Welcome to the ICT commission

Engineering the Knowledge Society

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

WFEO
World Federation of Engineering Organisation

ict.satw.ch

world summit on the information society
Geneva 2003 - Tunis 2005

ifip

Identity Management & Trust

Workshop SATW ICT Commission
Münchenwiler, 2./3. November 2006

Kurze Einführung durch Markus Fischer

2. November 2006

In a network(ed) environment, Identity is key

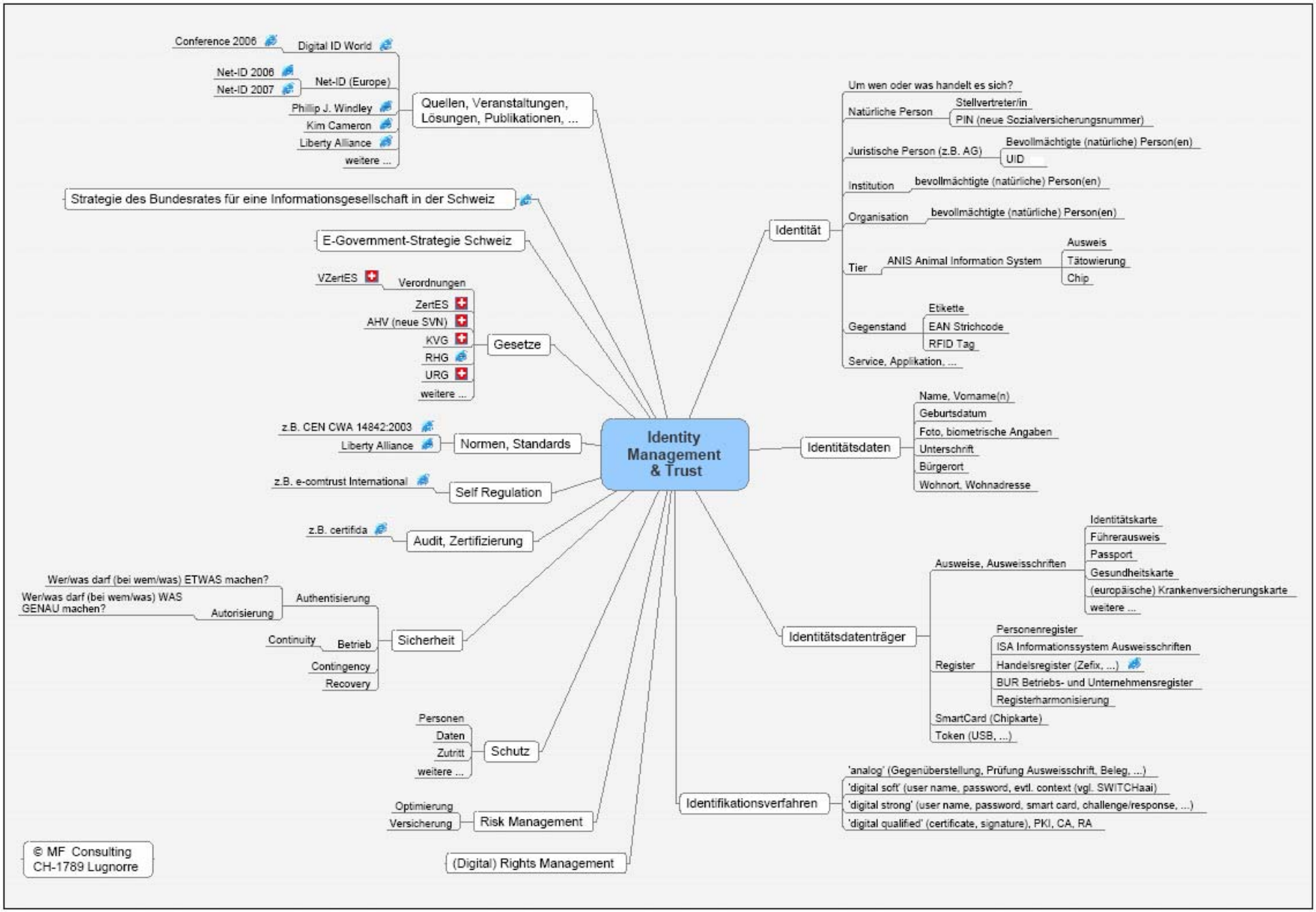
„When it comes to enabling a truly virtual world that can accommodate the breadth and depth of human endeavor, nothing is more important than identity.

Digital identity is the keystone that will ensure that the Internet infrastructure is strong enough to meet basic expectations for not just service and functionality, but security, privacy, and reliability.

Identity must become persistent through the continuum of any given business process, spanning not just multiple applications, but also multiple organizations.

Only then can identity provide the predicates for corporate governance, security, regulatory compliance, risk and liability management, and other core business functions.“

Jamie Lewis, CEO and Research Chair, Burton Group, February 2005
‚Digital Identity‘, Phillip J. Windley, O‘REILLY, August 2005


Identity Management & Trust
Quellen, Veranstaltungen, Lösungen, Publikationen, ...
Conference 2006
Digital ID World
Net-ID 2006
Net-ID 2007
Net-ID (Europe)
Phillip J. Windley
Kim Cameron
Liberty Alliance
weitere ...
Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz
E-Government-Strategie Schweiz
Gesetze
VZertES
Verordnungen
ZertES
AHV (neue SVN)
KVG
RHG
URG
weitere ...
Normen, Standards
z.B. CEN CWA 14842:2003
Liberty Alliance
Self Regulation
z.B. e-comtrust International
Audit, Zertifizierung
z.B. certifida
Sicherheit
Wer/was darf (bei wem/was) ETWAS machen?
Authentisierung
Wer/was darf (bei wem/was) WAS GENAU machen?
Autorisierung
Continuity
Betrieb
Contingency
Recovery
Schutz
Personen
Daten
Zutritt
weitere ...
Risk Management
Optimierung
Versicherung
(Digital) Rights Management
Identität
Um wen oder was handelt es sich?
Natürliche Person
Stellvertreter/in
PIN (neue Sozialversicherungsnummer)
Juristische Person (z.B. AG)
Bevollmächtigte (natürliche) Person(en)
UID
Institution
bevollmächtigte (natürliche) Person(en)
Organisation
bevollmächtigte (natürliche) Person(en)
Tier
ANIS Animal Information System
Ausweis
Tätowierung
Chip
Gegenstand
Etikette
EAN Strichcode
RFID Tag
Service, Applikation, ...
Identitätsdaten
Name, Vorname(n)
Geburtsdatum
Foto, biometrische Angaben
Unterschrift
Bürgerort
Wohnort, Wohnadresse
Identitätsdatenträger
Ausweise, Ausweisschriften
Identitätskarte
Führerausweis
Passport
Gesundheitskarte
(europäische) Krankenversicherungskarte
weitere ...
Register
Personenregister
ISA Informationssystem Ausweisschriften
Handelsregister (Zefix, ...)
BUR Betriebs- und Unternehmensregister
Registerharmonisierung
SmartCard (Chipkarte)
Token (USB, ...)
Identifikationsverfahren
'analog' (Gegenüberstellung, Prüfung Ausweisschrift, Beleg, ...)
'digital soft' (user name, password, evtl. context (vgl. SWITCHaai)
'digital strong' (user name, password, smart card, challenge/response, ...)
'digital qualified' (certificate, signature), PKI, CA, RA
© MF Consulting
CH-1789 Lugnorre

Identitäten in der ‚analogen' Welt

Person

repräsentiert durch

Einzelfirma

CH-217-3531433-1
EHRA-Id 762683
MWSt Nr. 621 778
AHV Nr. 812.263

- ausgegeben durch und geführt von/bei diversen Stellen der Öffentlichen Hand
- registriert in der zentralen Datenbank ISA (Informationssystem Ausweisschriften) des Bundesamtes für Polizei (Fedpol)

Identity, Authentication, Authorization…

(digital) (federated) Identity Management:

⇨ Antwort auf die Frage: Wer ***ist***…?

Authentisierung (authentication):

⇨ Antwort auf die Frage: Wer ***darf***…?

Autorisierung (authorization):

⇨Antwort auf die Frage: Wer darf ***was***…?

Governance:

⇨ ***Wer…***

⇨ ***hat…***

⇨ ***was…***
…wann
…womit

…gemacht?

[1] in the language of digital identity: persons and/or things, called subjects or entities

…zum Beispiel im e-Banking

1. Schritt:
Identitätsprüfung anlässlich Aufnahme der Geschäftsbeziehung

2. Schritt:
Regelung der ***Zeichnungsberechtigung,*** Vollmacht(en)

3. Schritt:
Objekte (Konti, Depot usw.), Funktionen, Output

4. Schritt:
Regelung des ***Zugriffs*** und der ***Transaktionen*** (Applikationen, Services, Devices)

Kunden-Dossier

Kopie von

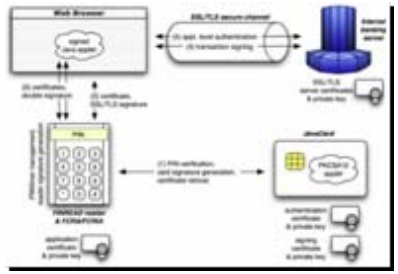
Unterschriftenkarte

Kundendaten

CIF, …

Aufträge, Auszüge, Belege

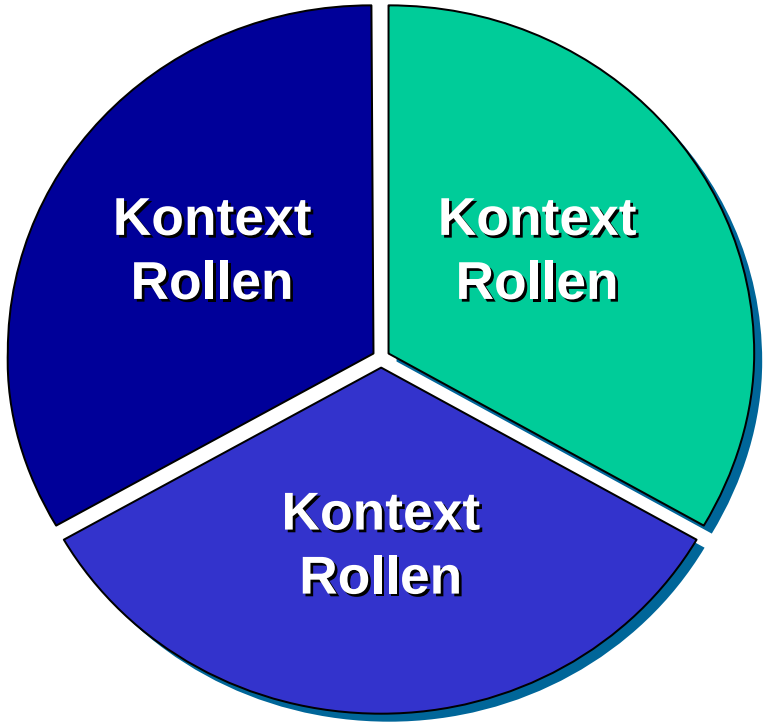
PIN, …



Identitäten und ihr Umfeld (Kontext)

Person

- Individuum
- Familie
- Freunde
- Bekannte
- Hobbies
- Reisen
- …



Beruf

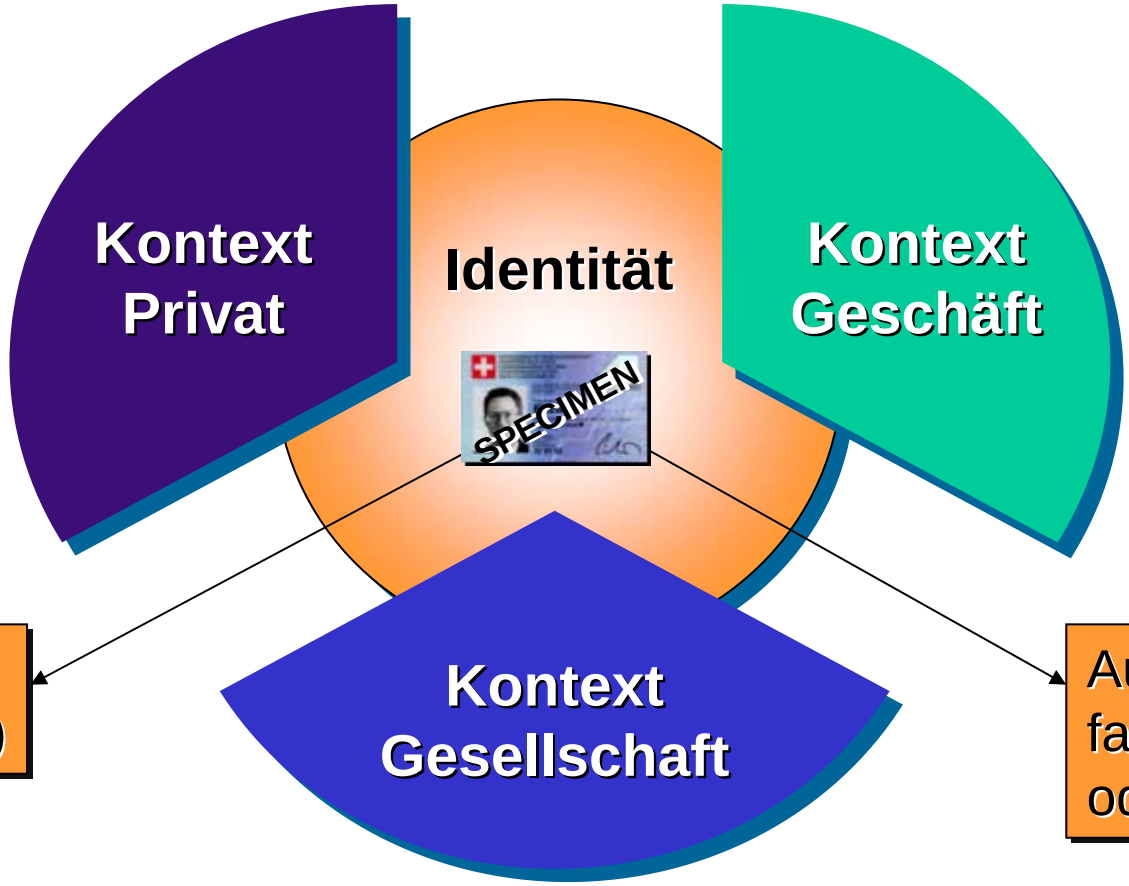
- Bildung
- Job
- Karriere
- Funktionen
- Leistungen
- Strukturen
- Prozesse
- Branchen
- Märkte
- …

Gesellschaft

- Bürger
- Gemeinde, Kanton, Staat
- Vereine, Verbände, Politik, Militär, …

Identitäten und kontextspezifische Rollen

- Mieter
- Konsument
- …



- Schule
- Arbeitgeber
- AHV
- Geschäfts-partner
- …

eindeutig!
(evtl. ‚Alias‘)

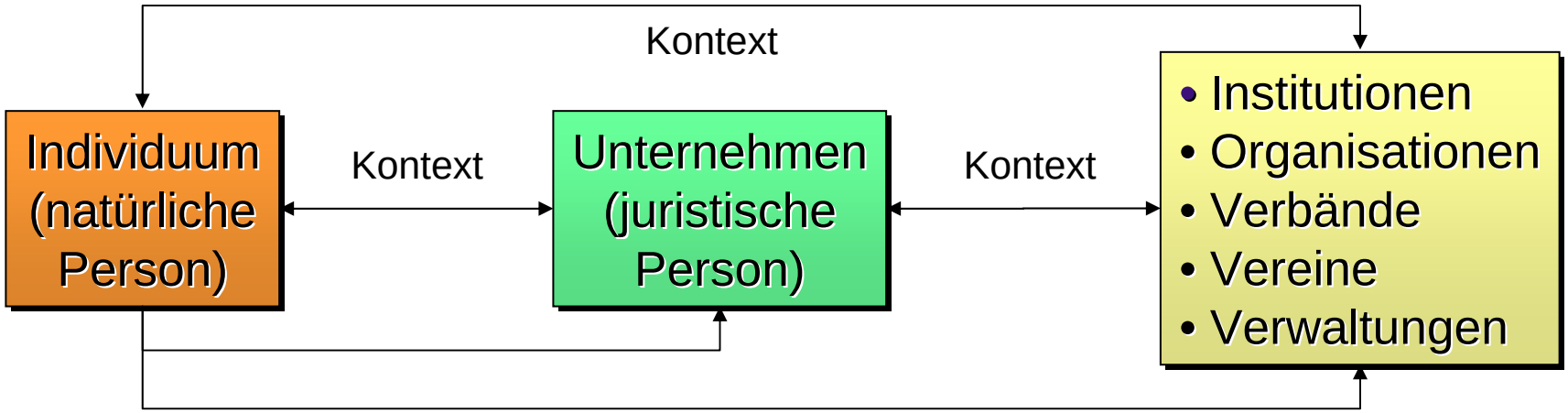
(‚DNA‘)

Ausweis
falls notwendig
oder bei Bedarf

(‚DNA-Test‘)

- Staatsbürger
- Vereinsmitglied
- …

HandeInde Identitäten generieren Profile

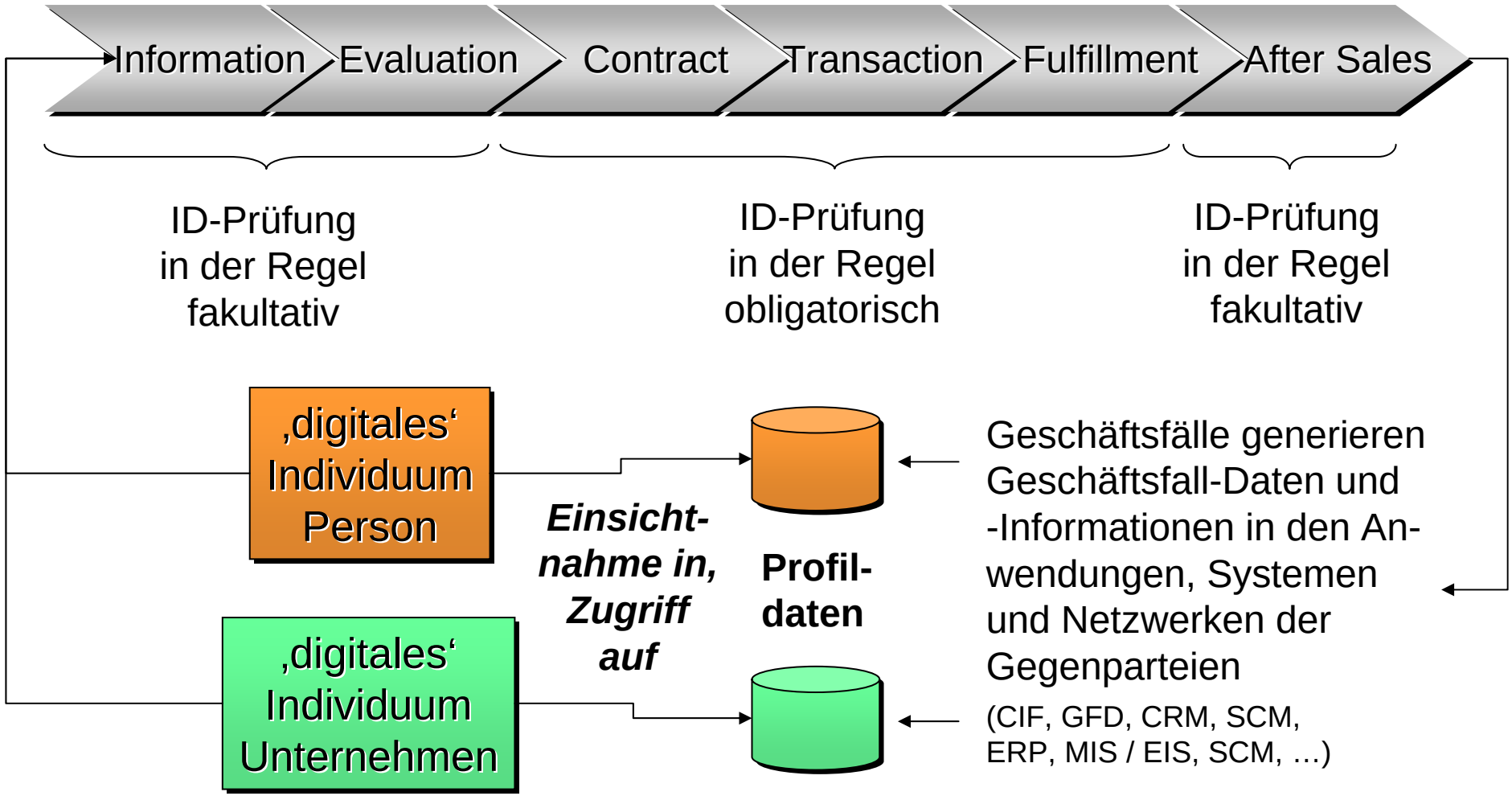


handelt

- *als*… (⇨ Funktionsträger)
- *entlang von*… (⇨ Geschäftsprozesse)
- *verantwortlich für*… (⇨ Menschen, Produkte, Verträge, …)
- *einzeln, kollektiv zu*… (⇨ HR, SHAB, Zefix, Teledata, …)

⇨ Formel: Identität + Rolle = Profil (generiert und bewirtschaftet von, bei ...)

Identitäten in ‚elektronischen' Prozessen



Die ‘Digitalisierung’ von Identitäten

Person: PIN

repräsentiert durch

- **PIN** (neue Sozial-versicherungsnr.)
- **Pass** mit biometri-schen Merkmalen (Daten in ISA)

Unternehmen: UID

CH-217-3531433-1

(EHRA-Id 762683)
(MWSt Nr. 621 778)
(AHV Nr. 812.263)

- **HR (zefix)** (öffentlich)
- **BUR** (nicht öffentlich)

Wesentliche Merkmale und Kriterien

1. Digitale Identitäten natürlicher und juristischer Personen als Datensätze, welche diese Identitäten eineindeutig beschreiben
2. Herausgabe, Registrierung, Führung und Bewirtschaftung dieser Datensätze (z.B. PIN, UID) in Registern der Öffentlichen Hand
3. Verfügbarmachung solcher Identitäts-beschreibender Datensätze auf persönlichen Datenträgern (SmartCard, USB Token usw.)
4. Einsatz solcher Datenträger im Kontext zu Interaktionen (Privat-wirtschaft, Öffentliche Hand, Gesundheitswesen usw.)
5. Einsatz von Organisationen, Instrumenten, Verfahren und Services (z.B. PKI) zwecks sicherer praktischer Abwicklung
6. Verwendung zusätzlich sichernder Instrumente und Massnahmen (z.B. digitale Signatur) für qualifizierte Transaktionen

Situation in der Schweiz

- Projekt ‚eID' 2002 ausgelöst, 2004 gestoppt
- UID konzipiert und realisiert, aber immer noch in Diskussion (BUR)
- Gesetz und Verordnug elektronische Signatur in Kraft
- Drei PKI Solution Providers sind inzwischen zertifiziert
- So gut wie keine Services für die breite Öffentlichkeit verfügbar; es mangelt an politischem Willen, an Commitment und an Führung, daher kommt die Umsetzung kaum voran

Aber

- erfreuliche Entwicklung seit Mitte 2005 (neue SVN = PIN)
- EPID hat über die SPIN ‚gewonnen'
- Konkrete Fortschritte insbesondere seit Mitte 2006

Situation und Entwicklung seit Mitte 2006

„Im Juni haben die eidgenössischen Räte mit einer umfassenden Änderung des AHV-Gesetzes die Einführung der neuen Sozialversicherungsnummer (SVN) und mit dem neuen Registerharmonisierungsgesetz (RHG) die Harmonisierung der kommunalen und kantonalen Einwohnerregister sowie der Personenregister des Bundes beschlossen.

Bundesrat und Parlament haben sich klar für die Einführung der neuen Sozialversicherungsnummer in einem **gesetzlich begrenzten Umfeld** ausgesprochen. Dieses besteht aus den Bereichen **Sozialversicherungen, Gesundheit, Steuern, Bildung** sowie dem **Einwohner-, Zivilstands- und Ausländerwesen**.

Zwar wurde der Anspruch einer universellen Personenidentifikationsnummer in der politischen Diskussion weder vom Bundesrat noch vom Parlament bestätigt. Kreise des Datenschutzes befürchteten sogar eine unkontrollierbare Ausweitung der Verwendung der neuen AHV-Nummer. Dennoch ist die **Verwendungsmöglichkeit der neuen SVN** nun **sehr weit gehend**, wenn man die Revision des AHV-Gesetzes und das neue RHG zu Grunde legt.“

Situation und Entwicklung seit Mitte 2006

„Leider ist insbesondere im Katalog der priorisierten Vorhaben der neuen **E-Government-Strategie Schweiz** dieser aktuelle gesetzgeberische Stand nicht ersichtlich.

Die beiden genannten gesetzlichen Reglungen bilden den **Grundstein für viele auf die Schweizer Bevölkerung bezogene E-Government Anwendungen**, übrigens auch für die **Versichertenkarte** gemäss KVG Art. 42a (in Kraft seit 1.1.2005).

Im Rahmen des RHG wird zum Beispiel eine **IKT-Plattform** aufgebaut, die **allen Gemeinden der Schweiz erlaubt, Daten bei Zu- und Wegzügen von Einwohnern medienbruchfrei auszutauschen**.

Sowohl in der E-Government-Strategie als auch im Bericht dazu sollte diese Funktion der gesetzlichen Regelungen aufgezeigt werden. …“

Die **Motion 04.3228 Digitale Identitäten** wurde in der Herbstsession 2006 aus Zeitmangel nicht behandelt und muss neu eingegeben werden.

Die Diskussion ist nötig und trägt zur Klärung offener Fragen bei

„… Die Authentifizierung der Benutzer ist an eine speziell zu diesem Zweck entwickelte Infrastruktur delegiert, bei der Authentifizierung und Autorisierung getrennt sind.

Der Sicherheitszone vorgelagert ist eine so genannte demilitarisierte Zone, wo die Abklärung von Identität und Berechtigung zentral erfolgt.

Dabei geht das Sicherheitssystem davon aus, dass **jeder Mensch nur eine einzige Identität** besitzt.

Die Erteilung der Rechte für die Ausführung bestimmter Funktionen obliegen den entsprechenden Verwaltungsabteilungen, wo die Informationen über den Benutzer und sein Aufgabengebiet vorhanden sind.

Die Benutzer … können so zwar **mehrere Rollen** in Bezug auf die Benutzung der Applikationen haben, diese müssen jedoch **zwingend mit einer einzigen Identität verbunden** sein. …“

InfoWeek Nr. 19, 30.10.2006, Schwerpunktthema Identity Management, Seite 46