Die Java Card als Programmier- und Ausführungsplattform für verteilte Applikationen

Dipl.-Inform. Stefan Fünfrocken

FG Verteilte Systeme

TU Darmstadt

Gemeinsame Arbeit

- Prof. Friedemann Mattern,
  ETH Zürich
- Dipl.-Inf. Marie-Luise Moschgath,
  ITO, TU Darmstadt

Gefördert durch die Deutsche Telekom AG

- Zentrum für Kartenanwendungen, Nürnberg
- Technologiezentrum Darmstadt

© Stefan Fünfrocken

Überblick

- Chipkarten
- Chipkarte als Anwendungsplattform
- Java Card
- Realisierte Prototypen
- Erfahrungen

© Stefan Fünfrocken

Chipkarten

- Speicherkarten
  - Benutzeridentifikation („secure token“)
- Karten mit integriertem Prozessor
  - Rechenleistung vorhanden,

Aber

  - Funktion „fest verdrahtet“ (Karte = passiver Server)
  - Programmierung erfordert Experten
  - Lange time-to-market Zeit

© Stefan Fünfrocken

Die Karte als Mini-PC

z.B. Siemens SL66

- Prozessoren mit zunehmender Leistung
- Mehr Speicher
- Klarer Technologietrend

⇨ Karte wird zum Rechner

  – mit ***aktiven*** Applikationen



- Moderne, multifunktionale Karten
  - **Java Card**
  - Multos
  - Microsoft Card

© Stefan Fünfrocken

Die Chipkarte als Plattform

- Einbindung in Kommunikationsnetze
  - Netzanschluß, Jini-Integration
  - Middleware-Integration (z.B. CORBA)
- „On-the-fly“ Installation von Software
  - am Terminal
  - über Netzanbindung
- Programmierbar durch „Jedermann“

IPv6 erlaubt Netzadresse für jede Karte

Statt Neuausgabe

© Stefan Fünfrocken



Die Java Card

- Java VM auf der Karte
- Programmierbar in Java
  - geringe time-to-market Zeiten
  - keine „Experten“ zum Programmieren nötig

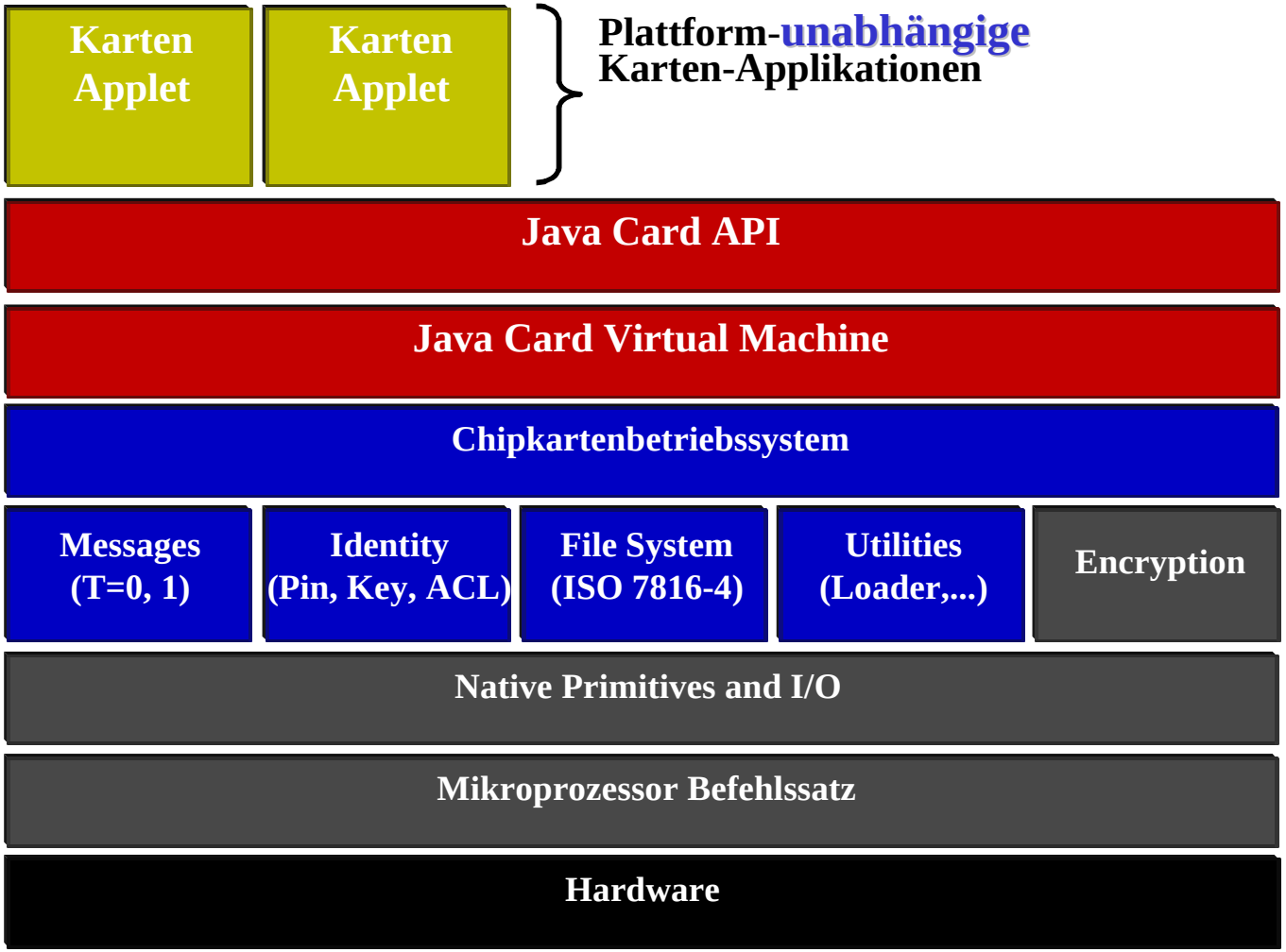
Wochen statt mehrere Monate

- Java Card API (aktuell 2.1)
  - eingeschränkter Sprach-/Funktionsumfang
  - genormte Schnittstelle zur Karte
  - Client-API proprietär



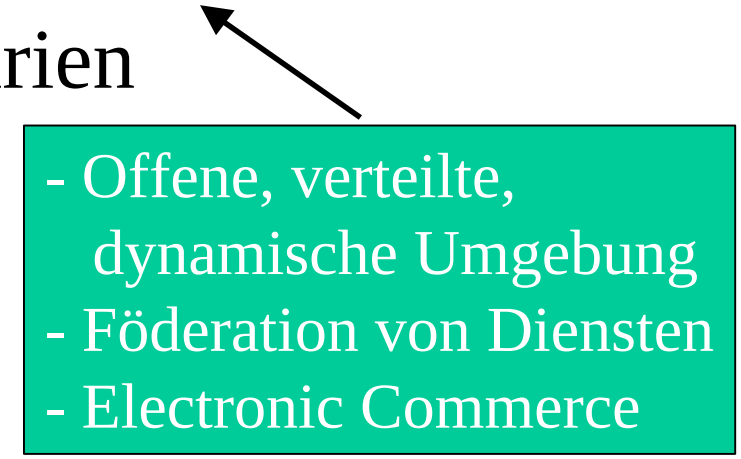
© Stefan Fünfrocken

Die Java Card-Architektur



Java Card - Globale Sicht

- „Natürliche“ Einbindung in Internet-basierte Anwendungsszenarien



- Java Card Vorteile
  - sichere, verläßliche, vertrauenswürdige Instanz
  - Plattformunabhängigkeit von Java
  - Computer in der Brieftasche
    (Weiterentwicklung analog zu µP und PC)

© Stefan Fünfrocken

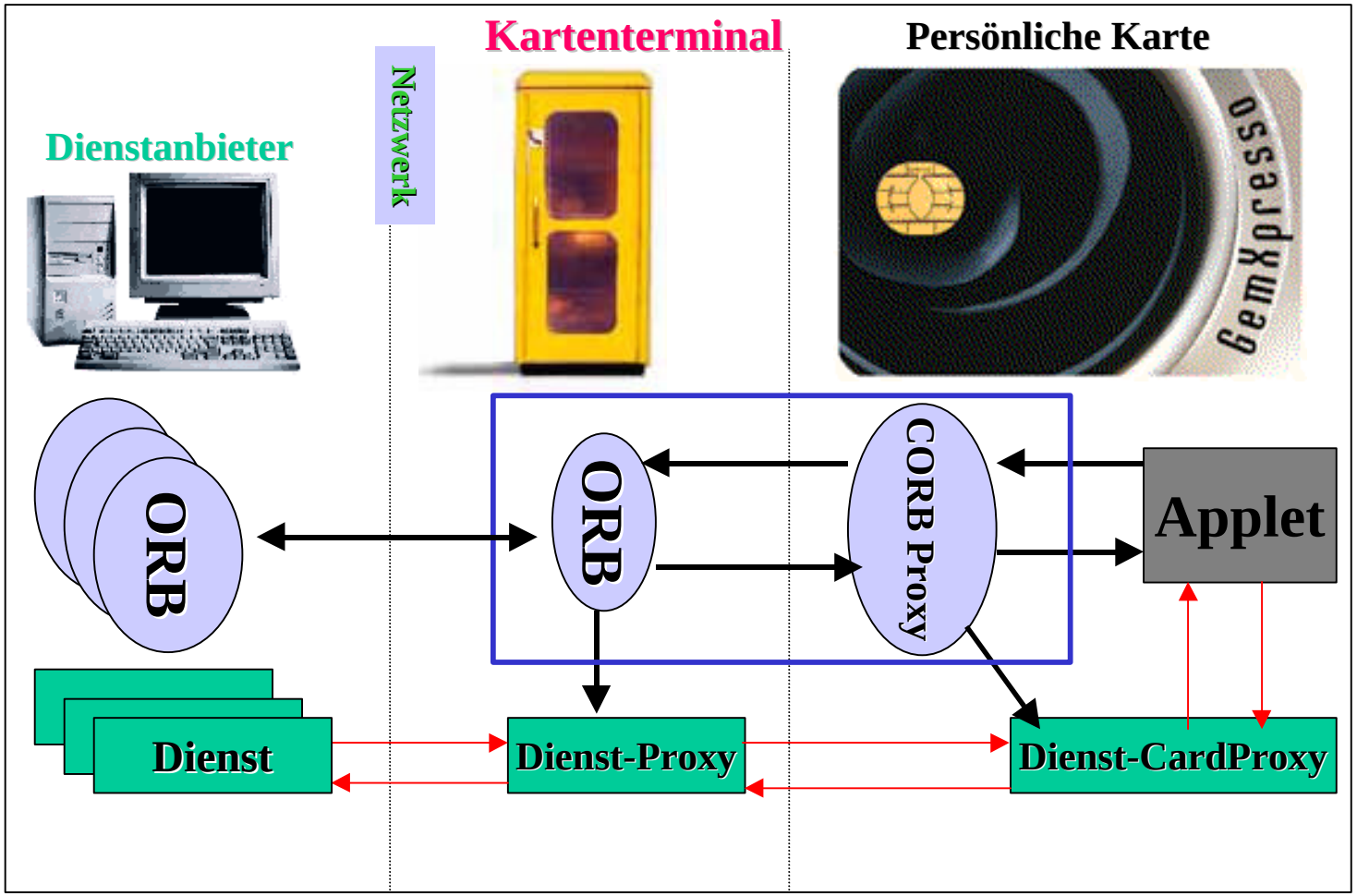
Prototyprealsierungen

- Machbarkeits-Studien
  - Infrastrukturmaßnahme: CORBA-Anbindung, einfache Jini-Anbindung
  - Applikation: Lotto-Spielen über GSM
- Verwendete Karten
  - CORBA, Jini: GemXpresso von Gemplus
  - GSM-Lotto: Cyberflex von Schlumberger
    - Java Card API 2.0, 16K

Neue Karte: Access 16K 2.1 API, stabiler

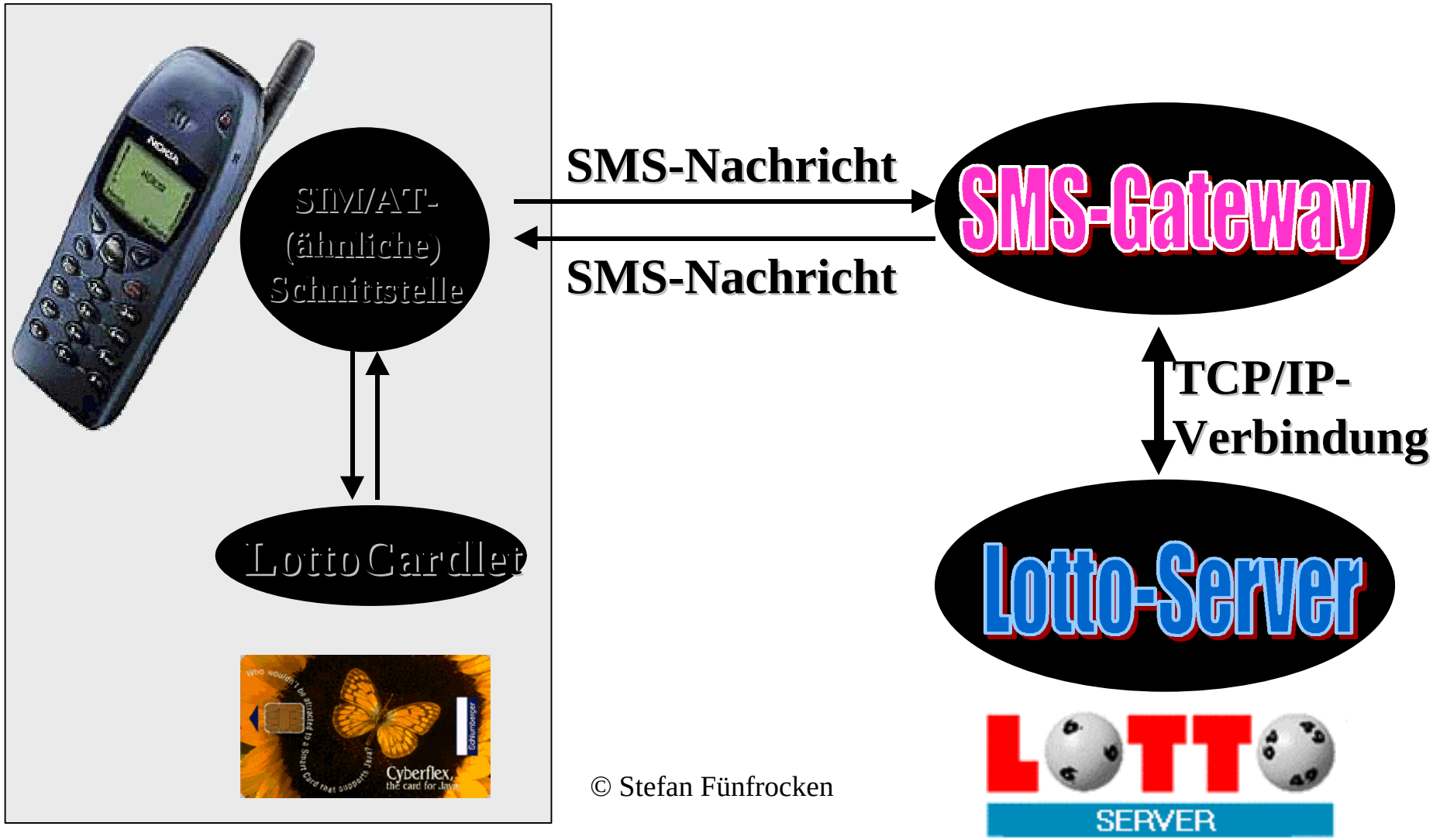
© Stefan Fünfrocker

CORBA Anbindung



© Stefan Fünfrocken

GSM Dienstleistungsszenario



© Stefan Fünfrocken

Erfahrungen

16K (10K+5K)
32/8 Bit CPU

– Ressourcen noch beschränkt
– Betriebssysteme noch „herkömmlich“
– „Bugs/Features“ vorhanden

Neue Karten sind stabiler und besser

+ Kartenhandling auch durch „Ungeübte“
+ Multifunktionalität einfach nutzbar
+ Exzellentes Entwicklungspotential

© Stefan Fünfrocken

Anforderungen

JavaVM:

- Ideal: Standard-VM auf der Karte
- Dateisystem + Zugriffssteuerung auf Applet-Ebene (minimale Unterstützung im API 2.1)
- Klassenlader und Serialisation
- Applet-Installation durch Applet
- Shared-Objects mit Zugriffssteuerung
  - im API 2.1 vorhanden

© Stefan Fünfrocken

Anforderungen

- Aufhebung der Master-Slave-Rolle
- Mehr Infrastruktur auf der Karte
  - Betriebssystem (inkl. Datenbank etc.)
  - TCP/IP-Stack und IP-Adresse
  - mehrere logische Kommunikationskänale nach außen
- Verfügbarkeit von Kryptographie
  (CoPro, Exportproblematik)

Card DB jetzt verfügbar

G&D: Sm@rtCafé
Schlumberger: Access

© Stefan Fünfrocken

Anforderungen

Infrastruktur für verteilte Anwendungswelt

- Integration in Kommunikations-Standards
  - z.B. CORBA (ORB auf der Karte)
  - Jini (kooperierende Java-VMs)
  - mobiler Code („Agenten“)
- Teil einer dynamischen, mobilen, „spontanen“ Internet-basierten Welt (Systeme um die Karte herum)

© Stefan Fünfrocken

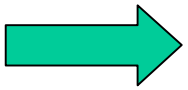
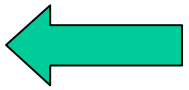
Die Zukunft

- SmartCards bei jedem Benutzer (Microsoft?)
- Mit Netzanschluß (überall, spontan, dynamisch)
  - CORBA: Kommunikation
  - Jini, Bluetooth
    „instant networking & communication“
- Vertrauenswürdige Hardware
  - „Tamperproof“, Daten in Benutzerhand
- Offene Plattform & beliebige Applikationen

© Stefan Fünfrocken

Zusammenfassung

- Trend: Multifunktionale SmartCards
- Karte als Kleinst-Computer
- Evaluation durch Prototyp-Anwendungen
- Betriebssystemerweiterungen nötig
- Keine Peer-to-Peer Funktionalität
- Noch geringer Speicherplatz

 Technik mit Zukunft 

© Stefan Fünfrocken

Kontakt

- Stefan Fünfrocken
  Technische Universität Darmstadt
  Alexanderstraße 6
  64283 Darmstadt
  fuenf@informatik.tu-darmstadt.de
  06151 16 5411
- Friedemann Mattern
- Marie-Luise Moschgath

© Stefan Fünfrocken

Copyright

Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that they have offered their works here electronically. It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit written permission of the copyright holder.

© Stefan Fünfrocken