



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Mobile Commerce

Sicherheit, Anwendungen und Perspektiven

Dr. Bernd Dusemund

Institut für Telematik

08.06.2001



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Inhalt

Part I: Sicherheit

- Gefährdungen im Mobile Commerce
- Sicherheit durch PKI
- WAP-Sicherheit: WIM und PKI



Inhalt:

Part II: Perspektiven Mobile Commerce

- Potentiale des Mobile Commerce
- Entwicklung mobiler Geräte
- Verschmelzung Handy und Internet
- neue Anwendungen

Gefährdungen im Mobil-Funk



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

- Abhören der Verbindung an der Luftschnittstelle
- Abhören beim Netzbetreiber
- Veränderung des Inhaltes der übertragenen Information (Integritätsverletzung)
- Missbrauch der SIM- Karte / Diebstahl oder **Kopie!!!**
- Missbrauch der Informationen auf der SIM-Karte (Adressen ...)
- Hardware- / Firmwaremanipulationen
- Erstellung von Bewegungs- und Kommunikationsprofilen



Technische Gegenmaßnahmen

- *Abhören*: Herstellen einer Ende zu Ende Verschlüsselung
- *Integritätsverletzung*: Verwendung einer dig. Signatur
- *Missbrauch der SIM-Karte*: Verwendung zertifizierter Karten
- *Missbrauch von Informationen auf der SIM-Karte*: Verschlüsselung der Daten, Biometrie
- *Hardware- / Firmwaremanipulationen*: Zertifizierung der Geräte
- *Erstellung von Bewegungs- und Kommunikationsprofilen*: Anonymisierung der Karte



Technische Gegenmaßnahmen

- *Abhören*: Herstellen einer Ende zu Ende Verschlüsselung
- *Integritätsverletzung*: Verwendung einer dig. Signatur
- *Missbrauch der SIM-Karte*: Verwendung zertifizierter Karten
- *Missbrauch von Informationen auf der SIM-Karte*: Verschlüsselung der Daten, Biometrie
- *Hardware- / Firmwaremanipulationen*: Zertifizierung der Geräte
- *Erstellung von Bewegungs- und Kommunikationsprofilen*: Anonymisierung der Karte

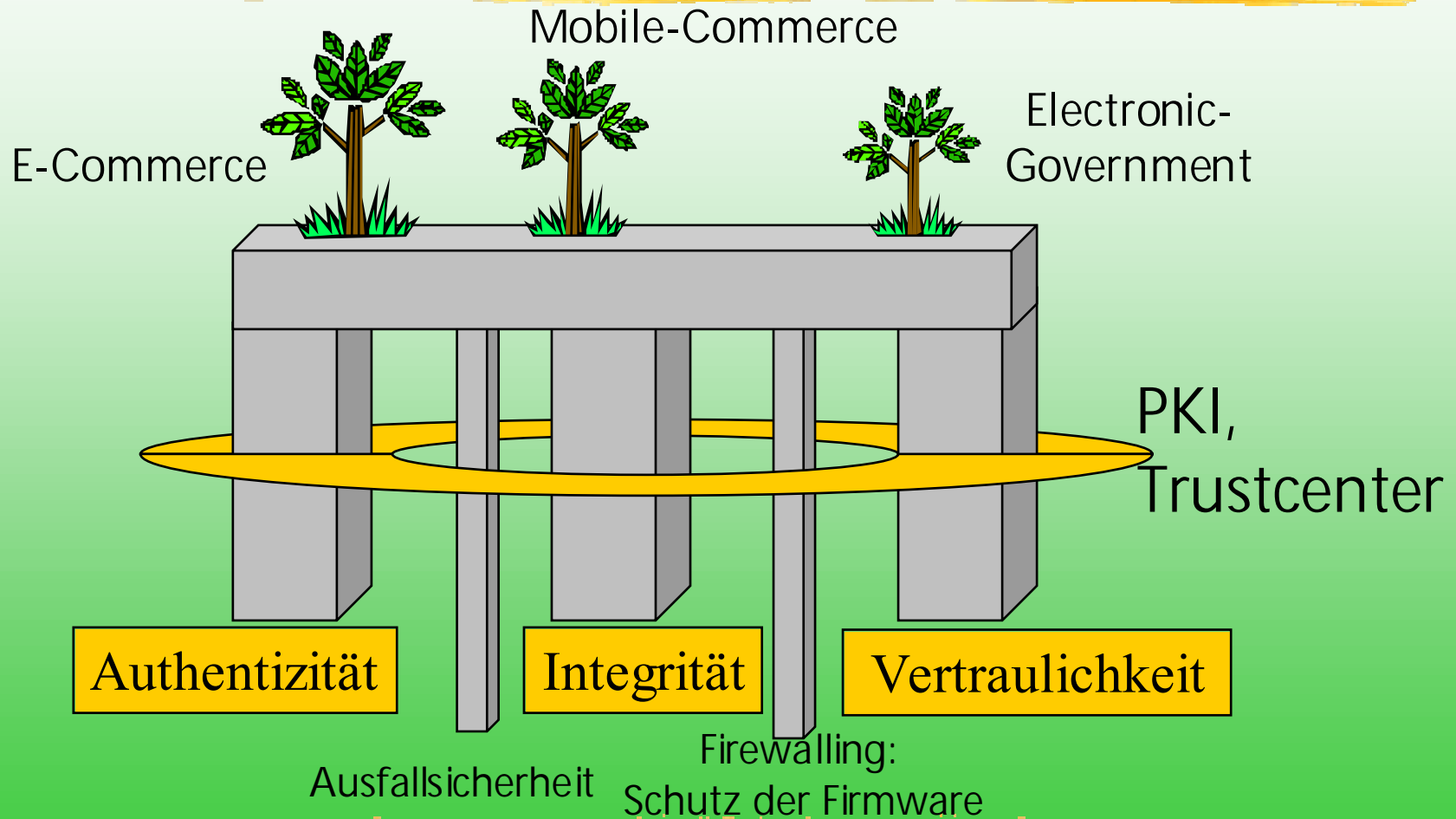
PKI

Sicherheit als Basis



Institut für Telematik

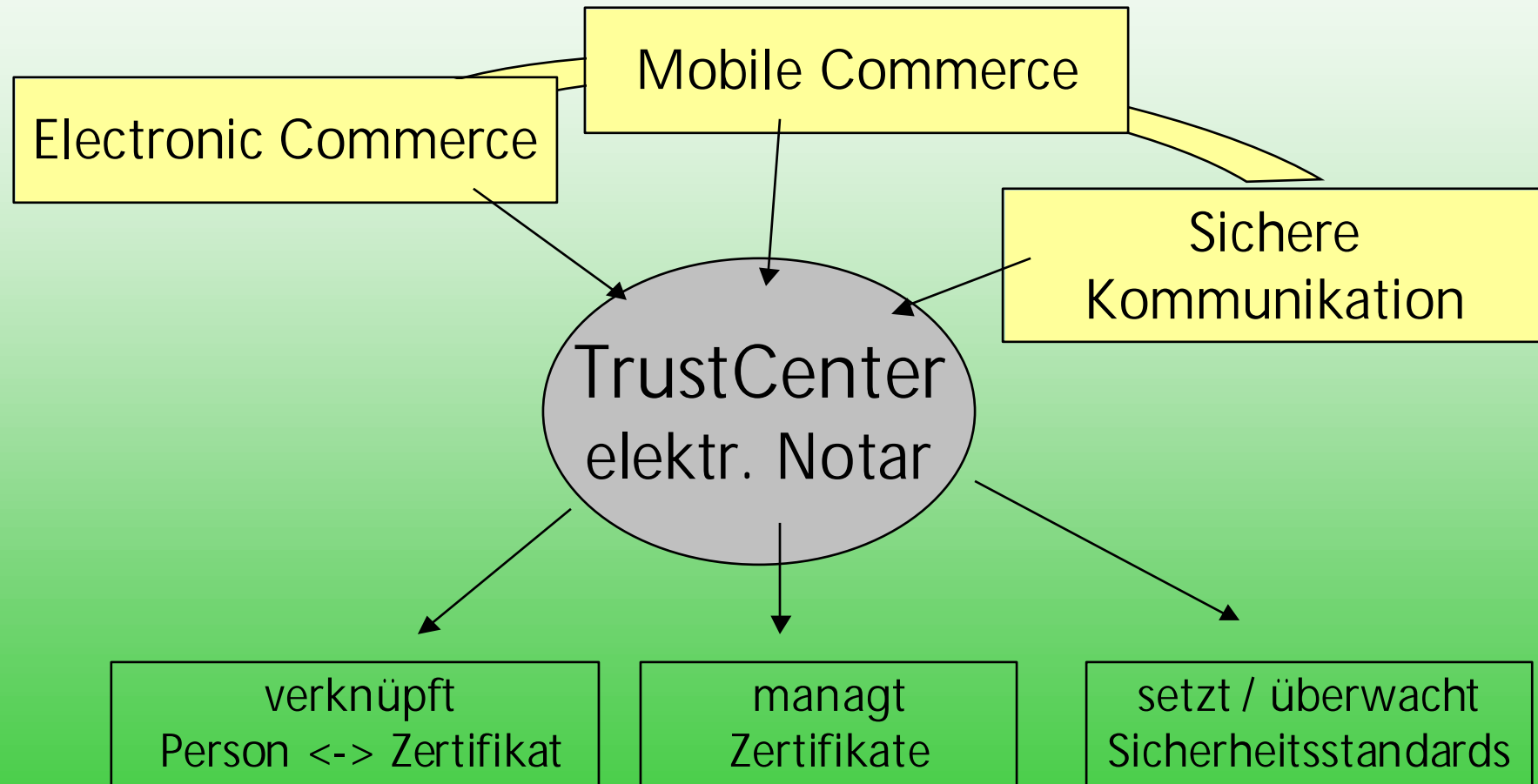
unter Betreuung der
Fraunhofer Gesellschaft



TrustCenter: Herz einer PKI



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft





Klassische Aufgabe der PKI:

Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Gleichstellung elektronischer und handschriftlicher Dokumente

- Signierung / Authentizität
- Unverfälschtheit des Inhaltes /
Integrität
- Verschlüsselung / Vertraulichkeit





Lösung: Kryptografie

Verwendung asymmetrischer Schlüsselpaare

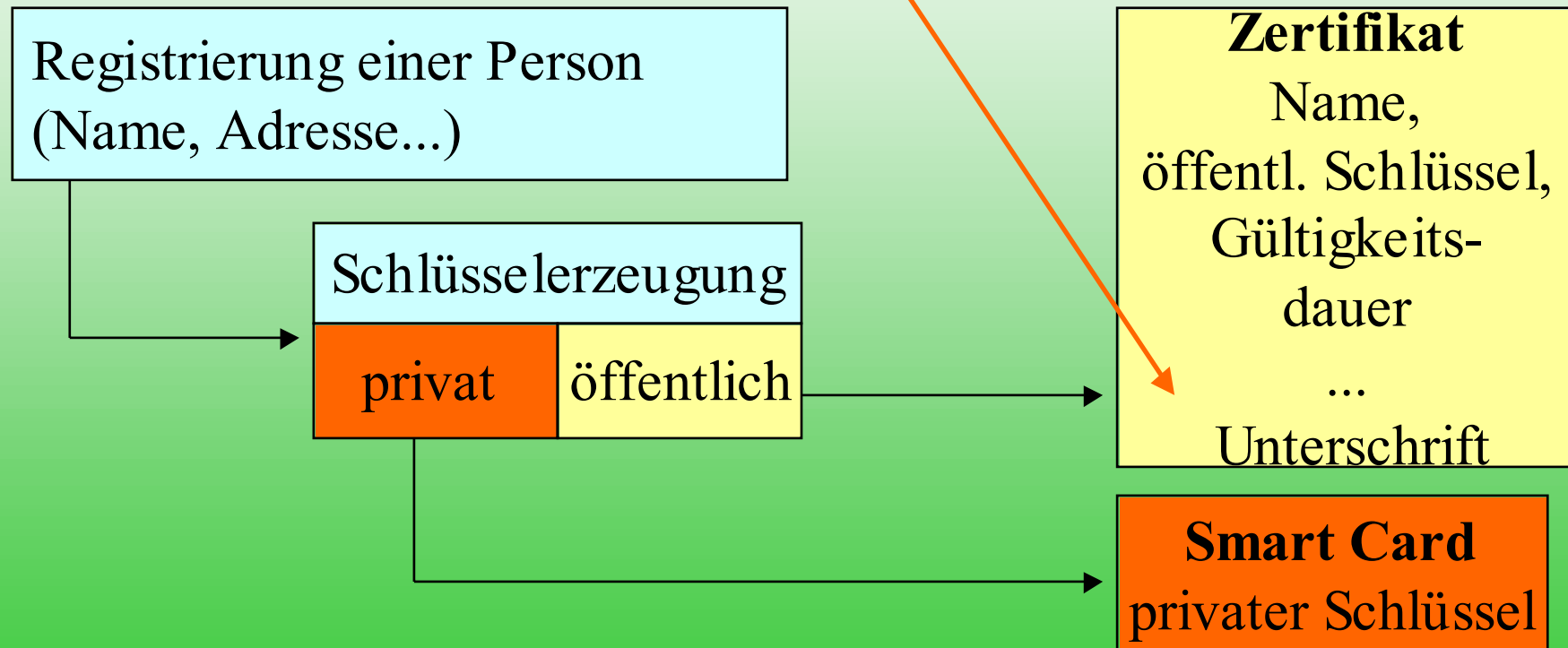
- **geheimer** (privater) Schlüssel auf **SmartCard** gespeichert
- **öffentlich zugänglicher** Schlüssel im Zertifikat

Verwaltung der Zertifikate / Ausgabe der SmartCards:
Trustcenter



Trustcenter:

Schlüsselvergabe + Unterschrift Zertifikat

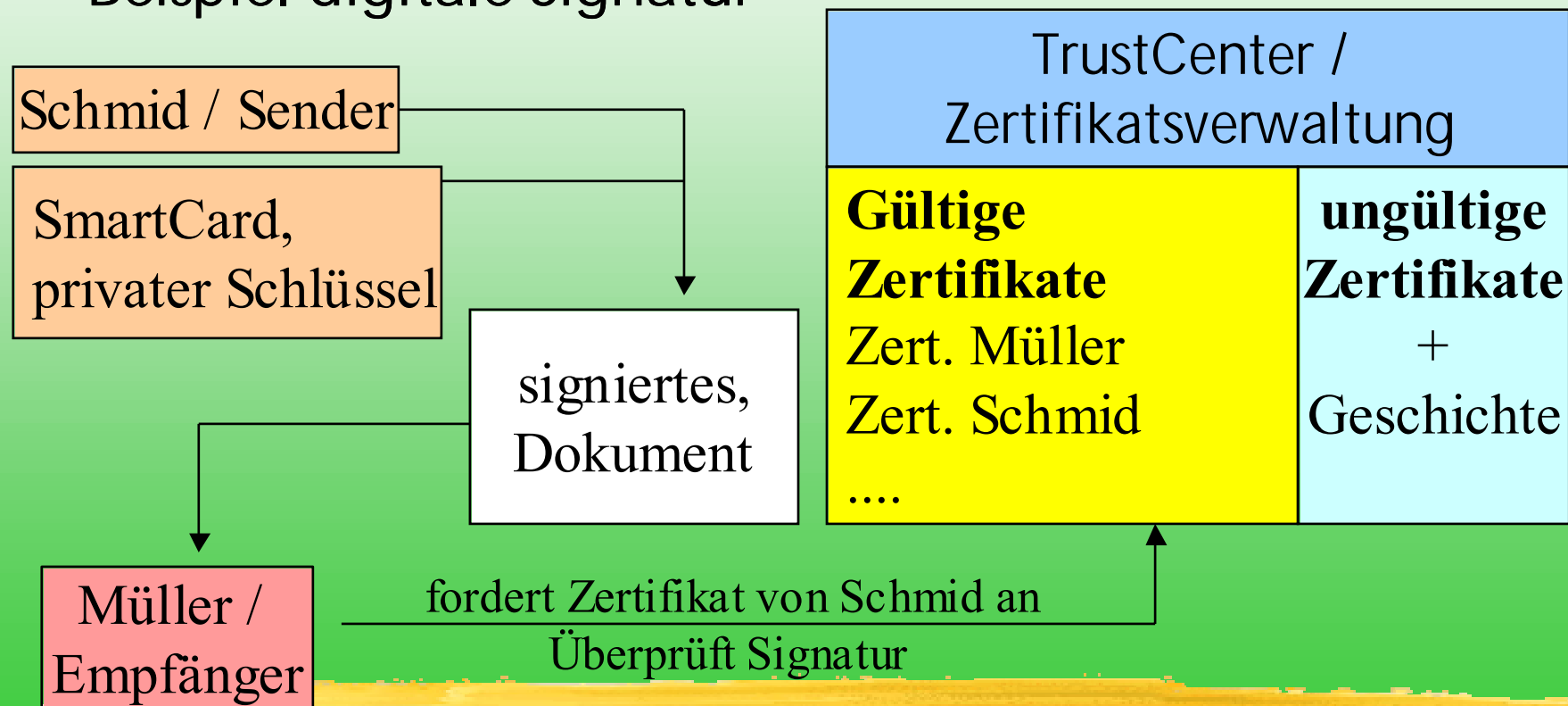


Trustcenter



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

Zertifikats Management Beispiel digitale Signatur



Vorgang



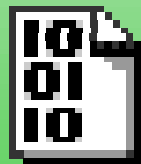
Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

digitales Signieren

Sender



Nachricht



Hash-Wert



Signatur

Empfänger

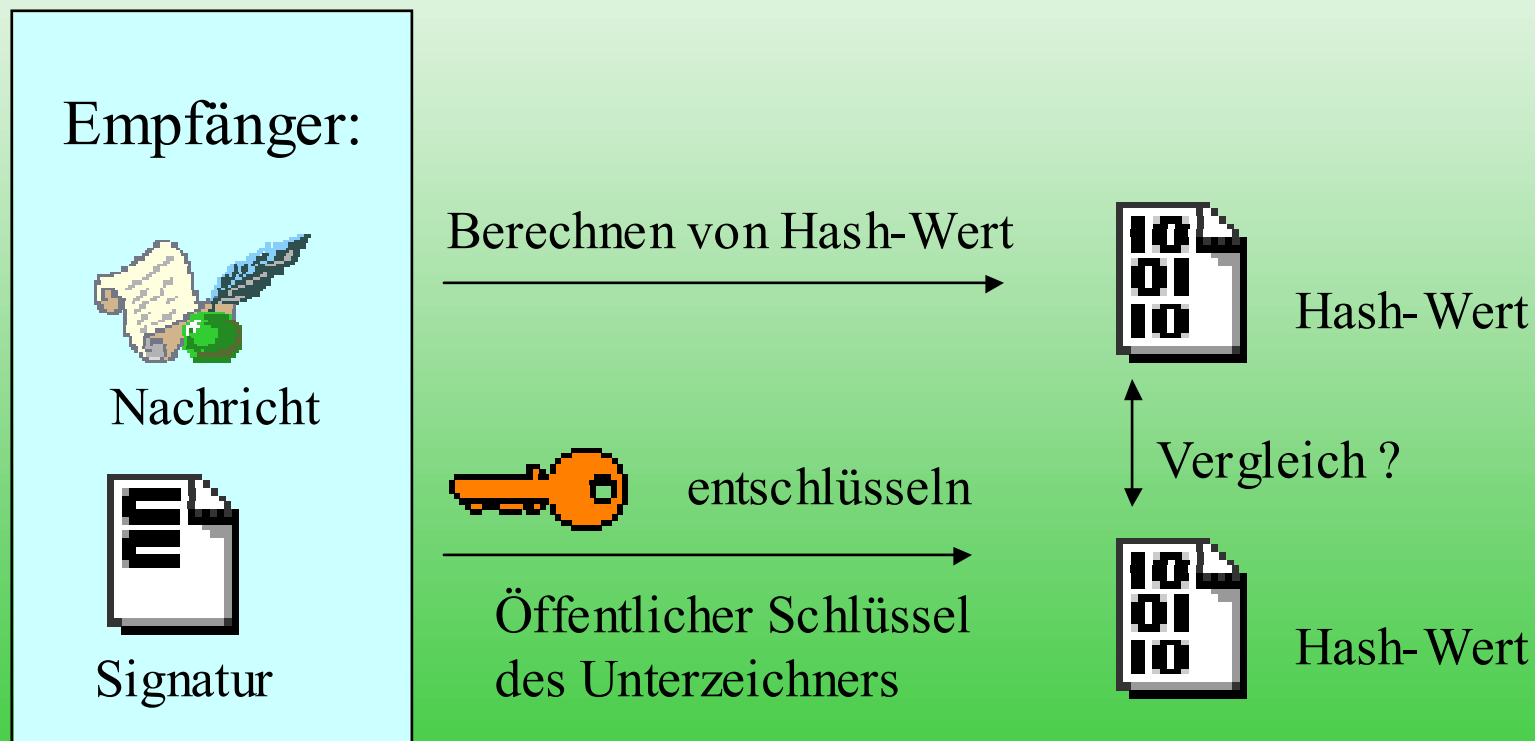


Nachricht



Verifikation

beim Empfänger



PKI- Basissteine:



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

Funktionalität auf der Anwenderseite:

- SmartCard – privater Schlüssel
- Sicheres Eingabegerät
- Anzeigemöglichkeit



SIM-Karte
+
Dig. Signatur
↓
WIM-Karte

WIM - Wireless Identity Module

Zusammenfassung



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

Sicherheit

*WIM und PKI bilden eine solide Plattform
zur Einführung von M-Commerce*

Fragestellungen, die sich auf die Abhörbarkeit von
Räumen beziehen, werden damit nicht gelöst.

Perspektiven: M-Commerce



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

- Dimension des Mobile Commerce
- Entwicklung und Wachstum
- Anwendungsfelder
- Buisness - Modelle
- Szenario: Zugangskontrolle



Dimension:

Mobile-Commerce

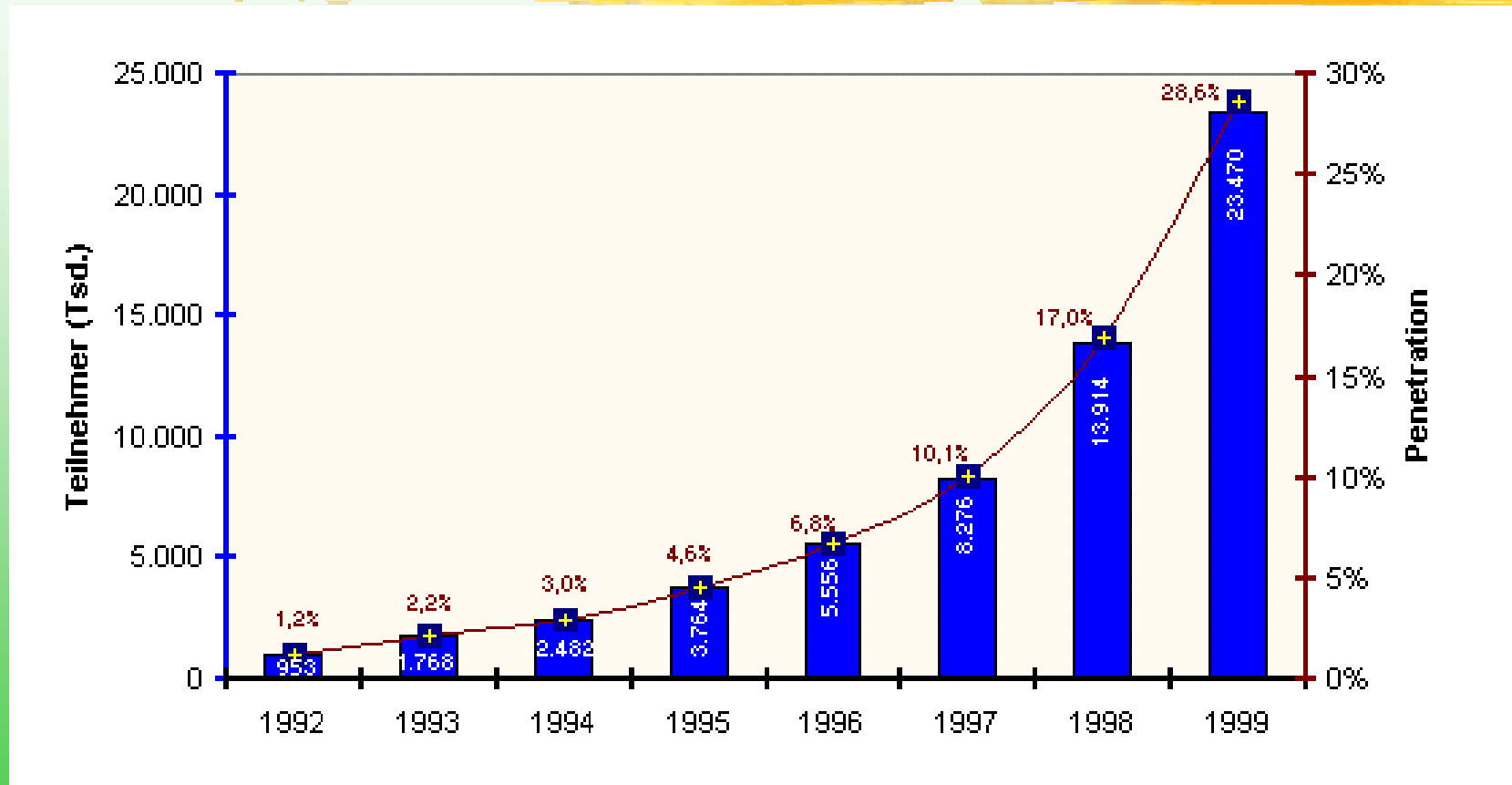
- Omnipräsenz - Nutzung von allen Altersgruppen
- Verfügbarkeit - überall, jederzeit
- Sicherheit - Authentisierung und Verschlüsselung
- Bequemlichkeit - einfach zu Nutzen
- Profilerstellung - individuell
- Lokalisierung - direkter Zugriff auf den Standort
- Inhalt - globaler Zugang, aktuell und genau

Entwicklung des Mobilfunks



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft



Quelle: Netzbetreiber/ Schätzung RegTP

Penetration bezogen auf die Gesamtbevölkerung

Anwendungen des Mobilfunks I



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Sprachübertragung

Banking

- Online Banking
- Mobile Brokerage
- Mobile Payment

M-Commerce

- Einkauf
- Online-Auktionen
- Elektronische Bücher

Unterhaltung

- Spiele, Chat-Räume
- Musik-, Videoübertragung

Anwendungen des Mobilfunks: Telematik



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Location based services

Straßenverkehr:

- Verkehrsinfo
- Routenplanung
- Pannen- / Notrufdienste
- Flottenmanagement

Informationsdienste

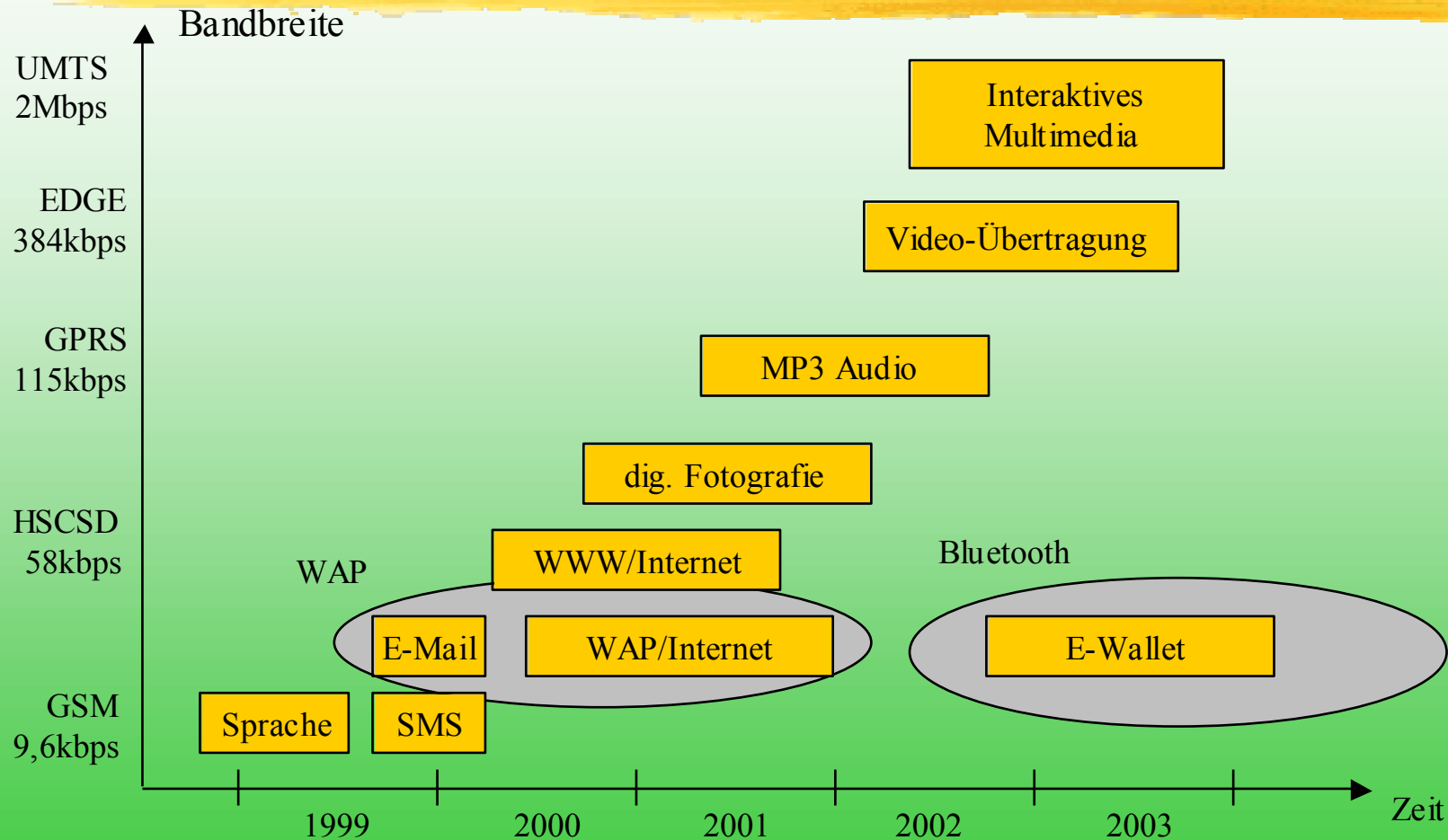
- Reservierungen
- Buchungen
- aktuelle Nachrichten

Anwendungen - Entwicklungen



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft





Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Szenario:

Verwirklichung einer Zugangskontrolle mit einem mobilen Telefon

Anforderungen:

- ✓ Authentizität
- ✓ Verschlüsselung
- Integrität

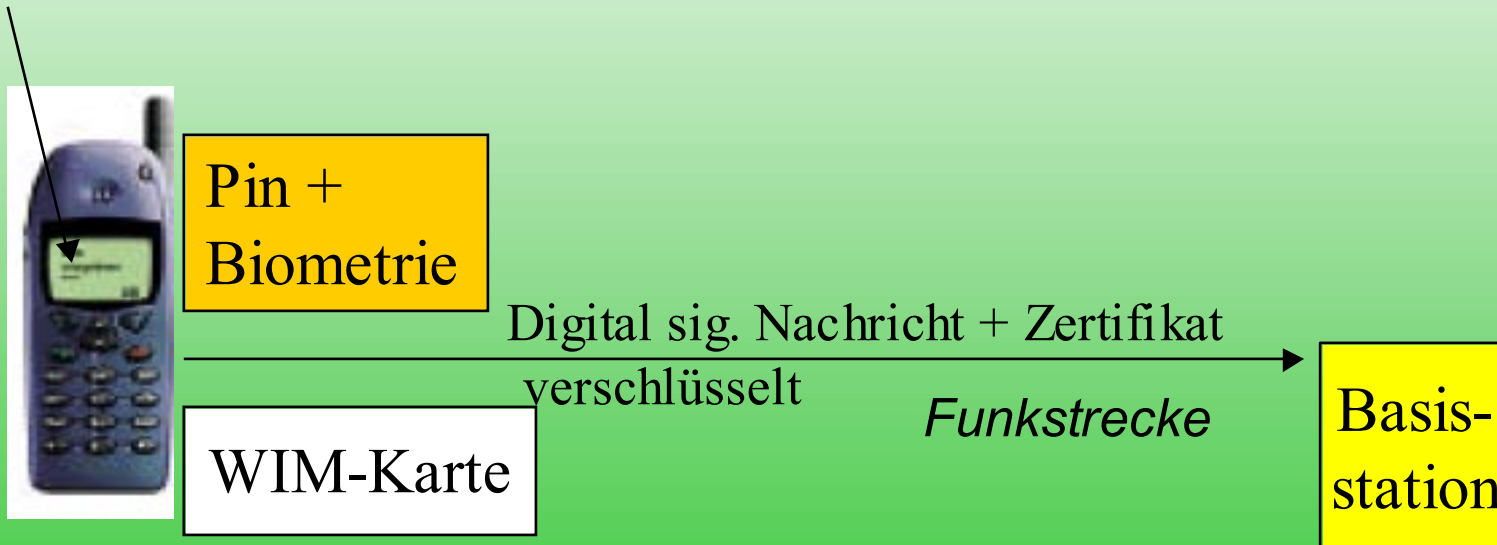
Ablaufschema 1



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

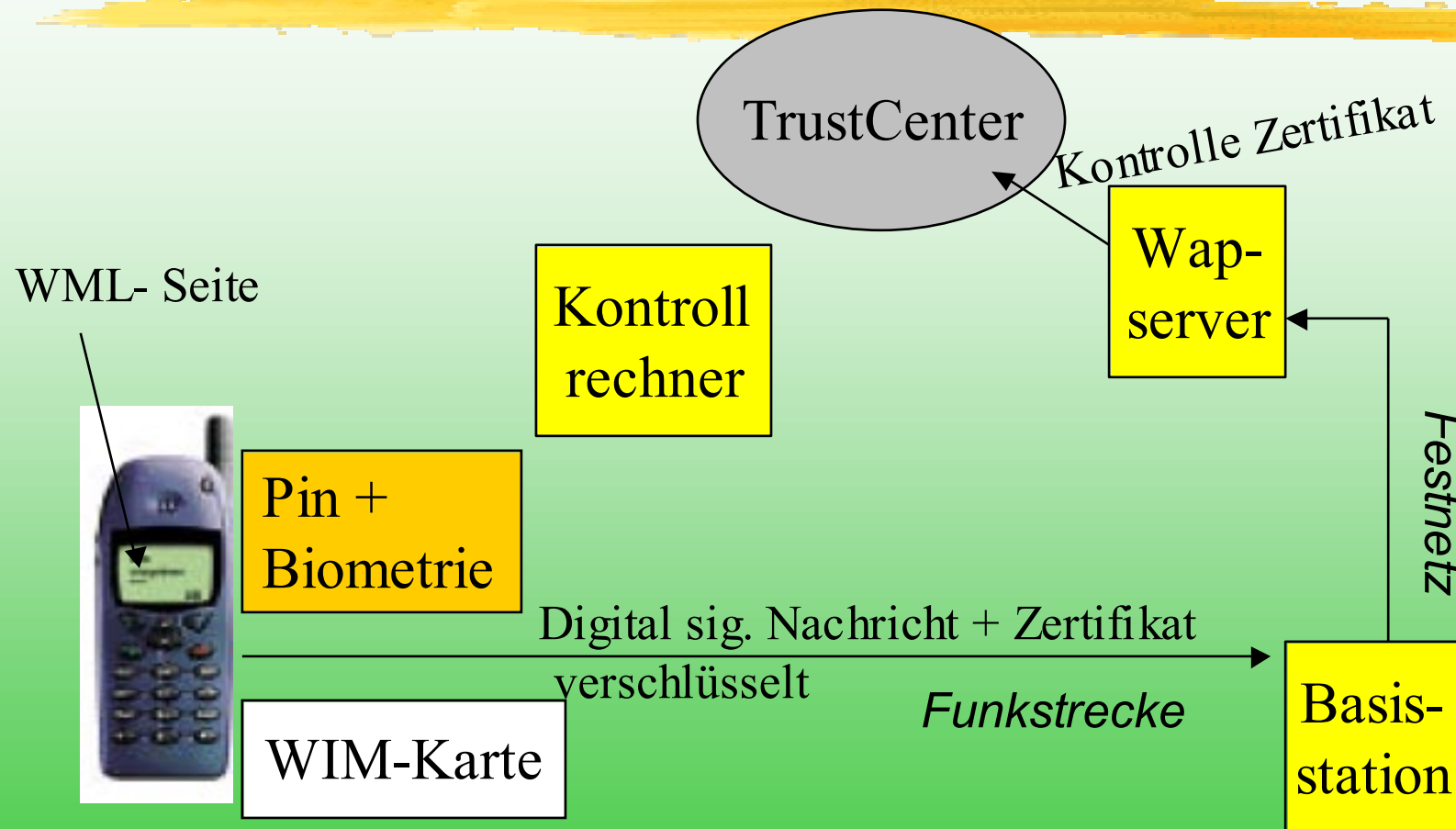
WML-Seite



Ablaufschema 2



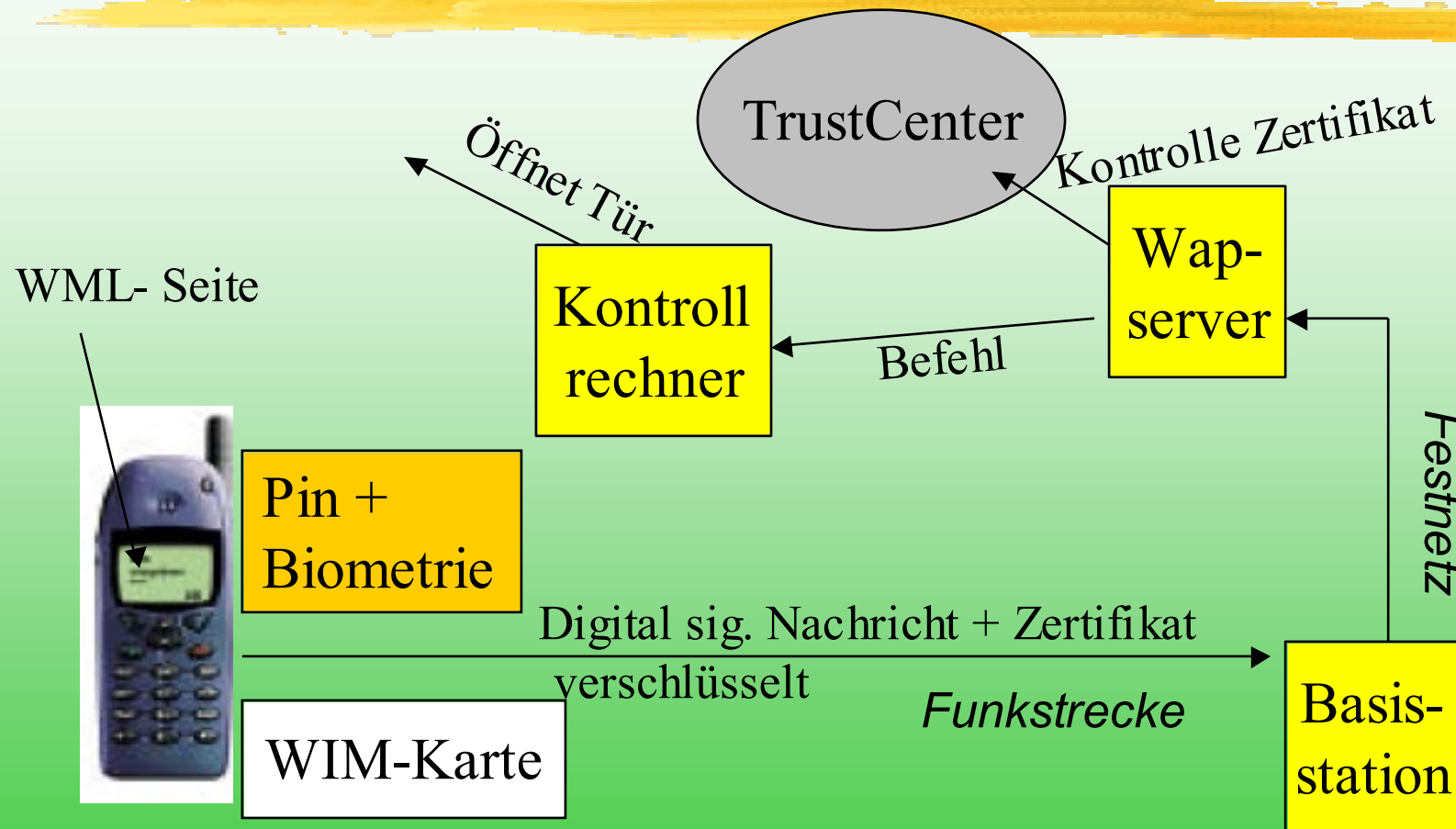
Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft



Ablaufschema 3



Institut für Telematik
unter Betreuung der
Fraunhofer Gesellschaft

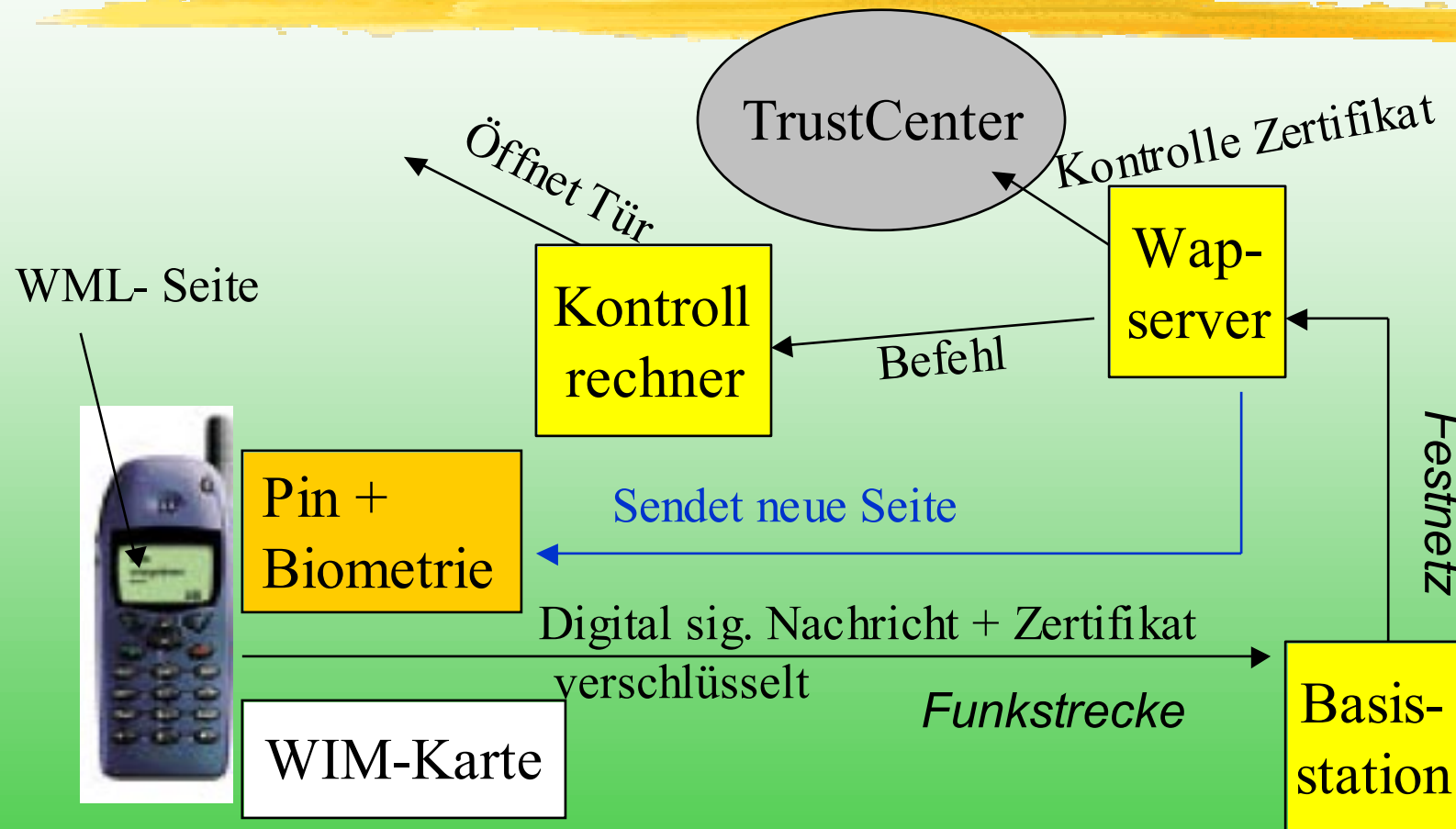


Ablaufschema 4



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft





Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Demonstration



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Danke für Ihre
Aufmerksamkeit,

für Ihre Teilnahme

und

gute Heimreise