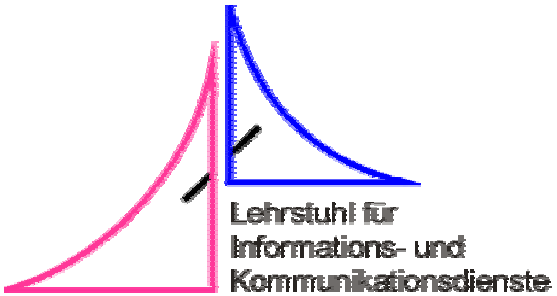
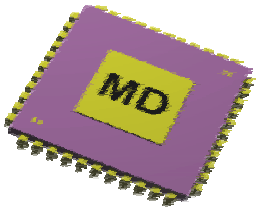
Hardware Security Concept for Spontaneous Network Integration of Mobile Devices

Prof. Clemens Cap
Dipl. Ing. Igor Sedov
Department of Computer Science
Chair for Information and Communication Services

Prof. Dirk Timmermann
Dipl. Ing. Marc Haase
Dep. Of Electrical Engineering and Information Technology
Institute of Applied Microelectronics and Computer Science



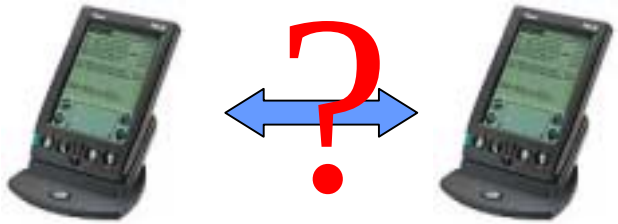


Outline

- Motivation
- Scenarios for mobile devices
- Requirements
- Architecture concept
- Realisation
- Conclusion

Motivation

- rapid growth of mobile devices
- **today's** applications:
  - personal information management



- **future** applications:
  - ad-hoc networking in ubiquitous environments over wireless networks

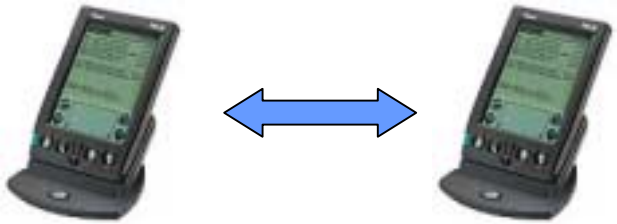
Scenarios for mobile devices

- receiving broadcast information's
  - news, cinema-program
- exchange personal cards
- storing personal information's
  - PIN, TAN, secret keys, credentials
- bank transactions
- signing contracts
- terminal for doctors in hospitals

Requirements

Wireless interface

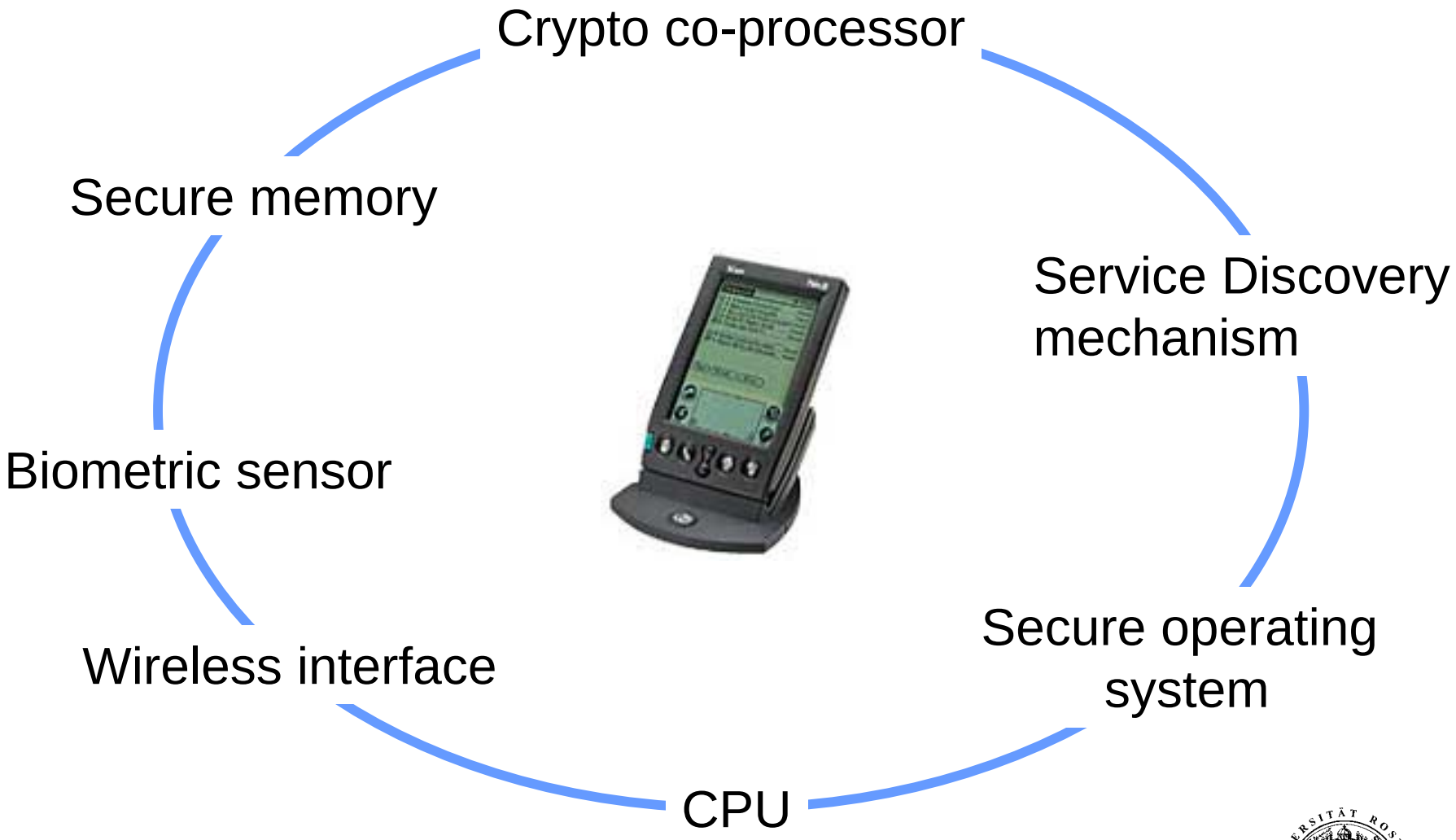
Service Discovery



Security

Power Management

Architecture Concept



Wireless Interface

technoloy	max. brutto datarate	range	connections	applications
IrDA	4 Mbit/s	1m	2	peer-to-peer between phones, notebooks, printer
DECT	128 kbit/s	50m	10	telephony support, data transmissions
Bluetooth	1 Mbit/s	10(100)m	8(+248 inactive)	universal ad-hoc-networking for mobile devices (data/voice)
HomeRF	2 Mbit/s	50m	>128	telephony support, data transmissions for home networking
IEEE 802.11b	11 Mbit/s	30-100m	ca. 10 pro Access Point	wireless LAN
HiperLAN2	54 Mbit/s	150m	ca. 10 pro Access Point	higher data transmissions

Security

Access Levels:

- Level 1:
  - non-secure
- Level 2:
  - only Authentication
- Level 3:
  - Authentication, Authorisation

Device Levels:

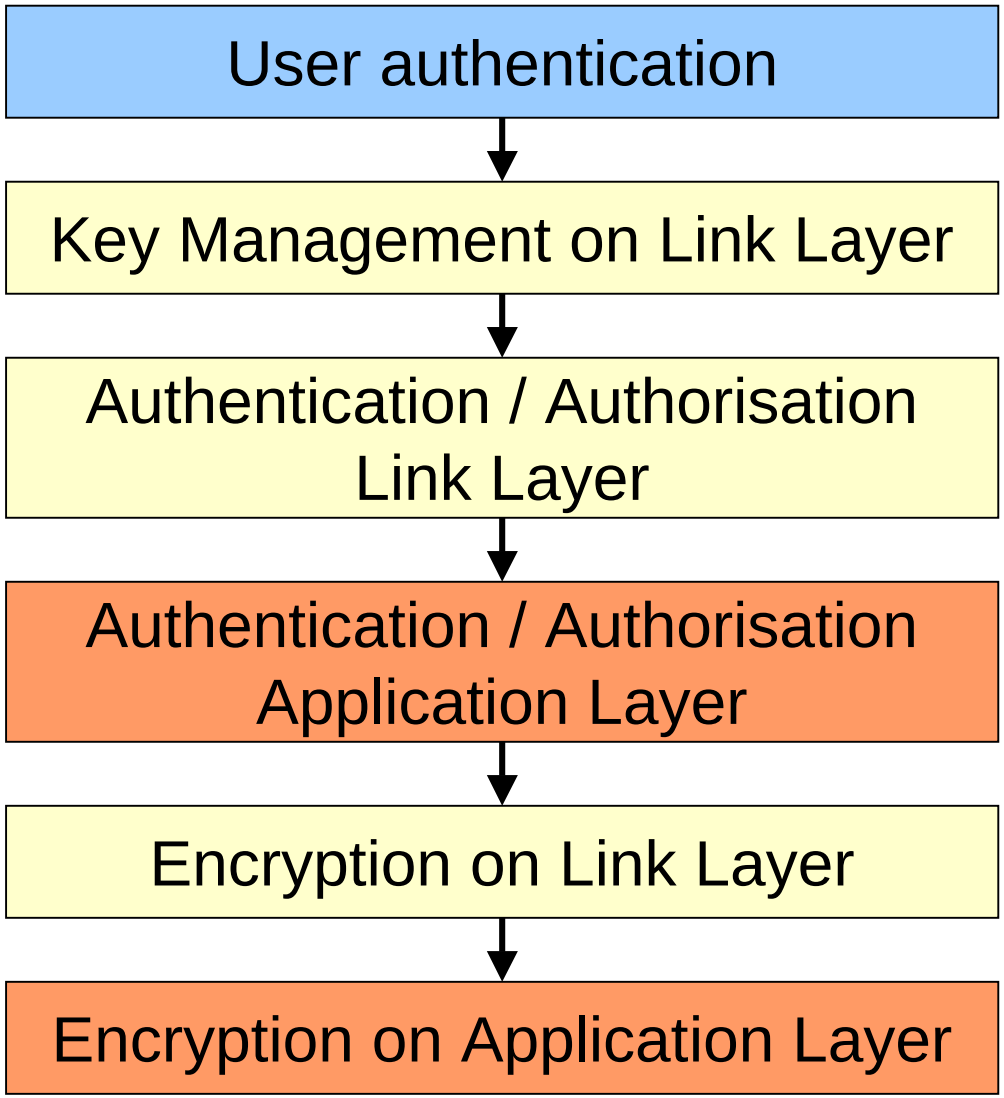
- Unknown Device
- Untrusted Device
- Trusted Device

Key Management

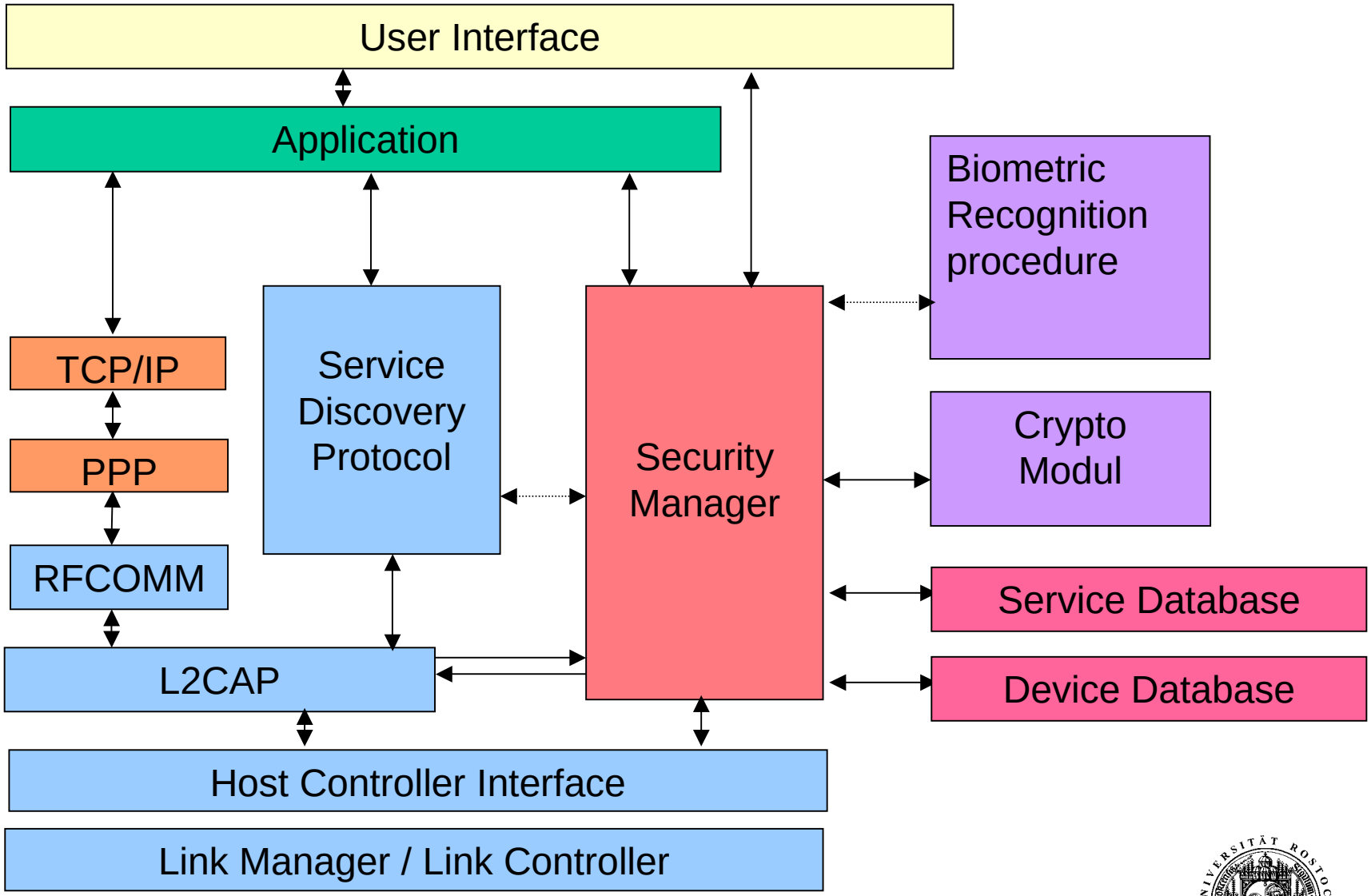
Encryption Management

Security Manager

Security Manager Architecture



Security Manager Architecture (2)



Biometric Recognition Methods

- Authorisation of transactions
- Authentication of users

- Fingerprint:
  - well usable
  - easy integration
  - matching on board
  - no abuse of biometric data

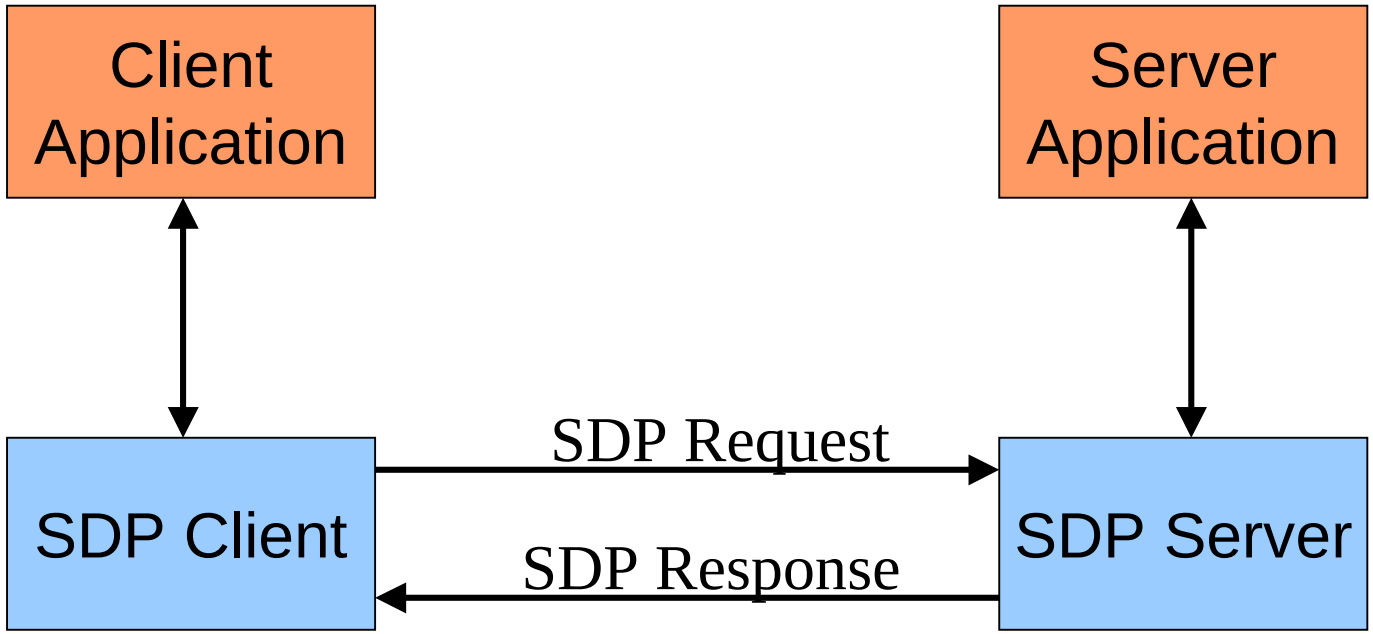
Crypto Co-processor

- **algorithms**: DES (Triple DES), RSA
- **example**: DES (RSA 100-1000 x slower)

type	clock	throughput	
typ. smartcard processor	4 MHz	3,7	KBit/s
AMD-K6	266 MHz	3,6	MByte/s
XILINX FPGA recurrent	4 MHz	1,9	MByte/s
XILINX FPGA pipelined	4 MHz	30,7	MByte/s

- **advantages** of crypto co-processors
  - performance enables appliance
  - scalable parallelism and pipeline (VHDL core)

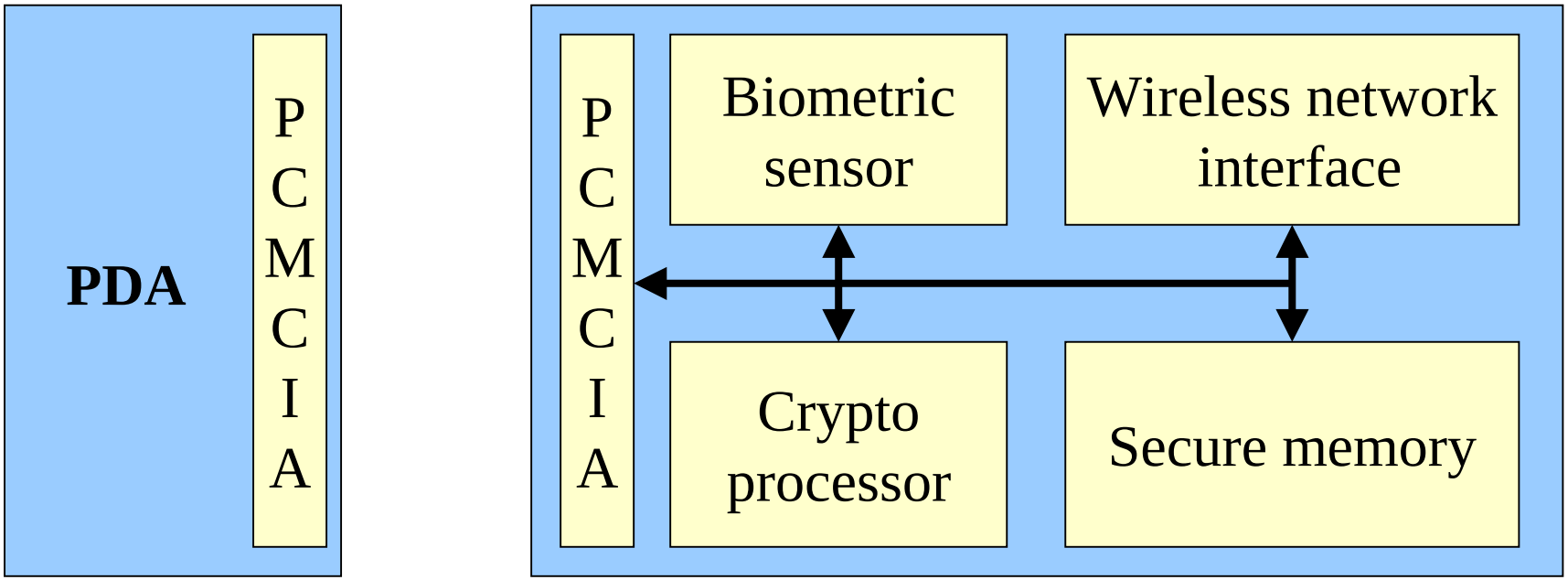
Service Discovery



Bluetooth - SDP

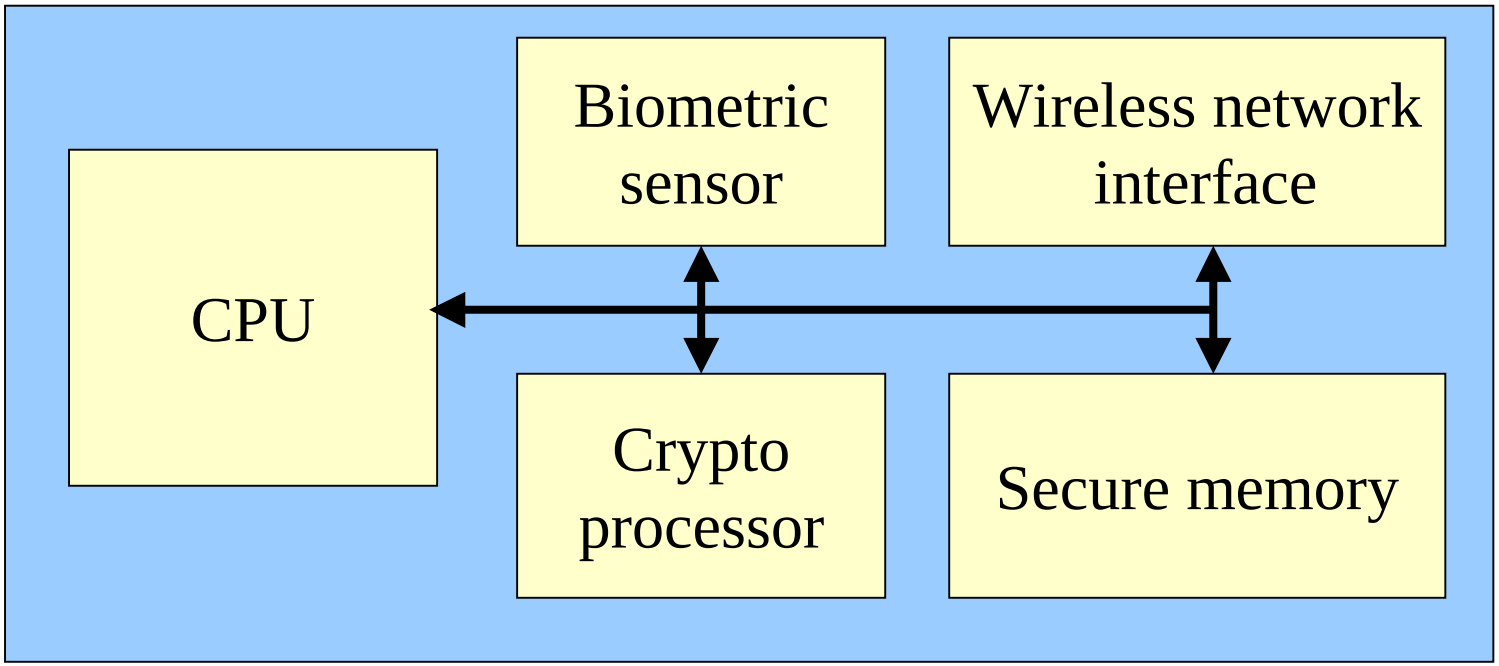
- only service information
- no access to services

Realisation – Add-on card



Expansion card for actual mobile devices

Realisation – Smart Badge



- active card
- optional: display & input device

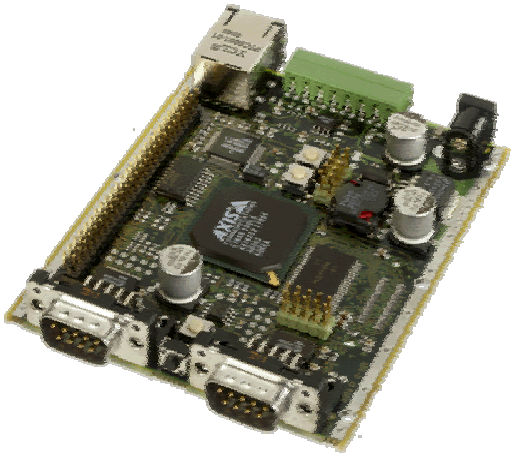
Development System

Hardware

- IPAQ H3650
  - 206 MHz S-ARM
  - 64MB RAM
  - 16MB Flash
- Axis Etrax 1000LX
  - 100MIPS 32bit RISC
  - 8MB RAM
  - 2MB Flash
- Sigma Bluetooth Controller
  - Spec. 1.0B
  - Ser/USB

Software

- Linux Kernel 2.4
- Bluetooth Stack **openBT**



Conclusion

spontaneous network integration of mobile devices

- enables:
  - variable communication possibilities
  - new service structures

- requires:
  - additional hardware components
  - security architecture to provide safe data transmissions
  - authorisation & authentication of services and devices