Datenschutz und Sicherheit bei Mobile Devices

Matthias Hirsch

20. BDIP-Expertenforum, 19.05.2014, Berlin

Übersicht

- Das BSI
  - Aufgaben, Zielgruppen, Dienstleistungen
- Mobile IT-Sicherheit
  - Sicherheit von Smartphones und Tablets
- BSI-Dienstleistungen zu mobiler IT-Sicherheit
  - Sicherheitskomponenten für mobile Systeme
  - Sichere Mobile Systeme für die Bundesverwaltung
  - Unabhängige Prüfungen
  - Sicherheitsempfehlungen, Standards

Übersicht

- **Das BSI**
  - **Aufgaben, Zielgruppen, Dienstleistungen**
- Mobile IT-Sicherheit
  - Sicherheit von Smartphones und Tablets
- BSI-Dienstleistungen zu mobiler IT-Sicherheit
  - Sicherheitskomponenten für mobile Systeme
  - Sichere Mobile Systeme für die Bundesverwaltung
  - Unabhängige Prüfungen
  - Sicherheitsempfehlungen, Standards

Das BSI …

… ist die unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

- Gründung 1991
- Geschäftsbereich des BMI
- 574 Mitarbeiter (2013)
- Haushaltsbudget: ~ 80 Mio. € (2012)

BSI-Gebäude in Bonn

Das BSI

Zentrale Meldestelle für IT-Sicherheit

Einheitliche und verbindliche Sicherheitsstandards

Schutz der Netze des Bundes

Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (2009)

Warn- und Beratungsfunktion

Prüfung, Zertifizierung und Akkreditierung

Erkennung und Abwehr von Angriffen

Das BSI

Zielgruppen des BSI

Operativ:
Bundesverwaltung

Informativ:
Bürger,
Öffentlichkeit

Kooperativ:
Wirtschaft,
Forschung,
Medien

Das BSI

Produkte und Dienstleistungen

Regierung und Verwaltung

- IT-Sicherheitsberatung
- Entwicklung von Kryptosystemen
- CERT Bund
- Betrieb des Regierungsnetzes
- Unterstützung E-Government
- Cyber-Abwehrzentrum
- Unterstützung von Großprojekten, z.B. nPA, Galileo

Wissenschaft

- Mitwirkung beim IT-Sicherheitsforschungsprogramm des BMBF
- Finanzielle Förderung von Kompetenzzentren für die IT-Sicherheitsforschung: BSI ist einer der Assessoren
- Kooperation mit Universitäten

Bürger

- Sensibilisierungskampagnen
- BSI-Internetangebote
- Informationsmaterialien
- Service-Center für Privatanwender

Wirtschaft

- Zertifizierung von Produkten
- BSI IT-Grundschutz
- Kooperation mit ISPs
- Kooperation mit „UP KRITIS“
- Allianz für Cyber-Sicherheit

Das BSI

Sicherheit in der Informationstechnik:

	Schutz gegen unbefugte …
Vertraulichkeit	***… Kenntnisnahme***
Integrität / Authentizität	***… Veränderung (Manipulation)***
Verfügbarkeit	***… Vorenthaltung***

von Daten und Diensten

Das BSI

Gefährdung der IT-Sicherheit durch …

Staaten

Hacker

Organisierte Kriminalität

Hacktivismus

Übersicht

- Das BSI
  - Aufgaben, Zielgruppen, Dienstleistungen
- **Mobile IT-Sicherheit**
  - **Sicherheit von Smartphones und Tablets**
- BSI-Dienstleistungen zu mobiler IT-Sicherheit
  - Sicherheitskomponenten für mobile Systeme
  - Sichere Mobile Systeme für die Bundesverwaltung
  - Unabhängige Prüfungen
  - Sicherheitsempfehlungen, Standards

Mobile IT-Sicherheit

- **Sicherheit der Dienste, die durch mobile Geräte bereitgestellt** werden und der **Daten, die durch mobile Geräte übertragen, verarbeitet und gespeichert** werden.

  - → Mobile Netze
  - → Mobile Endgeräte
  - → Dienste
  - → Infrastrukturen

Mobile Endgeräte

- Mobiltelefone („Handies“)
- Laptops, Notebooks

- **Smartphones und Tablets**
  - Anwendersicht: **Mobiltelefon und Laptop in einem Gerät**

Smartphones und Tablets

- *Unterschied zum PC/Laptop:* Smartphones und Tablets …
  - … sind i.d.R. **immer eingeschaltet**, immer sofort **verfügbar**
  - … sind **immer da wo der Nutzer ist**: Das Smartphone kennt den räumlichen Standort des Nutzers, seine zurückgelegten und geplanten Strecken, aufgesuchte Orte, …
  - … verarbeiten die **gesamte Fernkommunikation** des Nutzers: Telefon, E-Mail, SMS, Chats, Kommunikation in sozialen Netzwerken und Portalen

  - … sind an wesentlich mehr Dingen des Lebens beteiligt: Vor Ort bezahlen, (**Mobile Payment**, **Mobile Banking**, Abrechnungen über mobile Netze), überall erreichbar sein, überall kommunizieren, navigieren, **berufliche Nutzung** (BYOD: privates Smartphone für **Zugriff auf Firmendaten**)

Smartphones und Tablets

- **Smartphones und Tablets sind noch stärker als PC auf den Nutzer, sein Verhalten, seine Kommunikation und sein Umfeld zugeschnitten**. Sie sind …
  - … die „**wahren PC**“ (= **Personal** Computer)

Sicherheit von Smartphones und Tablets

- **Smartphones und Tablets sind noch stärker als PC auf den Nutzer, sein Verhalten, seine Kommunikation und sein Umfeld zugeschnitten**. Sie sind …
  - … die „**wahren PC**“ (= **Personal** Computer)
  - … ein **sehr lohnendes Ziel** für Hacker, Nachrichtendienste, organisierte Kriminalität

- Betroffen sind …
  - … Privacy des Nutzers
  - … Sicherheit von geschäftlichen Prozessen
  - … Sicherheit bei beruflicher Nutzung

Sicherheit von Smartphones und Tablets

- **Angriffsvektoren:**
  - ***Allgemeine (aus der PC-Welt bekannte) Angriffe* +**
  - ***Smartphone-/Tablet-spezifische Angriffsvektoren***

Malware: Viren, Trojaner, …

Unsichere räumliche Umgebung

Zuverlässigkeit der Hardware

Abgriff von Daten in (mobilen) Netzwerken

Zuverlässigkeit des Betriebssystems

Abgriff von Daten auf zentralen Servern

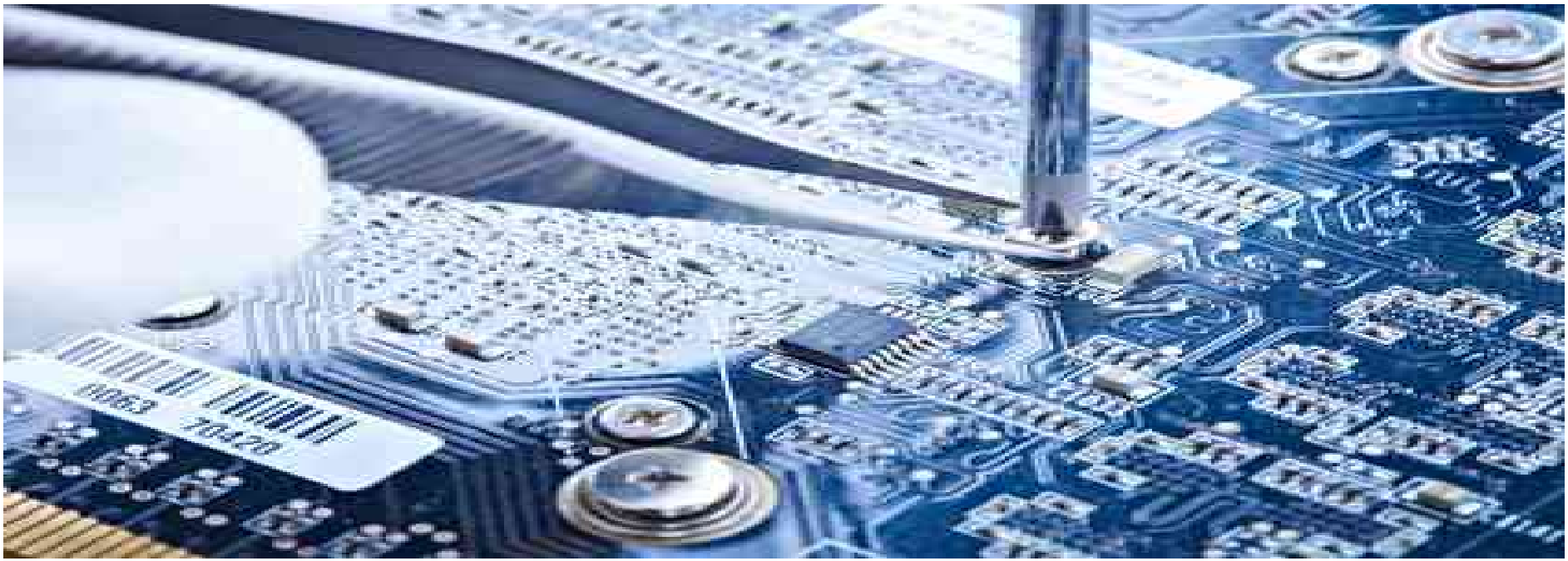
Zuverlässigkeit von Apps

Zugriff auf Daten und Dienste über Geräte-Schnittstellen

Sicherheit von Smartphones und Tablets

Zuverlässigkeit der Hardware:

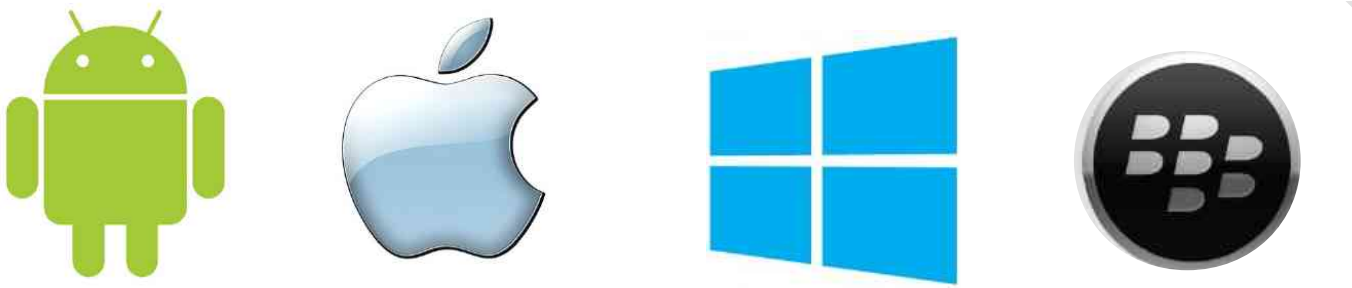
- **Hohe Packungsdichte**
- Tendenz: „**All in one Chip**“
- **Wenige Chiphersteller als Zulieferer** für alle großen Mobile Phone Hersteller
- HW-Specs werden gegenüber Dritten nicht veröffentlicht
- Für unabhängige Prüfer: **Black Box**
  - Unabhängige Prüfung zu zeitaufwendig für die hohe Frequenz neuer Modelle



Sicherheit von Smartphones und Tablets

Zuverlässigkeit der mobilen Betriebssysteme:

- Open Source basierte OS:
  - Vorteil: **Prinzipiell evaluierbar** (Specs und Source Code stehen zur Verfügung)
  - Nachteil: **Verteilte Verantwortung für Security Patches.**
- Auf propritären Sources basierende OS (Sources gehören Unternehmen):
  - Vorteil: **Zentral gemanagte Sicherheitsverantwortung**, schnelle Patches
  - Nachteil: Specs und Source Code stehen nicht bei allen Herstellern zur Verfügung (**Black Box**-Situation)



- Sandboxing: Mobile OS separieren Apps zum Schutz vor Malware
- OS-Hersteller unterliegen im Hinblick auf Datenschutz und Sicherheitsinteressen **ausländischer Gesetzgebung** (keine Wirksamkeit von BDSG oder EU-Richtlinien)

Sicherheit von Smartphones und Tablets

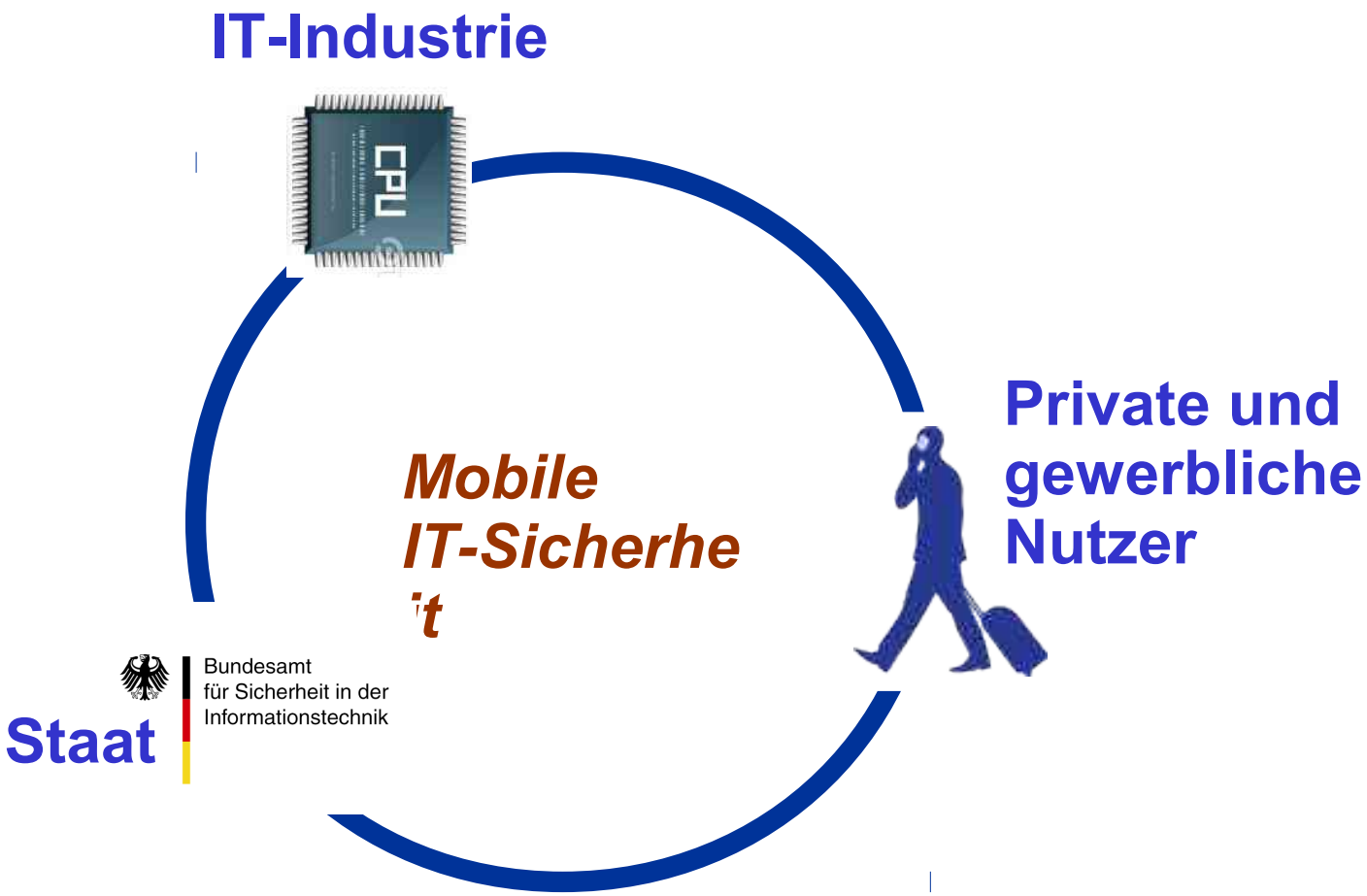
Zuverlässigkeit von Apps:

- Nutzerverhalten bei Smartphones/Tablets: **Häufiges, schnelles Runterladen** von vielen Apps möglich
- Oft von kleinen SW-Unternehmen. **Qualitätsmanagement?** Stehen bei der Programmierung **Datenschutz und Sicherheit im Vordergrund?**
- Oft relativ preiswert, weil: **Nutzer bezahlt die App oft mit seinen persönlichen Daten**
- Sicherheitslücken durch unklare Definition von **erwünschtem / unerwünschten App-Verhalten**
- Sicherheitsüberprüfung durch App Stores:
  - Black Box-Tests (Laufzeit-Inspektion)
  - Sicherheitstests unterliegen Sicherheitsverständnis und Geschäftsmodell des Store-Betreiber

Übersicht

- Das BSI
  - Aufgaben, Zielgruppen, Dienstleistungen
- Mobile IT-Sicherheit
  - Sicherheit von Smartphones und Tablets
- **BSI-Dienstleistungen zu mobiler IT-Sicherheit**
  - Sicherheitskomponenten für mobile Systeme
  - Sichere Mobile Systeme für die Bundesverwaltung
  - Unabhängige Prüfungen
  - Sicherheitsempfehlungen, Standards

Herausforderung Mobile IT-Sicherheit

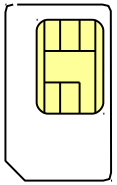


BSI-Dienstleistungen für mobile IT-Sicherheit

- Bereitstellung von Sicherheitskomponenten für mobile Systeme
- Bereitstellung sicherheitsgeprüfter mobiler Systeme für die Bundesverwaltung
- Unabhängige Prüfungen
- Veröffentlichung von Sicherheitsempfehlungen und Standards

Sicherheitskomponenten für mobile Systeme

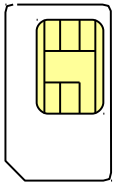
- Prinzip: **Separate Sicherheitskomponente** mit eigenem Prozessorsystem und SW, die in Verbindung mit Tablets und Smartphones betrieben wird.



- **Auslagerung sicherheitsrelevanter Funktionen** aus dem Smartphone/Tablet.
- Verbindung zum Smartphone/Tablet über NFC, Bluetooth, USB oder Micro-SD-Card
- Sicherheitskomponente enthält alle privaten Schlüssel, insbes. **elektronische Identität**

Sicherheitskomponenten für mobile Systeme

Sicherheitsvorteile von Smartcards:

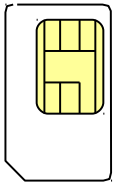


- **Hochspezialisiert auf Sicherheit**
- **Unabhängig evaluiert und zertifiziert**
- **Langjähriger Einsatz**, langjährige Erfahrung der Hersteller und Zusammenarbeit mit BSI
- **Leicht integrierbar**, adaptierbar an unterschiedlichste Systeme (bspw. als SD-Karten oder als NFC-Chips)
- Verwendbar als **e-ID** in Verbindung mit etablierten Sicherheitsdiensten (PKI, **Zertifizierungsdienste**)

Sicherheitskomponenten für mobile Systeme

Beispiele für den mobilen Einsatz von Smartcards:

- SIM (Zugang zu Mobilnetz)



- **nPA**

Quelle: Samsung

- **Sicherheitsanker für Smartphones der Bundesverwaltung**

nPA

- **Ziel**
  - Nachhaltige Nutzbarmachung des nPA mit mobilen Endgeräten wie Smartphones und Tablets
- **Rückblick**
  - Steigende Anzahl mobiler Geräte mit integrierter NFC-Schnittstelle
    - Aber: Inkompatibilitäten bestehender NFC-Controller zum nPA
    - Geringe Anzahl kompatibler Smartphones (z.B. Sony Xperia L)

nPA

- **Komplexe Kommunikation i. Vgl. zum Standard-Szenario „Tag auslesen“**
  - Übertragung großer Daten (Zertifikatskette)
    - Unterstützung von **Extended Length-APDUs** erforderlich
      - **Von derzeit verbauten NFC-Controllern nicht unterstützt**
  - Lange Kommunikationsverbindung
    - Stabiles Feld erforderlich
- **Browser-Plug-in-Abhängigkeit**
  - Integration in Browser aufwendig
  - Keine standardisierten Schnittstellen
- **Smartphones verfügen über keine Sicherheitsfunktionalität**
  - Z.B. schlechte Zufallszahlen für kryptographische Operationen

nPA

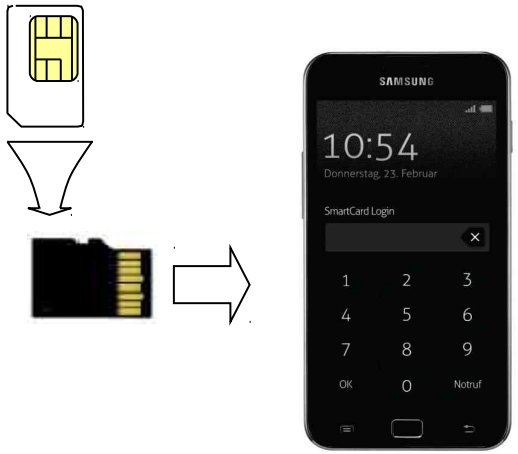
- **Umstellung eID-Infrastruktur auf alternative eID-Aktivierung erfolgt**
  - Abhängigkeit von Browser-Plugins entfällt
- **Mobile eID-Client Software bereits verfügbar**
- **Teilnahme am NFC-Forum durch BSI**
  - Aufnahme EL-APDUs in den Standard
  - Aufbau eines Zertifizierungsschemas für NFC-Devices
  - Höhere Feldstärke-Anforderungen in Diskussion
- **Smartphones verfügen über neue Sicherheitsfunktionalitäten**
  - Secure Elements (im NFC-Controller / Neue SIM-Karten)
    - Z.B. Nutzung als Zufallszahlengenerator

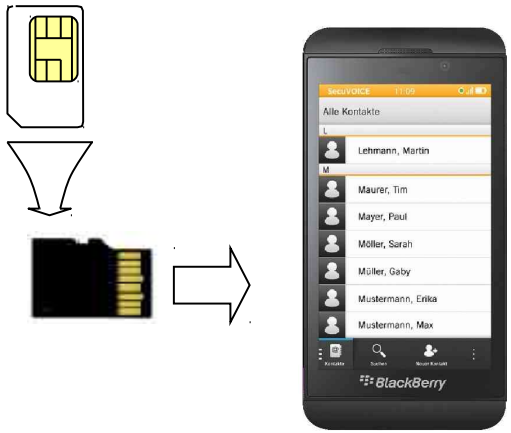
Übersicht

- Das BSI
  - Aufgaben, Zielgruppen, Dienstleistungen
- Mobile IT-Sicherheit
  - Sicherheit von Smartphones und Tablets
- BSI-Dienstleistungen zu mobiler IT-Sicherheit
  - Sicherheitskomponenten für mobile Systeme
  - **Sichere Mobile Systeme für die Bundesverwaltung**
  - Unabhängige Prüfungen
  - Sicherheitsempfehlungen, Standards

Sichere mobile Systeme für die Bundesverwaltung

- **SiMKo3** (T-Systems)
  - Samsung Galaxy S3 und S4 und Tablet
  - „Gehärtetes“ Android auf Separation Kernel
- **SecuSUITE** (SecuSmart/Blackberry)
  - Blackberry Z10 und Q10
- Beide Systeme durch BSI **zugelassen für VS-NfD**
- **Sichere Sprache** (Ende-zu-Ende-verschlüsselt)
- **Sichere Datendienste** über VPN zu Gateways in Hausnetzen
- **Beide Systeme mit Smartcard-Sicherheitsanker**
  - Adaptiert als Micro-SD-Card

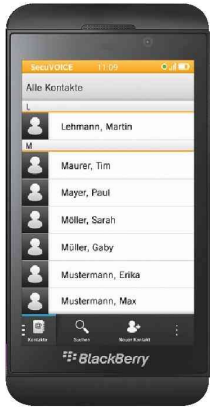




Sichere mobile Systeme für die Bundesverwaltung

Beide Systeme bieten **separierte Arbeitsbereiche**:

Umschalten jederzeit ohne neu zu booten



- SiMKo3: Separierung durch **Separation Kernel** (Trust2Core)
- SecuSUITE: Separierung durch **Betriebssystem** (BB OS)
- Nutzersicht: „**2 Geräte in 1**“
- Motivation für Nutzer, keine weiteren Geräte zu verwenden („Schatten-IT“)
  - In der Bundesverwaltung: Kein BYOD!

Übersicht

- Das BSI
  - Aufgaben, Zielgruppen, Dienstleistungen
- Mobile IT-Sicherheit
  - Sicherheit von Smartphones und Tablets
- BSI-Dienstleistungen zu mobiler IT-Sicherheit
  - Sicherheitskomponenten für mobile Systeme
  - Sichere Mobile Systeme für die Bundesverwaltung
  - **Unabhängige Prüfungen**
  - Sicherheitsempfehlungen, Standards

Unabhängige App-Prüfungen

- Prinzip: **App-Prüfungen unabhängig von App Stores**
- Transparente Prüfkriterien, Bewertungen, Sicherheitsklassifizierungen
- Geplant: Rahmenvertrag des Bundes mit Prüfdienstleistern:
  - Prüfung von Apps für **SecuSUITE und SiMKo3**
  - Prüfung von Apps für den „**Bundes-App Store**“ (www.govapps.de)
- Geplant: Veröffentlichung von **Programmierrichtlinien für App-Programmierer**

Übersicht

- Das BSI
  - Aufgaben, Zielgruppen, Dienstleistungen
- Mobile IT-Sicherheit
  - Sicherheit von Smartphones und Tablets
- BSI-Dienstleistungen zu mobiler IT-Sicherheit
  - Sicherheitskomponenten für mobile Systeme
  - Sichere Mobile Systeme für die Bundesverwaltung
  - Unabhängige Prüfungen
  - **Sicherheitsempfehlungen, Standards**

Standards und Empfehlungen

- Veröffentlichungen von Standards, Empfehlungen
  - Cybersicherheitsempfehlung (CSE) zu iOS
  - CSE zu Android wird in Kürze veröffentlicht
  - Publikationen zu BYOD und Consumerization, MDMs
  - …
  - Siehe www.bsi.bund.de

Kontakt

Vielen Dank für Ihre Aufmerksamkeit

Matthias Hirsch
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat K15 (Sicheres mobiles Arbeiten)
Godesberger Allee 185 – 189
53179 Bonn

matthias.hirsch@bsi.bund.de
Tel.: +49 3018 9582 5515
Fax: +49 3018 109582 5514

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