

PKI: Quo vadis?
4. Berner Tagung für Informationssicherheit
November 2001

PKI und Staat: Aktuelle Hintergründe und Modelle

Urs Bürge
Bundesamt für Justiz
urs.buerge@bj.admin.ch

EJPD Bundesamt für Justiz

PKI und Staat: Aktuelle Hintergründe und Modelle

Inhaltsübersicht

Grundsätzliches zu PKI und Staat

- PKI & Staat: Vier Berührungspunkte
- Staatliche PKI-Regulierung
- PKI-Konstellationen

Brauchen wir einen Amtlichen Digitalen Ausweis ?

- Beweggründe für einen ADA
- Situation in anderen Ländern
- Entwicklungs-Szenarien
- Handlungs-Optionen

EJPD Bundesamt für Justiz

PKI und Staat: Aktuelle Hintergründe und Modelle

PKI & Staat: Vier Berührungspunkte

- **Staatliche PKI-Regulierung (& Co.)**
 - Zertifizierungsdienste-VO (April 2000)
 - ZertES (im Parlament)
- **Interne PKI des Bundes / des Staates**
 - PKI für verwaltungsinterne Bedürfnisse
 - Pendant zu firmeninternen PKIs
- **PKI für eGovernment-Anwendungen**
und in diesem Zusammenhang:
Amtlicher Digitaler Ausweis? Dazu mehr ->
- **Staatliche Intervention im Fall Swisskey?**

EJPD Bundesamt für Justiz

PKI und Staat: Aktuelle Hintergründe und Modelle

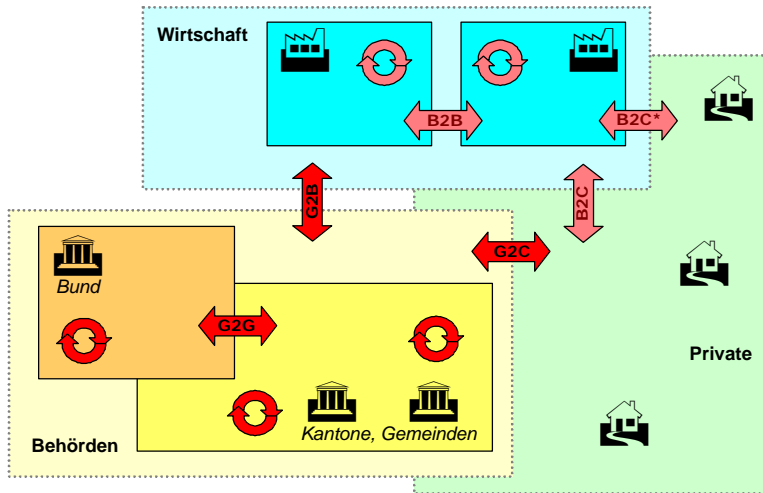
Staatliche PKI-Regulierung (& Co.)

- **Zertifizierungsdiensteverordnung, ZertDV, SR 784.103**
 - VO vom 12. April 2000 über Dienste elektronischen Zertifizierung
 - und SR 784.103.1, VO des BAKOM vom 15. August 2001, Technische und administrative Vorschriften
- **Entwurf: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, ZertES**
 - Inhalt: ZertDV++, Anerkennung DigSig für Privatrecht und Register
 - Art. 20 Abs. 3: Staatliche CA oder Beteiligung an privater CA
- **Bisherige Doktrin bezüglich Aufgabe des Staates**
- **Weiteres rechtliches Umfeld**
 - z.B. Anerkennung DigSig im Behördenverkehr in OG-Revision!

EJPD Bundesamt für Justiz

PKI und Staat: Aktuelle Hintergründe und Modelle

PKI-Konstellationen I



PKI und Staat: Aktuelle Hintergründe und Modelle

PKI-Konstellationen II

- **Nach Abdeckung:**
 - Projektbezogen
 - Anwendungsbereich flächendeckend
 - Branche flächendeckend
 - Gebiet flächendeckend (Schweiz, EU, ...)
- **Nach Rollen-Verteilung**
 - firmenintern, bzw. bundesintern
 - RA intern / CA extern (Teil-Outsourcing)
 - private CA (Outsourcing)
 - private öffentliche CA
- **Nach eGov-Anwendungsbereich**
 - bundesintern
 - verwaltungsintern, eGov: G2G
 - eGov: G2B
 - eGov: G2C
- **Nach ‚Staatsnähe‘**
 - beliebige CA
 - anerkannte CA
 - staatlich anerkannte CA
 - CA mit staatl. Beteiligung
 - staatliche CA

PKI und Staat: Aktuelle Hintergründe und Modelle

Amtl. Digitaler Ausweis? - Beweggründe

- **Stärkeres Vertrauen**
 - Gewisse eGov-Anwendungen verlangen erhöhtes Vertrauen
- **Standortförderung**
 - Huhn-Ei-Problem überwinden; eLawine losstreifen;
Transformation zur Informationsgesellschaft beschleunigen
- **eGovernment-Automatisierung**
 - Eindeutige Identifikation als Voraussetzung für effizientes eGov
- **Staatliche Infrastrukturleistung (Kollektivgut)**
 - wie Fall Swisskey zeigt
- **Personenidentifikation als Staatsaufgabe**

EJPD Bundesamt für Justiz

PKI und Staat: Aktuelle Hintergründe und Modelle

ADA? - Situation in anderen Ländern

- **Beispiel Finland (FINEID)**
 - Für Verwaltung und Private
heute: ca. 30'000 Beamte, ca. 10'000 Private
 - Multi-purpose: eGov/eCommerce/...
- **Andere europäische Länder**
 - Schweden: Staatlich def. Standard
 - Österreich: Bürgerkarte (insbes. Sozialversicherung)
- **Kanada / USA**
- **eEurope**
 - SmartCards Charter
Trailblazer 1: Public Identity
(Minimalanforderungen an digitalen Ausweis)



EJPD Bundesamt für Justiz

PKI und Staat: Aktuelle Hintergründe und Modelle

ADA? - Entwicklungs-Szenarien

Wie entwickelt sich der Bereich (unabhängig von uns)?

- **Globales Oligopol**
 - Wenige globale Anbieter setzen sich durch (wie heute bei Kreditkarten)
- **Vielfalt von Zertifikaten und Zertifizierungsstellen**
 - Je nach Verwendungszweck
 - Staatliches Zertifikat eines unter vielen (falls überhaupt)
- **Primär staatliche Zertifikate**
 - Mittelfristig staatliches Monopol wie bei Banknoten und Pässen
- **Zertifikate setzen sich nicht durch**
 - Zuwenig Nutzen / kein Vertrauen / Technik wird obsolet

PKI und Staat: Aktuelle Hintergründe und Modelle

ADA? - Handlungs-Optionen

- **Abwarten, bzw. keine staatliche Intervention**
 - Kein Risiko; Was gut ist, setzt sich auch durch
 - Förderung indirekt durch staatliche Aufträge für interne PKI
- **Einführung des ‚amtlichen Digitalen Ausweises‘**
 - Skalierbar in der Intensität (Breite, Geschwindigkeit)
 - Starke Förderwirkung für eGov und Informationsgesellschaft
 - Beträchtliche Kosten und Diverse Risiken
- **Nein, stattdessen Beteiligung an privater Zertifizierungsstelle**
 - Skalierbar in der Intensität; dito für Kosten
 - evt. staatliche Stellen für Registrierung
- **Staatliche Intervention bei Standardisierung**