swisscom solutions

# *Swisscom der erste Dienstanbieter für qualifizierte Signaturen in der Schweiz*

## *Die qualifizierten elektronischen Signatur, Einsatzgebiete im Behördenverkehr*

*Lorenz Neher*
Dipl. El. Ing. FH, CISSP, CISA

Das digitale Zertifikat als Schlüssel für zuverlässige, verbindliche elektronische Transaktionen

# 1. Schweizer Gesetzesgrundlagen für el. Signaturen

***OR Art. 14 Abs. 2bis:*** Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003[1] über die elektronische Signatur beruht. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.

***ElDI-V:*** Verordnung des EFD über elektronisch übermittelte Daten und Informationen (ElDI-V) Art. 3 Beweiskraft: Die in Artikel 43 Absatz 1 MWSTGV verlangten Voraussetzungen für die Beweiskraft elektronischer Daten sind erfüllt, sofern:

- die Übermittlung und Aufbewahrung von Daten mittels digitaler Signatur abgesichert ist;
- das durch einen Zertifizierungsdiensteanbieter gemäss den Bestimmungen von Artikel 2 Absatz 2 ausgestellte Zertifikat zum Zeitpunkt der Signaturerstellung gültig war;

***GeBüV Artikel 9:*** "Zur Aufbewahrung von Unterlagen sind zulässig:

- unveränderbare Informationsträger, namentlich Papier, Bildträger und unveränderbare Datenträger; ...
- veränderbare Informationsträger, wenn:
  technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren), der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z.B. durch «Zeitstempel»), die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden, und die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie die entsprechende Hilfsinformationen (wie Protokolle und Log files) ebenfalls aufbewahrt werden."

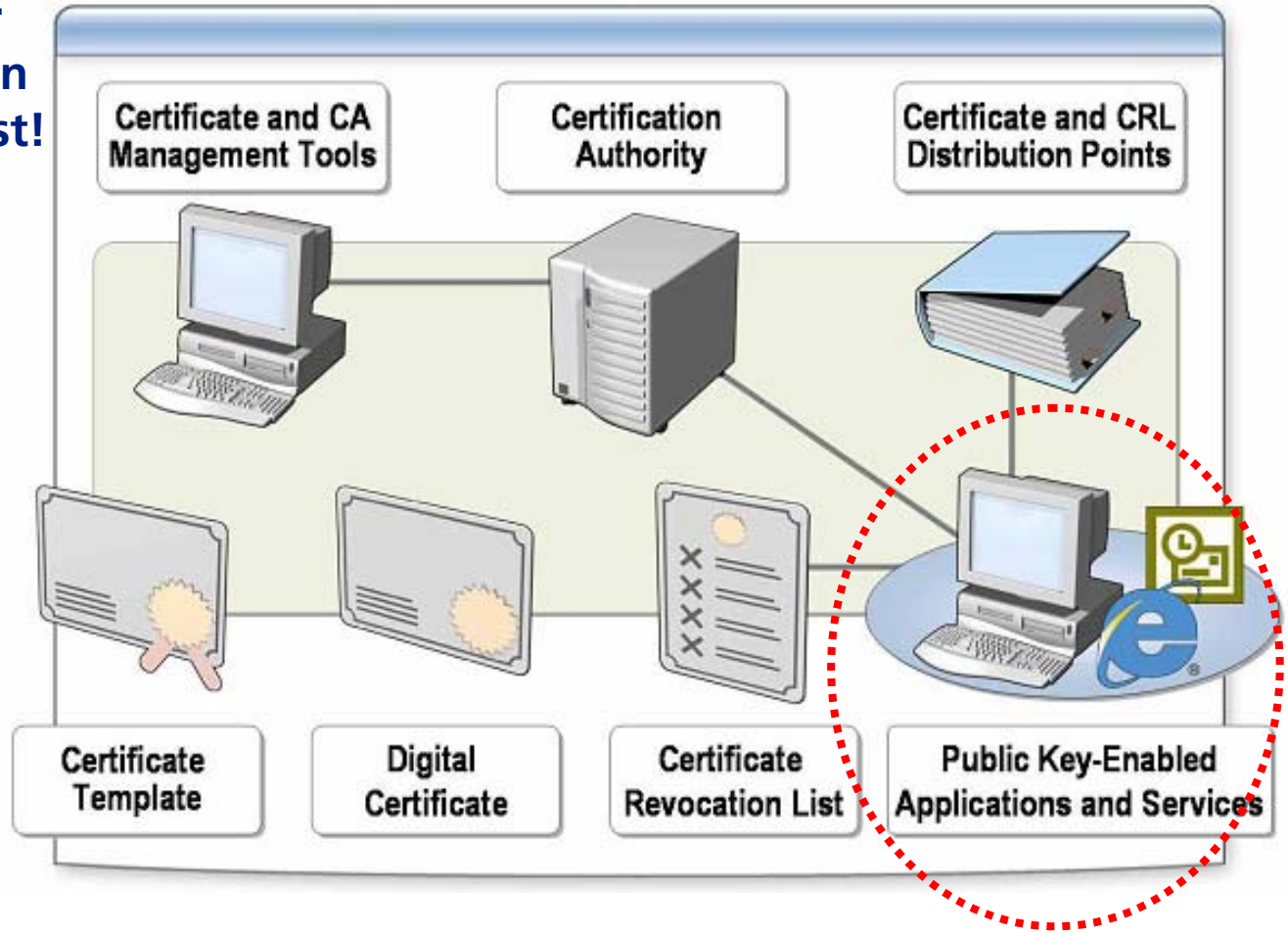
[1] SR 943.03; AS 2004 5085

# 2. Nutzen eines digitalen Zertifikates

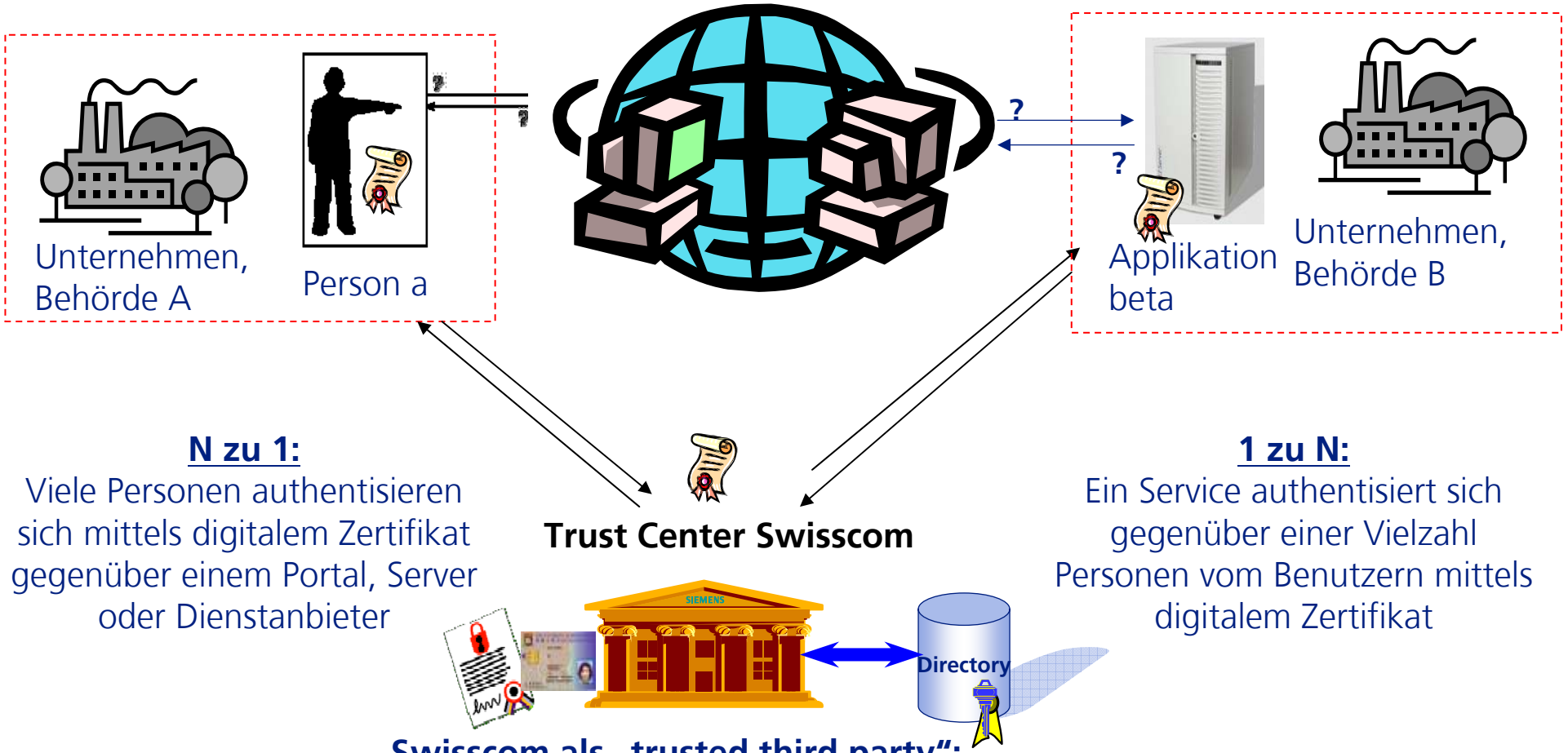
**Ein digitales Zertifikat hat nur dann einen Nutzen, wenn es in einer Anwendung integriert ist!**

**PKI ist eine technische Lösung für:**

- ***Integrität***
  → Message Digest, Hash
- ***Vertraulichkeit***
  → Verschlüsselung
- ***Authentizität***
  → signieren
- ***Nicht-Abstreitbarkeit***
  → Message Digest, signieren



# 3. Einsatzgebiete digitaler Zertifikate

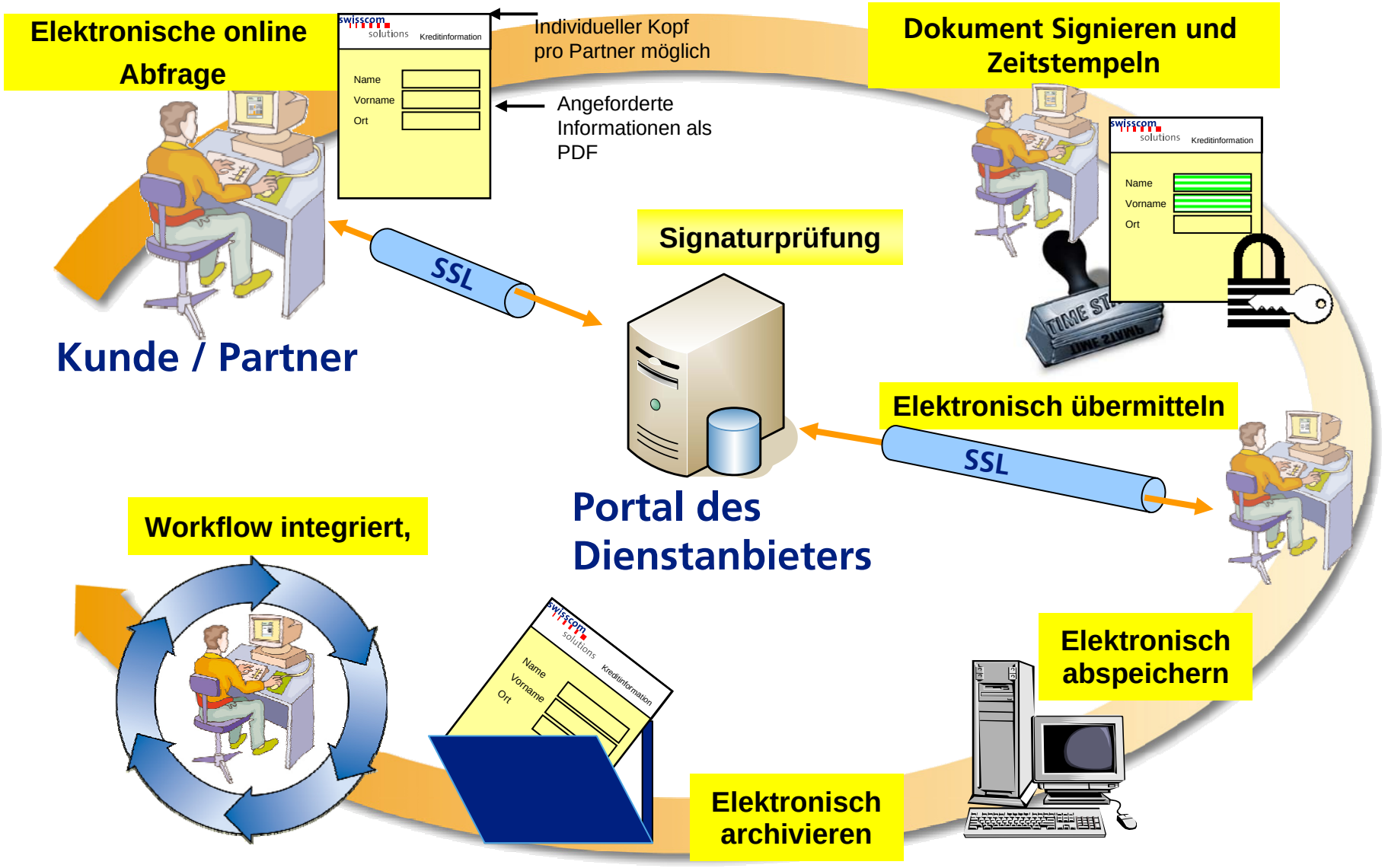



**N zu 1:**
Viele Personen authentisieren sich mittels digitalem Zertifikat gegenüber einem Portal, Server oder Dienstanbieter

**1 zu N:**
Ein Service authentisiert sich gegenüber einer Vielzahl Personen vom Benutzern mittels digitalem Zertifikat

**Swisscom als „trusted third party“:**
Als qualifizierter CSP garantiert Swisscom, dass jedes Zertifikat hält was es verspricht

# 4. Das eFormular im Adobe Formular Workflow



# 5. Massenverarbeitung mit XML

**Stapelverarbeitung**

**Kunde / Partner**


**XML erzeugen, Signieren und Zeitstempeln**

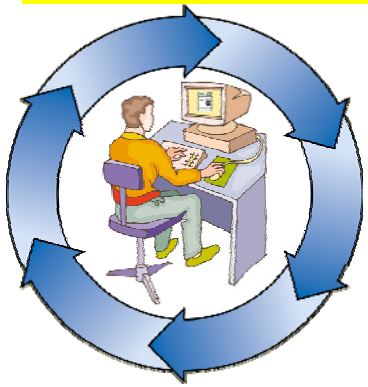
**SSL**

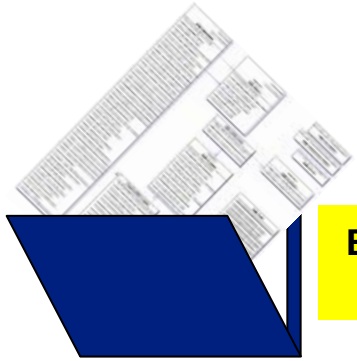
**Elektronischübermitteln**

**Signaturprüfung**

**Dienstanbieter**

**Workflow integriert,**





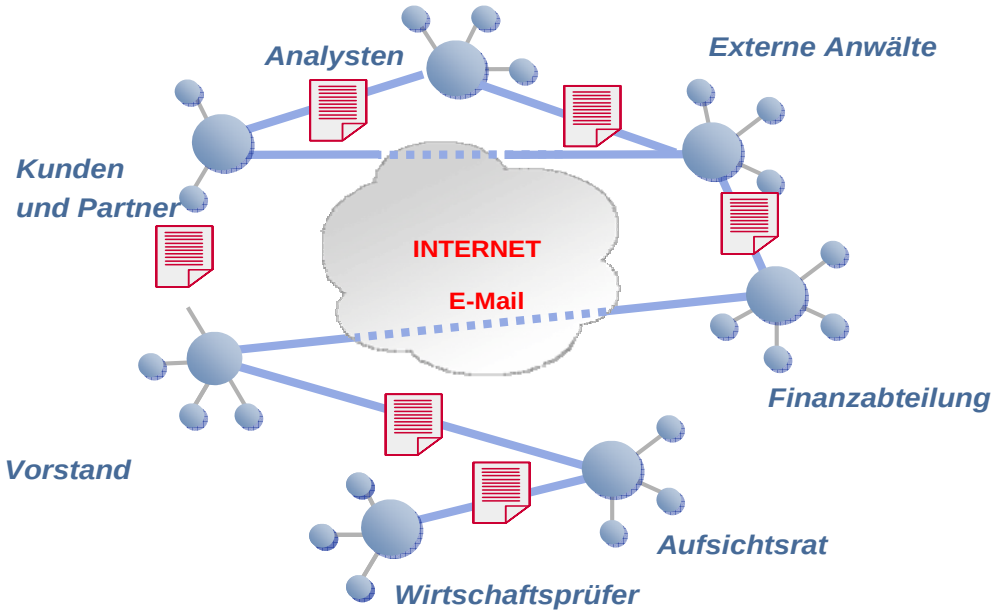
**Elektronisch archivieren**

**Elektronisch abspeichern**

# 6. Anwendung: Secure Collaboration

## Traditionelles E-Mail

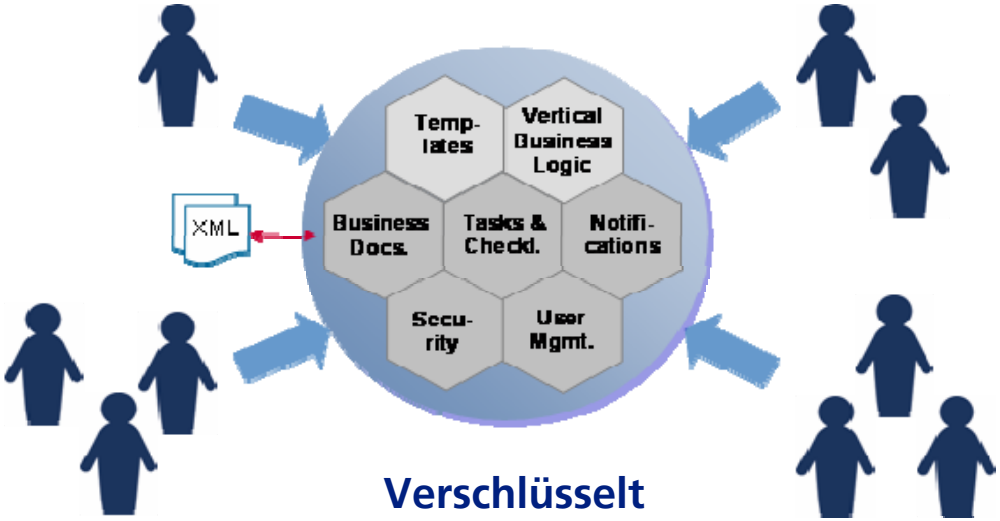
Die Meisten e-Mail Nachrichten werden unverschlüsselt verschickt.




**Ineffizient + Unsicher!**

## Secure Collaboration Platform

Ermöglicht die Ablage und Bearbeitung von vertraulichen Dokumenten an einem Ort ohne lokale Software und ohne Training extrem sicher




**Verschlüsselt**
**Signiert**
**Verifiziert**
**Zeitgestempelt**

# 7. Anwendung: SSO Portal

**Das Eidgenössische Justiz- und Polizeidepartement (EJPD) hat seine Applikationen in einer einheitlichen Sicherheits- und Authentisierungsinfrastruktur konsolidierte.**

- Ab 1.6.2006 müssen sich alle 15'000 Benutzer der angebundenen Applikationen stark am SSO Portal authentisieren (SmartCard).

**Zusammen mit dem Kanton Zürich pilotiert Swisscom Solutions die Swisscom Zertifikate als universeller Authentisierungstoken. Vorteile dieser Lösung:**

- Zusätzlich zum Sign-on Zertifikat kann jeder Benutzer ein qualifiziertes Zertifikat für rechtsgültige Signatur von Dokumenten und gesichertes e-Mail bekommen
- Zertifikate haben Gültigkeit auch ausserhalb der geschlossenen Anwendung
- Die Kantone und Gemeinden können mit unserem Franchising Modell die Registrierung der Benutzer und/oder die Erstellung ihrer SmartCards selbst durchführen
- Eine Verbreitung der Zertifikate ermöglicht auch anderen Dienstanbietern (Behörden, Ämter) diese Art der Authentisierungs für die eigenen Dienstleistungen zu verwenden ohne selbst eine PKI betreiben zu müssen

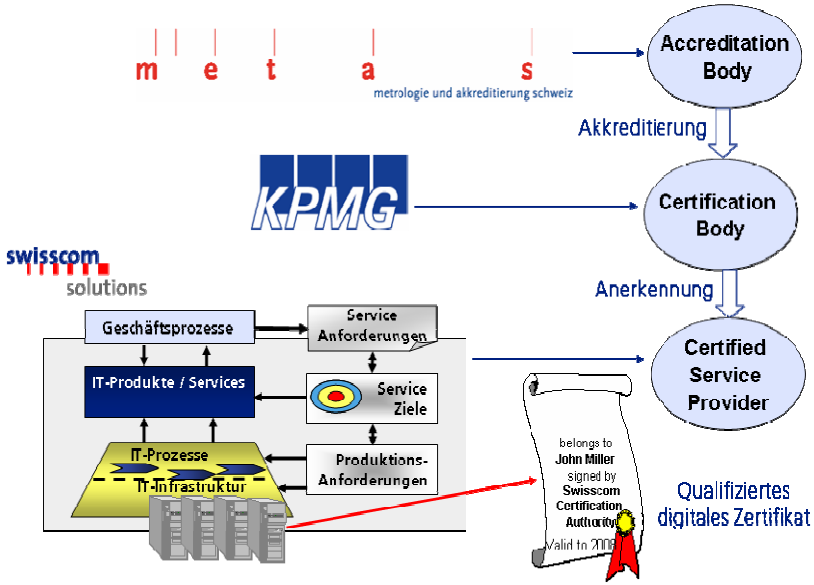




# 8. Nutzen der qualifizierten elektronischen Signatur

- Rechtskräftige Willensäusserung als elektronischer Ersatz für die handschriftliche Unterschrift gemäss Signaturgesetz (OR Art. 14)
- Anerkanntes Mittel zur Sicherstellung der Authentizität und Integrität für verbindliche elektronische Übermittlung (ElDI-V)
- Anerkanntes Mittel für die verbindliche elektronische Aufbewahrung auf veränderbaren Medien (ElDI-V, GeBüV)
- qualifizierte Zeitstempel zur zweifelsfreien Deklaration des Zeitpunkts der Signatur

Das qualifizierte Zertifikat geniesst auch im Ausland eine gute Reputation, da es auf internationalen Standards basiert, über ein dichtes Regelwerk klar definiert ist und dessen Einhaltung durch eine akkreditierte Prüfstelle jährlich kontrolliert wird



# 9. Nächste Schritte zur Umsetzung

1. Identifikation einer Business-Applikation innerhalb ihrer Organisation wo digitale Zertifikate einen grossen Nutzen bringen (medinbruchfrei, verbindlich, nachvollziehbar, verschlüsselt, GeBüV, ElDI-V, etc.)
2. Grob-Konzept mit allen Schnittstellen und Beteiligten für die Einbindung der digitalen Zertifikate innerhalb der Organisation
3. Grob-Konzept für Zertifikats-Lifecycle (wer benötigt Zertifikate, wie werden die Zertifikate verteilt, was passiert wenn verloren, ungültig, etc.)
4. „Proof of concept“ / Pilotinstallation
5. System Integration / Implementation, Aufbau der Enterprise-RA beim Kunden, etc.

→ **Swisscom betrachten Digital Certificate Services als Projekt-Geschäft**

→ **Das Konzept wird von Swisscom zusammen mit dem Kunden und eventuellen Systempartnern des Kunden erarbeitet**

# Zusammenfassung

- Das ZertES verlangt, dass eine Person **eindeutig identifiziert** wird bei der Ausgabe des qualifizierten digitalen Zertifikates
- mit qualifizierter elektronischen Signatur darf nur **„signiert“** werden
- qualifizierte elektronische Signatur erfordern ein „**Secure Signature Creation Device**“ (SmartCard, USB-Token) worauf mehrere Schlüssel passen
- Das digitale Zertifikat ist der Schlüssel für zuverlässige elektronische Transaktionen
- Nicht jeder muss eine PKI aufbauen, um Zertifikate nutzen zu können. Es reicht, wenn Swisscom dies tut und möglichst viele die digitalen Zertifikate **einsetzen** und **akzeptieren**
- Mit unserem RA-Partner Modell kommen wir so nahe wie möglich an die Benutzer und die Dienstanbieter
- Jeder benötigt mehrere Zertifikate: zum signieren, authentifizieren, verschlüsseln

swisscom
solutions

Swisscom Solutions AG
ICT Security Solutions
Müllerstrasse 16
CH-8004 Zürich

Phone +41 1 294 88 44
Fax +41 1 294 81 39

eMail solutionsr@swisscom.com

www.swisscom.com/solutions

# Backup: Preisstruktur

swisscom solutions

**„Initialkosten“**

## Vorbereitung

**Enterprise RA-Konzept Definition**

- Konzept und Interfaces
- Betriebsprozesse
- Prozessdefinition
- Risiko Analyse

**Enterprise RA-Service Setup**

- Aufnahme der bestehenden Infrastruktur
- Aufnahme der der bestehenden Betriebsprozesse
- Implementation RA Prozesse
- Roll-out der RA Officer Zertifikate, Instruktion und Dokumentation

**„Wiederkehrende Kosten“**

## Jährliche Gebühren

**Enterprise RA-Service Kosten pro Jahr:**

- Enterprise RA für qualifizierte Zertifikate
- Enterprise RA für nicht qualifizierte Zertifikate

**Enterprise RA Kosten pro Jahr:**

- Wiederverkäufer
- Managed PKI
  - “Swisscom Brand“
  - “White Label”

## Volumenabhängige Gebühren

**Zertifikats Kosten pro Jahr:**

- **„Diamant“** qualifiziertes Zertifikat
- **„Saphir“** Fortgeschrittenes Zertifikat
- **„Rubin“** Software Zertifikat
- Zeitstempel-Dienst
- Web-Server Zertifikat
- Device Zertifikat
- Zertifikate für HSM