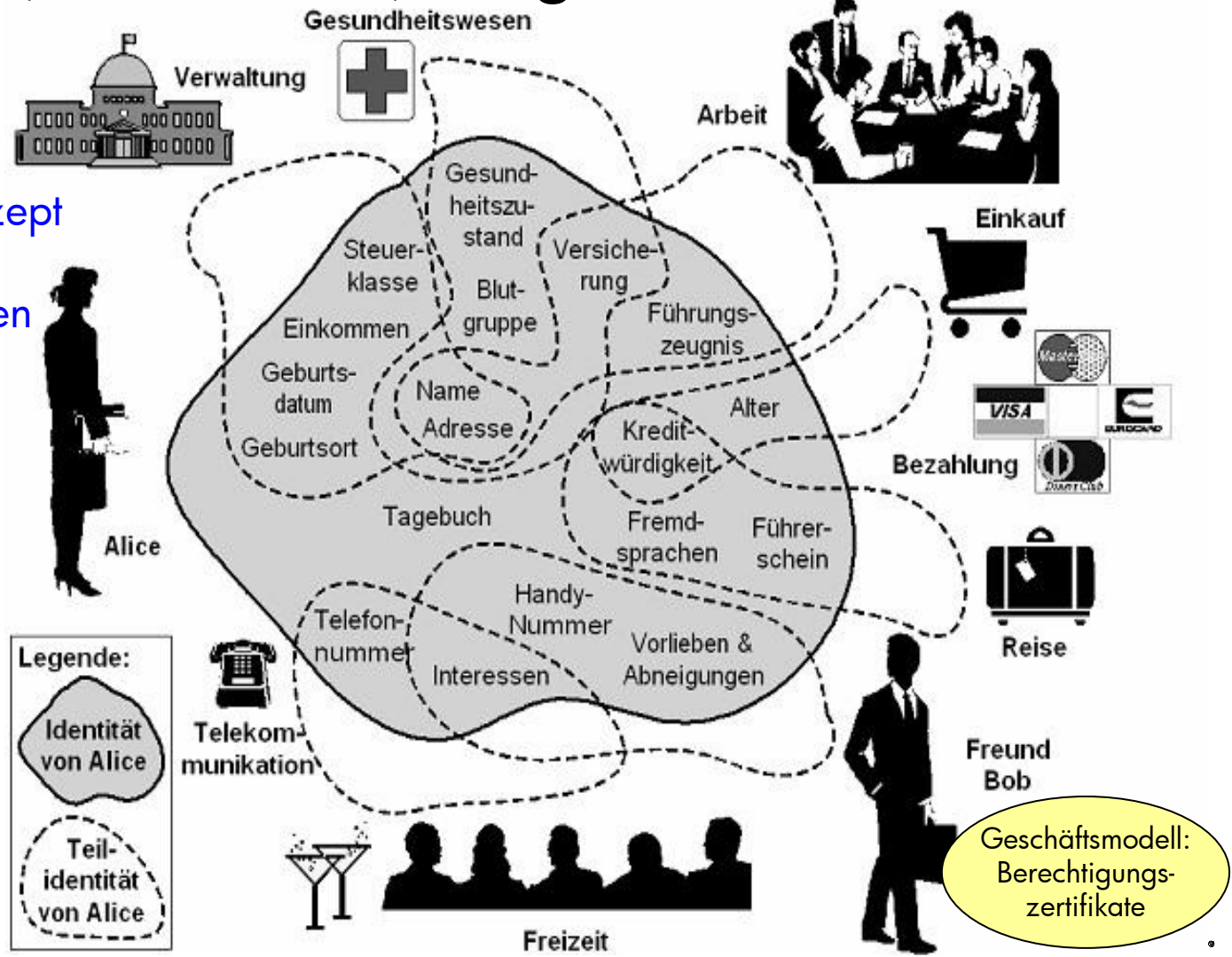
Halterwechsel

e-work:

Zutritt Arbeitsort

e-finance:

Online-Zahlungen



Quelle: Marit Hansen, ULD Schleswig-Holstein - Zitiert aus BITKOM Leitfaden „Web Identitäten Begriffsbestimmungen und Einführung in das Thema“ www.bitkom.org

„Ein Tag im Leben von ...“

Geschäftsreise von Frau XY:

- identifiziert sich bei automatischer **Passkontrolle** und am Zoll mittels ID-Karte
- geht zur Arbeit, passiert die **Zutrittskontrolle** zum Gebäude mittels ID-Karte
- logt sich ebenfalls mit der ID-Karte an seinem PC ein
- wickelt die **Steuererklärung** für die Mehrwertsteuer ab und überprüft eine Baubewilligung.
- tauscht einige **vertrauliche Dokumente** mit Juristen aus und unterzeichnet online einen Partnervertrag
- wickelt **E-Banking-Zahlungen** und **altersabhängige e-Services** im Internet ab
- fährt er nach Hause und wird auf dem Weg Zeuge eines Unfalls: Verletzte konnten schnell behandelt werden, da die Ärzte mittels Karten sofort online **Zugriff auf die Gesundheitsprofile** hatten
- Zeugenaussage **mit eID-Karte unterschrieben**.
- **Pay-TV** zu Hause akzeptiert ID-Karte zur Registrierung
- Polit-Sendung hilft bei Wahlentscheidung. Danach Abstimmung mittels **E-Voting**
- ...

Sind viele Identitäten in verschiedenen Kontexten ein Problem ? → Ja und Nein!

- **Nein – Vielfach Absicht, verschiedene Identitäten zu besitzen:**
 - je nach Kontext, Rolle oder Funktion
 - je nach Schutzbedürfnis & Zugangskontrolle (Passwort, Token, Biometrie)
 - je nach Notwendigkeit Anonymität und Informationen preiszugeben.
- **Ja – viele Identitäten & Zugriffspasswörter, die es zu verwalten gilt!**

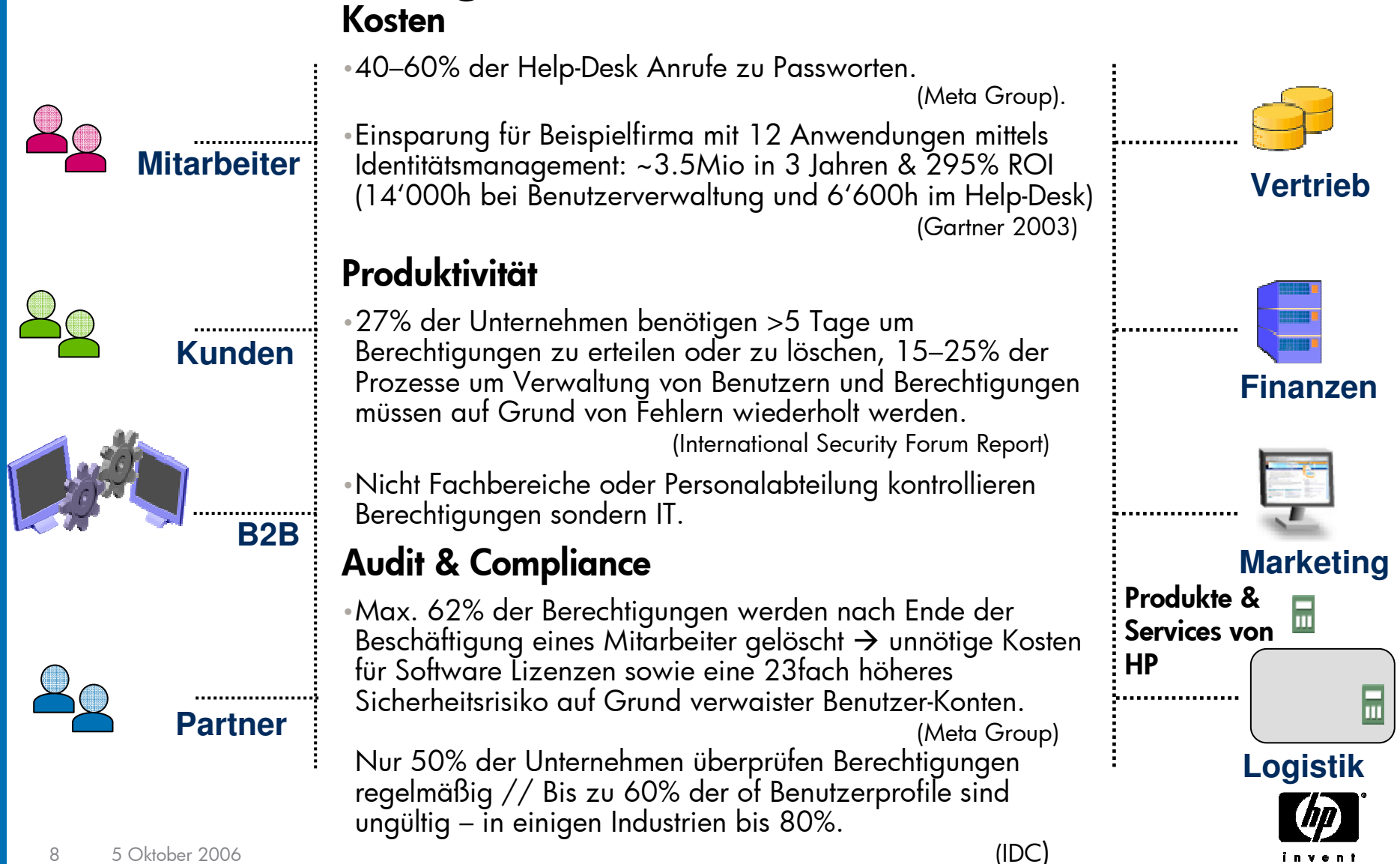
Passwort-Rücksetzen ist ein Kostentreiber für Help-Desks, weswegen Alternativen mit automatisierten Prozessen implementiert werden

 - **Passwort Manager** zum persönlichen Gebrauch (z.B. Token – Vortrag O. Winzenried).
 - **Identitätsmanagementlösungen** (IAM) in Unternehmen mit zentraler Benutzerverwaltung und Zugriffskontrolle, Single-Sign-On (SSO) Lösungen z.B. für Portale (zwischen Unternehmen: ID-Föderation – Vortrag H. Wieser)
 - Gemeinsame **Authentisierungsplattform** von Öffentlichen und kommerziellen Dienstleistungsanbietern (z.B. T-Online Netzausweis – Vortrag M.Gärtner, oder Electronic Service Delivery (ESD) Life Portal in Hongkong: <http://www.esd.gov.hk/home/eng/>) → Unterstützung mehrerer Verfahren

Inhalt

- Einführung ins Thema Identitätsmanagement
 - Begriffskontext
- Identitätsmanagement in Unternehmen
 - Treibende Faktoren und Anwendungsszenarien
 - RFID - ID for everything
- eID-Karten
 - Ganzheitlicher Ansatz mit Beispielen aus anderen Ländern
 - Grundsatzfragen & Erfolgsfaktoren

Was sind die treibenden Faktoren für Identitätsmanagement? → Geschäftsmodell !



„Ein Tag im Leben von ...“ Corporate ID card

Anwendungsszenarien:

- Zutrittskontrolle
- Parkplatz
- Zeiterfassung
- PC-Login
- E-Payment
- Remote-Zugriff
- Digitale Signatur
- E-Mail Verschlüsselung
- ...

Quelle:
SIEMENS



09:00 h

Access to the company's parking lot and the office



09:10 h

Time logging



09:15 h

Authentication for starting PC and further PC applications



12:00 h

Paying for lunch at the canteen



13:00 h

Leaving the company grounds to visit customers



14:00 h

Setting up a protected connection to the corporate network from the customer's



15:00 h

Signing a proposal in PDF format directly at the customer's



16:00 h

Access to the company's parking lot and the office



17:30 h

Mailing an encrypted revised concept design to the customer



18:00 h

Travel expenses are accounted for via an Intranet portal using digital signature

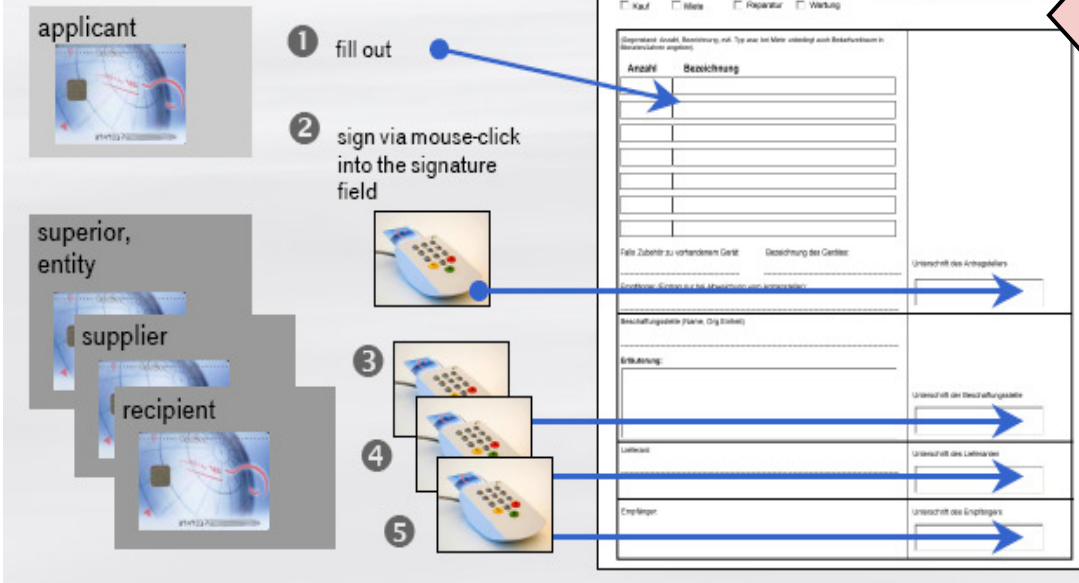


19:00 h

Time logging when leaving the office

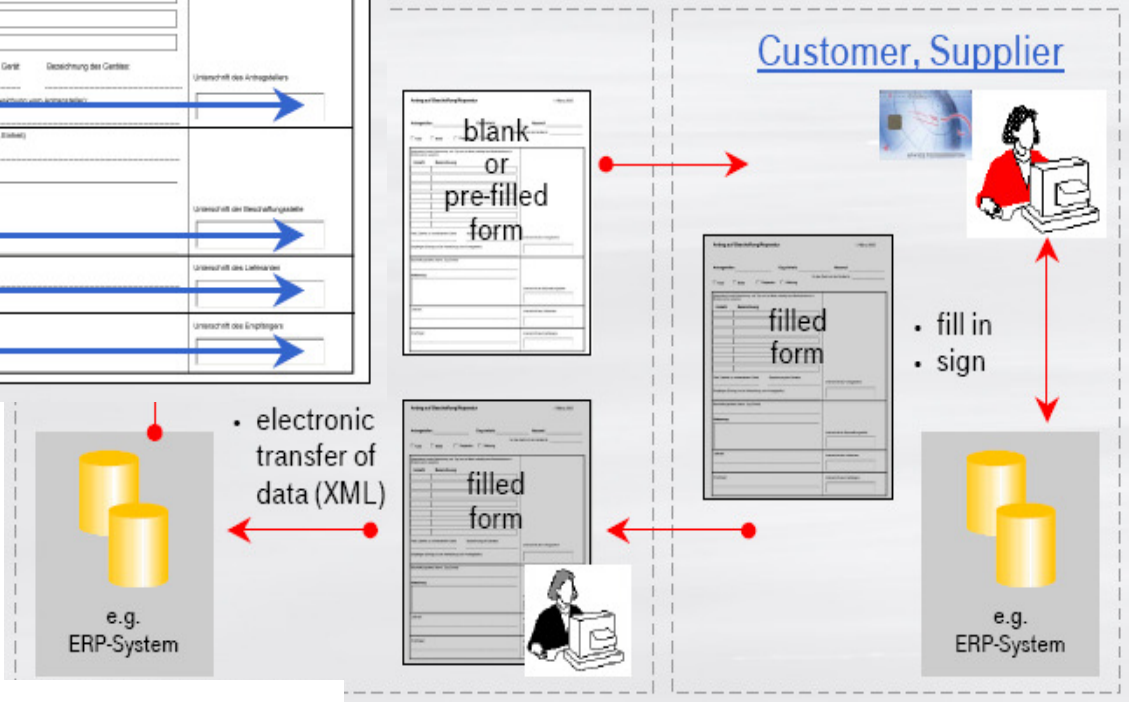
„Ein Tag im Leben von ...“ Optimierung von Geschäftsprozessen

■ Example: Application for Supply (e.g. a computer)



**Optimize Business Processes.
Releases, Approvals, Commitments,
Folder with Documents to be Signed.**

**Incorporate External Parties into Business Processes.
Forms as Documents and Data container.**



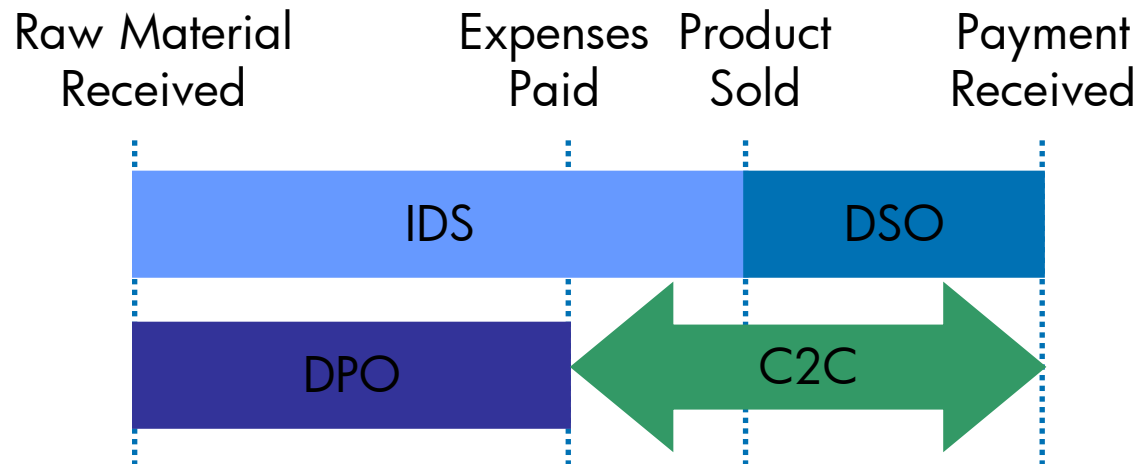
Quelle: **T** Systems

ICT-Security: Innovative Solutions
Systems Integration
PKA: May 17, 2006, Page 15/16



RFID – Anwendungsszenario

Wie zahlt es sich aus ?



IDS: Inventory Days of Supply (DOS)
 DSO: Days of Sales Outstanding
 DPO: Days of Payables Outstanding
 C2C: Cash to Cash Time

Beispiel-Schätzungen von HP

Receivables (DSO)	↘	-10 days → 2029m\$
+ Inventory DOS (IDS)	↘	-10 days → 1441m\$
- Payables	/	+1 days → 145m\$
= Cash to cash (d) (\$)		-21 days → 3615m\$

Verbundene Maßnahmen:

- Abstimmung von Konten
- Vendor Managed Inventory VMI
- Kollaborationen

RFID-Standard: EAN-UCC → EPC (Elektronic Product Code → EPC Global)

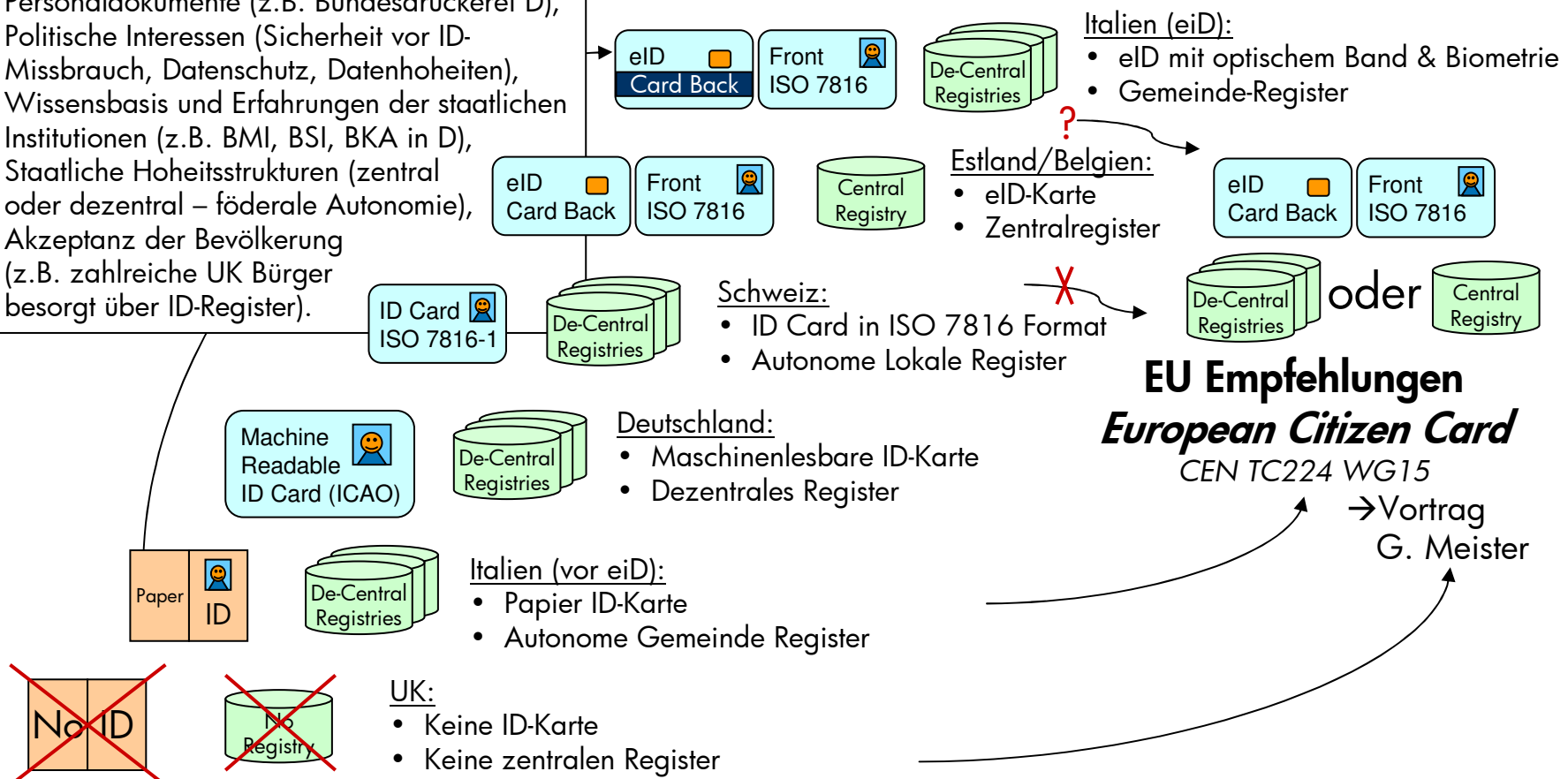
Inhalt

- Einführung ins Thema Identitätsmanagement
 - Begriffskontext
- Identitätsmanagement in Unternehmen
 - Treibende Faktoren und Anwendungsszenarien
 - RFID - ID for everything
- eID-Karten
 - Ganzheitlicher Ansatz mit Beispielen aus anderen Ländern
 - Grundsatzfragen & Erfolgsfaktoren

eID Interoperabilität (Situation in Europa)

Unterschiedliche Randbedingungen der Europäischen Staaten:

- Gesetzliche Grundlagen (z.B. keine ID in UK, allgemeiner Sichtausweis in D),
- Nationale Produzenten der Personaldokumente (z.B. Bundesdruckerei D),
- Politische Interessen (Sicherheit vor ID-Missbrauch, Datenschutz, Datenhoheiten),
- Wissensbasis und Erfahrungen der staatlichen Institutionen (z.B. BMI, BSI, BKA in D),
- Staatliche Hoheitsstrukturen (zentral oder dezentral – föderale Autonomie),
- Akzeptanz der Bevölkerung (z.B. zahlreiche UK Bürger besorgt über ID-Register).



EU Empfehlungen
European Citizen Card
 CEN TC224 WG15

→ Vortrag
 G. Meister

2000

2005

2008



Gesamthafte Betrachtung unter 6 Blickwinkeln

Technische & organisatorische Machbarkeit sind im Kontext von gesetzlichen & politischen Anforderungen, gesellschaftlicher Akzeptanz und Benutzerfreundlichkeit zu betrachten.

Anforderungen, Rahmenbedingungen und Lösungskomponenten sind unter folgenden Blickwinkeln zu analysieren:

Organisation & Prozesse

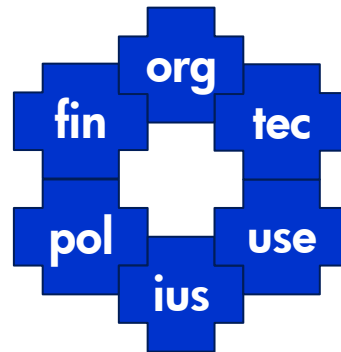
Beantragung, Herausgabe, Produktion, Betrieb, Dienstleistungen

Geschäftsmodelle

Kommerzielle & öffentliche e-Services

Politik & Gesellschaft

Breite Akzeptanz & Vertrauen



Technische Lösung

Infrastruktur & Anwendung & Karten

Ergonomie & Benutzung

Mehrwert & Benutzerfreundlichkeit

Gesetze, Verordnungen & Standards

Rückgriff auf Nationale, Europäische, Internationale Vorgaben

Öffentlicher Sektor

Privater Sektor

Gesamthafte Betrachtung unter 6 Blickwinkeln

Technische & organisatorische Machbarkeit sind im Kontext von gesetzlichen & politischen Anforderungen, gesellschaftlicher Akzeptanz und Benutzerfreundlichkeit zu betrachten.

Anforderungen, Rahmenbedingungen und Lösungskomponenten sind unter folgenden Blickwinkeln zu analysieren:

Organisation & Prozesse

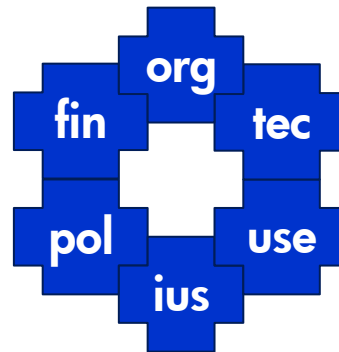
+Biometrie, +Verzeichnisse, +Call Center – *SLA und mobile Registrierung in Bulgarien*

Geschäftsmodelle

eID in eGov in Hong-Kong

Politik & Gesellschaft

Stakeholderansatz Österreich



Technische Lösung

Leser – gratis ab 12 in Belgien

Ergonomie & Benutzung

Vision: einfach, universell, überall

Gesetze, Verordnungen & Standards

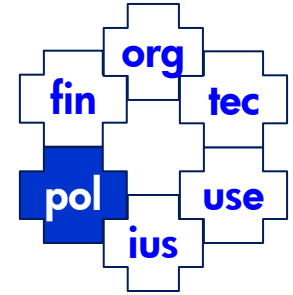
ICAO, CEN, Technische Standards, Datenschutz in Italiens eID

Öffentlicher Sektor

Privater Sektor

Politik & Gesellschaft

→ *Einbeziehung aller „Stakeholder“*

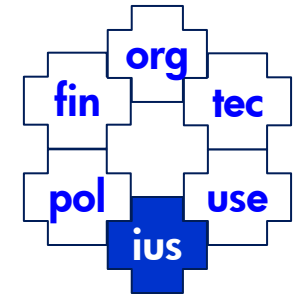


Bürgerkarte Österreich – erfolgreiches Zusammenspiel von Wissenschaft, Staat und Unternehmen schafft Vertrauen & Akzeptanz

- Identity Management von Bürgern und juristischen Personen (Firmen, Vereine) mittels Bürgerkarte
 - wahlweise auf Handy, Bank-Karte oder eCard
 - **Datenschutz** basiert auf einer geheimen Stammzahl, die aus dem zentralen Register mit dem Schlüssel der ausstellenden Behörde abgeleitet wird, außerdem werden eindeutige bereichsspezifische Personenkennzeichen (pBK) erzeugt, die für spezifische Bereiche gelten.
- Ganzheitlicher Ansatz bei der Realisierung von FinanzOnline (Quelle: J. Makolm, BMF, IRIS Tagung Wien 06): Integration aller Betroffenen – **Stakeholder Theorie**
 - Betroffene Stakeholder: Finanzverwaltung & SteuerzahlerInnen
 - Beeinflussende Stakeholder, Lobbys: Kammern der Wirtschaftstreuhänder, Rechtsanwälte und Notare, Gemeindebund, etc.
 - Definition: Projektziele → Stakeholder-Verantwortung → Arbeitspakete

Gesetze, Verordnungen & Standards

→ *Rückgriff auf Internationale Vorgaben*



Verwendung existierender Standards & Spezifikationen fördert Interoperabilität und spart Kosten

• Internationale Vorgaben für Reisedokumente

- Europäische Direktiven (Verordnung des Rates 2252/2004 (13.12.2004))
- ICAO Doc 9303 Amendment e-Passport Technical Advisory Group (TAG) Biometrics deployment of Machine Readable Travel Documents (MRTD)

• Internationale Standards für digitale Signaturen & eID-Karten

- Arbeitsgruppen des European Committee for Standardization CEN - CEN Workgroup Agreements, z.B. CWA 15264 [Architecture for a European interoperable eID system](http://www.cenorm.be/) (<http://www.cenorm.be/>) (Vortrag → G. Meister)

• Beispiel eID-Karte Italien für Daten Schutz

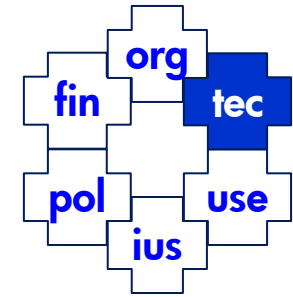
- Gehashte Personeninformationen im Common Name (CN) des Zertifikates - Vorteil der Anonymisierung in den Verzeichnissen.

Wesentliche Standards:

Zertifikate	X509
Contact Cards	ISO 7816
Contact-less Cards	ISO 14443
OS/reader	PC/SC
Application Interface	CAPI/CSP or PKCS#11

Technische Lösung

→ *Leser-Infrastruktur essentiell*



Keine Kartenbenutzung ohne Leser-Infrastruktur, Treiber und Software → Vermeiden etwas anschaffen oder installieren zu müssen

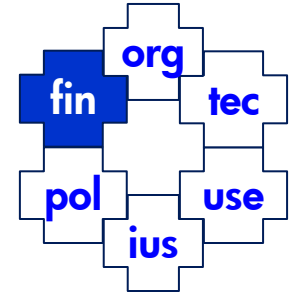
- Herausforderung:
 - Card-OS (Native, JavaCard, MULTOS) mit speziellen Applikationen.
 - PC SW-Module erforderlich, das Chip unterstützt und eine Standard-Schnittstelle (PKCS#11, MS CAPI) für Applikationen bereitstellt.
 - PC/SC Treiber für kompatible Kartenleser bereits Betriebssystem-Standard\$
- **Beispiel eID-Karte Belgien für Jugendliche ab 12 Jahre**
 - Staat schenkt ihnen „zum Geburtstag“ einen Kartenleser, um den direkten Einsatz zu ermöglichen (relativ günstiges Programm, um Problem fehlender Infrastruktur zu adressieren (mögliche Dienstleistungen speziell für Generation X)

Idealerweise sind Kartenleser und Softwarekomponenten in allen Neugeräten bereits installiert (vgl. USB)



Geschäftsmodelle

→ *Kommerzieller & öffentlicher Nutzen*

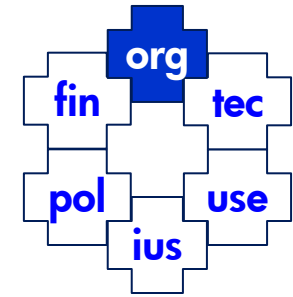


Status heute: entweder Verwendung zu selten oder Einsatz ist nur für beschränkte Zielgruppe relevant

- **Beispiel ESD Life Hong Kong** – nur 14 von >200 eGovernment Services benötigen eID, z.B. jährliche elektronische Steuererklärung oder Adressänderung
- **Geschäftsmodell aus Sicht des Staates:**
 - eGovernment-Anwendungen reichen nicht aus. Doch für Staat reicht Grenzkostenbetrachtung: Chip & Zertifikat zur e-Authentisierung sind zu relativ geringen Grenzkosten zum Personalausweis zu haben.
 - Höhere Einsatzfrequenz und mehr Einsatzbereiche durch kommerzielle Anwendungen (Einnahmen aus Attributs- und Berechtigungs-zertifikaten)
- **Geschäftsmodell aus Sicht kommerzieller Service-Anbieter:**
 - große Verbreitung ist notwendig → verkürzte Einführungszyklen und Anreizsysteme ?
 - Haftungsfragen müssen geklärt sein → "economy of scale" für Kosten von Karten, Chips und Zertifikaten, jedoch nicht für Versicherung der Haftung, die von Höhe der getätigten Transaktionen abhängt

Organisation & Prozesse

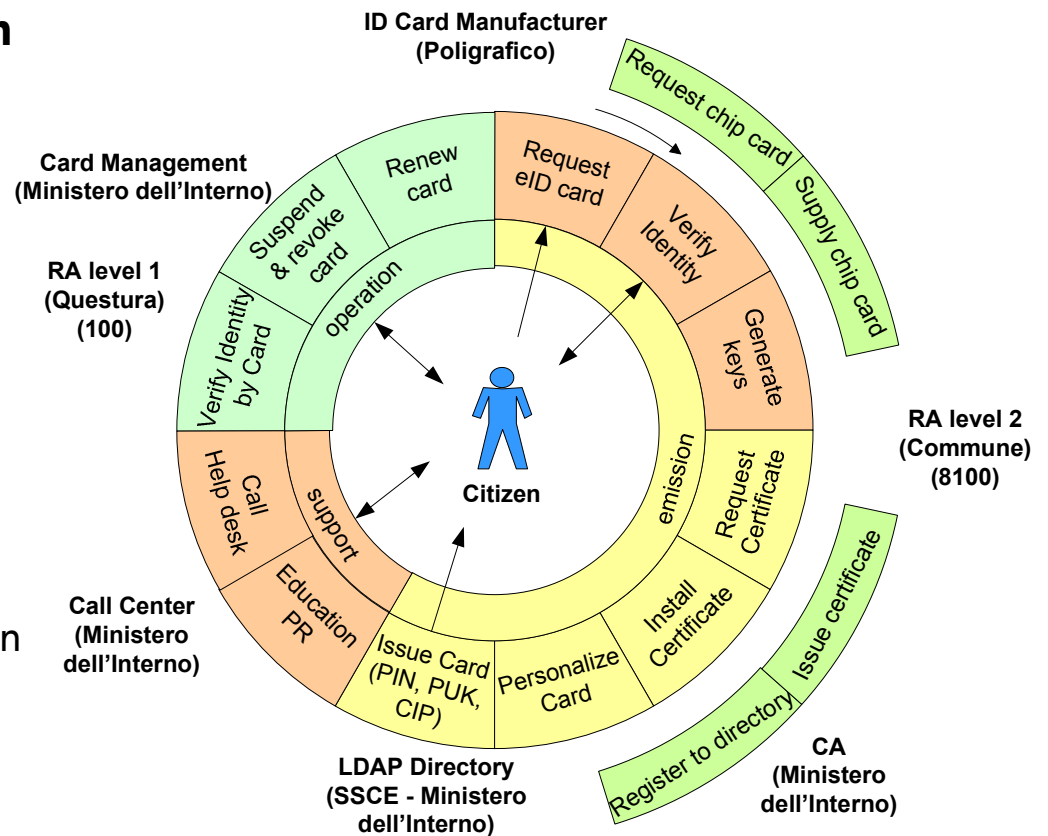
→ ID Lebenszyklus elektronisch erweitert



Prozesse um Beantragung, Herausgabe, Produktion, Betrieb und Dienstleistungen sind bezüglich Aufnahme und Prüfung biometrischer Daten, Zertifikaten, Verzeichnisdiensten, Call-Center Funktionen, Leser-Infrastruktur etc. zu erweitern

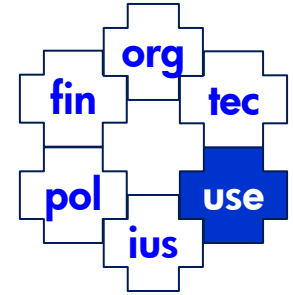
→ Beispiel Italien:

- Beispiel Ausstellung von Personaldokumenten in Bulgarien
 - Service Level Agreements für Passausstellung innerhalb 24 Stunden bzw. 3 Tagen, für Aufenthaltsbewilligungen generieren zusätzliche Einnahmen
 - Anreize für beschleunigte Ausbreitung: Tombolas, TV-Spots, mobile Antragstellung vor Ort in Betrieben, uvm.



Ergonomie & Benutzung

Universalität & Benutzerfreundlichkeit



Vision zum Elektronischen Personalausweis

- einfach in der Handhabung,
- universell in der Anwendbarkeit
- kosten-günstig durch Erreichen von Skaleneffekten.
- Der elektronische Personalausweis ist das allgemein gültige Mittel zur Identifikation, welches **in der realen und digitalen Welt gleichermaßen** eingesetzt wird.
- Der Benutzer weiß von der elektronischen ID-Karte nicht mehr, als dass er sich nach **Einführen der Karte in einen Kartenleser und Eingabe der PIN** gegenüber einem System elektronisch ausgewiesen hat und dass er diesen digitalen Ausweis auch über das Internet sicher einsetzen kann.
- Der Bürger erwartet, dass sein elektronischer Personalausweis **einfach, sicher und immer und überall funktioniert**, das heißt so einfach verwendbar ist wie eine Bank- oder Kreditkarte.

Grundsatzfragen und Erfolgsfaktoren

- **Politischen Rahmenbedingungen** müssen stimmen
 - Förderung der eID durch Staat, der nur Grenzkosten betrachten muss: ID-Karte gibt er bereits heraus – muss also „nur“ noch der Chip rauf oder rein.
 - Übergreifende Koordination der Kartenprojekte (Job, Health, ID) → **Identitätskarte** versus Datenkarte
- Aufbau & Ausbreitung der **Infrastruktur**
 - Durchbrechen des „Huhn und Ei Problems“ bei der Infrastruktur (Kartenleser, Karten mit Chip) und den Anwendungen
- Schaffung von Vertrauen & **Akzeptanz** in der Bevölkerung
 - Kartenbenutzung inkl. Umgang mit PIN-Nummern ist bekannt
 - Nutzen zeigen und Datenschutz & Sicherheit gewährleisten
- Internationale Standards und **Interoperabilität**
 - ID-Pflicht in D, B, GR, E, ... freiwillig in A, SF, F, I, L, NL, S, ...
 - Gültigkeit & Standardisierung innerhalb EU/Schengen-Staaten
- **Finanzierung** / Business Case
 - Wer macht Initialinvestitionen in die Infrastruktur?
Was ist Bürger bereit zu zahlen?
 - Klärung der **Aufgabe des Staates** und der Wirtschaft

Vielen Dank

Vision zum Elektronischen Personalausweis

- einfach in der Handhabung,
- universell in der Anwendbarkeit
- kosten-günstig durch Erreichen von Skaleneffekten.

