Sicherheitsmechanismen für vertrauenswürdige mobile (Signatur-)Anwendungen

Utz Gnaida

Bundesamt für Sicherheit in der Informationstechnik

Workshop Betriebssystemsicherheit „IT-Sicherheit für unsere Gesellschaft“

UniBw München, 5. Dezember 2008

Vertrauen in der Praxis

Quelle: FAZ

Übersicht

- Motivation
- Grundlagen Trusted Computing
- Sicherheitsanforderungen
- Lösungsansatz
- MoTrust-TrustedSigner (PC, Notebook)
- MoTrust-TrustedSMS (Smartphone)
- Ausblick
- Zusammenfassung

Motivation (1)

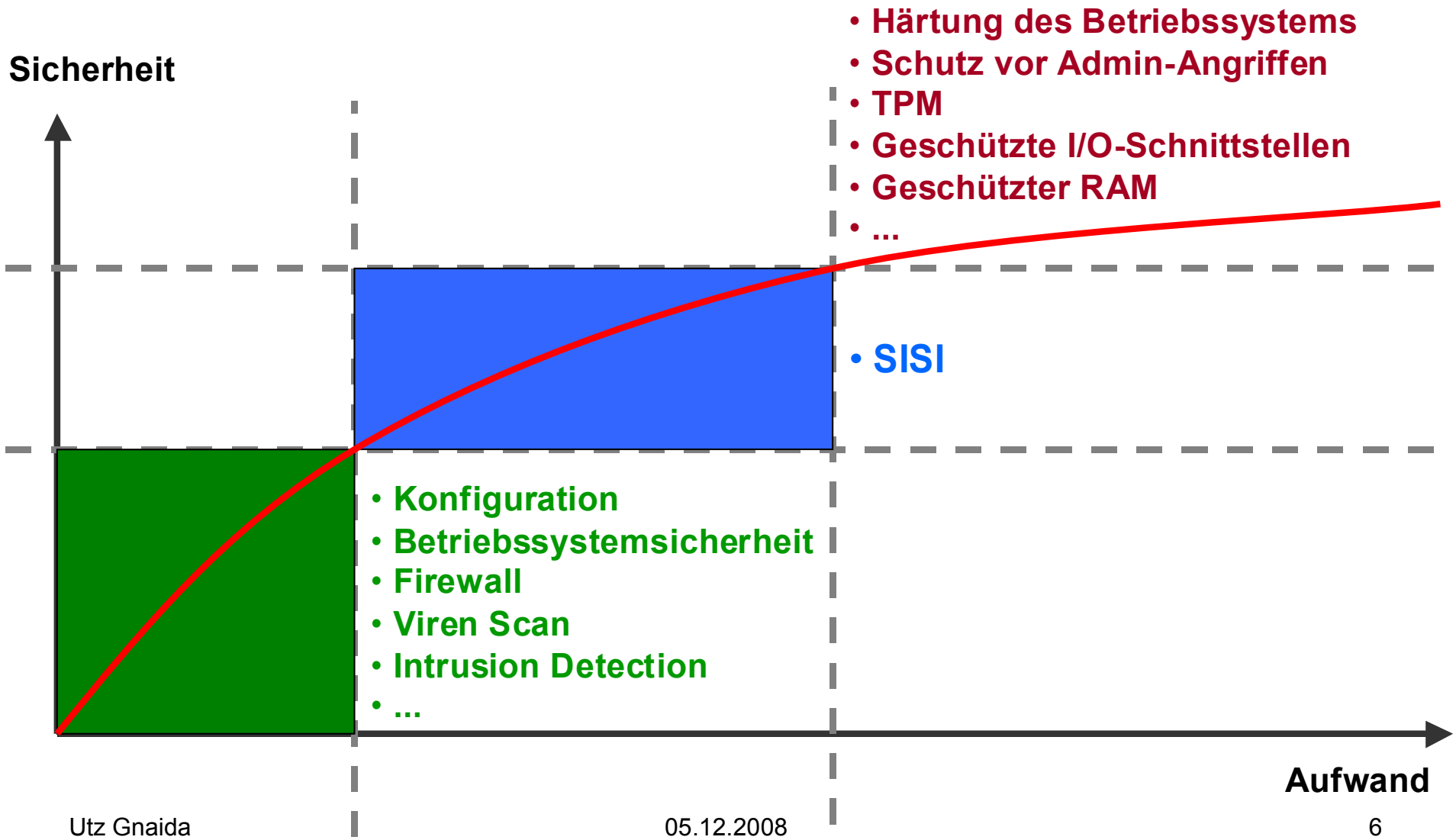
- Der Einsatz von (qualifizierten) elektronischen Signaturen wird in Zukunft stark ansteigen
  - eCard-Stategie der Bundesregierung,
  - elektronische Gesundheitskarte (eGK)
  - elektronischer Personalausweis (ePA)
- Eklatante Sicherheitsmängel verbreiteter Betriebssysteme
  - Manipulation des Betriebssystems möglich
  - Manipulation der Signaturanwendung möglich
  - Manipulation der Dokumentenausgabe möglich
  - Vertraulichkeit der Benutzereingabe (z.B. PIN) fraglich

Motivation (2)

Untersuchungsergebnis ☑ Applikation resistent ☒ Penetration erfolgreich ☐ Penetration möglich	Smartcard-Kommunik.: Datei-Austausch	Benutzer-oberfläche: Auslesen von Elementen	Benutzer-oberfläche: Manipulation	Applikations-komponente: Modifikation	Eingabe-schnittstelle: Mitschnitt der Eingaben
[redacted]	☒	☒	☑	☑	☒
	☐	☒	☒	☑	☒
	☐	☑	☑	☑	☒
	☐	☑	☑	☑	☒
	☐		☑	☒	
	☒	☑	☒	☒	☒
	☒	☒	☑	☑	☒
	☒		☒	☒	☒
	☐		☒	☒	
	☒	☑	☑	☒	☒
	☒	☒	☒	(☒)	☒

Quelle: BSI-interne Studie SISI

Motivation (3)

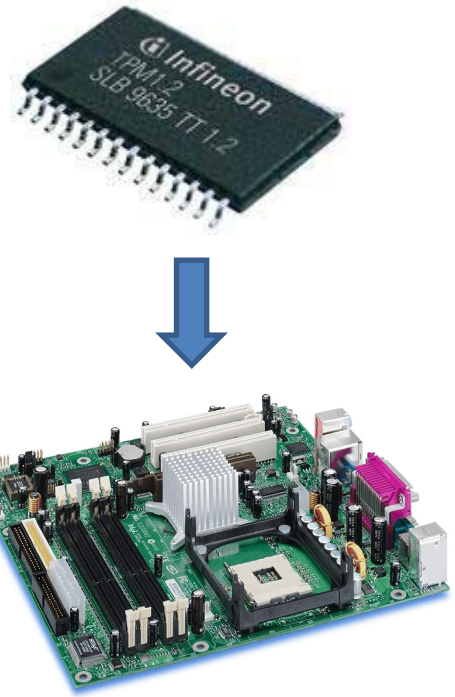


Motivation (4)

- **MoTrust**: Verbesserung der Sicherheitseigenschaften mittels Standard Hard- und Softwarekomponenten
  - **Turaya**: Sicherheitsarchitektur zur Isolation der Signatur- und Verifizierungsanwendung
  - **TPM**: Trusted Computing Technologie ermöglicht dem Verifizierer die Überprüfung der Signaturumgebung
- Erhöhung der Akzeptanz von elektronischen Signaturen
- Beispielanwendungen
  - **MoTrust-TrustedSigner**:
    Vertrauenswürdige Signatur- und Verifizierumgebung
    mit Plattformzertifikat
  - **MoTrust-TrustedSMS**:
    Vertrauenswürdige SMS-Erstellung/Signatur
    auf einer Smartphone-Plattform

Grundlagen Trusted Computing

- Trusted Computing Technologie bietet benötigte Sicherheitsfunktionen
  - Trusted Boot:
    „Messen“ der Plattformkonfiguration beim Bootvorgang
  - Sealing:
    Binden von Daten an Plattformkonfigurationen
  - Remote Attestation:
    Attestierung der Plattformkonfiguration mittels digitaler Signatur
  - Random:
    Kryptografisch sichere Zufallszahlen



TCG - Trusted Computing Group

- Konsortium von mehr als 100 Unternehmen
  - AMD, BSI, HP, IBM, Microsoft, Sun, ...
- Schwerpunkt ist die Entwicklung von Trusted Computing-Lösungen für verschiedene Plattformen
- Veröffentlichte Spezifikationen (Auszug)
  - Trusted Platform Module (TPM)
  - Mobile Trusted Module (MTM)
  - Trusted Software Stack (TSS)
  - Trusted Network Connect (TNC)
- TPMs werden seit mehreren Jahren verbaut, aber kaum genutzt

Sicherheitsanforderungen

(1) Isolation des Signaturschlüssels
- Vertrauenswürdigkeit von Schlüsseldaten und Code

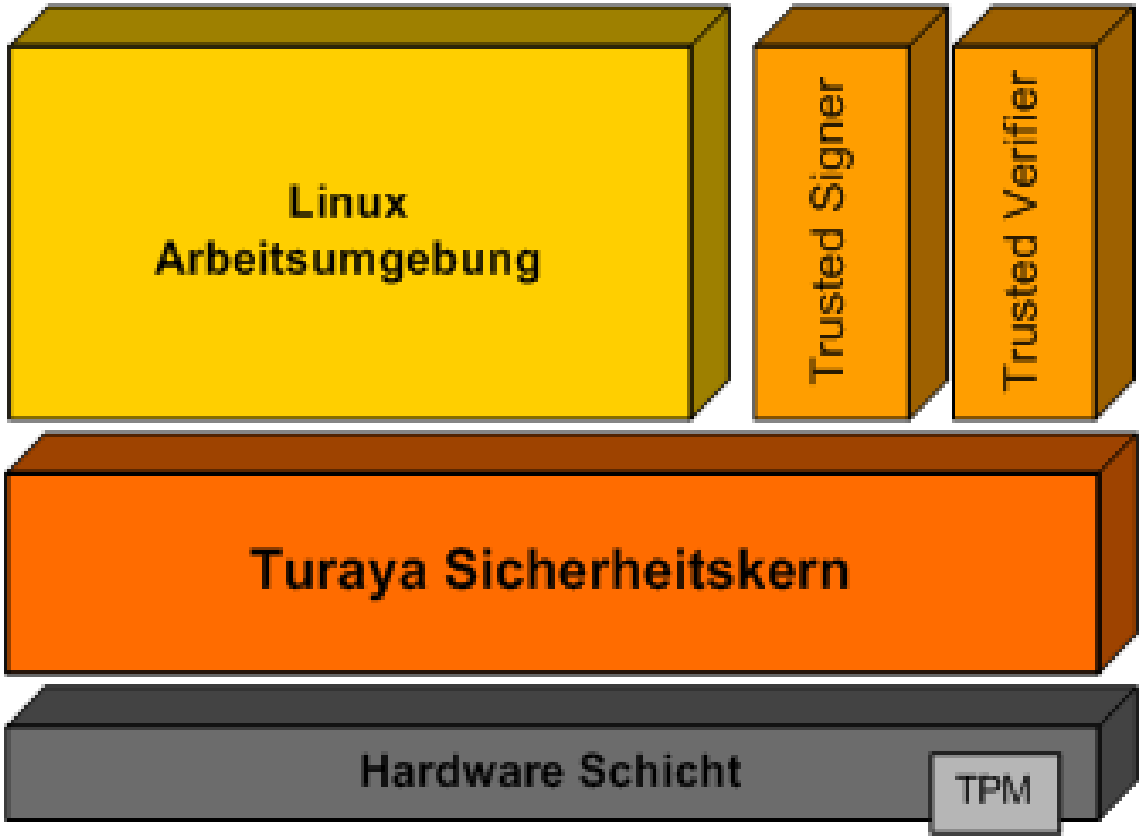
(2) Vertrauenswürdigkeit der Benutzereingabe
- Smartcard-PIN, Passwort, etc.

(3) Integrität der Systemausgabe (Trusted Viewer)
- What You See Is What You Sign (WYSIWYS)

(4) Isolation der Signaturanwendung
- Zur Laufzeit und im Offline-Zustand

(5) Authentifikation der Signaturanwendung
- Überprüfbarkeit der Signaturumgebung

Lösungsansatz (1)



Anwendungen

- Standard-Arbeitsumgebung
- Signaturanwendung
- Verifikationsanwendung

Sicherheitskern

- Isolation
- Prozesskommunikation
- Secure GUI

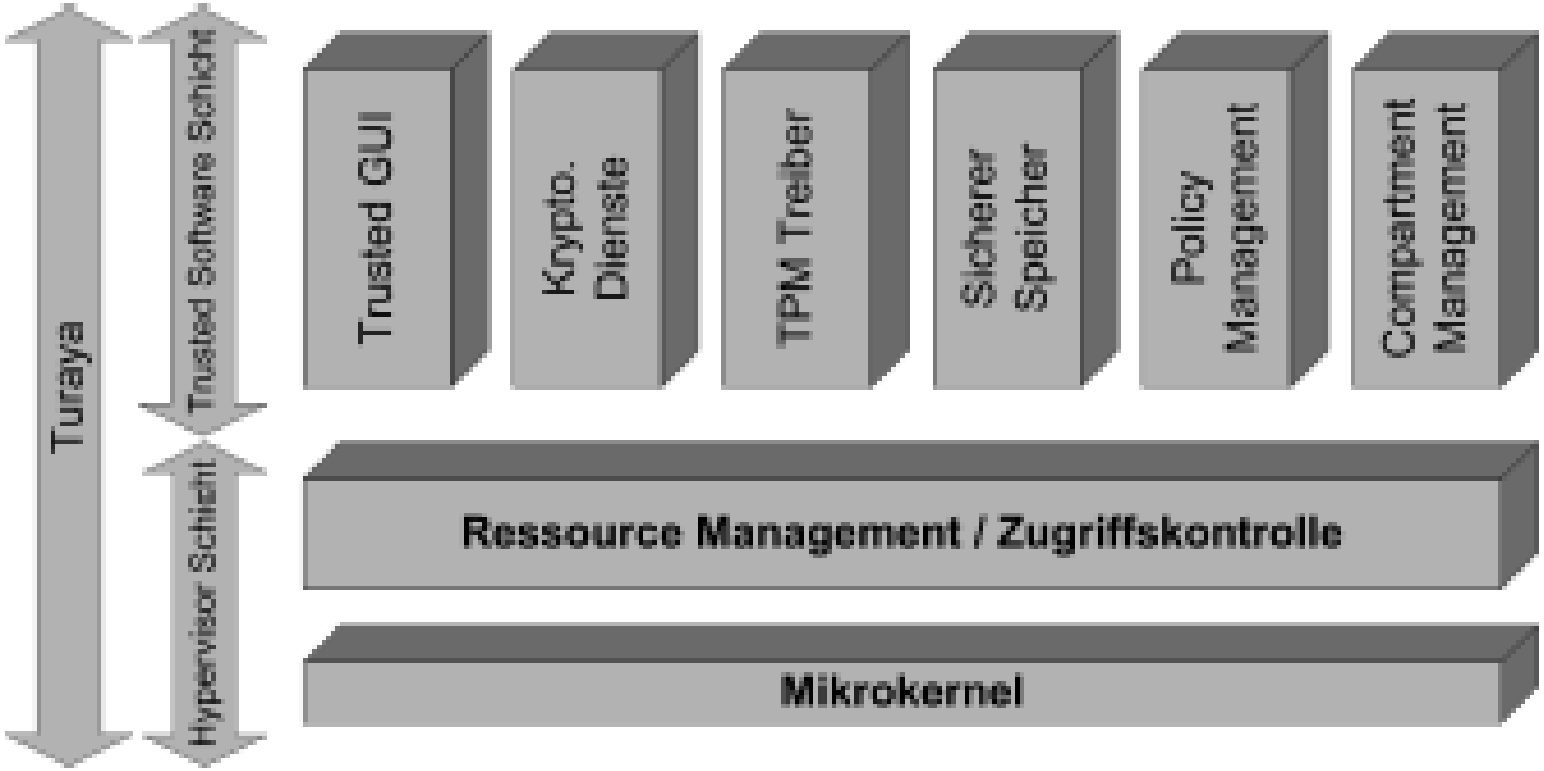
Hardware

- Standard-Hardware
- Trusted Computing Technologie

Lösungsansatz (2)

- **Turaya-Sicherheitskern**
  - Open-Source-Lösung mit langjähriger Historie
  - Bietet eine vertrauenswürdige Signaturumgebung
  - Isolation von normaler Arbeitsumgebung und Signer/Verifier
- **Trusted Computing-Technologie**
  - Vertrauenswürdigkeit sensitiver Daten im Offline-Zustand durch Sealing
  - Nachweis der Konfiguration der Signaturumgebung mittels Attestierung (Plattformzertifikat)

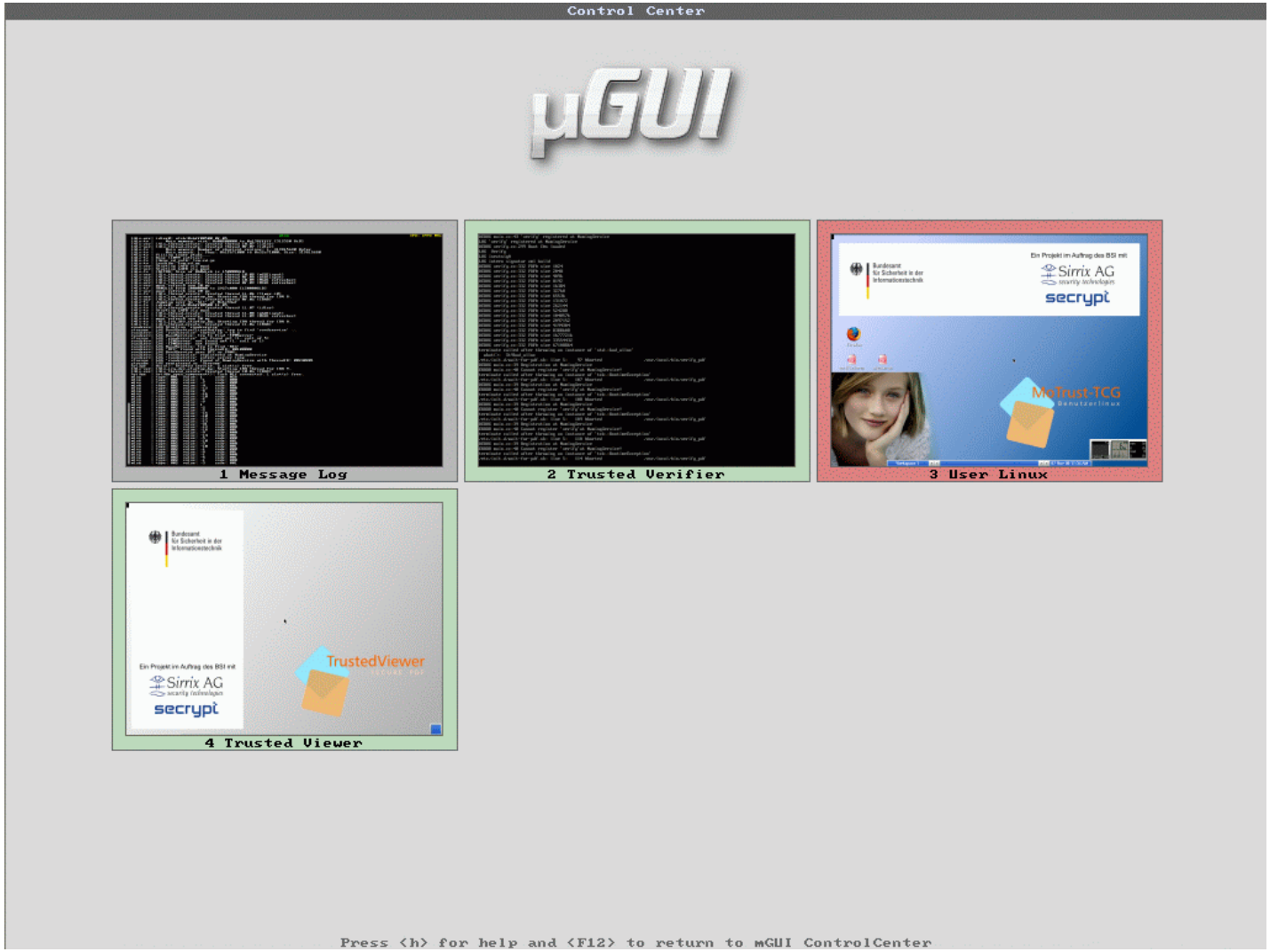
Turaya Sicherheitskern



MoTrust-TrustedSigner (1)

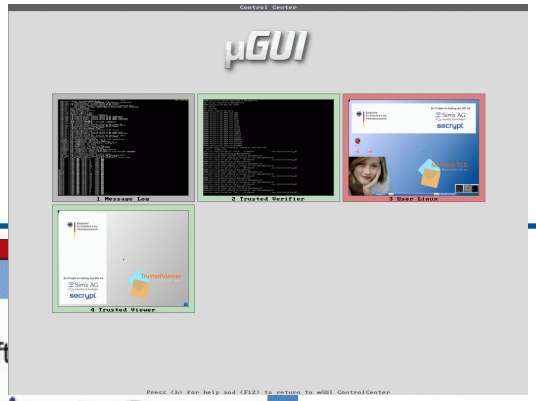
- Zielplattform
  - Entwickelt für mobile PC-Architekturen, z.B. Notebooks
  - Basierend auf Turaya/L4 und einem TPM
    - L4/Fiasco: an der TU-Dresden entwickelter Mikrokern
- Status
  - Bootet von R/O-Partition eines USB-Memory Sticks
  - Signaturerstellung/-verifikation
    - Smartcard (Ziel: Teil des USB Sticks)
    - Mit und ohne Plattformzertifikat
  - Registry-Server
    - Trusted Third Party zur Verwaltung von Plattformzertifikaten
  - Geplante Fertigstellung: Q1/2009

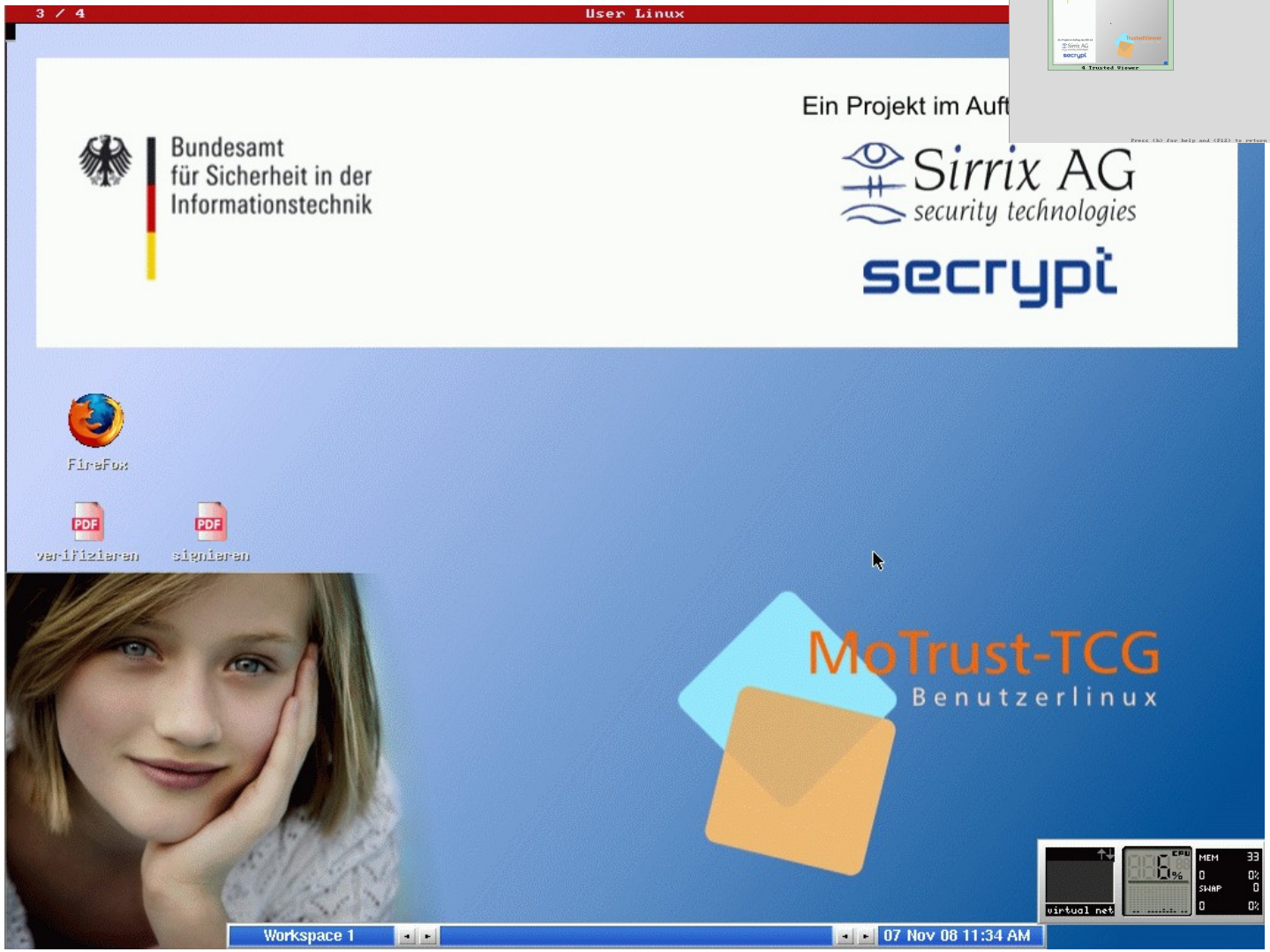
MoTrust-TrustedSigner (1)



TrustedGUI nach dem Booten von MoTrust-TrustedSigner (hier mit Debugging-Konsolen)

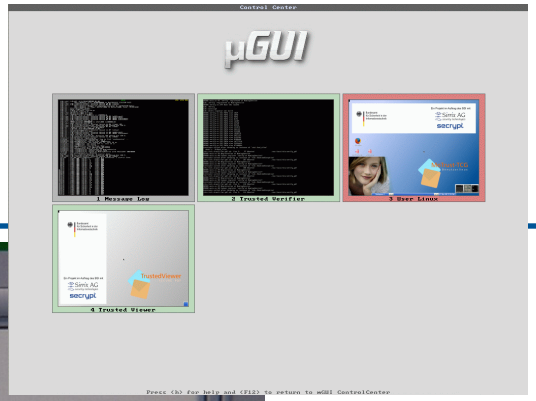
MoTrust-TrustedSigner (2)

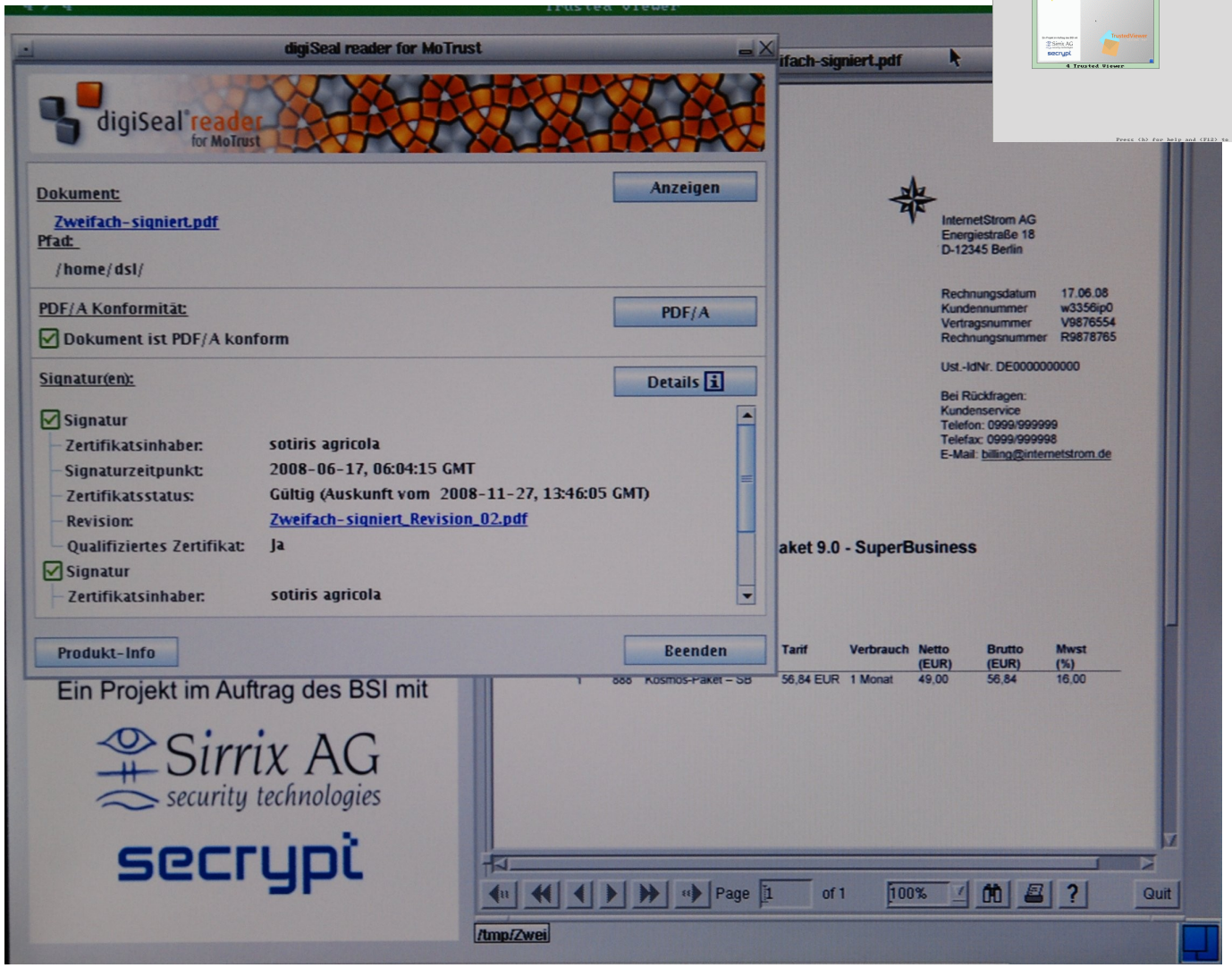




Vollständige Ansicht der normalen Arbeitsumgebung

MoTrust-TrustedSigner (3)

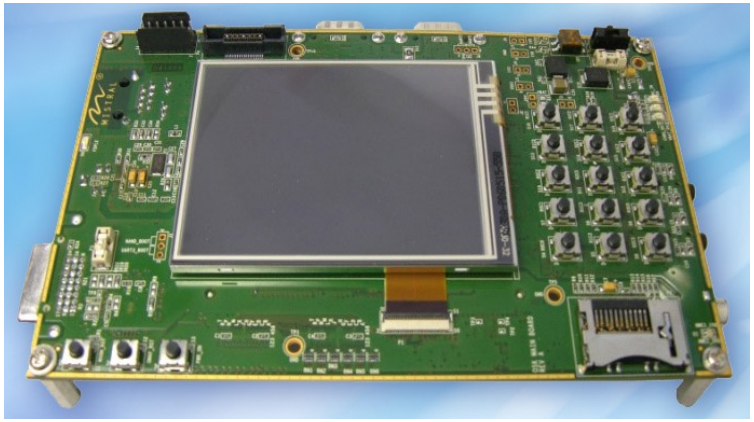




Wechsel in den TrustedViewer, um eine erstellte Signatur zu überprüfen

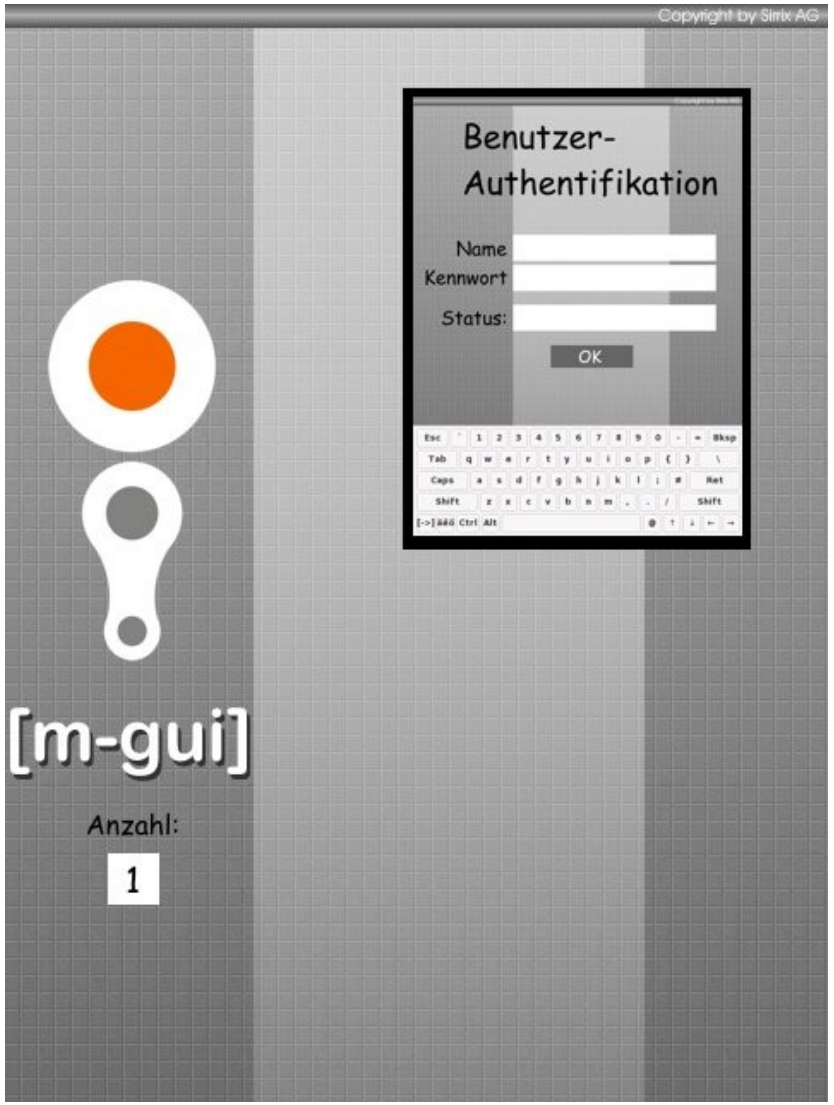
MoTrust-TrustedSMS (1)

- Zielplattform
  - Smartphone bzw. PDA mit Mobile Trusted Module (MTM)
  - Turaya/PikeOS basierend auf TI OMAP-35xx Entwicklerboard
    - PikeOS: kommerzieller Mikrokern der Firma Sysgo
  - Erster Prototyp für Turaya/OKL4 auf OpenMoko
    - OKL4: Mikrokern der Open Kernel Labs, Uni Sydney



MoTrust-TrustedSMS (2)

- Status
  - TrustedGUI für OpenMoko auf Turaya/OKL4
  - MicroTSS zur Entwicklung eines MTM
  - Geplante Fertigstellung: Mitte 2009



Ausblick

- Weitere Entwicklungsmöglichkeiten
  - SecureBoot
    - Authentifikation der Plattformkonfiguration gegenüber Benutzer
    - Basierend auf moderner PC-Hardware (Intel TXT oder AMD Pacifica)
  - SecureDMA
    - Schutz vor unsicheren Treibern und Hardware
    - Mittels 64-Bit PC Virtualisierungtechnologie von Intel oder AMD

Zusammenfassung

- Die Nachfrage nach vertrauenswürdige(re)n Signaturumgebungen wird sich weiter erhöhen
- Kryptografische Aspekte der Anwendungen bisher stark im Fokus, Plattformsicherheit wenig diskutiert
- Die vorgestellte Sicherheitslösung stellt einen möglichen Ansatz basierend auf Turaya und Trusted Computing Technologie dar
- Erhöhte Sicherheit mit Standardkomponenten
- Steigerung der Akzeptanz von Signaturanwendungen
- Exempl. Entwicklung von zwei vertrauenswürdigen Anwendungen
  - Signaturanwendung für PC-Architekturen mit TPM
  - SMS-Anwendung f. Embedded/Smartphone-Architekt. m. MTM
- Derzeit Entwicklungsphase einer prototypischen Lösung, interne Diskussion über (ggf. kommerzielle) Verwendung

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Utz Gnaida
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-99-9582-5783
Fax: +49 (0)228-99-1095825783

utz.gnaida@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de