Sirrix AG
security technologies

# High-Assurance Security Kernel (HASK)

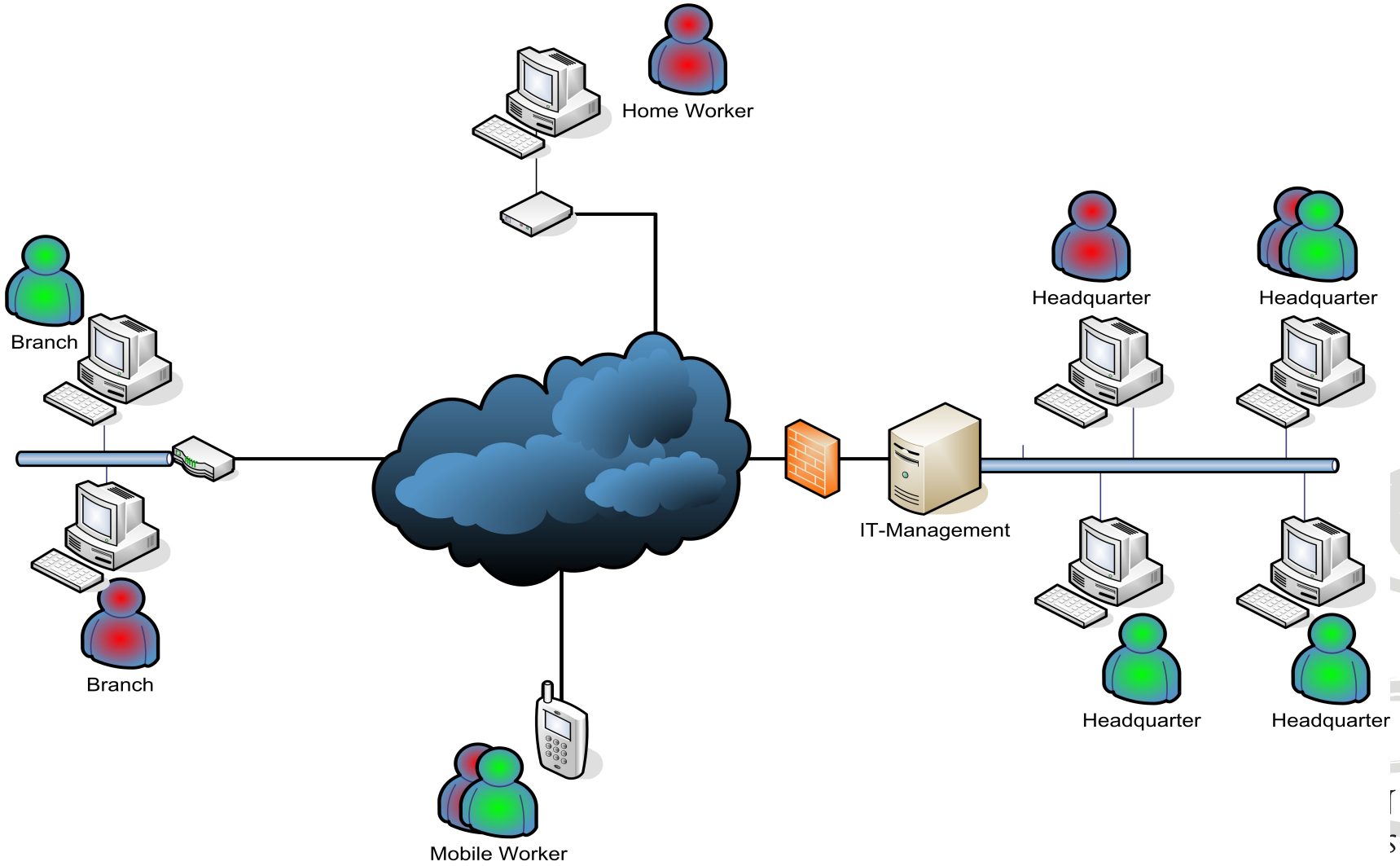
Christian Stueble (stueble@sirrix.com)

# Übersicht

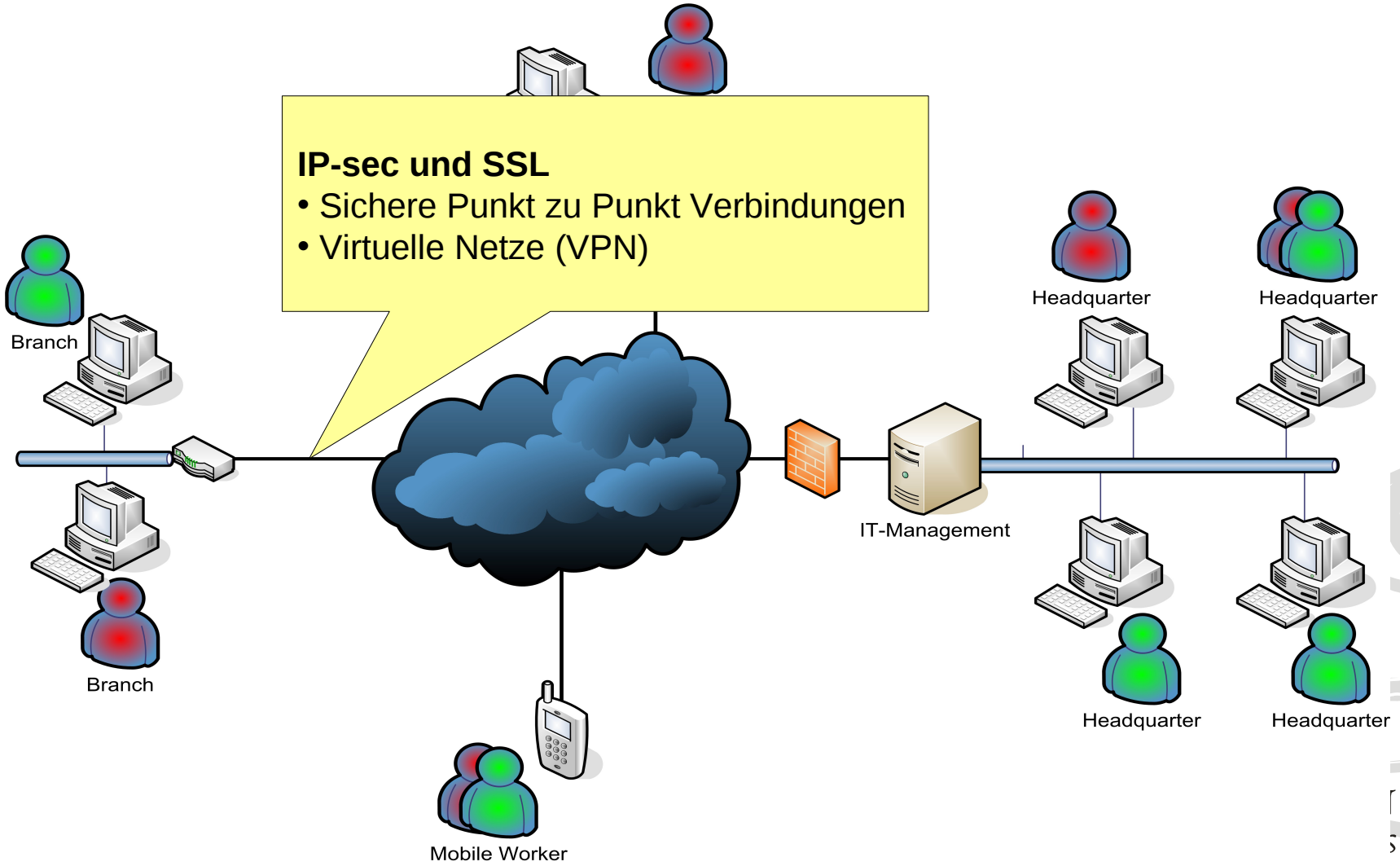
- **Einleitung**
  - Probleme herkömmlicher IT-Infrastrukturen
  - Ziele und Bausteine
- **Das HASK Protection Profile**
  - Common Criteria Protection Profiles
  - Übersicht und Motivation
  - Besondere Eigenschaften
- **Lösungsansätze**
  - Trusted Computing Technologie
  - Sichere Betriebssysteme
  - Vertrauenswürdige IT-Infrastrukturen
- **Zusammenfassung**

Sirrix AG
security technologies

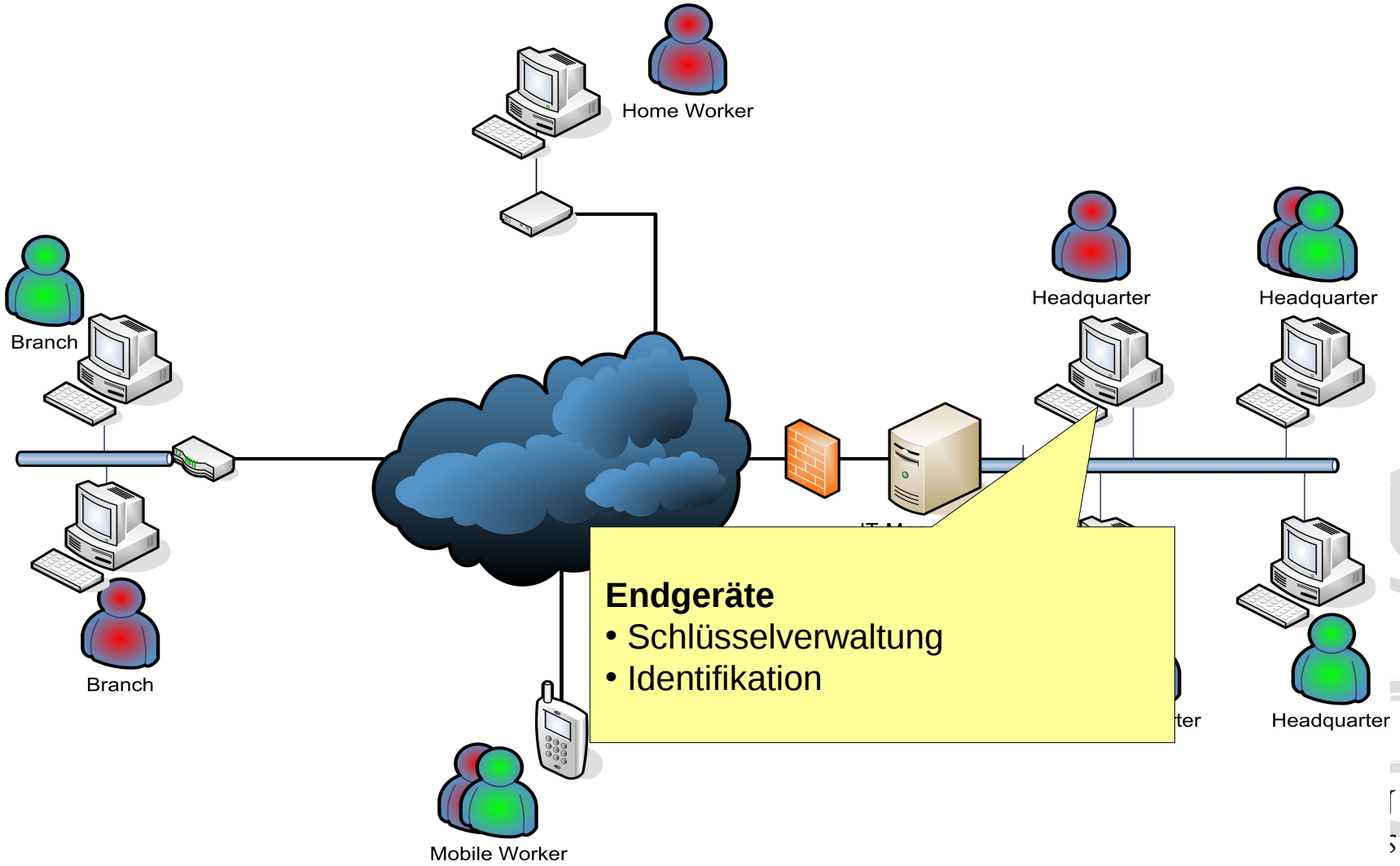
# Probleme herkömmlicher IT-Infrastrukturen



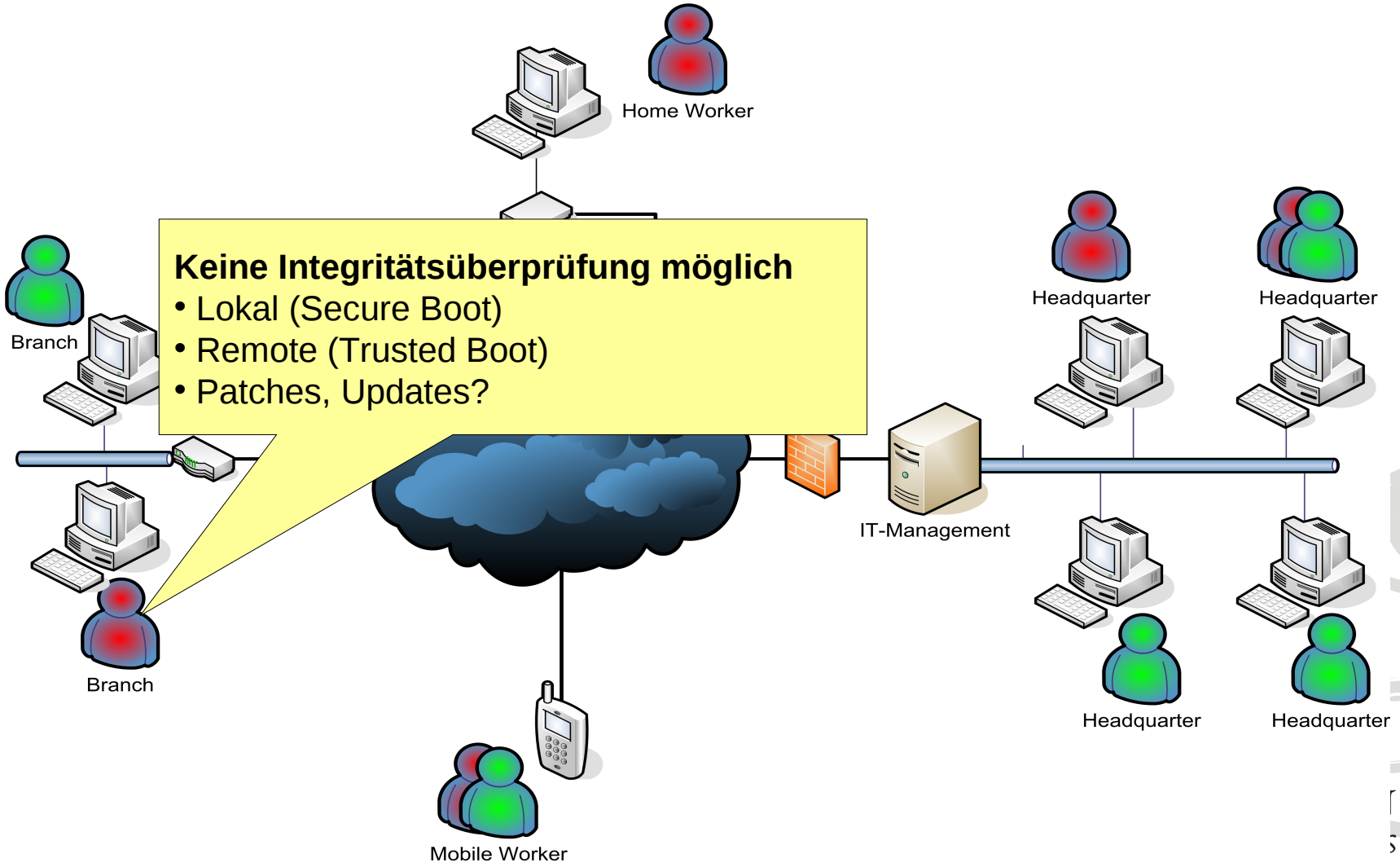
# Probleme herkömmlicher IT-Infrastrukturen



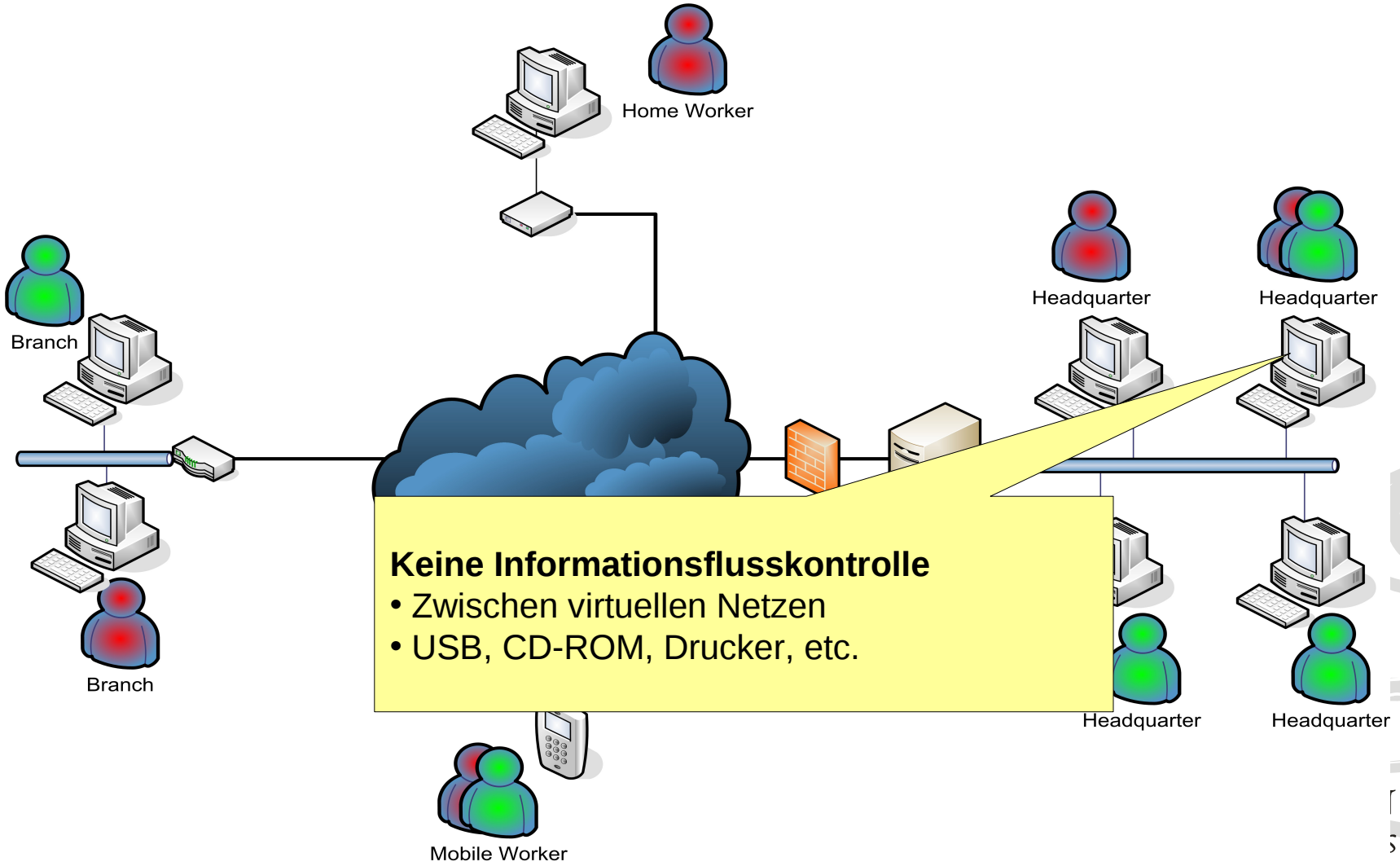
# Probleme herkömmlicher IT-Infrastrukturen



# Probleme herkömmlicher IT-Infrastrukturen



# Probleme herkömmlicher IT-Infrastrukturen



# Ziele und Bausteine

- **Sicherheitsziele**
  - Erhöhung des Sicherheitslevels auf ein akzeptables Maß
    - Business-Umgebung, Verwaltung, Behörden
    - Keine Hochsicherheit
- **Technische Ziele**
  - Zentrale Konfiguration der IT-Infrastruktur
    - Clients (Server, Gateways, Desktop, Mobile)
    - Sicherheitsmanagement
  - Überprüfbarkeit der Integrität
  - Isolation und kontrollierte Kommunikation einzelner Arbeitsumgebungen
  - Verwendung von Standardhardware und -software

Sirrix AG
security technologies

# Common Criteria Protection Profiles

- **Common Criteria**
  - Die Common Criteria sind ein Anforderungskatalog für die Erstellung und Evaluation von sicherheitskritischen Produkten
  - Nachfolger von ITSEC, Orange Book, ...
  - Anerkannt in 24 Ländern
  - Evaluation Assurance Level (EAL) 1-7
- **Protection Profile**
  - Neues Konzept der Common Criteria
  - Produkt- und implementierungunabhängige Anforderungsspezifikation
  - Beschreibt eine Produkt- bzw. Funktionsklasse
  - Definiert eine EAL-Prüftiefe
  - Wird selbst evaluiert und zertifiziert

# Das HASK-Protection Profile

- **High-Assurance Security Kernel (HASK)**
  - Höheres Sicherheitsniveau als herkömmliche Betriebssysteme
  - Evaluation Assurance Level (EAL) 5
  - Fokus liegt auf Data Leakage Protection
  - Abstrakte Konzepte zur Integritätsprüfung
- **Beteiligte**
  - BSI (Auftraggeber), Sirrix AG, atsec GmbH, EU-Projekt OpenTC (RUB)
- **Motivation**
  - Ein Protection Profile für eine Klasse von Produkten
  - Verschiedene Lösungskonzepte vertreten
- **Zielplattformen**
  - Server, Desktop, Notebook, Mobile (PDA oder Smartphone)

Sirrix AG
security technologies

# Wichtige Eigenschaften des HASK-PP

- **Strenge Isolation von Compartments**
  - Anwendungen, Virtual Maschines, Partitionen oder Mengen davon
  - Kontrollierte Inter-Compartment Kommunikation
  - Kommunikation mit externen IT-Systemen
- **Integritätsmanagement**
  - Kontrolliertes Booten
    - Secure-, Trusted-, Verified- und Authenticated Boot
  - Integritätsnachweis des Sicherheitskerns
  - Integritätsmanagement von Compartments
- **Trusted Channel**
  - Integritätsüberprüfung von Kommunikationsendpunkten
- **Datenbindung**
  - Benutzerdaten können an Anwendung gebunden werden

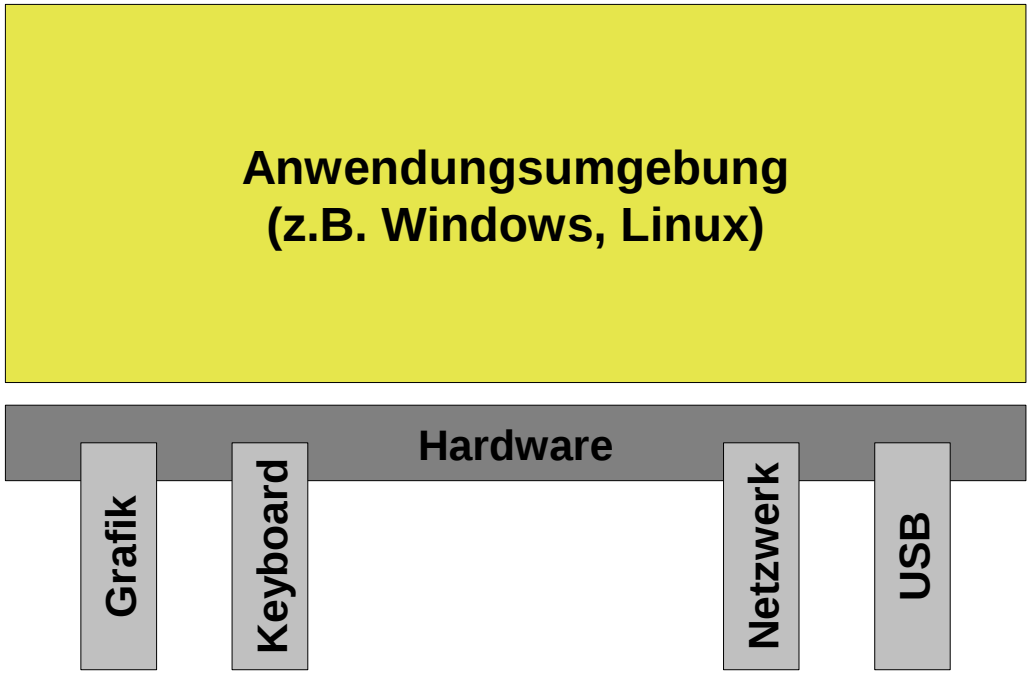
Sirrix AG
security technologies

# Trusted Computing Technologie

- **Trusted Computing Group (TCG)**
  - Internationales Konsortium aus mehr als 100 Unternehmen und Behörden
    - AMD, BSI, HP, IBM, Intel, Microsoft, SUN
- **Spezifikation von Hard- und Softwarekomponenten**
  - Trusted Platform Module (TPM)
  - Mobile Trusted Module (MTM)
  - Trusted Network Connect (TNC)
  - Trusted Software Stack (TSS)
- **TPM-Funktionen**
  - Trusted Boot: 'Messen' von Softwarekonfigurationen
  - Remote Attestation: Digitale Signatur der gemessenen Konfiguration
  - Sealing: Binden von Daten an Konfiguration
  - HW-Zufallsgenerator

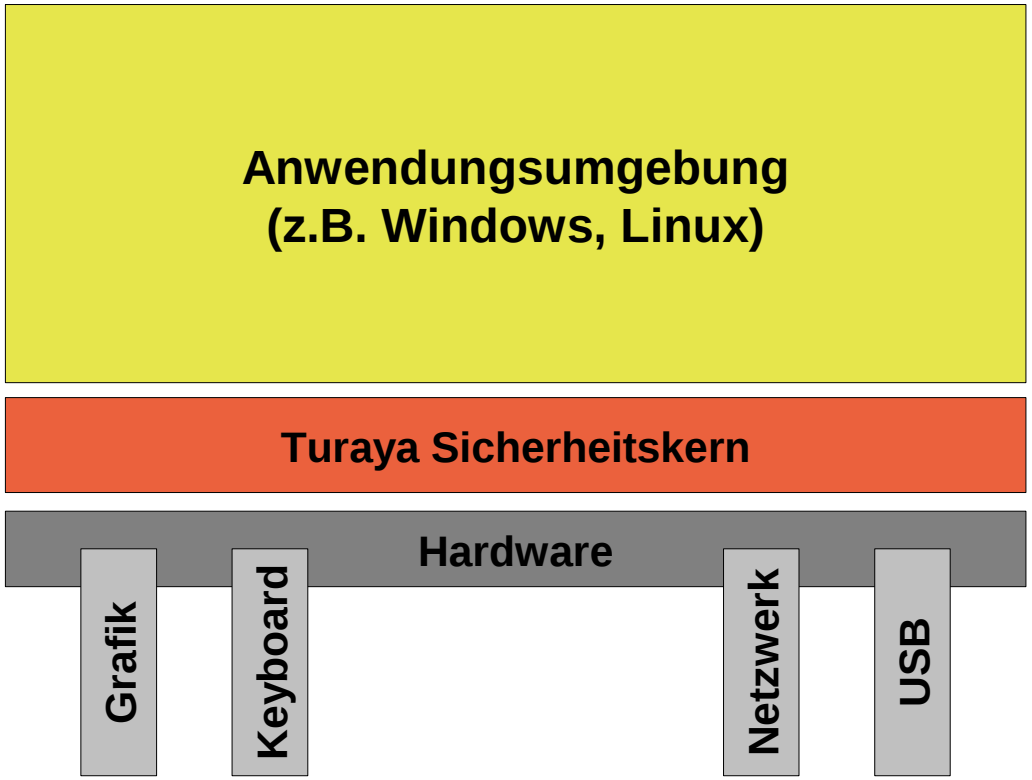
Sirrix AG
security technologies

# Turaya Sicherheitskern (1)



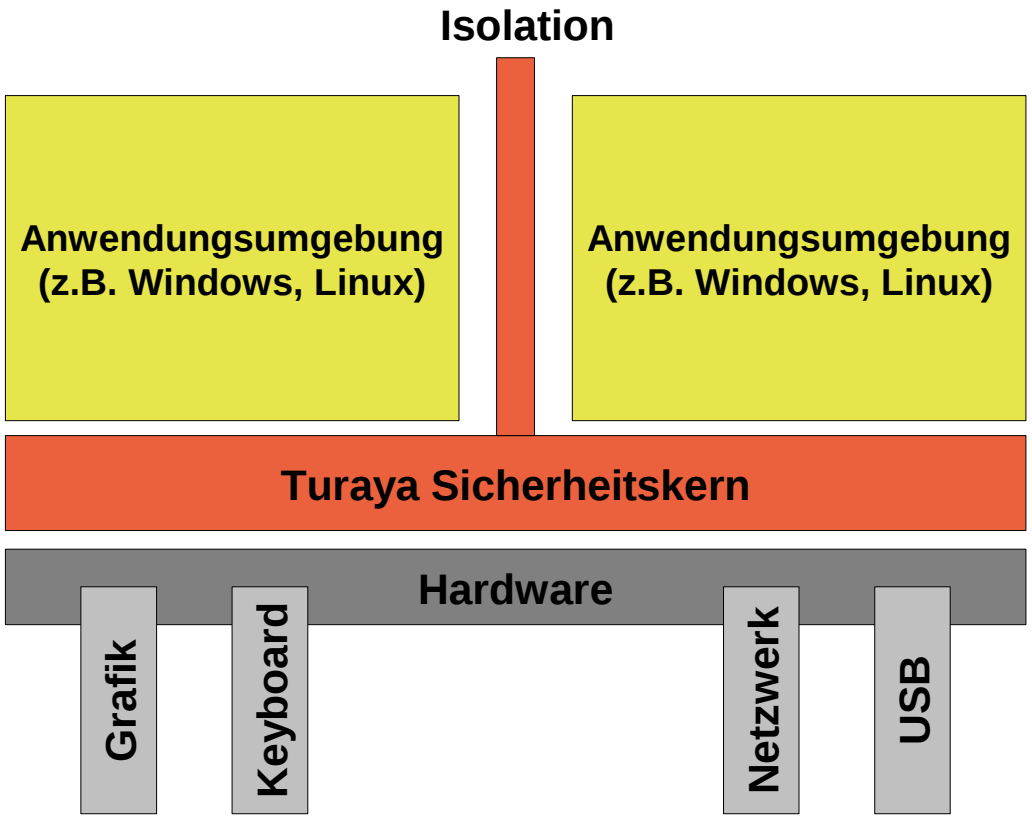

Sirrix AG
security technologies

# Turaya Sicherheitskern (2)




Sirrix AG
security technologies

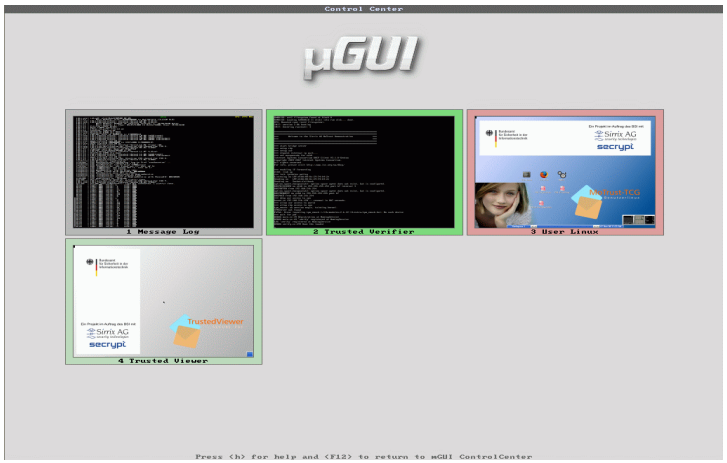
# Turaya Sicherheitskern (3)




Sirrix AG
security technologies

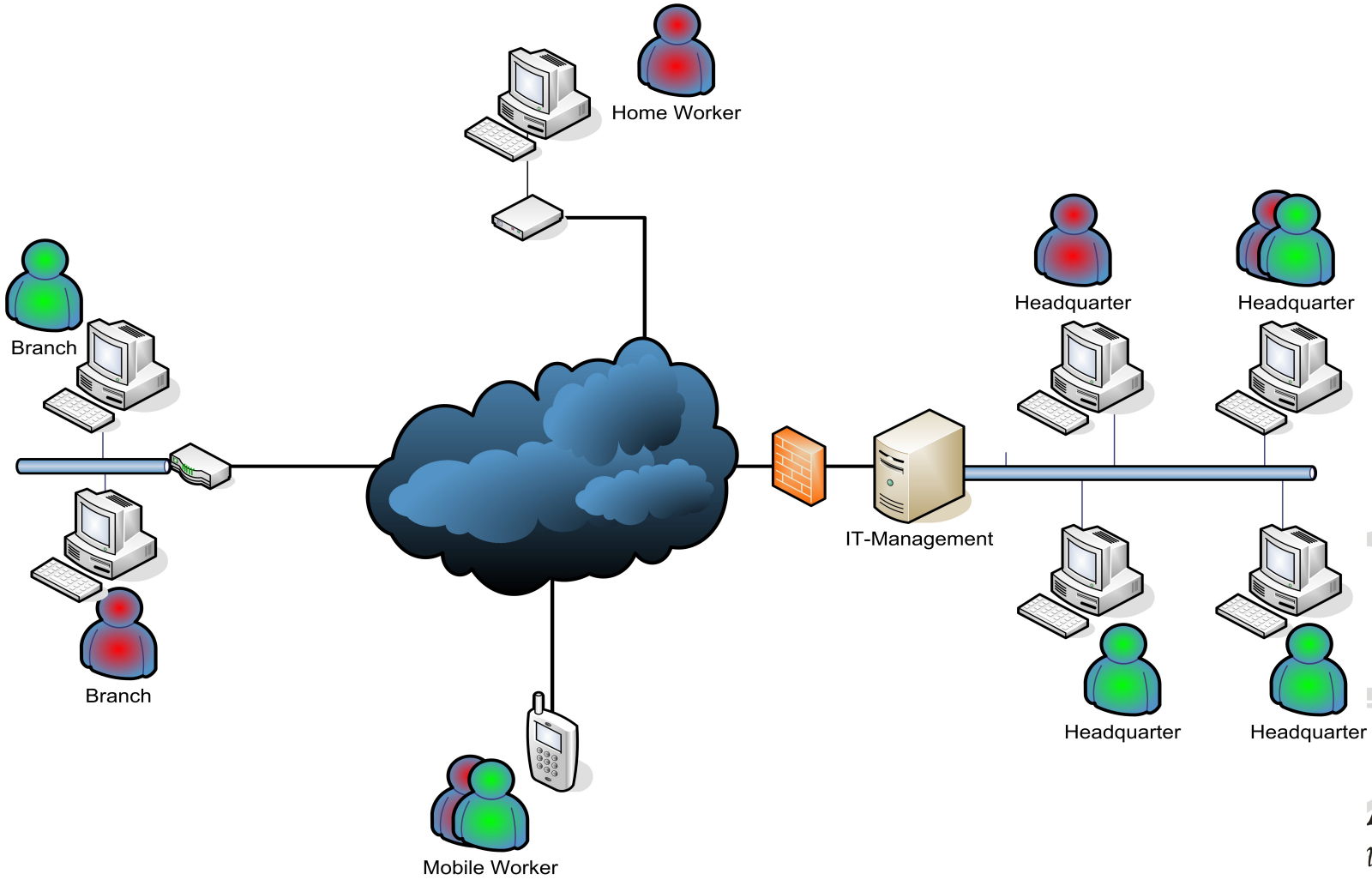
# Der Turaya Sicherheitskern (4)

- **Verfügbare Sicherheitsdienste**
  - TrustedGUI (µGUI, mGUI)
  - Secure Storage (data binding)
  - Remote Attestation (integrity proof)
  - Embedded TSS (eTSS)
- **Unterstützte Basisarchitekturen**
  - GNU/Linux (x86)
  - L4/Fiasco (x86)
  - L4/OKL4 (ARM)
  - PikeOS (ARM, MIPS)

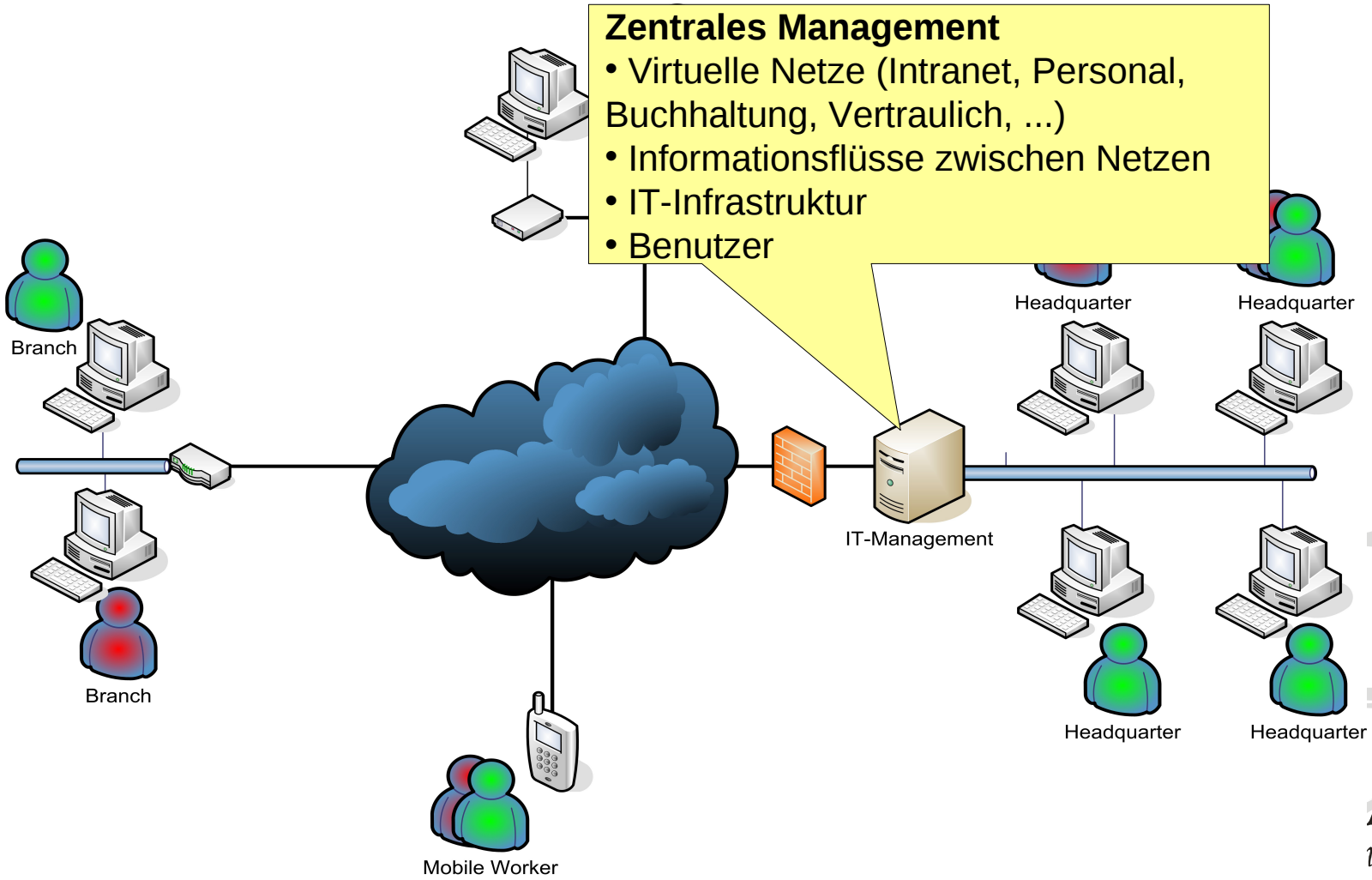




Sirrix AG
security technologies

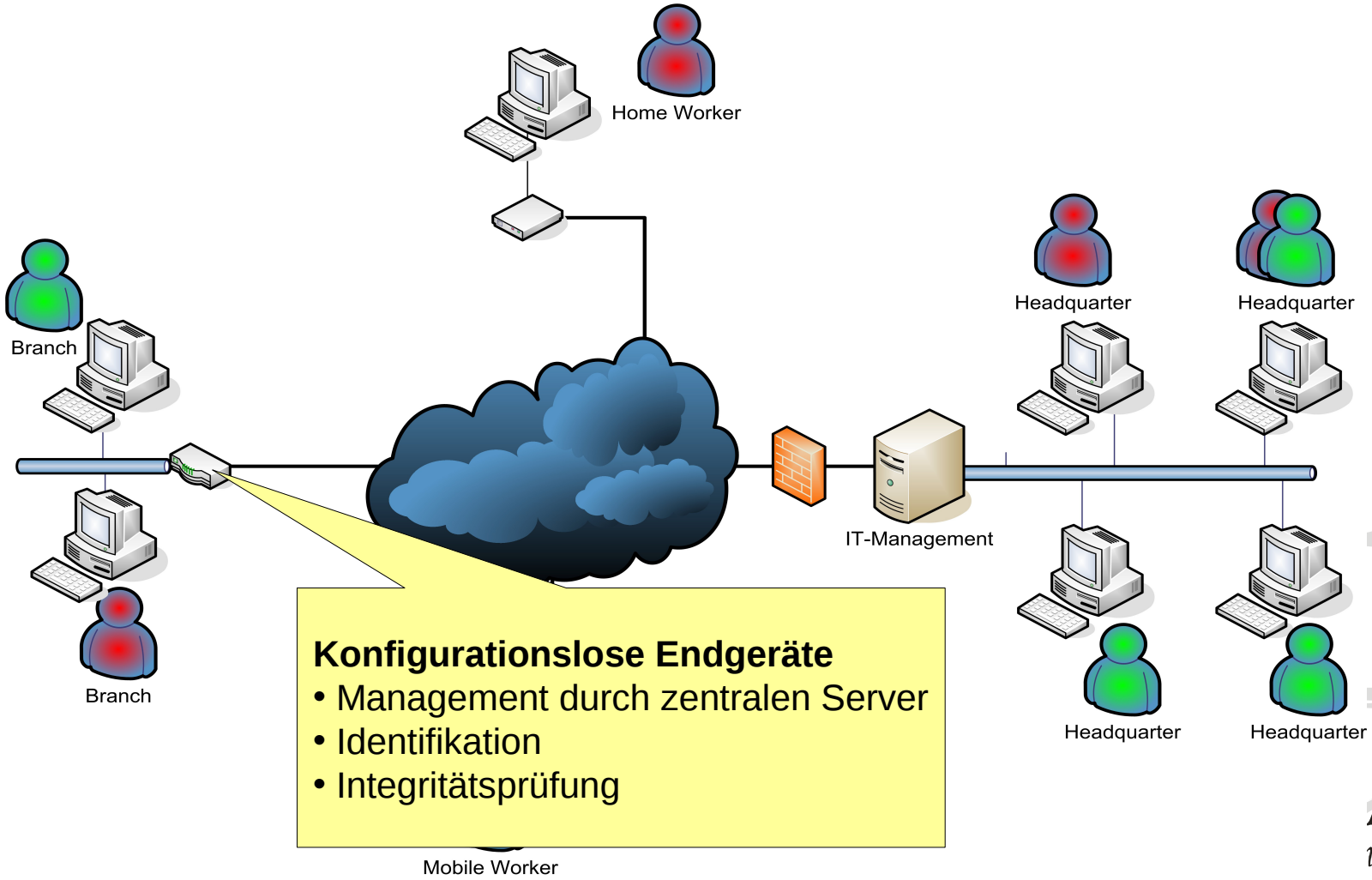
# Vertrauenswürdige IT-Infrastrukturen



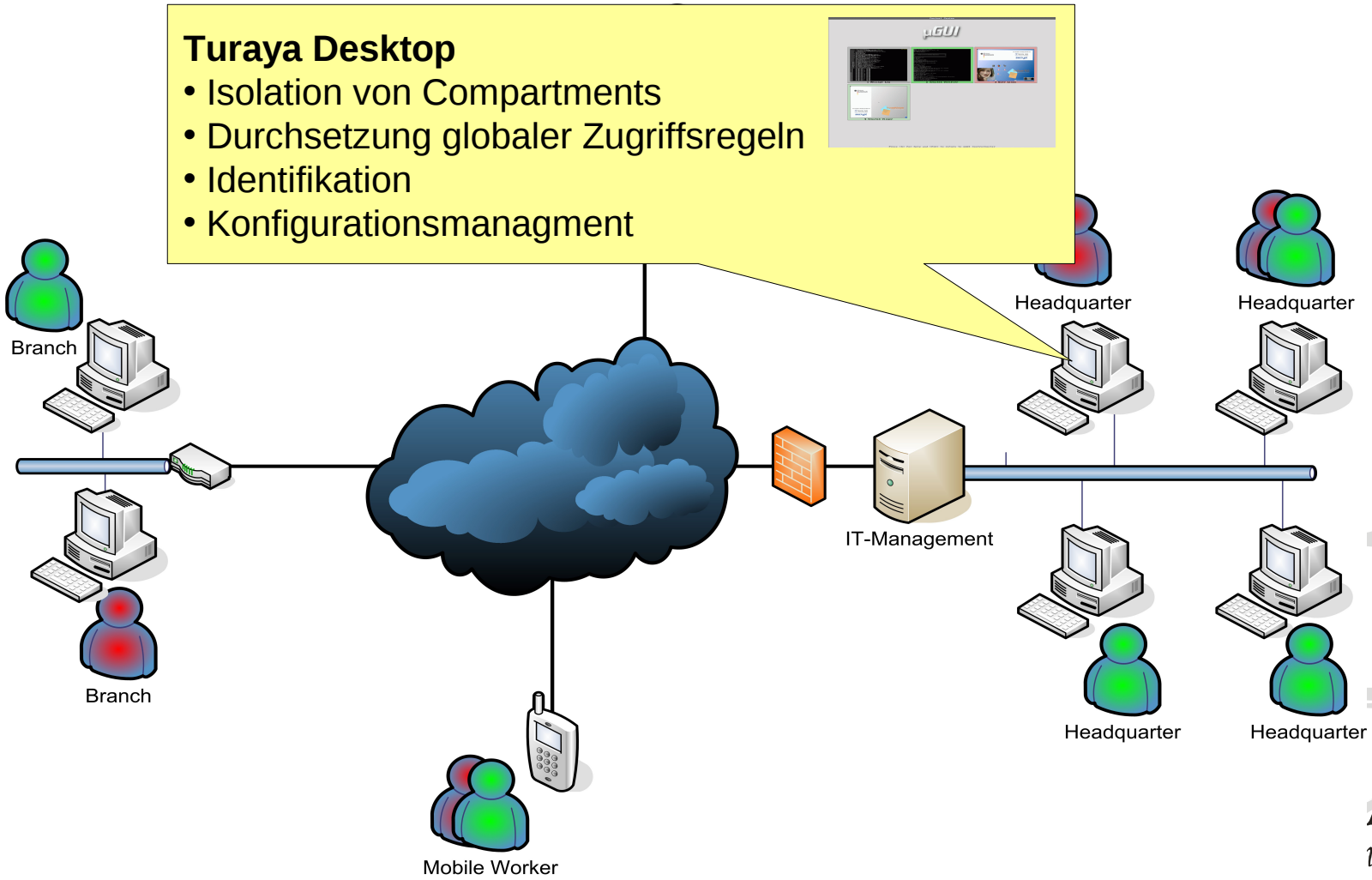
# Vertrauenswürdige IT-Infrastrukturen



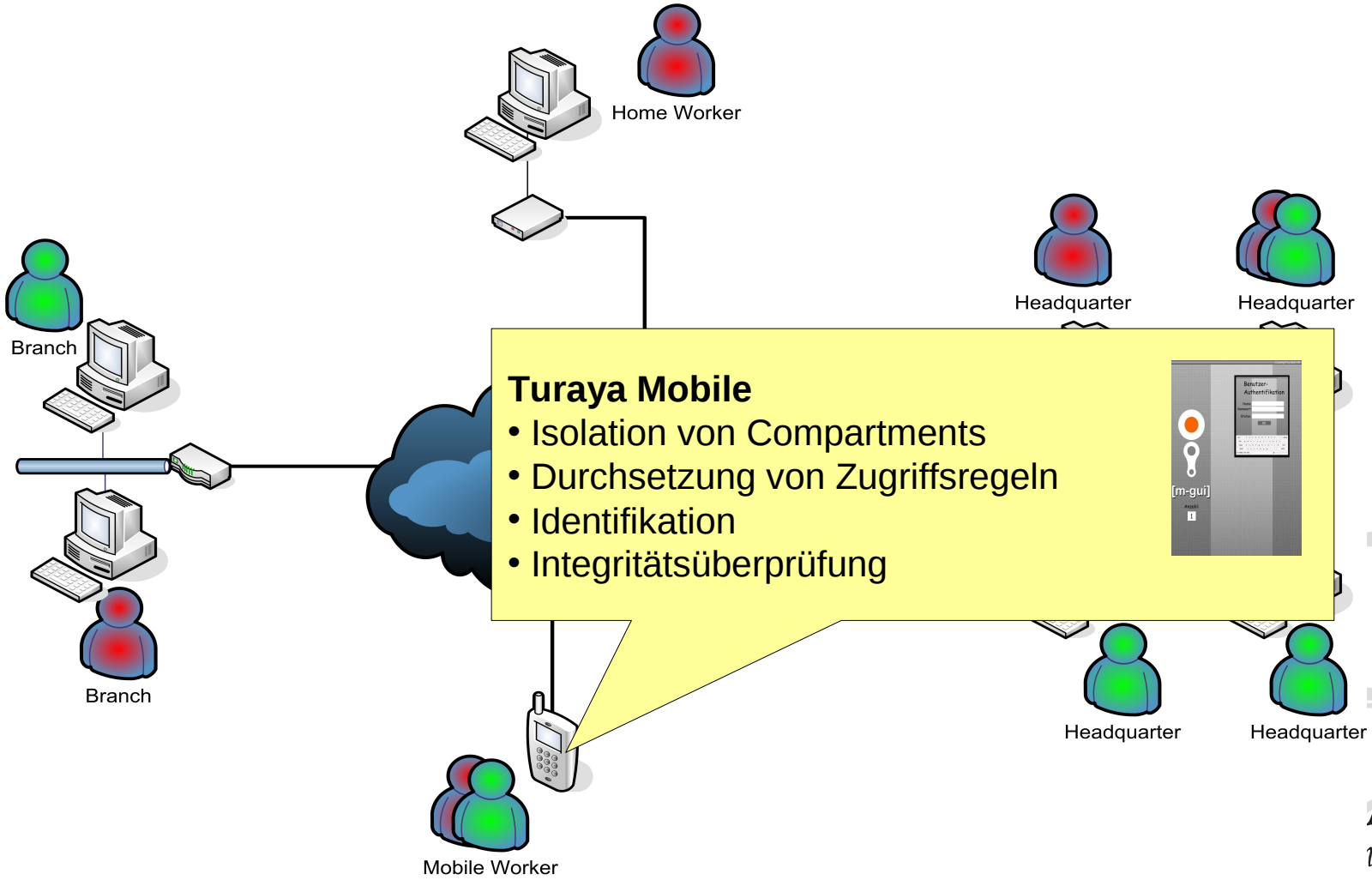
# Vertrauenswürdige IT-Infrastrukturen



# Vertrauenswürdige IT-Infrastrukturen



# Vertrauenswürdige IT-Infrastrukturen



# Zusammenfassung

- **Existierende IT-Infrastrukturen sind nicht in der Lage, Sicherheitsregeln zuverlässig durchzusetzen**
- **Herkömmliche Betriebssysteme sind der größte Schwachpunkt im Gesamtkonzept**
- **Trusted Computing Technologie kann zusammen mit einem effizienten Sicherheitskern das Sicherheitsniveau wesentlich erhöhen**
- **Die nötigen Anforderungen für eine vertrauenswürdige Basisplattform sind im HASK-PP (EAL 5) zusammengefasst**
- **Protection Profile for a High Assurance Security Kernel Version 1.14, BSI-CC-PP-0039-2008**

Sirrix AG
security technologies

# It’s your turn now . . .

**Sirrix AG**
**Christian Stüble**
**Lise-Meitner-Allee 4**
**44801 Bochum, Germany**

**Phone +49-234-610071-0**
**Fax +49-234-610071-500**

**stueble@sirrix.com**
**http://www.sirrix.com**

Sirrix AG
security technologies

# Sirrix AG security technologies

- Founded in 2001 as a technology spin-off from the for Cryptography and Security at German Researc Institute for Artificial Intelligence
- Founder: Prof. Dr. Birgit Pfitzmann, Ammar Alkassa Prof. Dr. Ahmad Sadeghi, Christian Stüble et al.
- All corporate shares held privately by management
- Member of the European Center for IT-Security since December 2005
- Close collaboration with well-known research institutes and companies:
  - IBM Research Zurich Labs, IBM Watson, HP Bristol Labs, Microsoft Innovation Center EMIC, Nokia Research, Netherlands Forensic Institute, Institute de la Gendarmerie Nationale, ...
  - German Re[illegible] Intelligence (DFKI), University of Bochum ([illegible] Saar[illegible]iversity of Darmstadt, Stevens Institute [illegible]nol[illegible]ology, [illegible]niversity of Leuven, [illegible]ven

SecurITy made in Germany

TRUSTED COMPUTING GROUP™

eurobits Europäisches Kompetenzzentrum für IT-Sicherheit • Bochum

Sirrix AG security technologies

# Sirrix AG security technologies

**Main focus:**

- Leading technology in the areas of cryptography, security of information and communication
- Design, analysis and development of cryptographic protocols and schemes
- Secure operating system platforms, Trusted Computing and Multilateral Security

**Technologies:**

- PERSEUS/TURAYA™: High-Assurance Security Kernel, Multi-Level OS
- UNISTEP: Security architecture for end-to-end communication in heterogeneous networks: TrustedVPN, Gateways for secure VoIP, GSM, ISDN etc. (see also SCIP)
- TPM compliance test suite
- Technologies in the domain of highly efficient authenticated encryption (Secure VoIP, 10G+ Encryption) as well as highly-parallelizable and hybrid (combined in hardware and software) cryptographic systems

**Customers:**

- BSI, NATO, BMWi and other security-related authorities
- Infineon, ST Microelectronics, SAP, T-Online, T-Systems, Wincor-Nixdorf, SCA, Bechtle, ND-Satcom Defense, Raytheon, Trusted Computing Group, Dialogika, et al.
- Strong, product-related business and customers worldwide

Sirrix AG
security technologies

# Sirrix AG security technologies

- Founded in 2001 as a technology spin-off from the for Cryptography and Security at German Researc Institute for Artificial Intelligence
- Founder: Prof. Dr. Birgit Pfitzmann, Ammar Alkassa Prof. Dr. Ahmad Sadeghi, Christian Stüble et al.
- All corporate shares held privately by management
- Member of the European Center for IT-Security since December 2005
- Close collaboration with well-known research institutes and companies:
  - IBM Research Zurich Labs, IBM Watson, HP Bristol Labs, Microsoft Innovation Center EMIC, Nokia Research, Netherlands Forensic Institute, Institute de la Gendarmerie Nationale, ...
  - German Re[illegible] Intelligence (DFKI), University of Bochum ([illegible] Saar[illegible]iversity of Darmstadt, Stevens Institute [illegible]nol[illegible]ology, [illegible]niversity of Leuven, [illegible]ven,

SecurITy made in Germany

TRUSTED COMPUTING GROUP™

eurobits Europäisches Kompetenzzentrum für IT-Sicherheit • Bochum

Sirrix AG security technologies

# Sirrix AG security technologies

**Main focus:**

- Leading technology in the areas of cryptography, security of information and communication
- Design, analysis and development of cryptographic protocols and schemes
- Secure operating system platforms, Trusted Computing and Multilateral Security

**Technologies:**

- PERSEUS/TURAYA™: High-Assurance Security Kernel, Multi-Level OS
- UNISTEP: Security architecture for end-to-end communication in heterogeneous networks: TrustedVPN, Gateways for secure VoIP, GSM, ISDN etc. (see also SCIP)
- TPM compliance test suite
- Technologies in the domain of highly efficient authenticated encryption (Secure VoIP, 10G+ Encryption) as well as highly-parallelizable and hybrid (combined in hardware and software) cryptographic systems

**Customers:**

- BSI, NATO, BMWi and other security-related authorities
- Infineon, ST Microelectronics, SAP, T-Online, T-Systems, Wincor-Nixdorf, SCA, Bechtle, ND-Satcom Defense, Raytheon, Trusted Computing Group, Dialogika, et al.
- Strong, product-related business and customers worldwide

Sirrix AG
security technologies

# It’s your turn now . . .

**Sirrix AG**
**Name**
**Building D3²**
**66123 Saarbrücken, Germany**

**Phone +49-681-936251-0**
**Fax +49-681-936251-500**

**name@sirrix.com**
**http://www.sirrix.com**

Sirrix AG
security technologies