

RSACONFERENCE2009

Security for Mobility – Think Bigger!

Ammar Alkassar
Sirrix AG

Axel Stett
certgate GmbH

04/22/09 | Session ID: SPO-201



IT-Security Made in Germany

certgate, NCP, T-Systems

SiMKo 2

Secure Mobile
Handheld

BSI, Sirrix AG, secript, ifis

Mo-Trust TCG

Mobile Signatures with
Platform Integrity Proof

Atsec, BSI, Sirrix AG

HASK PP

Protection Profile for
High-Assurance
Security Kernel

Infineon, Sirrix AG

TECOM

Embedded Trusted
Computing: First MTM -
Reference



Sirrix AG
security technologies

IT-Security Made in Germany

secunet

SINA Mobile Disk

Secure and mobile persistent storage for higher security requirements.



Kobil

mIdentity

Mobile Identity Token, to access corporate data from everywhere



Rohde&Schwarz SIT

TopSec Mobile

Mobile voice encryption via Bluetooth connection for almost every mobile phone



Sirrix AG
security technologies

IT-Security Made in Germany



CORISECIO

Mobile PKI

Fully automatic mobile
PKI with RIM
Blackberry support.

cv cryptovision

Crossplatform PKI

Management of Digital
Signatures on
Windows, Linux and
Mobile systems.

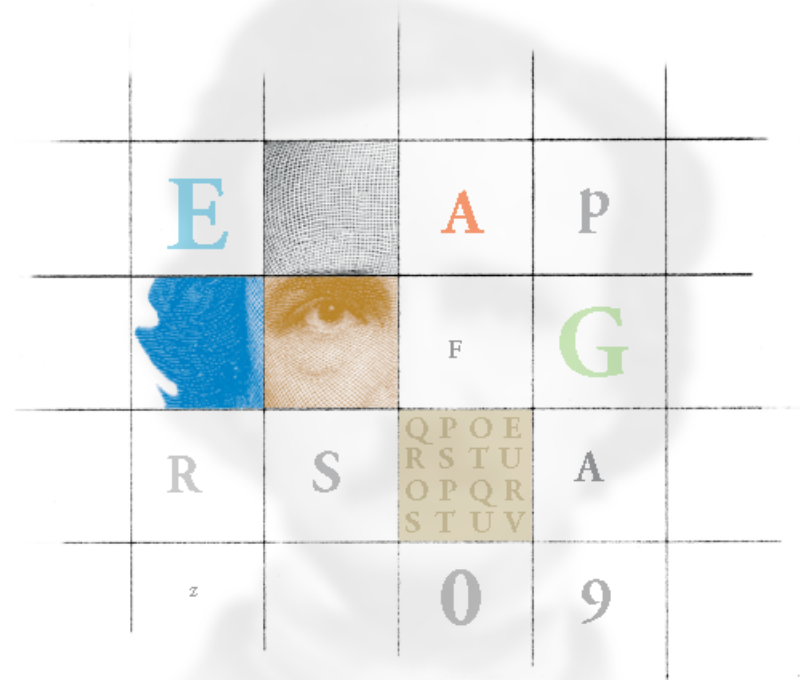
RSACONFERENCE2009

High-Assurance and Mobility

Ammar Alkassar

Sirrix AG

04/22/09 | Session ID: SPO-201



Sirrix AG
security technologies

asec
the information security provider

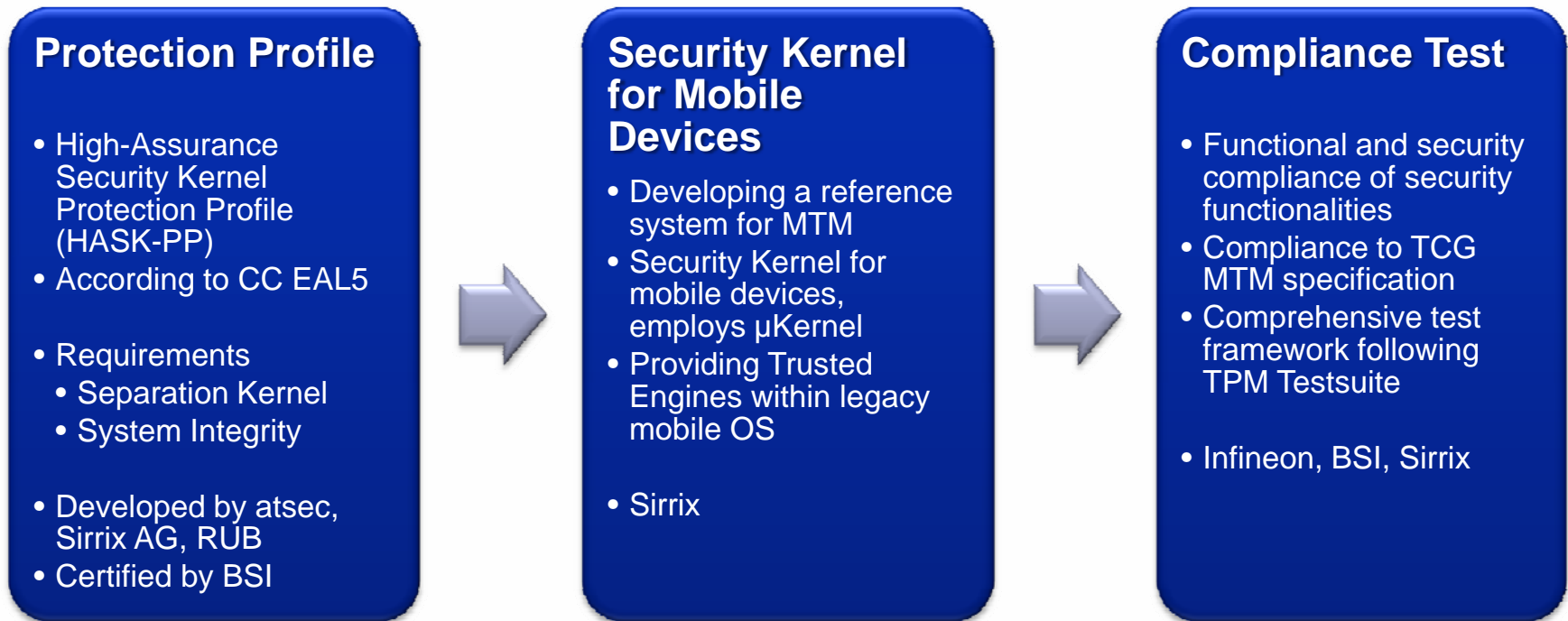
infineon

Collaborative Development „Made in Germany“

- Goal
 - Defining security requirements for next generation secure mobile devices formally.
 - Designing and developing a reference platform
 - Providing a standardized test framework for proving compliance with given standards.
- Collaborative Approach
 - Utilizing leading German synergies in security engineering



Use Case: Development Process



High-Assurance and Mobility

- Why is it an issue?
 - Mobile access to sensitive corporate and data is not a fancy feature any more – but a crucial requirement, for both enterprise and governmental environments.
 - Assurance of mobile devices is still far behind to be adequate
- Which scenarios are considered?
 - Employee uses mobile device to access all personal and corporate data, including email, calendar and files
 - Parts of the data is accessed online, parts are stored inside the mobile device
 - Mobile device is used as main communication utility

High-Assurance and Mobility

- What are the threats?

Infection by malicious software

- Viruses and bots, capturing devices
- Trojan Horses, for spying purposes (stored data, communication data and environmental data)

Lost of mobile device with sensitive data

- Sensitive data as stored addresses, mails and notices
- Content of device caches (mobile accessed data)
- Key material, e.g., VPN access keys



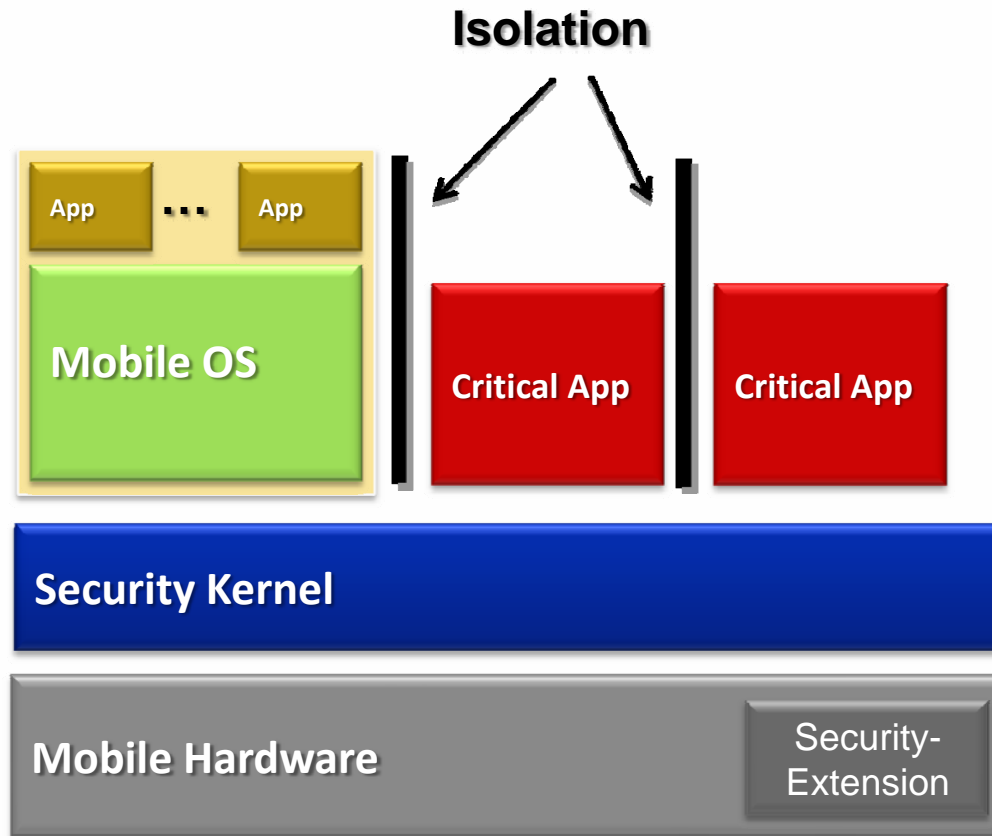
Internal attackers

- Leakage of corporate information by device users

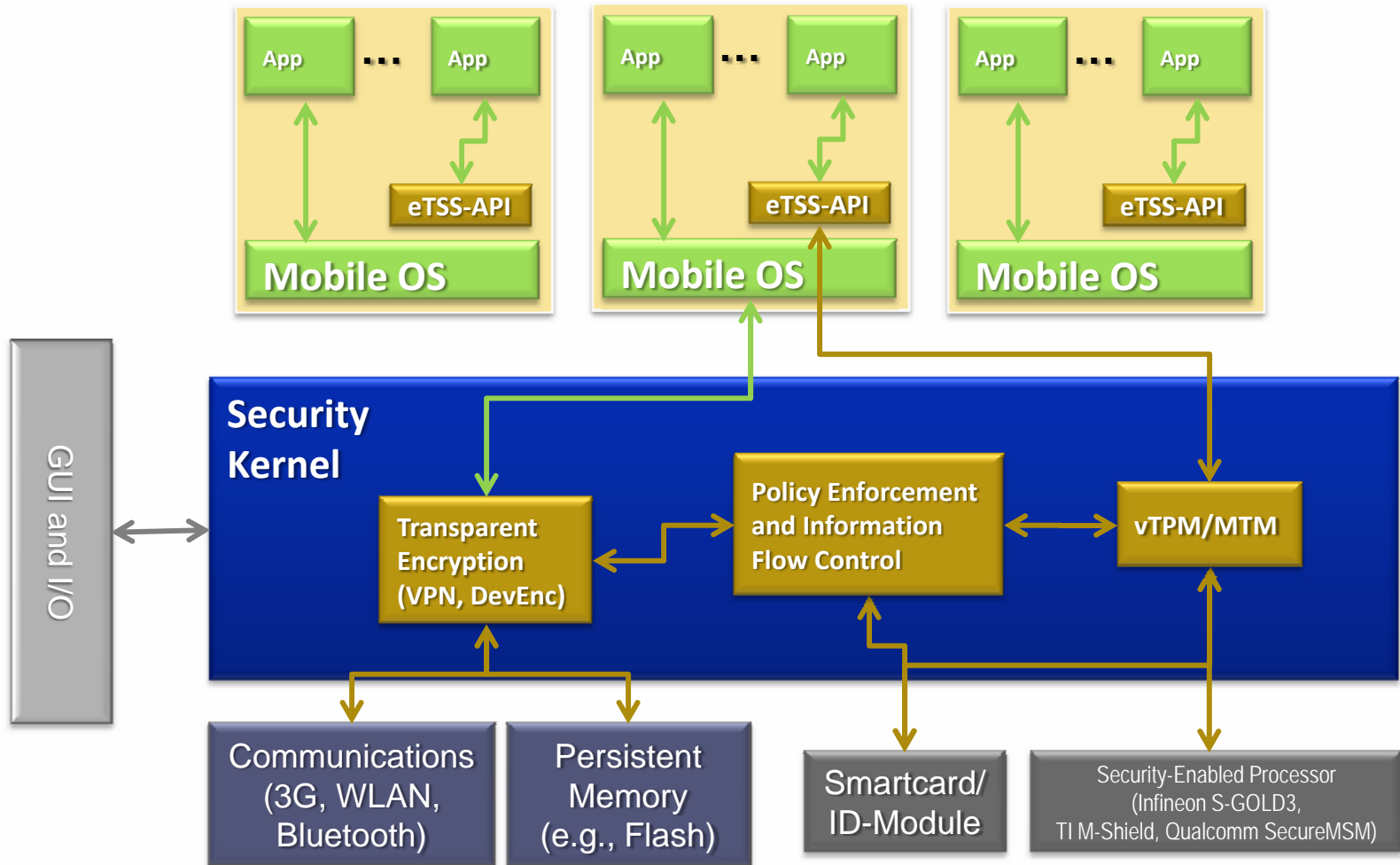
Shortcomings and Requirements

- Shortcomings of current solutions
 - No adequate process isolation and memory protection in current commercial mobile operating systems
 - Access control model – if any security is provided at all
 - User has unrestricted access to mobile device
- Technical and Security Requirements
 - Strong isolation at Kernel level
 - Information Flow Control, ensuring
 - Lifecycle protection of information
 - Attestation and integrity protection of code and configuration

Security Kernel for Mobile Applications

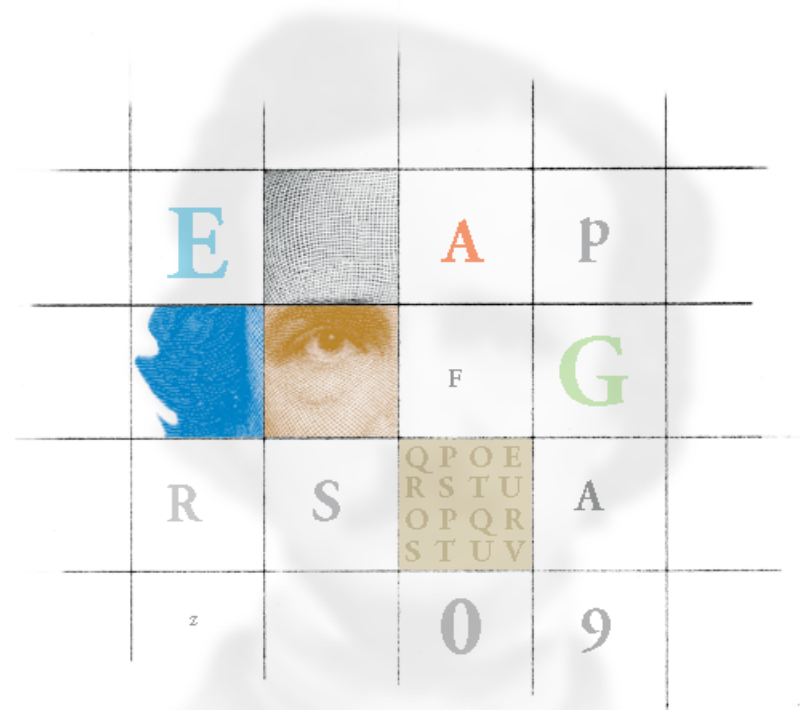


High-Assurance Security Kernel



RSA[®]CONFERENCE2009

Mobility by Trustworthy Pervasive Computing

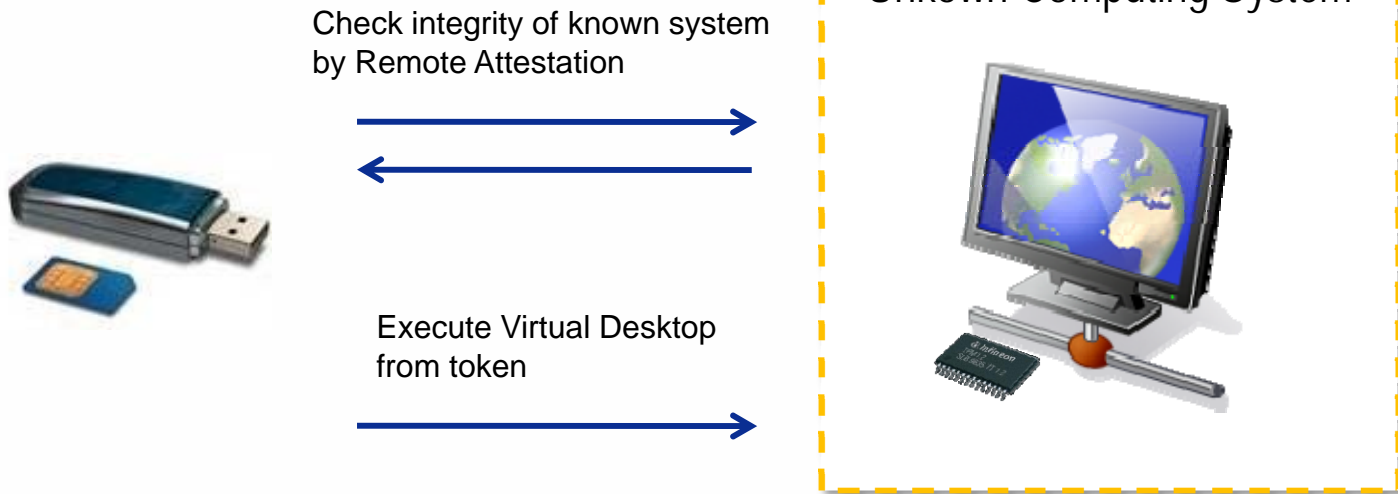


Mobility by Pervasive Computing

- In the last slides, we have seen Mobility in its classical meaning: Having a personal mobile device.
- But, what about having just a trustworthy system on token, using any computing system available?
- Solution can be: SmartToken + Virtualization + Remote Attestation



Personal Desktop in Any Environment



e.g., Kobil mIdentity



RSA[®]CONFERENCE 2009

SiMKo 2.0

by

T Systems

certgate
mobile security now!



NCP
SECURE COMMUNICATIONS

Axel Stett
certgate GmbH

SiMKo 2.0

- What is it good for
- Who contributed what
- How exactly does it work
- What comes next

SiMKo 2.0: General Environment



- Mobility increasing



- PDAs & smartphones fail to meet security requirements, are banned from security sensitive business processes



- Risk of data loss & data theft growing for mobile devices



- Higher compliance and lawmaking implications increase the pressure for data security



- Reputation and public image negatively impacted as a result of security loopholes and cases of fraud, theft or misuse



- Low level of user awareness to security requirements – negligence in password safety

SiMKo 2.0: Typical Threat Scenarios



SiMKo 2.0



Bundesamt
für Sicherheit in der
Informationstechnik

BSI Requirements:

- Secure smartphone for use in high security environments
- Security level must support handling of classified material
- Voice encryption not (yet) included
- PKI environments
- All interfaces other than GSM, EDGE and UMTS disabled, encrypted VPN mandatory for EDGE and UMTS
- Permanent/transparent user data encryption
- Pre-boot authentication and device control
- Incorruptible device self-lockup
- Smart card controlled PIN dialog, no PUK

SiMKo 2.0

Project Contributors:

- T-Systems

Sales and 1st / 2nd level support, adds smartphones (HTC Touch Pro, TC Touch HD, more coming), T-Mobile plan, backend server systems

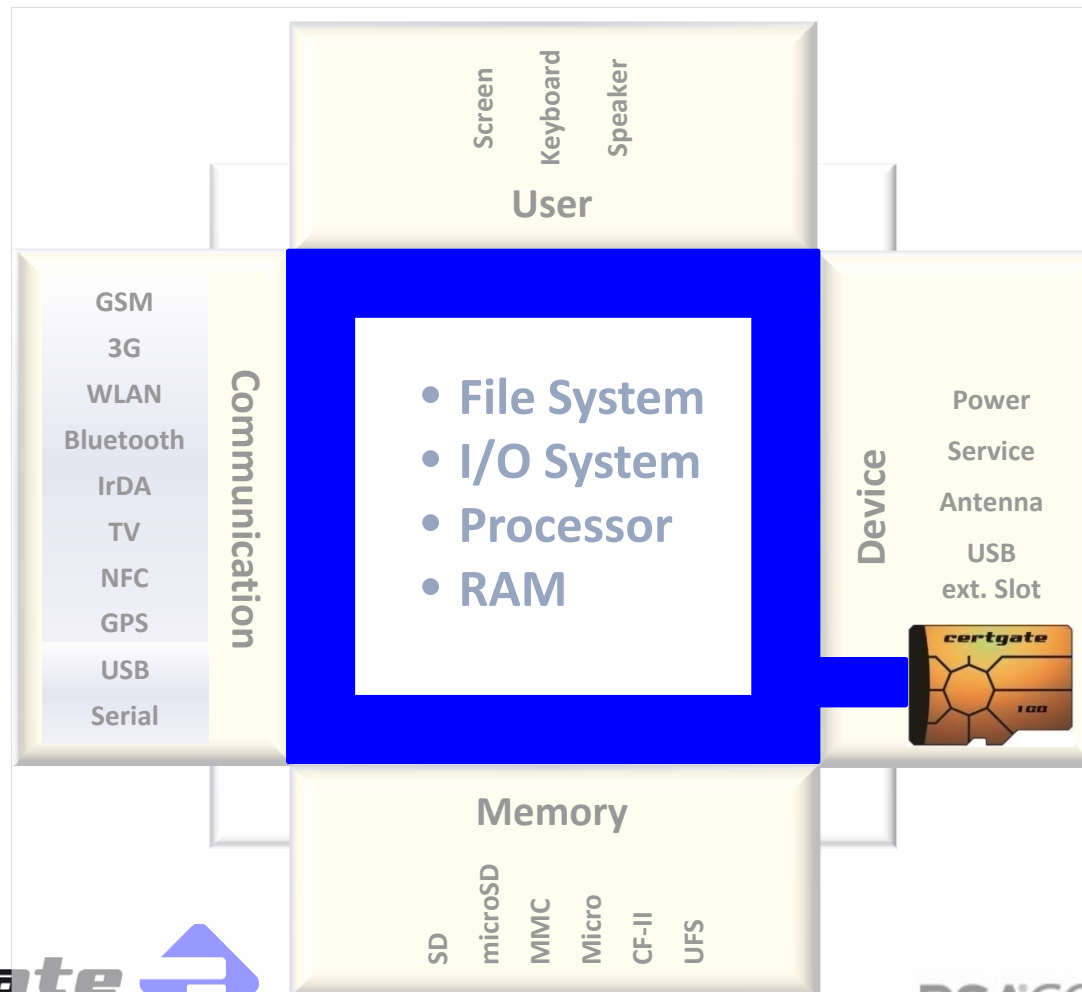
- certgate

smartcard equipped microSD to support all PKI operations, development of Windows Mobile kernel protection, implementation and BSI certification support

- NCP

SSL VPN client using certgate's PKCS#11 interface

SiMKo 2.0: Kernel Protection

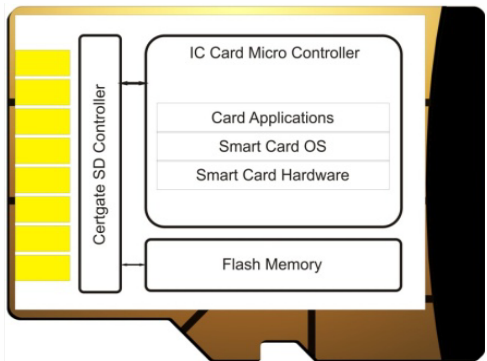


SiMKo 2.0: Standards

- Smart Card Logon, Single-Sign On, PIN and certificate management
- Device and microSD card encryption - RSA 2048 / AES 256 hybrid
- VPN Security Support
- MS Exchange Security Support –
S/MIME, ActiveSync/SSL with client authentication
- Certificate-based protection added for system and configuration files
- Security compromising functions irreversibly disabled



SiMKo 2.0: Standards



- First hardware security token in microSD™ form factor worldwide
- microSD™ standard flash memory card, 1 GB
- JavaCard™ 2.2, JavaCard™ 2.3, GlobalPlatform™ 2.1.1 conformity
- TCOS 3.0™ available
- On-card secure random number generator – FIPS PUB 140-2 and BSI AIS 31 compliant
- RSA 2048 bit on-card signature
- RSA 2048 bit on-card secure key generation
- Supports all relevant standards for smart cards and smart card readers - CSP, PKCS#11, PC/SC, etc.
- Works in most PCs, PDAs and smartphones

SiMKo Roadmap

- From SiMKo 2.0 – where are we going?
 - New smartphones
 - New OSs – Android, Open Symbian, iPhone once it comes with a microSD slot
 - New functions – Standardized Voice Encryption

Mobil Security - Think Bigger!

- Mobile devices come in various shapes and flavors...
- Mobil communication happens on notebooks, netbooks, PDAs, smartphones
- There is an industry ready to protect
- Check out our solutions and partner with us to create even more safety
- All users and businesses will certainly benefit greatly. Thank you.



Sirrix AG
security technologies

