ROOT-CA von der REGTP

Die Public Key Infrastruktur nach dem deutschen Signaturgesetz

Inhalt

- Problemstellung
- Signaturgesetz
- Public Key Infrastruktur in Deutschland
- Probleme und Ausblick

Inhalt

- **Problemstellung**
- Signaturgesetz
- Public Key Infrastruktur in Deutschland
- Probleme und Ausblick

Problemstellung

- Zunehmende Digitalisierung von Kommunikationsbeziehungen
- Ausschließlich handschriftliche Unterschrift galt als rechtsverbindlich
- Vor Signaturgesetz fehlte Rechtssicherheit bei digitalen Unterschriften

Inhalt

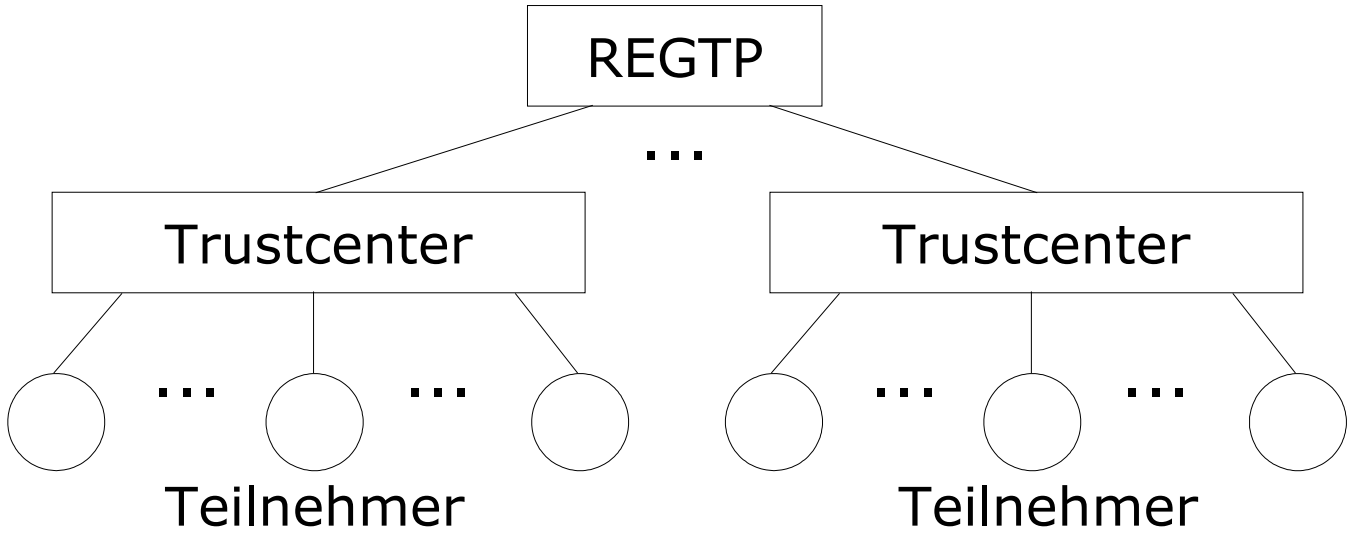
- Problemstellung
- **Signaturgesetz**
  - **Allgemeines**
  - **REGTP**
  - **Trustcenter**
  - **Qualifizierte Signatur**
- Public Key Infrastruktur in Deutschland
- Probleme und Ausblick

Signaturgesetz
Allgemeines (1/2)

- Gültig seit Mai 2001
- Definiert den Begriff „qualifizierte elektronische Signatur“
- Legt Rahmenbedingungen und Sicherheitsmaßnahmen fest
- Rechtsgültigkeit der qualifizierten Signatur durch andere Gesetze
  - Bsp.: Gleichstellung bei der Unterschrift von Verträgen im BGB

Signaturgesetz
Allgemeines (2/2)

- Das Signaturgesetz gibt eine Sicherheits-infrastruktur mit einer zweistufigen Hierarchie vor



- Klare Festlegung von Verantwortlichkeiten

Signaturgesetz

REGTP (1/2)

- Deutsche **R**egulierungsbehörde für **E**lektrizität, **G**as, **T**elekommunikation und **P**ost
- Ursprünglich zuständig für die Liberalisierung des Telekommunikations- und Postmarktes
- Wird vom Signaturgesetz als zuständige Behörde für die Umsetzung und Überwachung der Auflagen bestimmt

Signaturgesetz
REGTP (2/2)

- Zertifizierungsdiensteanbieter (Trustcenter) müssen Aufnahme des Geschäftsbetriebes der REGTP anzeigen
- REGTP erstellt mit dem eigenem privaten Schlüssel ein Zertifikat für jedes Trustcenter
- Stellt ein Verzeichnis mit den Zertifikaten aller Trustcenter zur Verfügung
- Verantwortlich für die freiwillige Akkreditierung von Trustcentern

RootCA der REGTP

Signaturgesetz
Trustcenter (1/2)

- Trustcenter sollen die Qualität der ausgestellten Zertifikate gewährleisten
- Trustcenter funktionieren nach dem Vorbild einer Meldebehörde
- Das Trustcenter stellt Zertifikate für die öffentlichen Schlüssel von Personen aus und signiert diese mit ihrem privaten Schlüssel
- Das **Trustcenter bürgt** dafür, dass der **Name** und der **öffentliche Schlüssel** im Zertifikat **derselben Person gehören**

Signaturgesetz
Trustcenter (2/2)

- Müssen ein Verzeichnis aller ausgestellten Zertifikate anbieten
- Legen der REGTP ein Sicherheitskonzept vor und sind für die Umsetzung verantwortlich
- Müssen mind. 250.000 € Deckungsvorsorge für Haftungsansprüche zurückstellen

Signaturgesetz
Qualifizierte Signatur

- Signatur basierend auf privatem Schlüssel mit qualifiziertem Zertifikat
- Lässt sich eindeutig einer natürlichen Person zuordnen
- Privater Schlüssel wird nur auf Smartcard gespeichert und darf nicht auslesbar sein
- Erstellung der Signatur direkt auf der Smartcard

Inhalt

- Problemstellung
- Signaturgesetz
- **Public Key Infrastruktur in Deutschland**
  - **Root-CA**
  - **Trustcenter**
  - **Anwender**
- Probleme und Ausblick

Public Key Infrastruktur in Deutschland
Root-CA - Allgemein

- Die erste Root-CA wurde im Jahre 1998 auf Grundlage des Signaturgesetzes von 1997 geplant und aufgebaut
- Zur Zeit wird ein neues System auf Grundlage neuer Technologien eingeführt
- Die REGTP betreibt Hauptsystem in Mainz
- Weitere Systeme, wie ein Hot-Standby des Verzeichnisdienstes und ein Cold-Standby der Zertifikatsproduktion werden an einem anderen Standort betrieben

Public Key Infrastruktur in Deutschland
Root-CA – Kosten für Aufbau

- Hochbau- und Infrastruktur: **348.000 €**
  - Hochsicherheitstrakt (z.B. gepanzerte Türen)
- IT-Infrastruktur: **358.000 €**
  - Hardware, Software, Schlüsselgeneratoren
- Prüfung und Bestätigung des Sicherheitskonzeptes: **0 €**
  - In Amtshilfe durch BSI durchgeführt
- Gesamtkosten für ein Privatunternehmen würden zwischen **2,5 und 7,5 Mio. €** liegen

Public Key Infrastruktur in Deutschland
Trustcenter - Leistungen

- **Identitätsfeststellung**
  - Das Trustcenter muss den Antragsteller zuverlässig identifizieren (i.d.R. mit Personalausweis)
  - Dem Antragssteller wird ein geeigneter eindeutiger Name zugeordnet
- **Schlüsselgenerierung (Nicht zwingend)**
  - Falls der Antragsteller kein selber generiertes Schlüsselpaar hat, kann vom Trustcenter ein eindeutiger Schlüssel generiert werden

Public Key Infrastruktur in Deutschland
Trustcenter - Leistungen

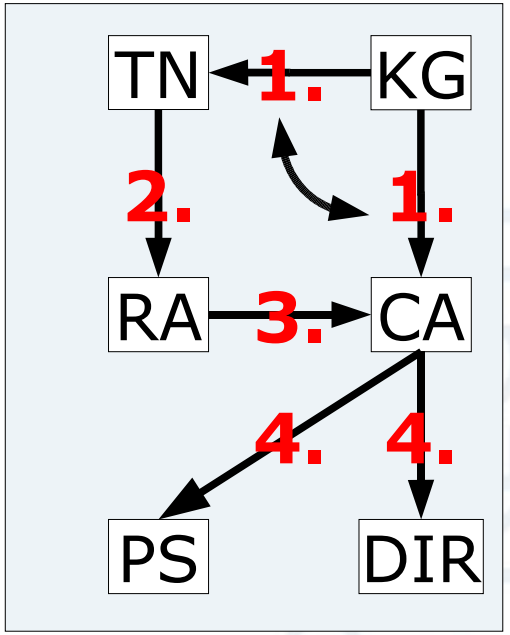
- **Zertifizierung der Teilnehmerschlüssel**
  - Die erforderlichen Daten eines Zertifikates, wie Name, Zertifikatinhaber, öffentlicher Schlüssel, etc. werden zusammengefasst und von der Zertifizierungsstelle signiert
- **Personalisierung der Signierkomponente**
  - Beim Personalisiervorgang wird das Zertifikat und der private Schlüssel auf ein Sicherheitsmedium (Smartcard) übertragen

Public Key Infrastruktur in Deutschland
Trustcenter - Leistungen

- **Verzeichnisdienst**
  - Alle erstellen Zertifikate müssen über den Verzeichnisdienst auf ihre Gültigkeit prüfbar sein
- **Zeitstempeldienst (Nicht zwingend)**
  - Muss nicht von jedem Trustcenter betrieben werden
  - Er verknüpft bestimmte digitale Daten authentisch mit einem bestimmten Zeitpunkt

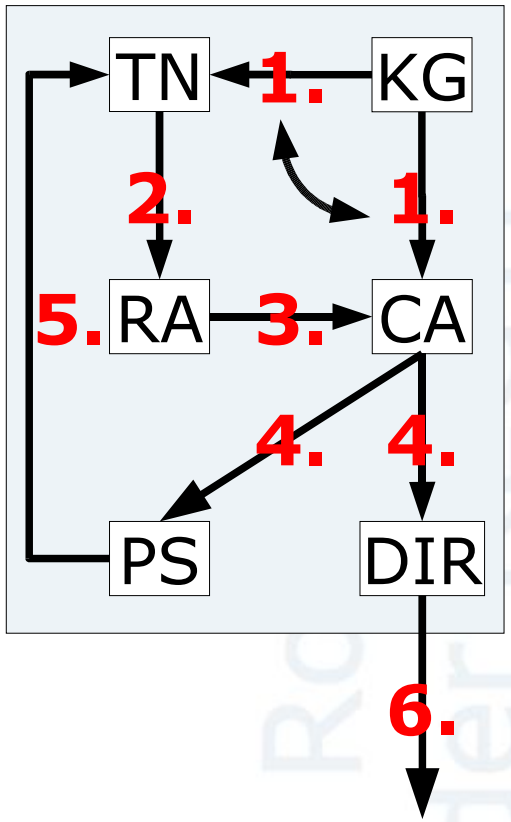
Public Key Infrastruktur in Deutschland
Trustcenter – Antragsbearbeitung

- 1.) Teilnehmer (TN) oder Zertifizierungsstelle (CA) generieren neues Schlüsselpaar
- 2.) Registrierungsdienst identifiziert Teilnehmer (TN)
- 3.) Die Zertifizierungsstelle (CA) erzeugt das Zertifikat
- 4.) Das Zertifikat wird an den Personalisierservice (PS) und den Verzeichnisdienst (DIR) weitergegeben



Public Key Infrastruktur in Deutschland
Trustcenter – Antragsbearbeitung

- 5.) Der Personalisierungdienst (PS) überträgt das Zertifikat auf ein Sicherheitsmedium und übergibt es dem Teilnehmer (TN)
- 6.) Die Gültigkeit des Zertifikates ist über öffentliche Kommunikationseinrichtungen nachprüfbar



Public Key Infrastruktur in Deutschland
Trustcenter – Sicherheitskonzept

- Sicherheitskonzept wird vom BSI in einem „Maßnahmenkatalog“ veröffentlicht
  - Bauliche Maßnahmen
    - Vorschlag für Raumaufteilung: Trennung von Sicherheits- und Besucher-Bereich
  - Energieversorgung
    - Netz-Ersatzanlage für 6h Betrieb
  - Zutrittskontrolle
    - Überprüfung biometrischer Eigenschaften
    - Smartcards mit PIN-Eingabe

Public Key Infrastruktur in Deutschland
Trustcenter – Marktüberblick

- 27 Anbieter von qualifizierten Zertifikaten
  - Davon 23 Anwalts-, Wirtschaftsprüfer- oder Steuerberaterkammern
  - Deutsche Post Signtrust
  - Deutsche Telekom TeleSec
  - Bundesdruckerei D-Trust
  - TC Trustcenter AG
    - Gegründet von vier großen deutschen Banken
    - Übernommen von Betrusted (USA)

Public Key Infrastruktur in Deutschland
Anwender

- Beispielprodukt von D-Trust
- Qualifizierte Signatur
- Zertifikatgültigkeit: 3 Jahre
- Kostenüberblick

Signaturkarte	161,24 €
Versand	22,04 €
Kartenlesegerät	114,84 €
	298,12 €

Inhalt

- Problemstellung
- Signaturgesetz
- Public Key Infrastruktur in Deutschland
- **Probleme und Ausblick**
  - **Sicherheit**
  - **Verbreitung**

Probleme und Ausblick
Sicherheit (1/3)

- Möglicher Angriffspunkt:
  Unsichere Technik beim Anwender
  - Kartenlesegerät der Klasse 1

  - Trojaner auf dem PC des Anwenders liest PIN mit

  - Kartenlesegerät der Klasse 2
    - Mit integrierter Tastatur zur PIN-Eingabe

Probleme und Ausblick
Sicherheit (2/3)

- Möglicher Angriffspunkt:
  Unsichere Technik beim Anwender
  - Kartenlesegerät der Klasse 2

  - Trojaner auf dem PC des Anwenders tauscht zu signierendes Dokument aus

  - Kartenlesegerät der Klasse 3
    - Mit integriertem Display zur Anzeige des Dokuments, das signiert wird

Probleme und Ausblick
Sicherheit (3/3)

- Möglicher Angriffspunkt:
  Unsichere Technik beim Anwender
  - Kartenlesegerät der Klasse 3

  - Angreifer verändert Hardware (Kartenlesegerät)

  - Kartenlesegerät der Klasse 4
    - Mit eigenem privaten Schlüssel

Probleme und Ausblick

Verbreitung

- Wenige Anwendungen für digitale Signatur
- Geringe Verbreitung von Signaturkarten
- Keine Killer-Applikation
- Änderungen am Signaturgesetz im November 2004 beschlossen
  - Ziel: Größere Verbreitung durch Signierfunktionen auf EC- und Versicherten-Karten

Diskussion

Fragen!