Mobile Identity Management auf Basis von SIMOIT und TNC@FHH

Evren Eren, Stephan Uhde, Kai-Oliver Detken

Wireless Communication and Information 2009

15.-16. Oktober, Berlin

Laboratory for IT-Security Architectures

Fachhochschule Dortmund
University of Applied Sciences and Arts

Prof. Dr. -Ing. E. Eren
Emil-Figge-Str. 42
44227 Dortmund
Fon: +49-(0)231-755-6776
Fax: +49-(0)231-755-6710
E-Mail: eren@fh-dortmund.de
Web: www.fh-dortmund.de/eren
Lab for IT Security: www.lisa.fh-dortmund.de

Mobile Identity Management

Mobile Identity Management

Mobilität und Trusted Computing

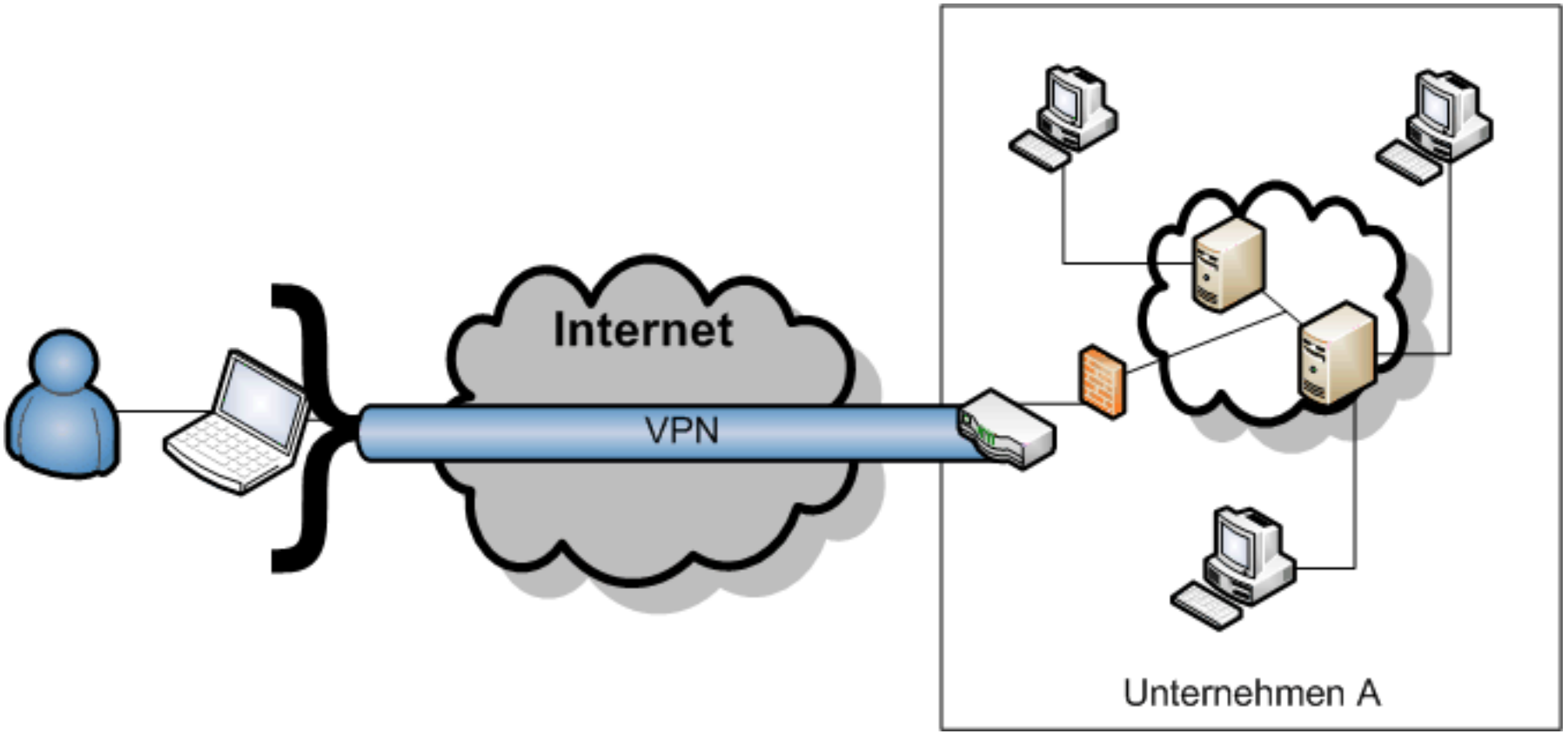
- **Zentrale Problematik:** Beherrschbarkeit von …
  - Applikationssicherheit
  - Benutzerauthentisierung
  - Geräteauthentisierung
  - Berechtigungsprüfung/Rechteverwaltung

- **Paradigma:**
  - Mobilfunknetzbetreiber nutzen zur Authentisierung SIM-Karte und PIN (Zwei-Faktorenauthentisierung).
- → **Problem:**
  - Häufiger Tausch des Endgeräts → Zuordnen zu einem Benutzer unmöglich

- Zuordnung Benutzer + Gerät + Nutzungskontext ist essentiell!

Mobile Identity Management

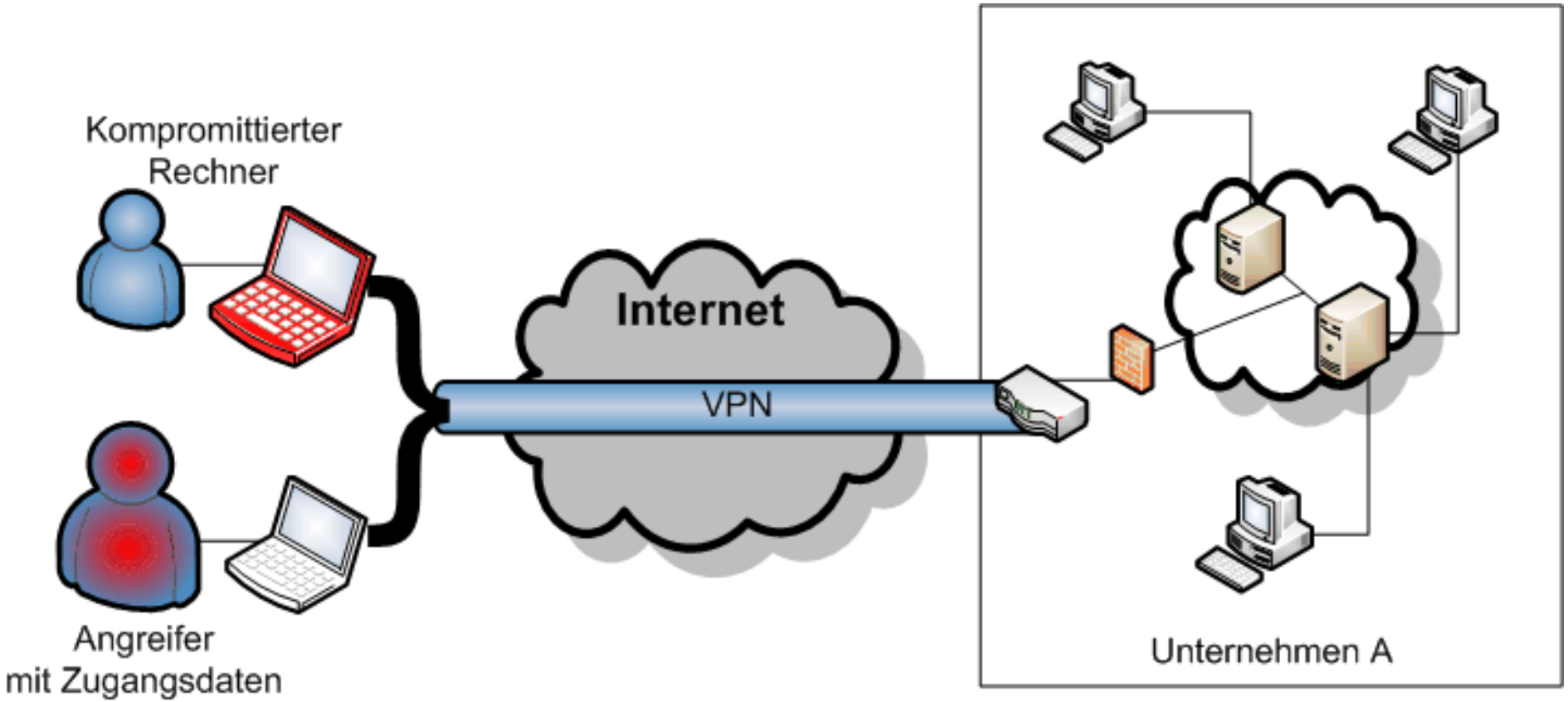
Klassisches Beispiel einer Einwahl …



Ein Mitarbeiter verbindet sich über VPN mit dem Unternehmen.

Mobile Identity Management

Klassisches Beispiel einer Einwahl …



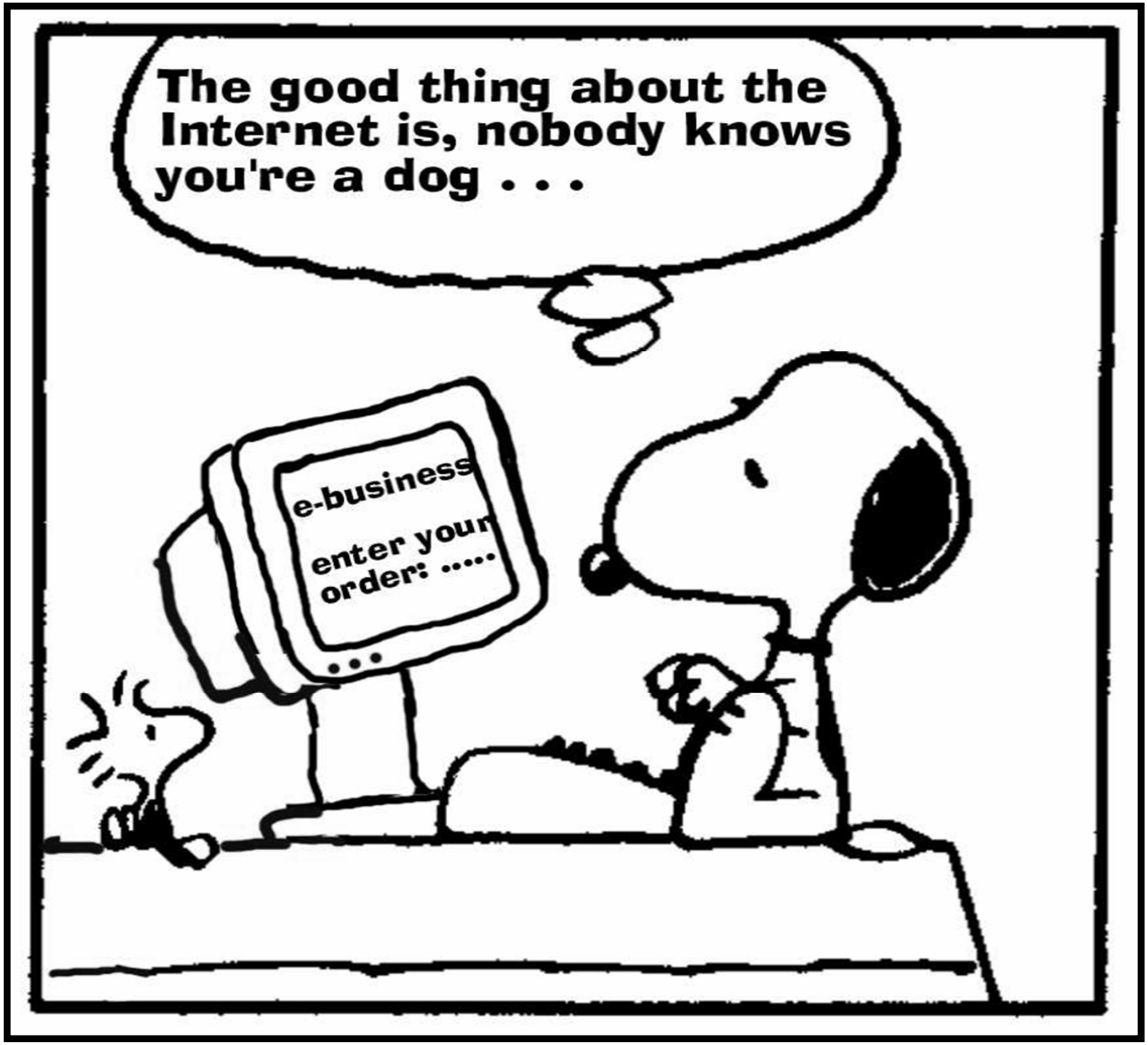
Warum Trusted Computing?

- Applikationssicherheit umfasst
  - Transaktionen und Prozesse eines Benutzers
  - Sicherheitskritische Daten

- Administration der applikatorischen Berechtigungen ist komplex und aufwändig. (Kontrolle gelingt nur unzureichend …)

- Konventionelle Zugangssteuerungssysteme im Netzwerkbereich sind hierfür bis dato unzureichend …
  - Es wird nicht erfasst, welches Gerät mit welchen Eigenschaften und welcher Benutzer in welchem Kontext (Rolle) den Zugang zu einer Ressource im Netz anfragt.

Mobile Identity Management



Mobile Identity Management

Anwendungssicherheit bedingt die Prüfung der Identität!

Warum Trusted Computing – Integrität von Kommunikationsendpunkten

- Vertrauenswürdigkeit und Zuverlässigkeit der kommunizierenden Endpunkte (z.B. Client und Server) hinsichtlich ihrer Integritätsbedingungen und ihrer Identitäten.

- **Integrität:**
  - Relative “Reinheit” von Endpunkten bezüglich eingesetzter Software und Hardware.
  - Reinheit ist Aussage über das Gefahrenpotential …: Was es bei sich selbst und beim Kommunikationspartner anrichten kann:
    - Angriffe und schadhafter Code.

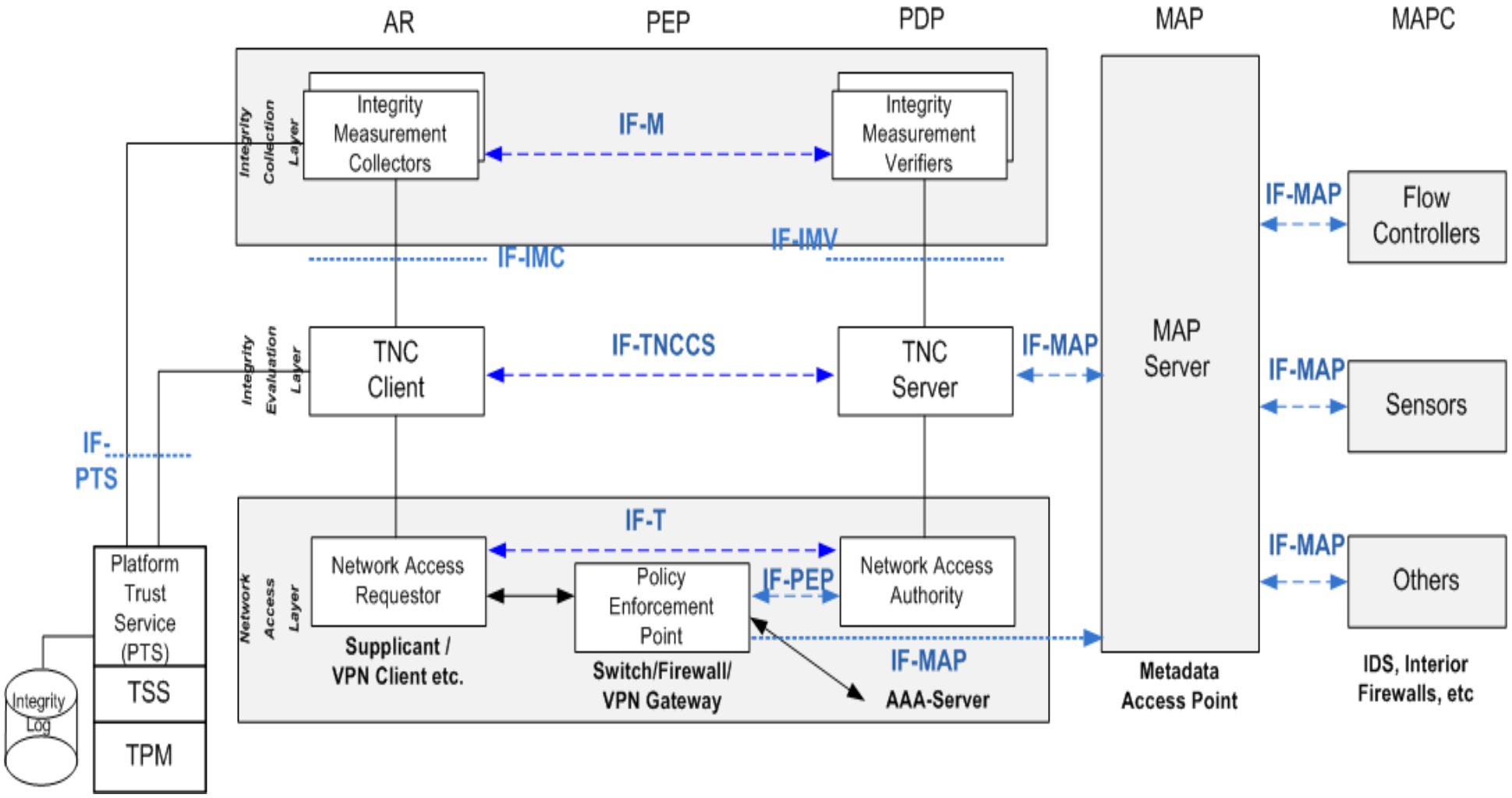
Mobile Identity Management

TNC- Trusted Network Connect

- TNC-Standard von der Trusted Computing Group (TCG) spezifiziert.
  - (aktuelle V1.4 – Mai 2009)
- Schafft einen gemeinsamen, offenen Standards zur Integritätsprüfung von Kommunikationsendpunkten, die einen Netzwerkzugang anfragen.
- Steuert Zugriff für Netzwerke Policy-abhängig.
- Verhindert jedwede Modifikation des Endgeräts.
- Schließt Sicherheitslöcher aus, z.B. aufgrund:
  - fehlerhafter und schwacher Gerätekonfiguration
  - Sicherheitsprobleme in Softwareanwendungen
  - Sicherheitsprobleme im Betriebssystem

Trusted Network Connect

TNC Architektur/Spezifikation 1.4 (Mai 2009)



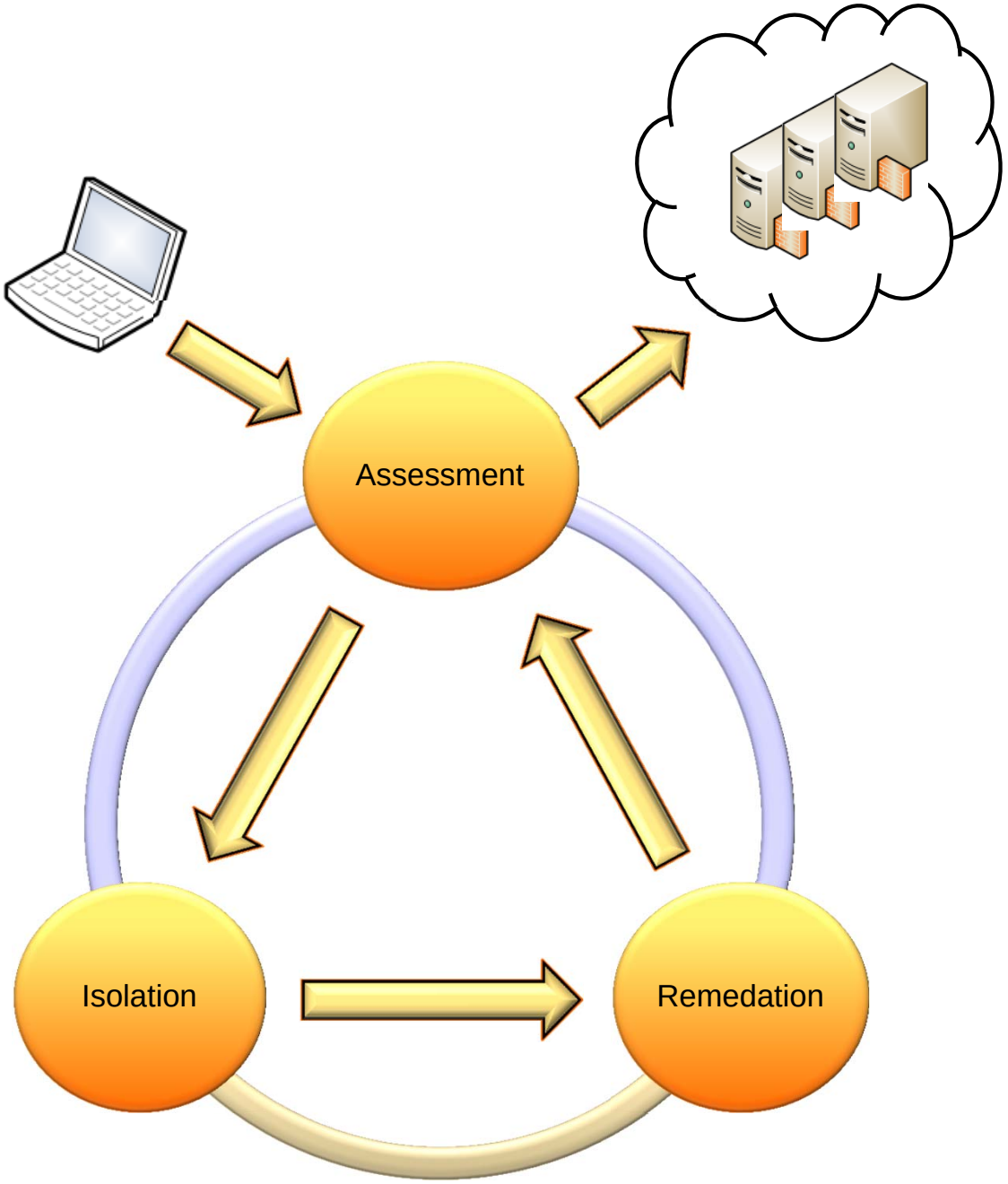
TNC- Trusted Network Connect

- **Integritätsprüfung**

- Assessment
  - Messen des Systemzustands (Konfiguration des Endgeräts).
  - Überprüfung des Zustands gemäß Security Policy.

- Isolation
  - Bei Nichterfüllung der Security Policy Auslagern in eine Quarantänezone.

- Remediation
  - Nach Wiederherstellung der Integrität Wiedereingliederung.



TNC- Trusted Network Connect

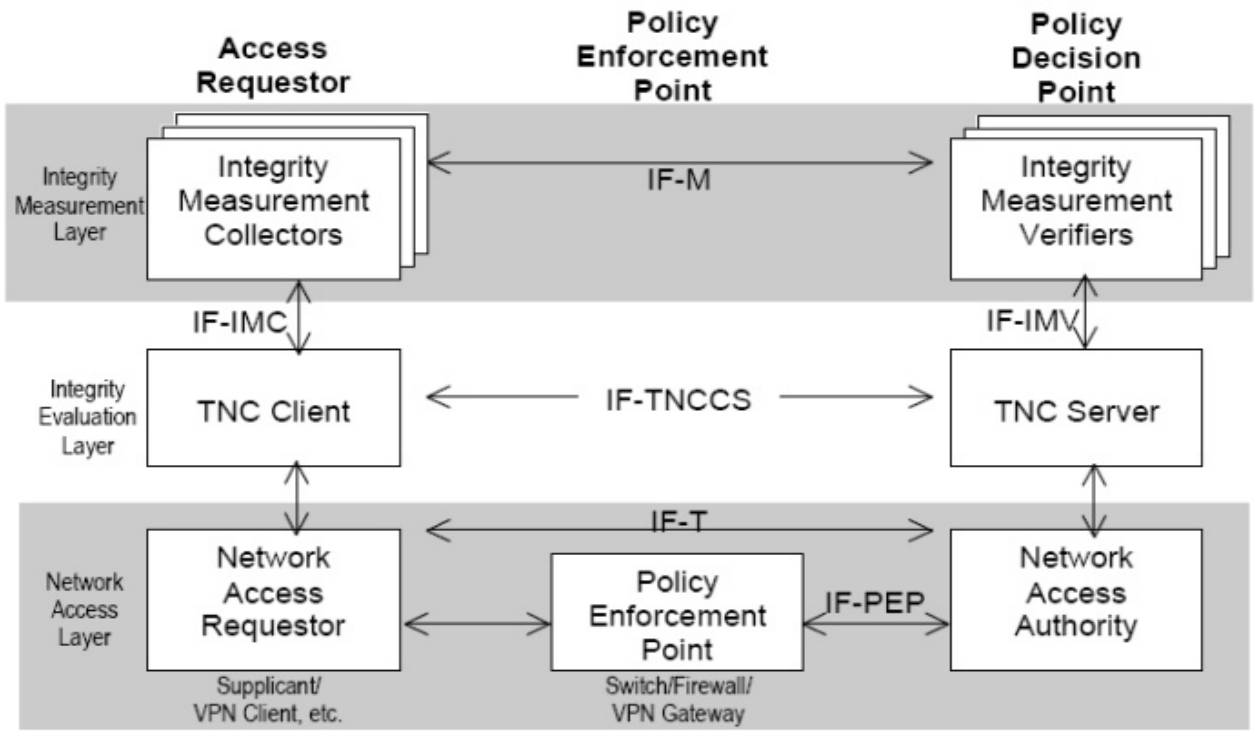
- Erweiterter Integritätscheck
  - Bindet Zugangsdaten an ein bestimmtes Rechnersystem
  - Signiert Messwerten
- „State Check“ (Health Check) des Endgeräts, typischerweise:
  - Version der Antivirus-Software
  - Konfiguration der Personal Firewall (falls vorhanden)
  - Konfiguration der Anwendungsprogramme
  - Patch-Level des Geräts (Firmware)
  - Patch-Level des Betriebssystems
- Trusted Services; TCG-Subsystem stellt Betriebssystemen vertrauenswürdige Dienste und Mechanismen zur Verfügung:
  - Hardware (Trusted Platform Module = TPM) / Firmware
  - Root of Trust for Measurement = RTM
  - Software (Trusted Software Stack = TSS)
- Isolation: Neben der Authentisierung (Benutzer- und Geräteidentifikation) richtet es eine Quarantänezone für ungesichertes Equipment ein.

TNC-Architektur

- **Access Requestor (AR):**
  - ***TNC-Client***
  - Software zur Netzwerkverbindung
  - IMC berichten über Client-Status

- **Policy Decision Point (PDP):**
  - ***TNC-Server***
  - Software kontrolliert den Netzwerkzugang
  - IMV vergleichen IMC-Stati gemäß Security Policy und senden Empfehlung an TNC-Server.

- **Policy Enforcement Point (PEP):**
  - Bewertet IMC-Daten
  - Bewertet TNC-Client



- **IMC** sammeln aktuelle Client-Status-Daten
- **TNC Client** sammelt IMC-Daten und überträgt sie an IMV
- **IMV** werten Messdaten der IMC aus
- **TNC Server:**
  - Steuert den Nachrichtenfluss zwischen IMC und IMV
  - Wertet die Client-Integrität aus

Mobile Identity Management

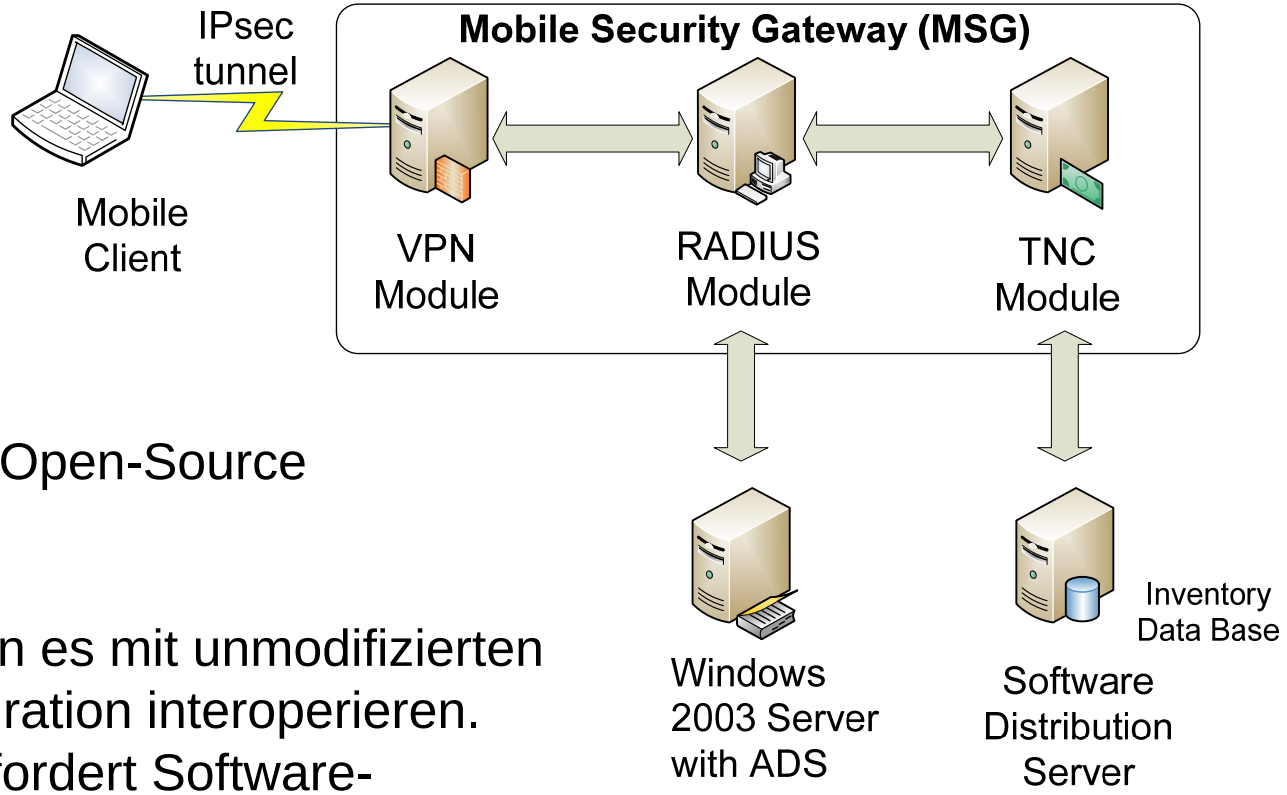
Das SIMOIT-Projekt

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- Im FuE-Projekt SIMOIT (www.simoit.de) wurde ein modulares, Serverseitiges Konzept entwickelt und der TNC-Ansatz in Form eines Prototyps implementiert.

Das SIMOIT-Projekt

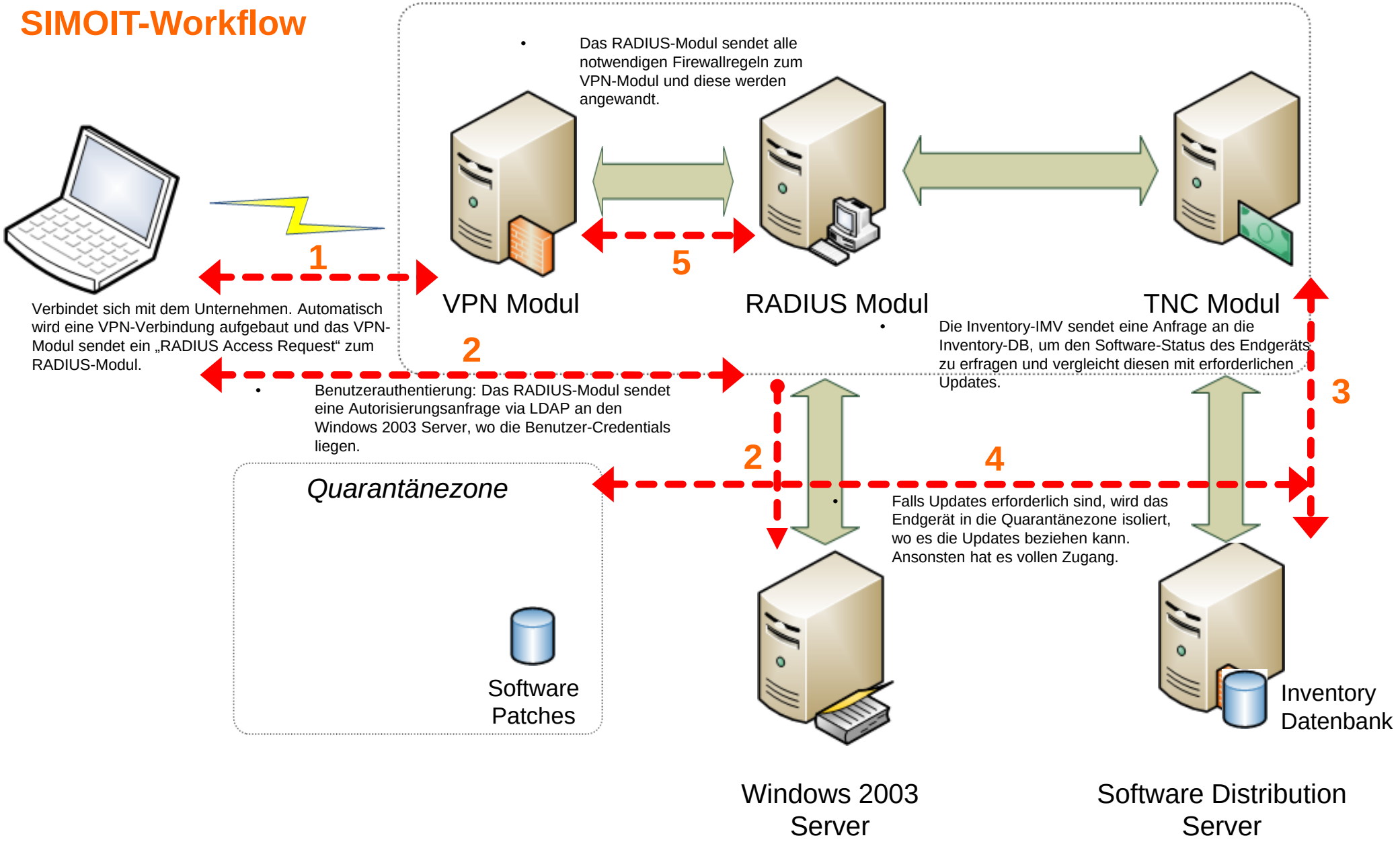
- Kernelement ist das sog. Mobile Security Gateway, das auf folgenden Einheiten besteht:
  - VPN-Modul /Firewall
  - RADIUS-Modul
  - TNC-Modul



- SIMOIT basiert vorangig aus Open-Source Komponenten.
- Als Serverseitige Lösung kann es mit unmodifizierten Clients und Standard-Konfiguration interoperieren. (Die volle TNC-Architektur erfordert Software-Agenten und IMCs im Client).

Mobile Identity Management

SIMOIT-Workflow



Das TNC@FHH-Projekt

- TNC@FHH-Ansatz ist auch eine „Open Source“-Implementierung der TNC-Architektur zur Integritätsprüfung von Endgeräten im Rahmen der Netzwerkzugangskontrolle.
- Es können bestehende Komponenten wie z.B. spezielle Firewall-Systeme eingebunden werden.
- Die TNC-Architektur basiert auf IEEE 802.1x.

- Integritätsprüfung des Clients:
  - Spezielle IMCs erfassen die aktuell laufenden Dienste wie z.B. Telnet und SSH und übermitteln diese Serverseitig an die IMVs, d.h. an den RADIUS/TNC-Server.
  - Die Informationen werden anhand der Security Policy ausgewertet.
  - Genügt das Endgerät der Policy, wird an den Network Access Server (IEEE 802.1x-fähiger Switch/Router) signalisiert, dass dieser dem Client den Netzwerkzugriff erlauben soll.

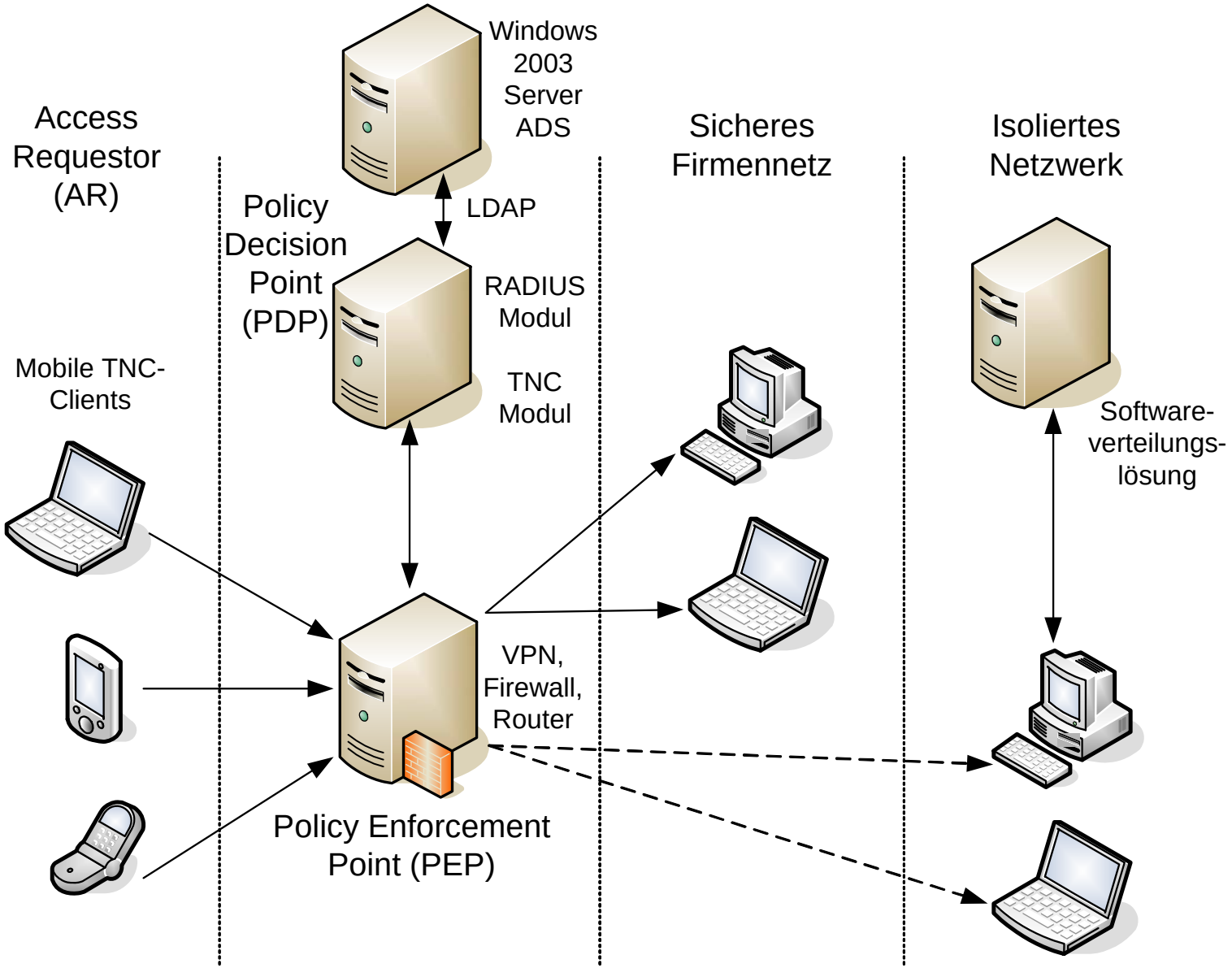
Mobile Identity Management

Vergleich SIMOIT ←→TNC@FHH

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen	TNC@FHH
➡ Speziell angepasster RADIUS-/TNC-Server (libtnc).	➡ Selbst entwickelte TNC-Client- und Server-Software (IMC/IMV-Paare sowie SW-Pakete TNCUtil und NAA-tncs).
➡ Softwareverteilungslösung sorgt dafür, dass die aktuelle Security Policy eingehalten wird.	➡ Prüfung der erlaubten Dienste (Ports) sorgt dafür, dass die aktuelle Security Policy eingehalten wird.
➡ Sicherer Netzwerkzugriff wird über Firewall erlaubt.	➡ Sicherer Netzwerkzugriff wird über 802.1x-Switch erlaubt.

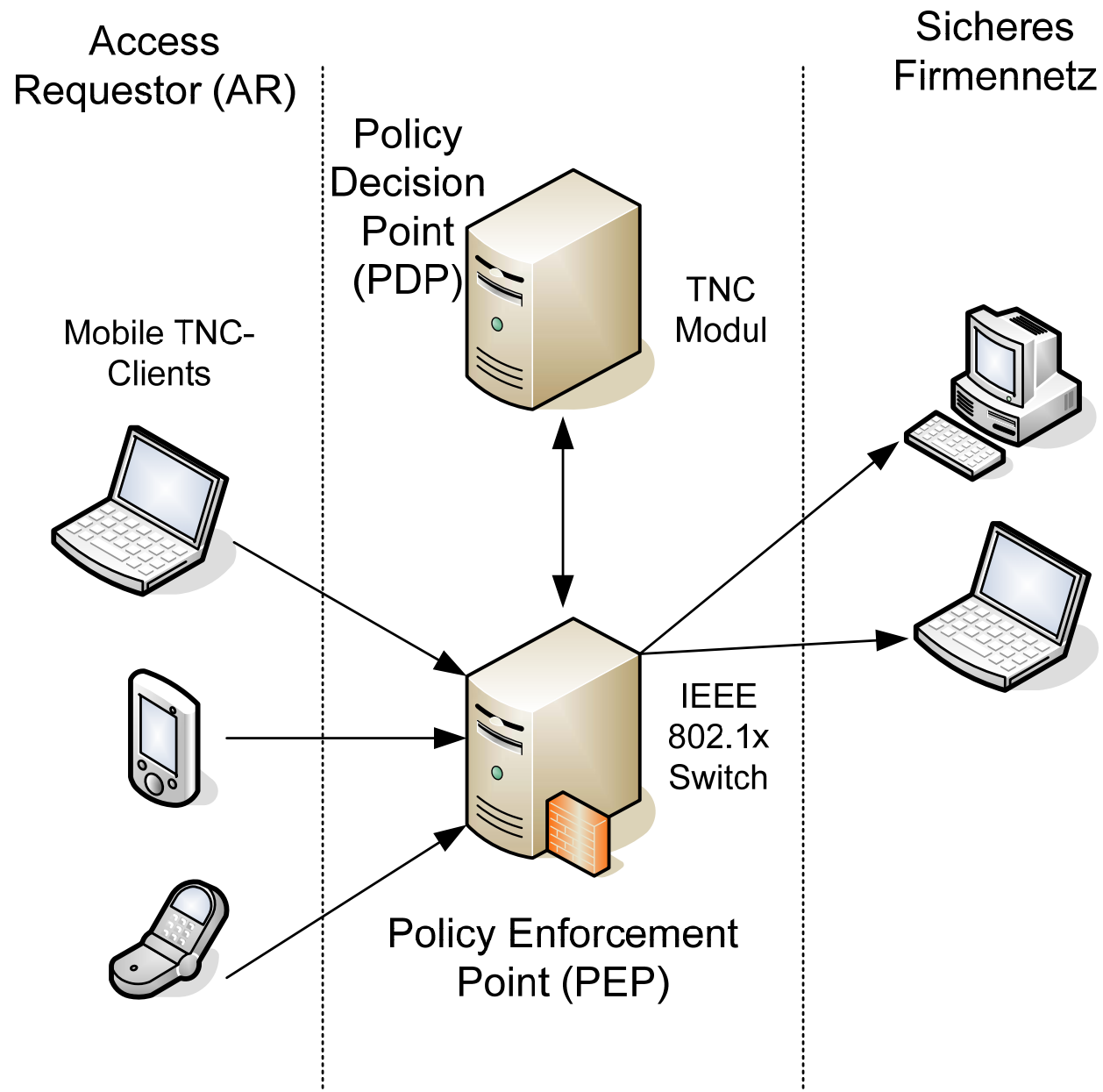
Mobile Identity Management

SIMOIT



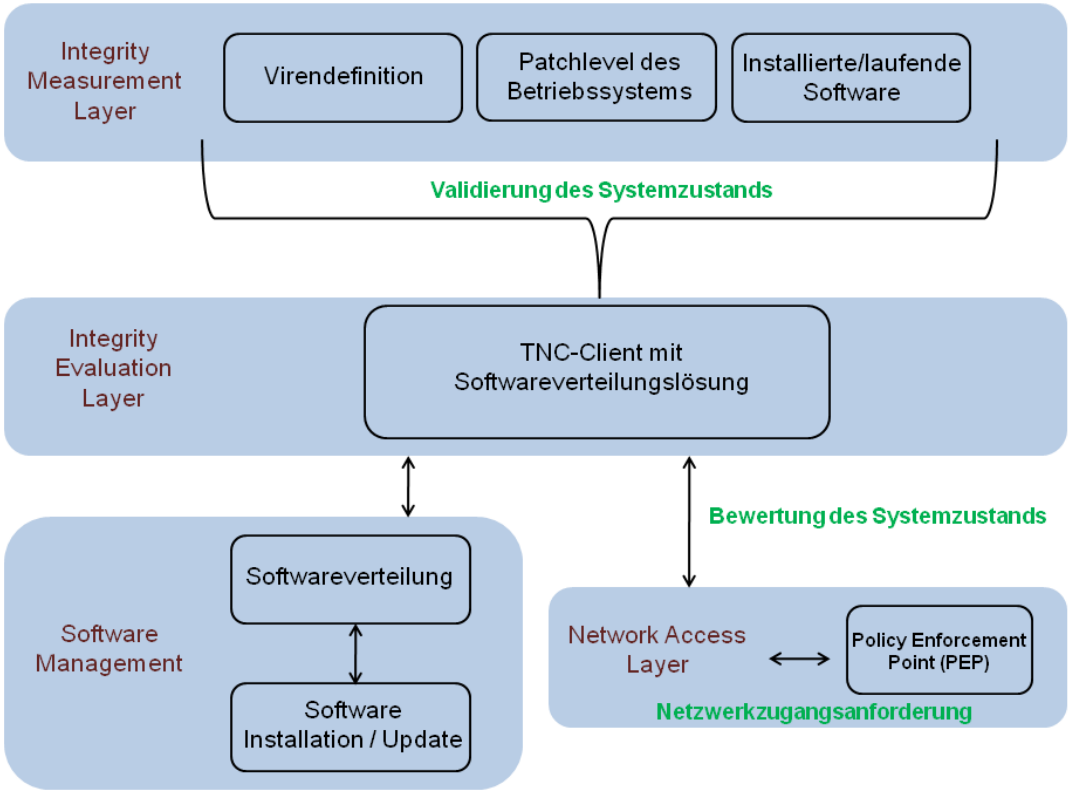
Mobile Identity Management

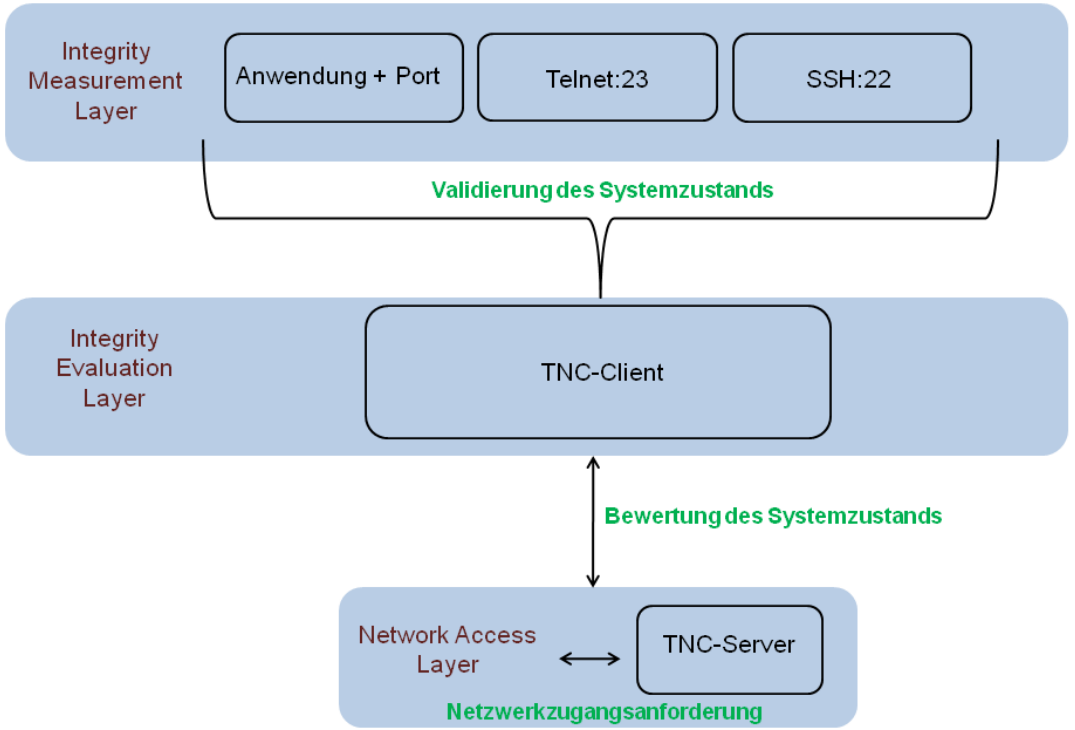
TNC@FHH



Mobile Identity Management

Vergleich SIMOIT und TNC@FHH





Laboratory for IT-Security Architectures

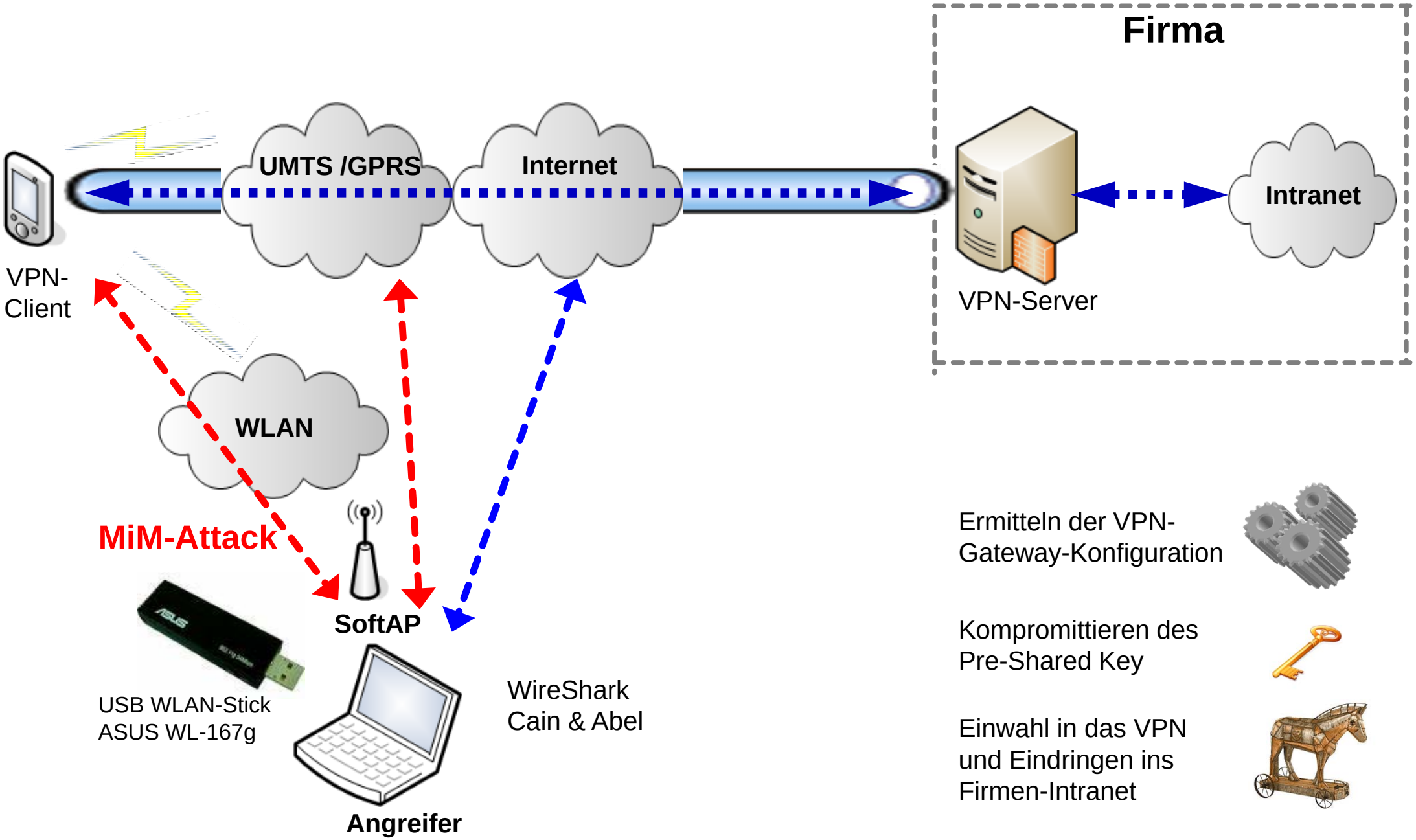
Fazit

- Nahtlose Integration von mobilen Benutzern in bestehende Netze durch ein zentrales Identity Management ist kein einfaches Unterfangen.
- Plattform-unabhängige Lösungen fehlen am Markt und sind meist proprietär.
- Insbesondere KMU benötigen flexible und einfach administrierbare Lösungen, da sie mit knappen Ressourcen auskommen müssen und sich keine Abteilung für IT-Sicherheit leisten können.
- Die vorgestellten TNC-Ansätze SIMOIT und TNC@FHH sind unterschiedliche „Trusted Computing“-Implementierungen für mobile Szenarien.
- SIMOIT fokussiert auf den Konfigurationsstatus (Software) des Endgeräts, TNC@FHH dagegen auf den Dienststatus (Ports).
- Beide Ansätze sind modular aufgebaut, so dass auch andere Herstellerlösungen (z.B. VPN-Gateways oder Firewalls) integriert werden können.
- Sie erlauben ein skalierbares und relativ hohes Sicherheitsniveau für mobiles Identity und Access Management.
- Sie wurden im *Laboratory for IT-Security Architectures* in einer typischen IT-Sicherheitsreferenzinfrastruktur implementiert und validiert.

Fazit

- In Zukunft sollen TNC-Clients für unterschiedliche mobile Betriebssysteme (Windows Mobile 6.1, Android und Symbian) entwickelt werden, damit der Einsatzbereich nicht nur auf Laptops beschränkt ist, sondern auch Smartphones sicher in ein Unternehmensnetz im Sinne des Trusted Computing eingebunden werden können.

Live-Hacking Szenario



Ermitteln der VPN-Gateway-Konfiguration

Kompromittieren des Pre-Shared Key

Einwahl in das VPN und Eindringen ins Firmen-Intranet

Live-Hacking Szenario

Live-Hacking Szenario

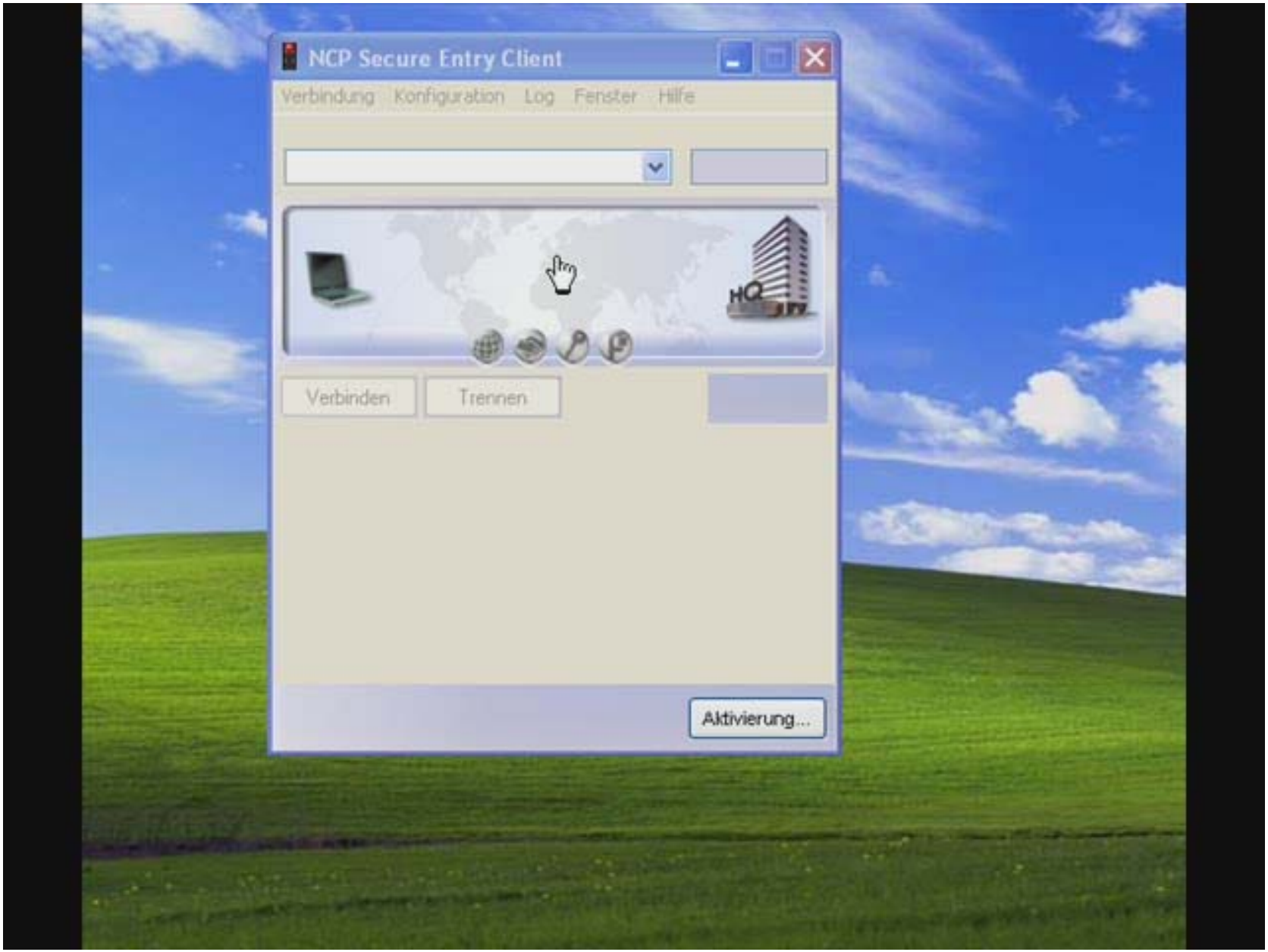
Live-Hacking Szenario

Live-Hacking Szenario

Live-Hacking Szenario

Live-Hacking Szenario

Live-Hacking Szenario



Laboratory for IT-Security Architectures

Lessons learned …

- Identitätsprüfung auf Basis von Credentials (Benutzername und Passwort, bzw. ID) reicht nicht aus!
- Gruppenidentifikation vermeiden!

- Stattdessen:
  - Mehrfaktorenauthentifizierung: Benutzer + Gerät
  - Kontextabhängige Prüfung
  - Profile
  - Kombination aus 802.1X+EAP+RADIUS+TNC

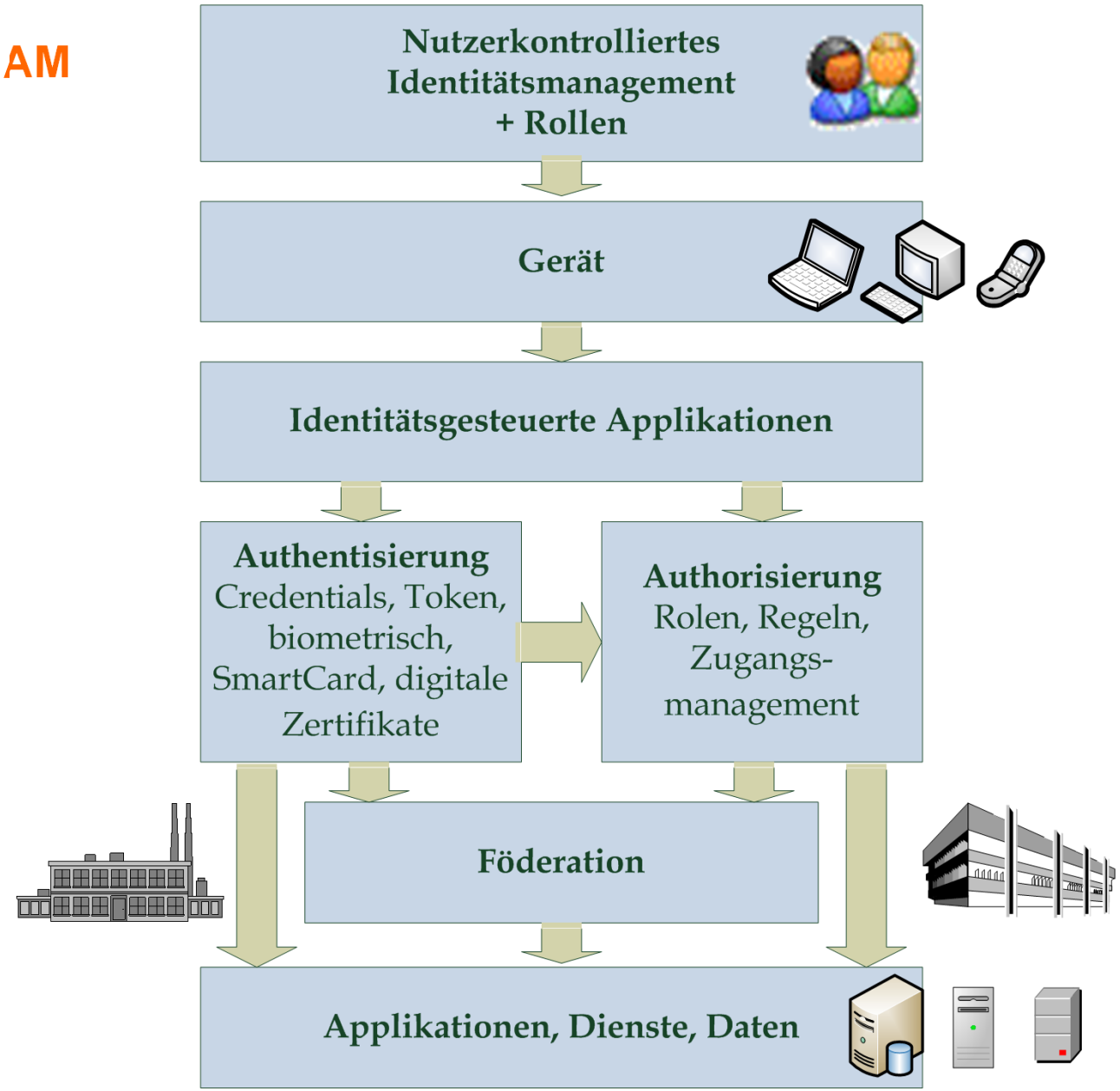
Mobile Identity Management

Multilevel Trusted Computing

Benutzer	Verlässliche Identifikation des Benutzers zur Autorisierung/Authentisierung beim Zugang zu Netzen und Diensten.
Gerät	Verlässliche Identifikation des Endgerätes zur Autorisierung und Authentisierung beim Zugang zu Netzen und Diensten.
Daten	Vertraulichkeit, Integrität und Verfügbarkeit von Daten.
System	Vollständige und nachhaltige Überprüfbarkeit der Sicherheit aller Systemkomponenten: Zustände und Konfigurationen müssen eindeutig, transparent und verständlich sein.
Organisation	IT-basierte Geschäftsprozesse benötigen Administration und Steuerung von Zugangsberechtigungen mit automatisierter und Rollenbasierter Zuweisung/ Rücknahme von Benutzerprivilegien – “User-Provisioning”.

Mobile Identity Management

Föderatives IAM



Vielen Dank …

Haben Sie Fragen?