cryptovision

cv cryptovision

Einsatz von Kryptographie zum Schutz von Daten

Verfahren und Sicherheitsaspekte

246. PTB-Seminar, Berlin, 18.02.2009

AGENDA

1. **Kryptographie**
    a. Grundlagen der Kryptographie
    b. Kryptographische Verfahren
    c. Sicherheitsaspekte
2. **INSIKA TIM**
3. **Fazit**

AGENDA

1. Kryptographie
   a. **Grundlagen der Kryptographie**
   b. Kryptographische Verfahren
   c. Sicherheitsaspekte
2. INSIKA TIM
3. Fazit

Grundlagen: Ziele beim Einsatz von Kryptographie

Geheimhaltung

- » Schutz gegen unbefugtes Abhören
- ➡ Verschlüsselung

Integrität

- » Schutz gegen unberechtigte Modifikation
- ➡ Message Authentication Codes (MACs), Digitale Signaturen

Authentizität

- » Nachweis der Urheberschaft
- ➡ MACs, Digitale Signaturen

Nicht-Bestreitbarkeit

- » Beweis der Urheberschaft (auch gegenüber Dritten)
- ➡ Digitale Signaturen

Grundlagen: Kryptographische Verfahren

Symmetrische Verfahren

- Verwenden einen einzelnen geheimen Schlüssel
- Basieren typischerweise auf einfachen Bitoperationen

Asymmetrische Verfahren

- Verwenden ein asymmetrisches Schlüsselpaar (privater und öffentlicher Schlüssel)
- Basieren im Allgemeinen auf komplexer Langzahlenarithmetik

Sonstige Verfahren

- Hash Funktionen (Kryptographischer “Fingerabdruck”)
- Zufallszahlen Generatoren (RNGs)

Grundlagen: Kryptographische Paradigmen

Kerkhoffs' Prinzip

- Die Algorithmen sind öffentlich bekannt
- Nur die Schlüssel werden geheim gehalten

Es gibt keine praxisnahe absolute Sicherheit

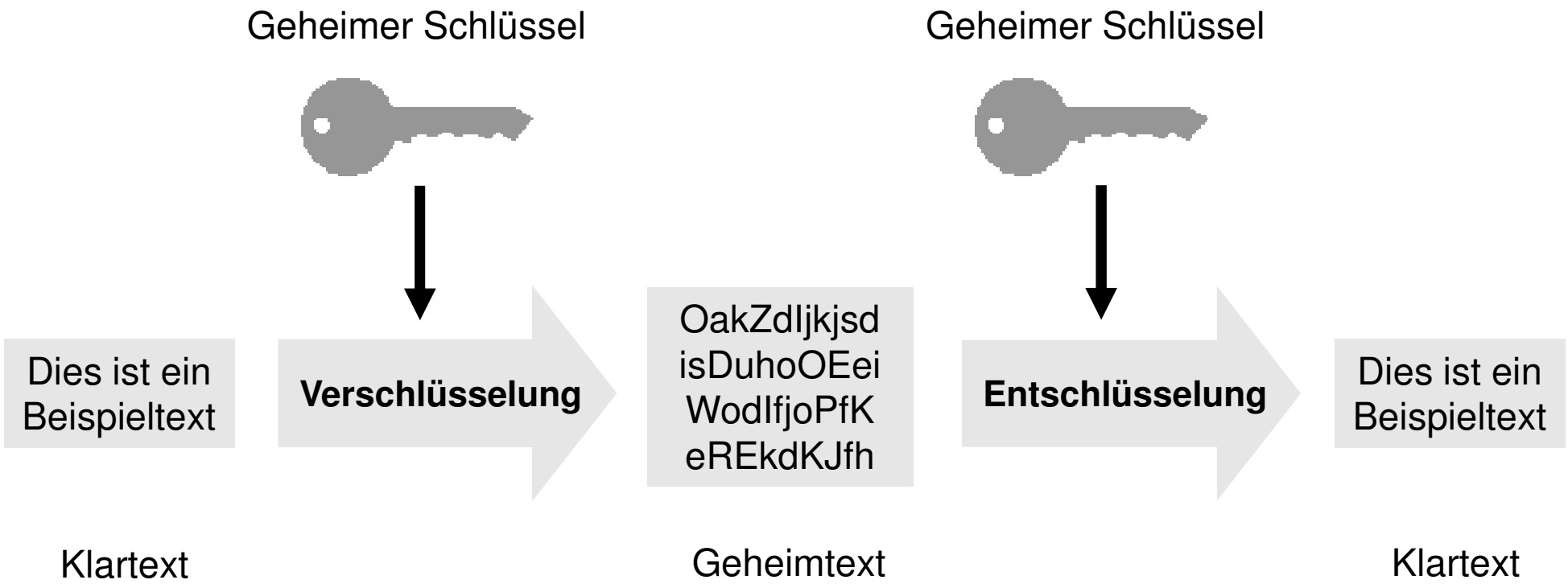
- Einmalschlüssel sind sicher aber nicht praxisnah einsetzbar
- Die Sicherheit moderner Kryptographischer Verfahren basiert auf Annahmen aus der Zahlen- und Komplexitätstheorie

AGENDA

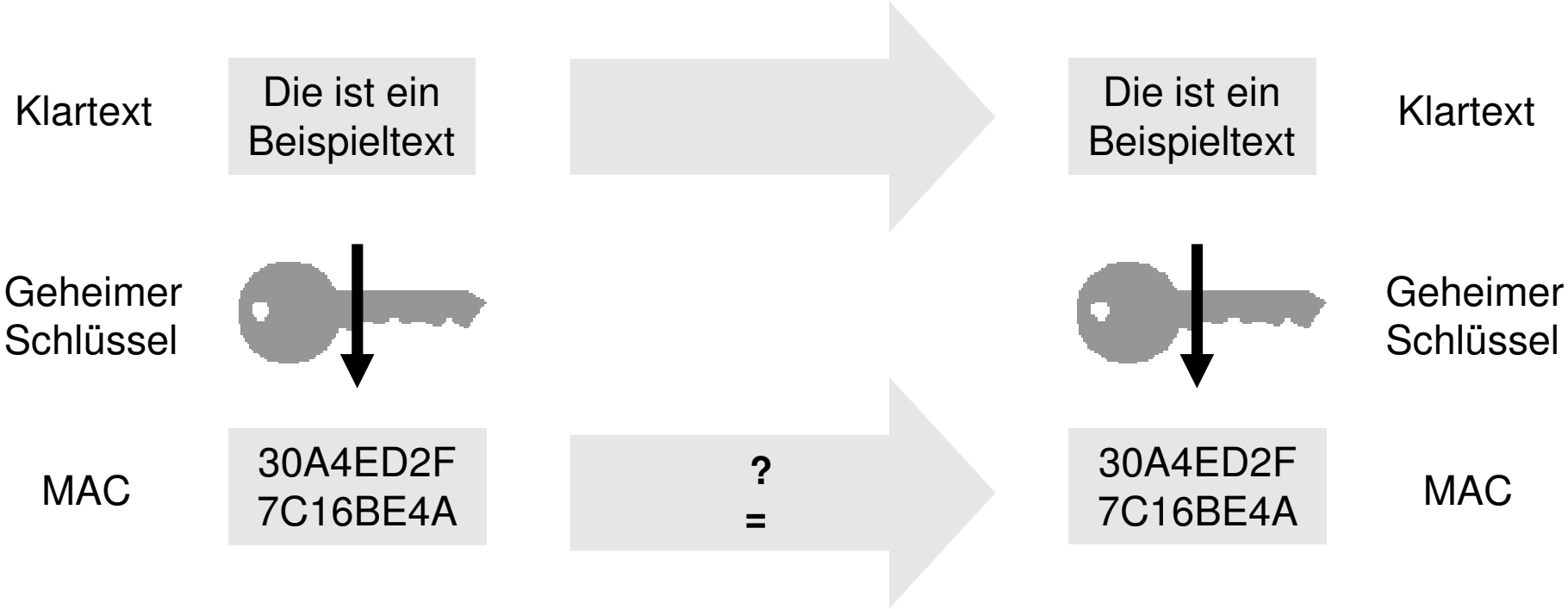
1. Kryptographie
   a. Grundlagen der Kryptographie
   b. Kryptographische Verfahren
   c. Sicherheitsaspekte
2. INSIKA TIM
3. Fazit

Symmetrische Verfahren I: Verschlüsselung

Der Startpunkt: symmetrische Verschlüsselung



Authentisierung mit Message Authentication Codes (MAC)



Charakteristik Symmetrischer Verfahren

Vorteile

- Leicht zu implementieren (in Hardware & Software)
- Sehr gute Performance (auch bei beschränkten Umgebungen)

Nachteile

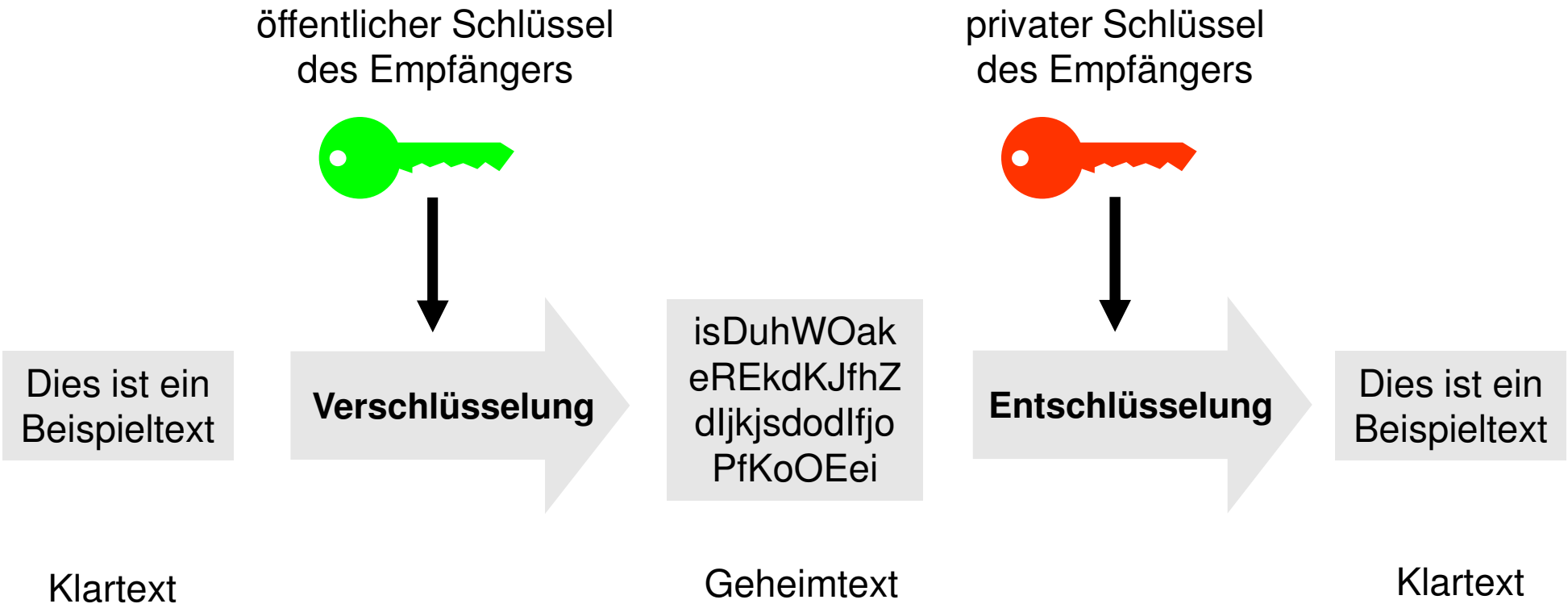
- Schlüsselverwaltung
  - Benötigt sicheren Kanal zum Schlüsselaustausch
  - Je zwei Teilnehmer benötigen eigenen geheimen Schlüssel
  - n Teilnehmer → $n^2/2$ Schlüssel, n-1 je Teilnehmer
- Keine eindeutige Zuordnung von Schlüssel zu Teilnehmer
  - Nicht-Bestreitbarkeit nicht erfüllbar

Häufig eingesetzte Verfahren

- DES, 3-DES, AES, RC4

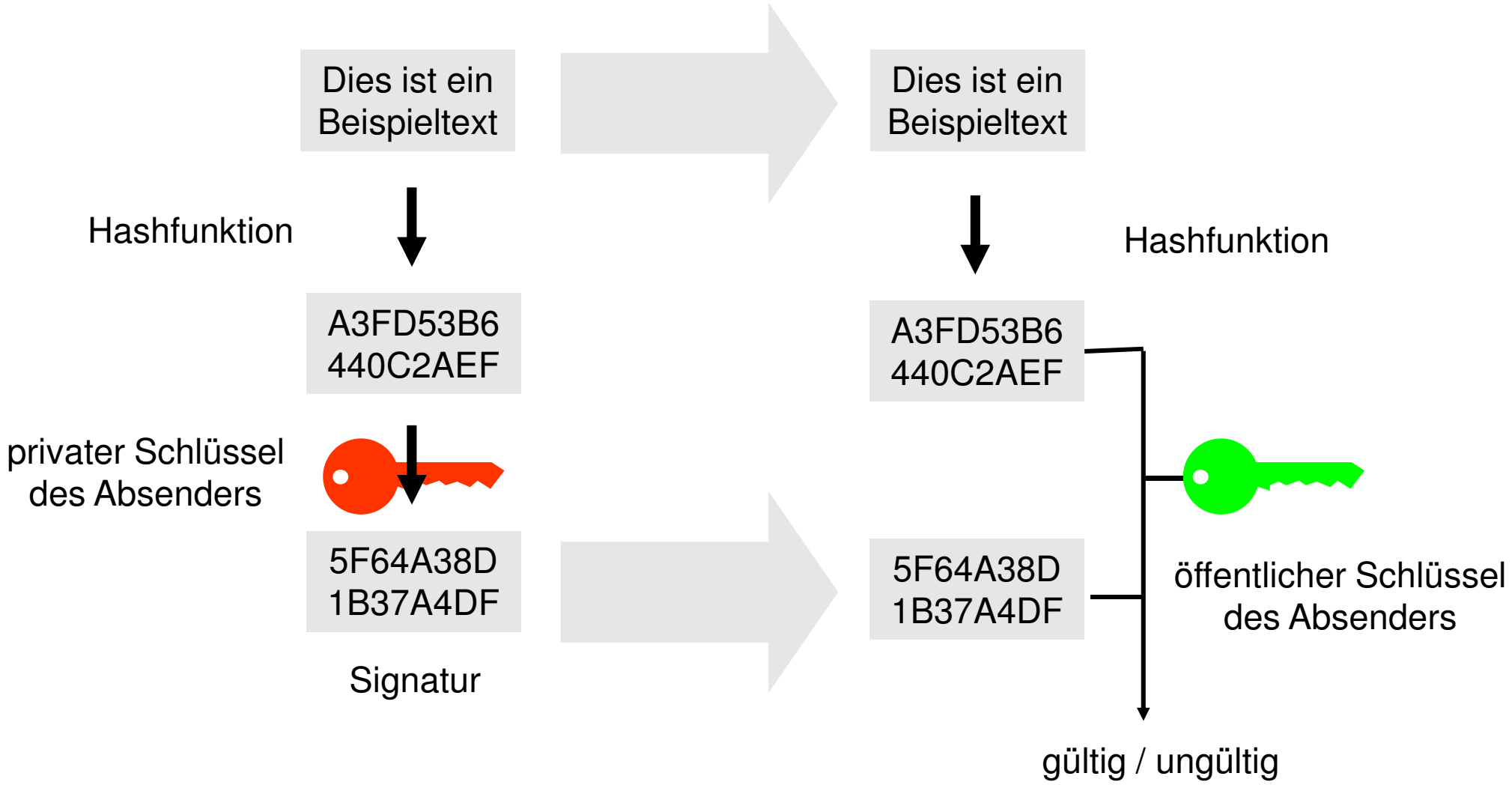
Asymmetrische Verfahren I: Verschlüsselung

Asymmetrische Verschlüsselung



cryptovision

Asymmetrische Verfahren II: Digitale Signatur



Charakteristik Asymmetrischer Verfahren

Vorteile

- Schlüsselverwaltung
  - durch Public Key Infrastruktur (PKI) realisierbar
  - durch sicheres Verfahren zum Schlüsselaustausch
- Eindeutige Zuordnung von Schlüssel zu Teilnehmer
  - Nicht-Bestreitbarkeit erfüllbar

Nachteile

- Aufwändig zu implementieren
- Geringere Performance

Sonstige Verfahren

Hashfunktionen

- Erzeugt einen kurzen “kryptographischen Fingerabdruck”
- Realisiert eine “kollisionsfreie” Einwegfunktion
- Beispiele: RIPEMD160, SHA-1, SHA-2

Zufallszahlengeneratoren (RNGs)

- Zufallszahlen werden in verschiedenen Protokollen benutzt
  - Schlüsselerzeugung, Challenge & Response, …
- RNGs erzeugen “kryptographisch nutzbare” Zufallszahlen
  - erwartungstreu, statistisch zufällig
  - nicht voraussagbar
- Es existieren Hardware- und Pseudo-RNGs
- Beispiel eines PRNG: Fips186-2

Asymmetrische Verfahren: RSA

RSA war das erste asymmetrische Verfahren

- Entwickelt: 1979
- von **R**ivest, **S**hamir & **A**dleman
- Patent im Jahr 2000 ausgelaufen

Bietet typische kryptographische Anwendungen

- Verschlüsselung, Signatur
- Kein generisches Verfahren zum Schlüsselaustausch

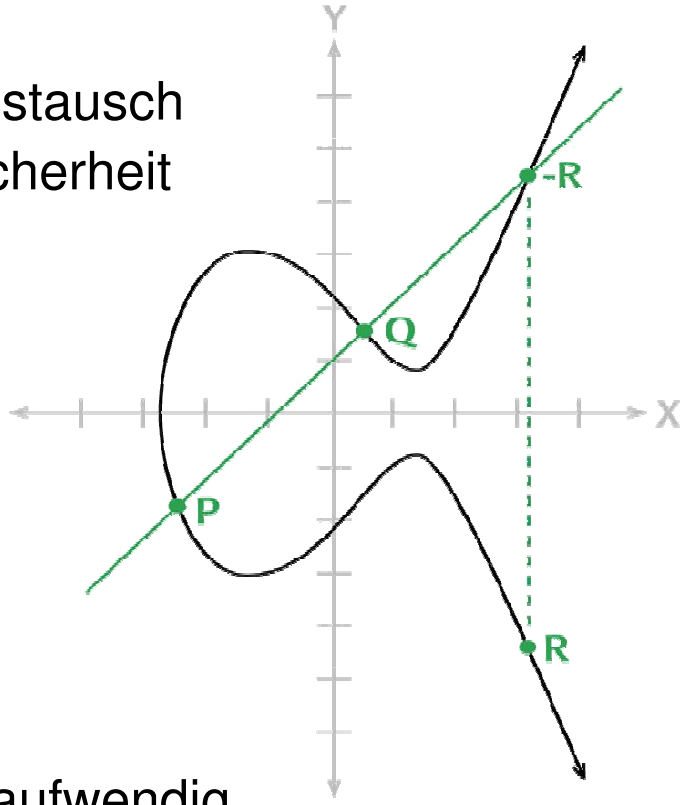
Das „Problem der Faktorisierung"

- Modulare Multiplikation ist leicht
- Faktorisierung einer Langzahl ist aufwendig

Asymmetrische Verfahren: ECC

Elliptic Curve Cryptography – eine populäre RSA Alternative

- “Erfunden” 1985
- Verschlüsselung, Signatur und Schlüsselaustausch
- Kürzere Parameter als RSA bei gleicher Sicherheit



Höhere Sicherheit & kürzere Parameter bieten

- höhere Performance
- effizientere Ressourcen-Nutzung
- bessere Skalierbarkeit

Das “Problem des Diskreten Logarithmus”

- Modulare Exponentiation ist leicht
- Berechnung des diskreten Logarithmus ist aufwendig

Asymmetrische Verfahren: RSA ↔ ECC

Schlüssellängen

- RSA – 2048 Bit
- ECC – 192 Bit

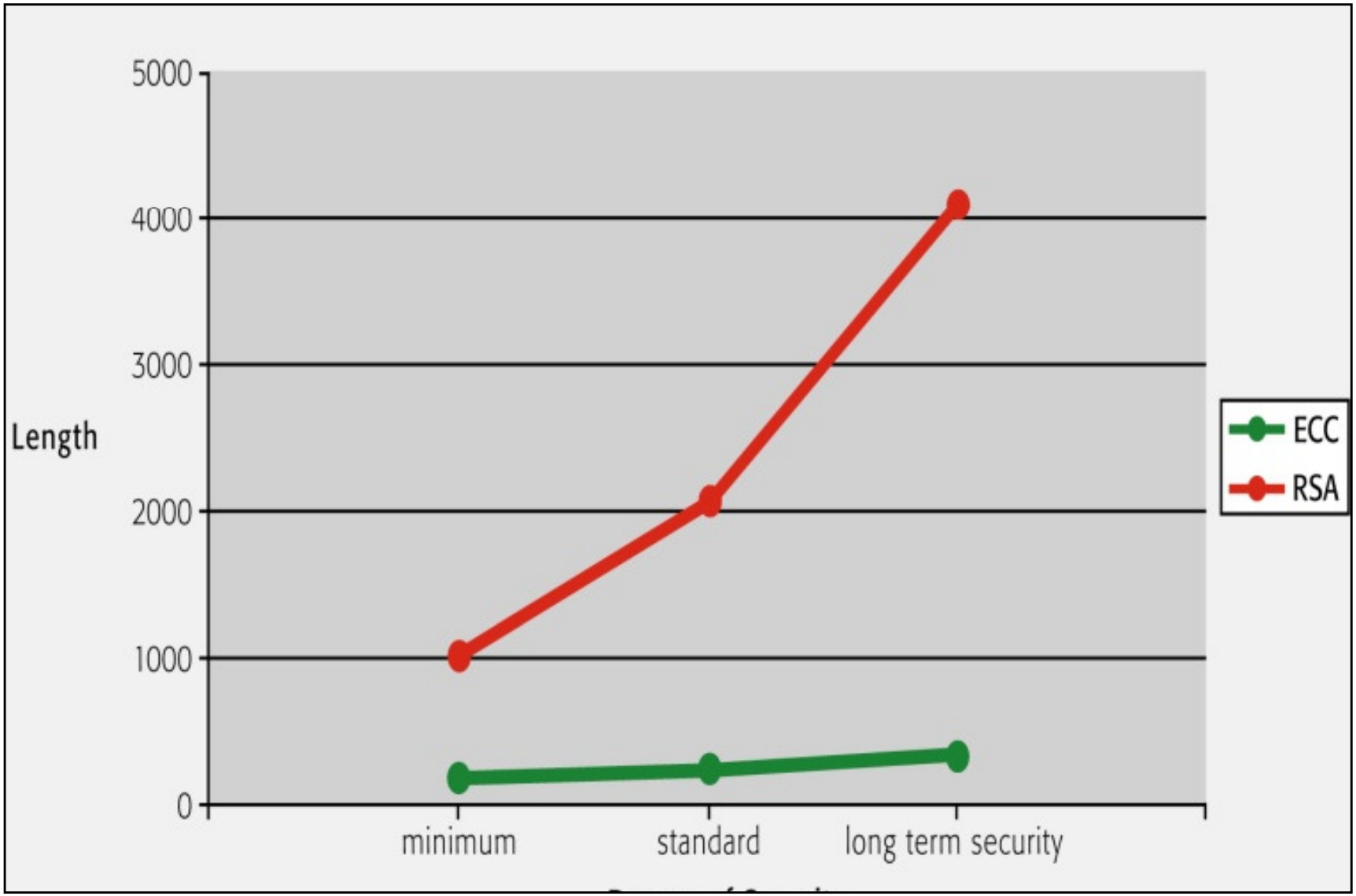
Performance

- RSA Signatur mit 2048 Bit – etwa 2 s
- ECC Signatur mit 192 Bit – etwa 160 ms

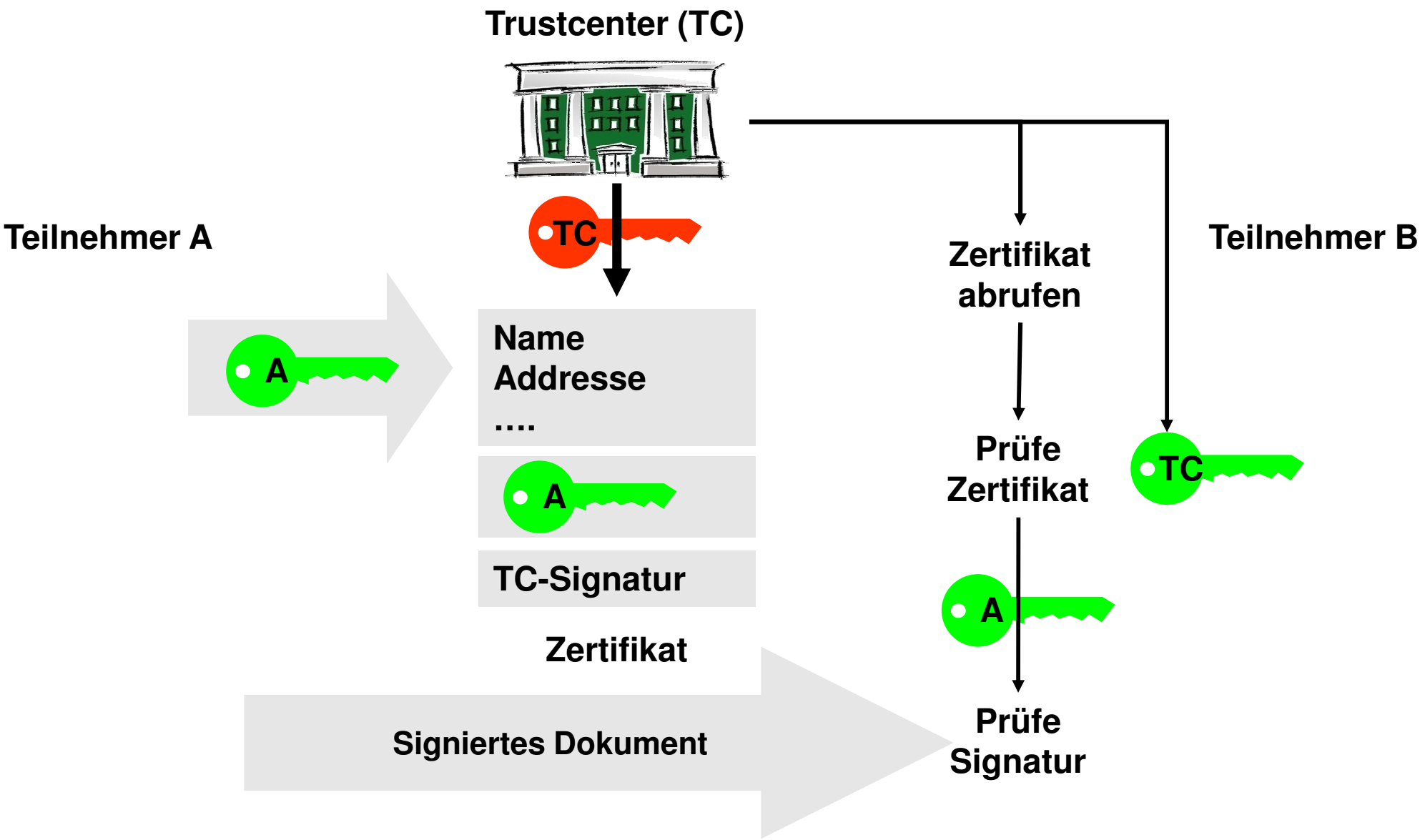
Beispiele für den Einsatz von ECC

- Elektronischer Reisepass
- Gesundheitskarte

Asymmetrische Verfahren: RSA ↔ ECC



Public Key Infrastructure (PKI): Zuordnung von Schlüsseln



AGENDA

1. Kryptographie
   a. Grundlagen der Kryptographie
   b. Kryptographische Verfahren
   c. Sicherheitsaspekte
2. INSIKA TIM
3. Fazit

Sicherheitsaspekte

Geheimhaltung und Verteilung von Schlüsseln

- Symmetrische Verfahren
- Asymmetrische Verfahren

Sichere Hardware

- Hardware Security Module (HSM)
- Smart Card

Performance

- RSA Signatur mit 2048 Bit – etwa 2 s
- ECC Signatur mit 192 Bit – etwa 160 ms

Sicherheitsaspekt: Schlüssellänge

Empfohlene Schlüssellängen für Elektronische Signaturen nach Signaturgesetz (SigG)

(Empfehlung BNetzA / BSI 11 / 2008)

	Früher	Heute	Zukunft
RSA	1024 Bit	1536 Bit	2048 Bit
ECC	160 Bit	180 Bit	> 192 Bit

AGENDA

1. Kryptographie
    a. Grundlagen der Kryptographie
    b. Kryptographische Verfahren
    c. Sicherheitsaspekte
2. **INSIKA TIM**
3. Fazit

INSIKA TIM: Überblick

Funktionen des TIM

- Verifikation der Umsatzdaten
- Aufzeichnung der Umsatzdaten
- Signatur der Umsatzdaten

Eindeutige und unveränderliche Identifikation

- einer Buchung
- des Steuerzahlers

Absicherung gegen Manipulation

INSIKA TIM: Funktionen I

Verifikation der Umsatzdaten

- Umsatzsummen
- Umsatzsteuer
- Umsatzsteuersätze

Aufzeichnung der Umsatzdaten

- Umsatzsummen
- Umsatzsteuer
- Umsatzsteuersätze

Signatur der Umsatzdaten

INSIKA TIM: Verifikation der Umsatzdaten

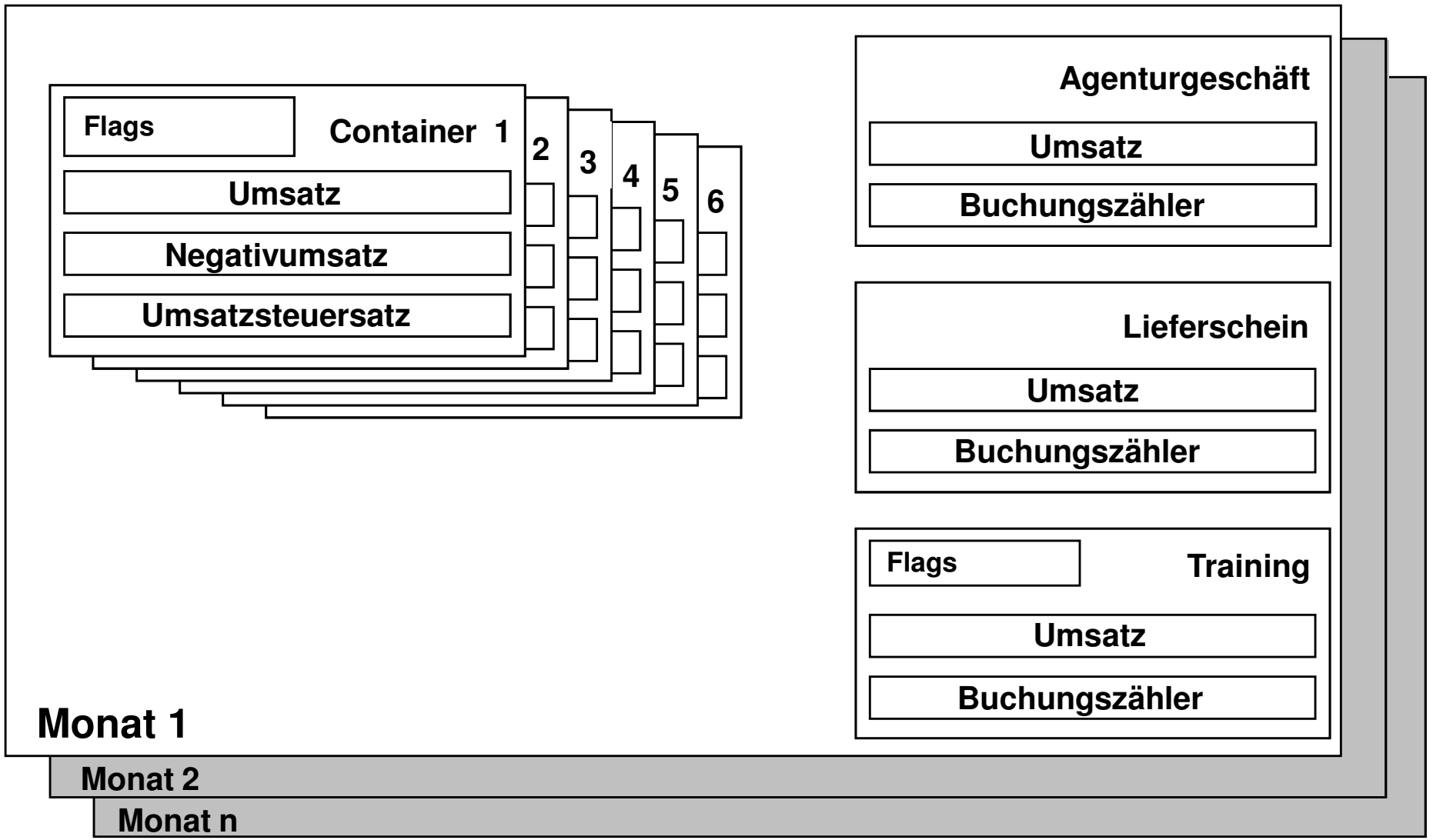
Daten

- Brutto- oder Nettoumsatz
- Umsatzsteuer
- Umsatzsteuersatz

Berechnungen

- Umsatzsteuer aus Umsatz berechnen
- Berechnete Umsatzsteuer mit übergebenem Umsatzsteuer-Betrag vergleichen
- Nettoumsatz und berechnete Umsatzsteuer zu Umsatzsummen addieren

INSIKA TIM: Aufzeichnung der Umsatzdaten



INSIKA TIM: Signatur der Umsatzdaten

Signatur einer Buchung

- Datum und Uhrzeit
- ID der Kasse
- ID des Benutzers
- Buchungsdaten
- Kennzeichen Brutto- / Nettoumsatz
- Kennzeichen Trainingsbuchung
- Eindeutige Sequenznummer
- Umsätze getrennt nach Umsatzsteuer-Sätzen

Signatur der Buchung wird

- im Kassenjournal gespeichert und
- auf dem Beleg ausgedruckt

INSIKA TIM: Funktionen II

Umgang mit verschiedenen Steuersätzen

- Steuersatz wird „von außen“ vorgegeben
- Änderungen der UStS werden aufgezeichnet

Reportfunktion

- Tagesabschluss
- Umsatzsummen
- Monatsgenau

Sonstige Funktionen

- Identifikation einer Buchung durch eindeutige Sequenznummer
- Identifikation der Kasse / des Steuerzahlers

INSIKA TIM: Sicherung gegen Manipulationen

Sicherung des TIM gegen Manipulationen

- „Read Only“ Speicherung aller Daten
- Generierung des Schlüsselpaares auf dem TIM
- Sichere Speicherung des privaten Schlüssels
- Eindeutige Seriennummer (Hardware basiert)
- Öffentlicher Schlüssel in Zertifikat gespeichert

INSIKA TIM: Referenzimplementierung

Referenzimplementierung des TIM

- CardOS V4.3b
- cryptovision ECC-Package
- INSIKA TIM-Package
- Nutzt SHA-1 und 192 Bit ECC
- Verwendung „längerer“ ECC Parameter möglich
- Umstellung auf SHA-256 möglich

AGENDA

1. Kryptographie
    a. Grundlagen der Kryptographie
    b. Kryptographische Verfahren
    c. Sicherheitsaspekte
2. INSIKA TIM
3. **Fazit**

Fazit

Kostengünstige Lösung durch Einsatz des TIM

Keine „Security by Obscurity“

Zukunftssicher

Vielen Dank für Ihre Aufmerksamkeit!

mathias.neuhaus@cryptovision.com