TOPAS – Trust Oriented Platforms for Advanced Security

Proj. Nr. 813437/12469

Kurt Dietrich
Kurt.Dietrich@iaik.tugraz.at

Institute for Applied Information Processing and Communications
Graz, University of Technology

TOPAS – Key Data

- Partners:
  - IAIK, Graz University of Technology
  - NXP Semiconductors Austria (formerly Philips)

  – Start: 2007 End: 2009
  – ~300.000 € Budget

- Research focus: Trusted Computing on Mobile Platforms

- Reuse of standard security components

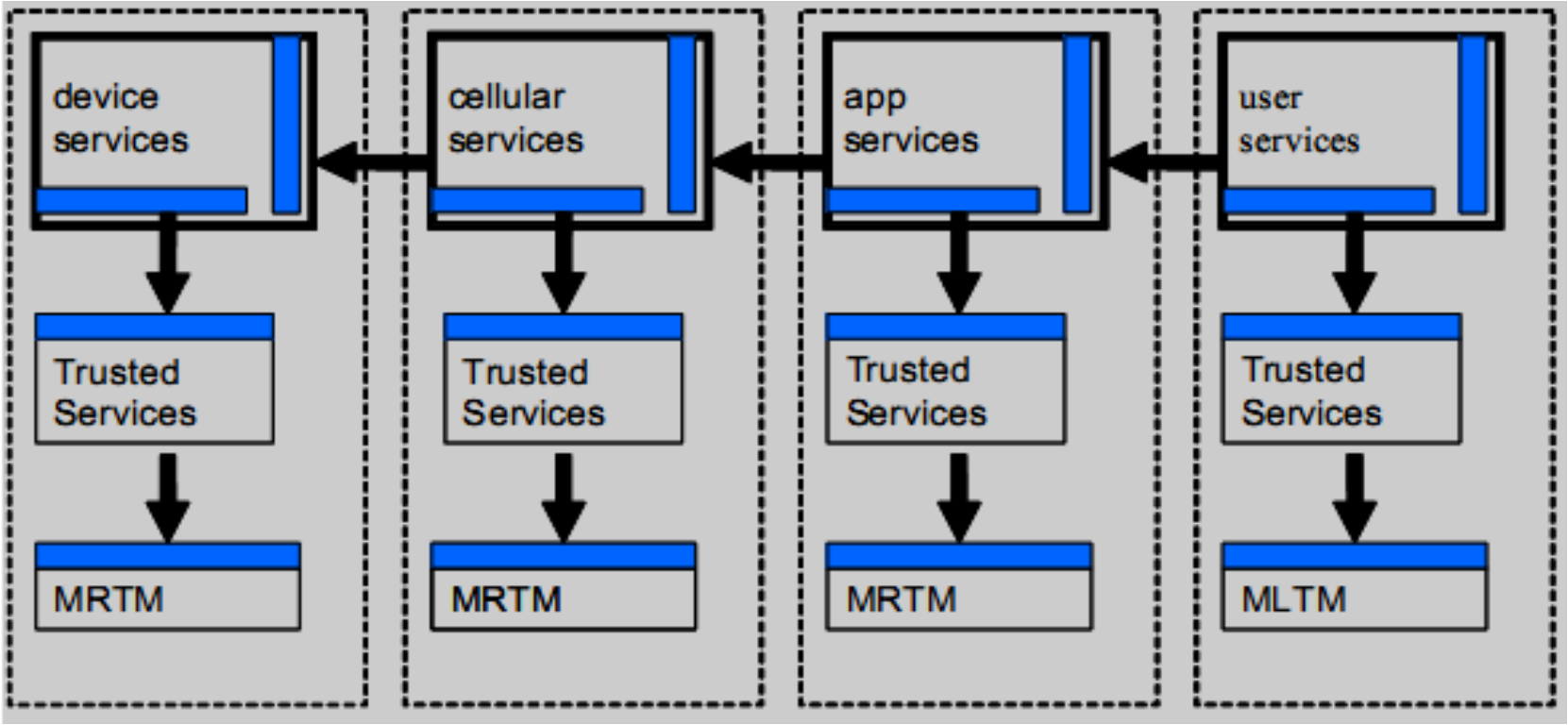
Why Mobile Trusted Computing?

- Use Cases:
  - Platform and application integrity
  - Attestation of software running on the device
  - Device authentication
  - Secure software download
  - Secure channel between device and UICC
  - User data protection and privacy
  - Mobile ticketing, mobile payment
  - SIMLock / Device Personalization

Mobile TPMs

- Core component: Mobile Trusted Modules (MTMs)
- New specification by TCG mobile phone working group (MPWG)
- Specification intentionally written in a „relaxed“ way
- MTM as a functionality rather than a HW-component
- May be implemented in software as a trusted service or as a dedicated hardware component

Interestgroups on a Mobile TC Platform

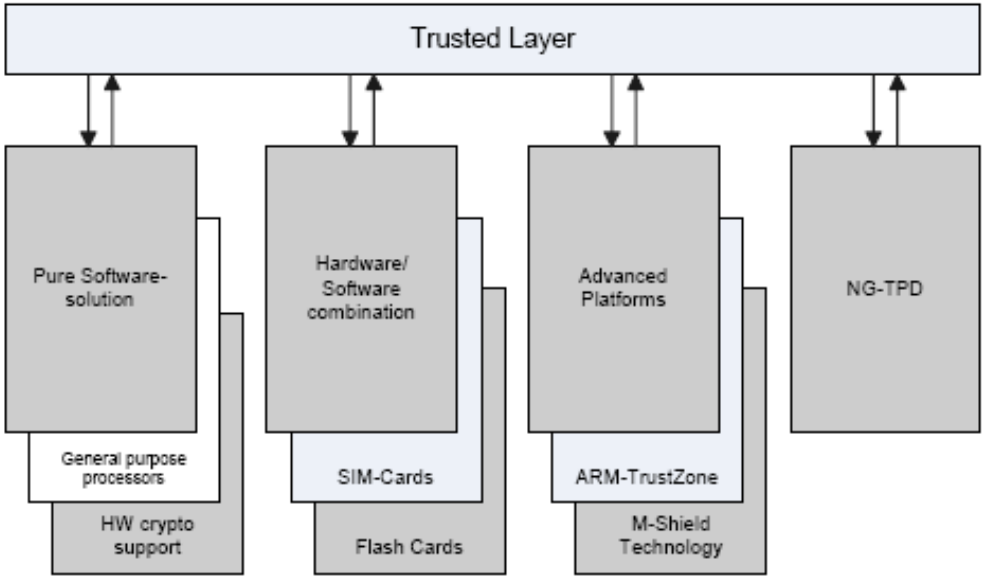


[TCG: mobile_spec_1.0]

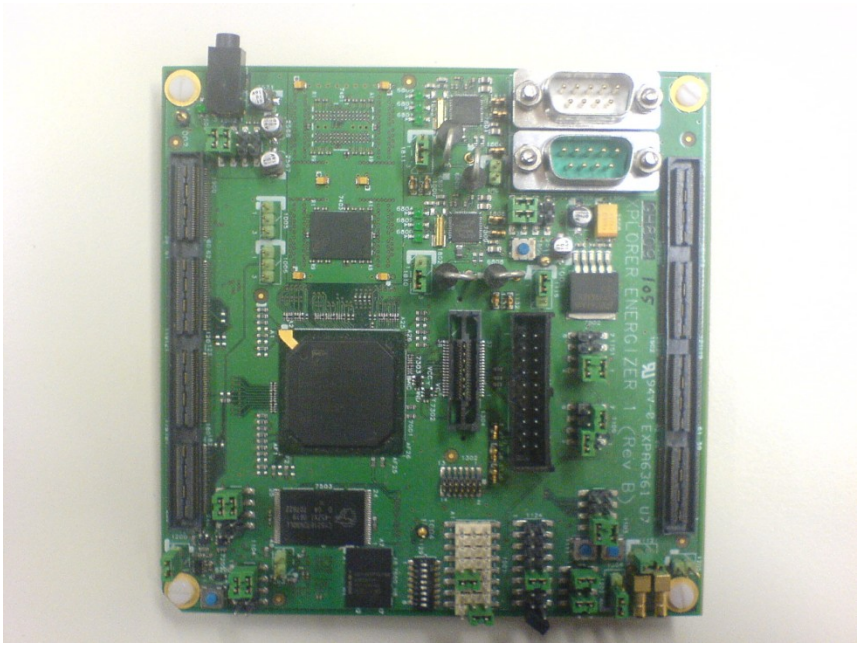
- Stakeholder: User, networkprovider, device manufacturer

TOPAS

- Look for alternative implementations of MTMs (mobile trusted module)
  - mainly in software
  - in combination with hardware (like JavaCard)
  - with some support of available hardware (like the processor)
- Close look at the ARM TrustZone & Secure Elements

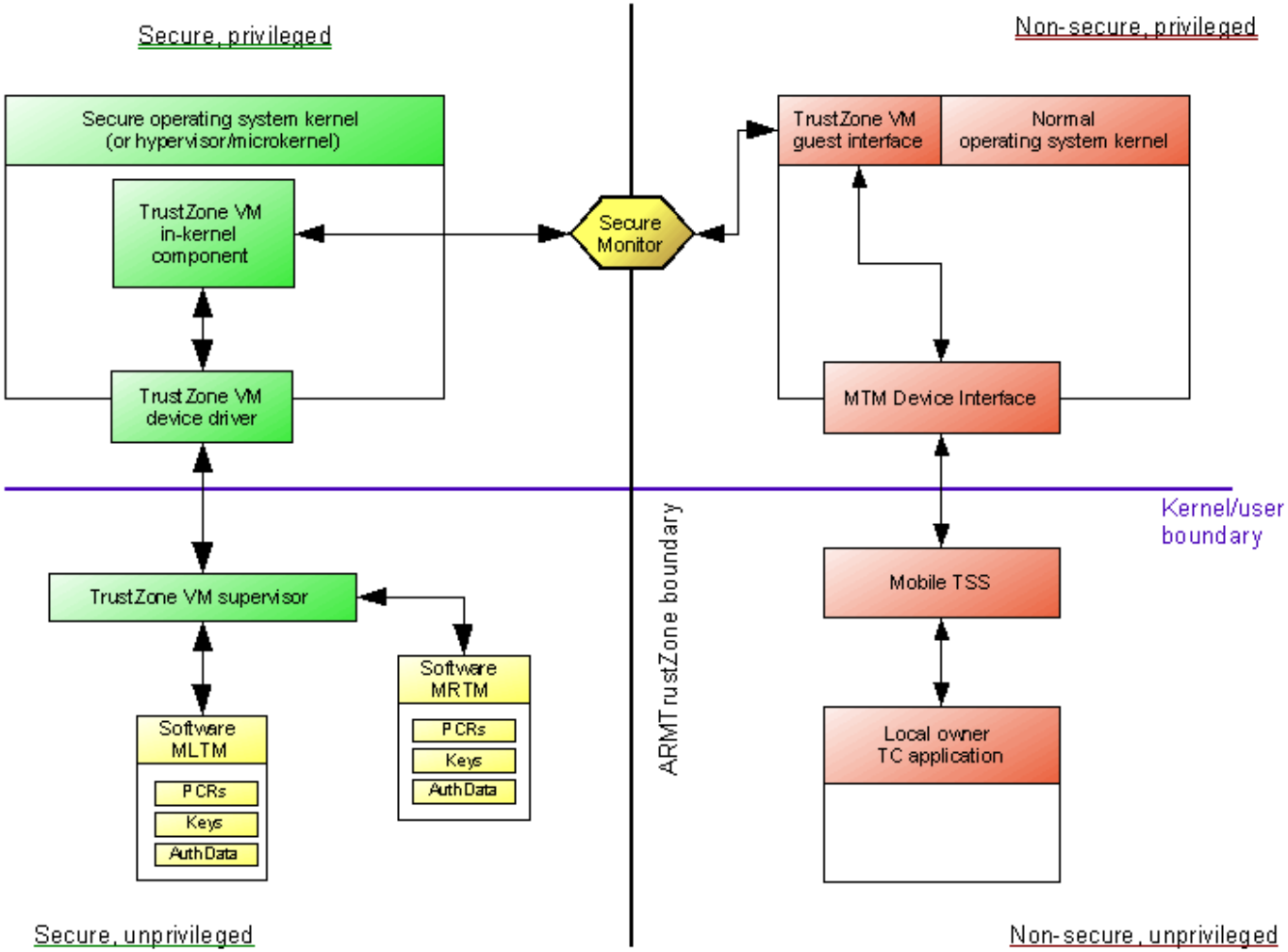


The prototype hardware platform

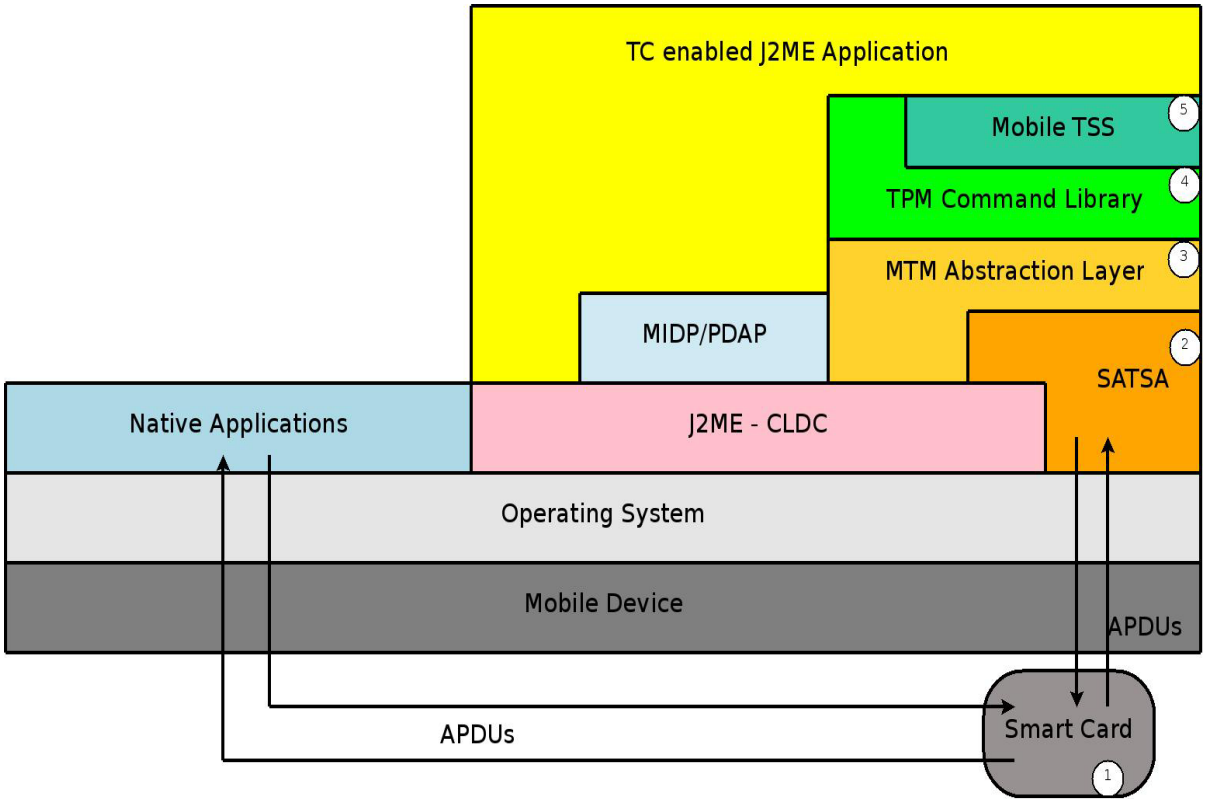


- ARM1176JZF-S core
  - ARMv6 with TrustZone
  - I- and D-TCMs, on-chip RAM
- Memory
  - 64MB Flash
  - 64MB DDR-RAM
  - 2MB SRAM
- I/O
  - 2x Serial ports
  - 2x I²C ports
- No crypto HW, etc.

Software platform based on TrustZone



JavaCard - MTM



1. JavaCard-MTM
2. Security and Trust Services API
3. MTM Abstraction-layer
4. J2ME TCG compatible Command Library
5. Mobile Trusted Software Stack

Reference Implementation: MTM

- Mobile-Trusted-Module
  - Secure Element
    - built-in Smart Card
  - MTM is a JavaCard applet
  - JavaCard with JCOP or SmartC@fe form G & D
    - ~72 kb flash memory
  - Target device: Nokia 6131 NFC
  - Conforming to MTM spec.
    - Features of MLTM & MRTM

Results

- Proposals under review by TCG
- Dissemination:
  - Lectures (TRUST2008, IAIK)
  - Organised research workshops at Univ. of Oxford and Ruhr Univ. Bochum (together with NOKIA)
  - Research Papers (published by: IEEE, LNCS and ACM)
    - Secure Boot Revisited (Dietrich, Winter)
    - A Secure and Reliable Platform Configuration Change Reporting Mechanism for Trusted Computing Enhanced Secure Channels (Dietrich)
    - An integrated architecture for trusted computing for java enabled embedded devices (Dietrich)
    - Trusted computing building blocks for embedded linux-based ARM TrustZone platforms (Winter)
    - Implementation Aspects of Mobile and Embedded Trusted Computing (Dietrich, Winter)

Thank You for Your Attention!