# VOGUE-Workshop

## Der Trusted Computing Ansatz im Android-Umfeld

VOGUE

*Prof. Dr.-Ing. Kai-Oliver Detken*

*DECOIT GmbH, http://www.decoit.de, detken@decoit.de*

# Kurzvorstellung

- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Entwicklung von Internet-Projekten
- Schaffung innovativer eigener **Produkte**
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen

VOGUE

# Inhalte

- IT-Sicherheitsfaktoren
- Eigenschaften mobiler Endgeräte
  - Mobile Betriebssystemkonzepte
  - Neue Sicherheitsrisiken
  - Vergleich mobiler Betriebssysteme
- Trusted Network Connect (TNC)
  - Architektur
  - Aufgaben
- Das VOGUE Projekt
  - Motivation und Hintergrund
  - Ansatz
  - Plattform
  - Projektstatus
- Fazit und Ausblick

VOGUE

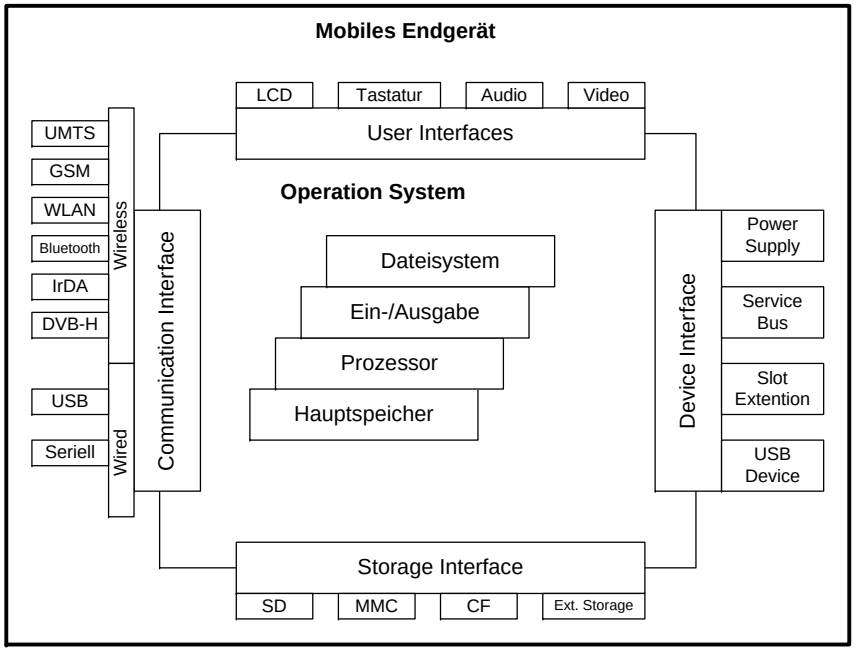
# IT-Sicherheitsfaktoren

- Ganzheitliche Sicherheit in einer IT-Infrastruktur verlässt sich im Wesentlichen auf folgende Faktoren
  - Zugangssteuerung/Zugriffskontrolle
  - Integrität
  - Originalität (Authentizität)
  - Authentifizierung
  - Autorisierung
  - Vertraulichkeit
  - Verfügbarkeit
  - Audit

VOGUE

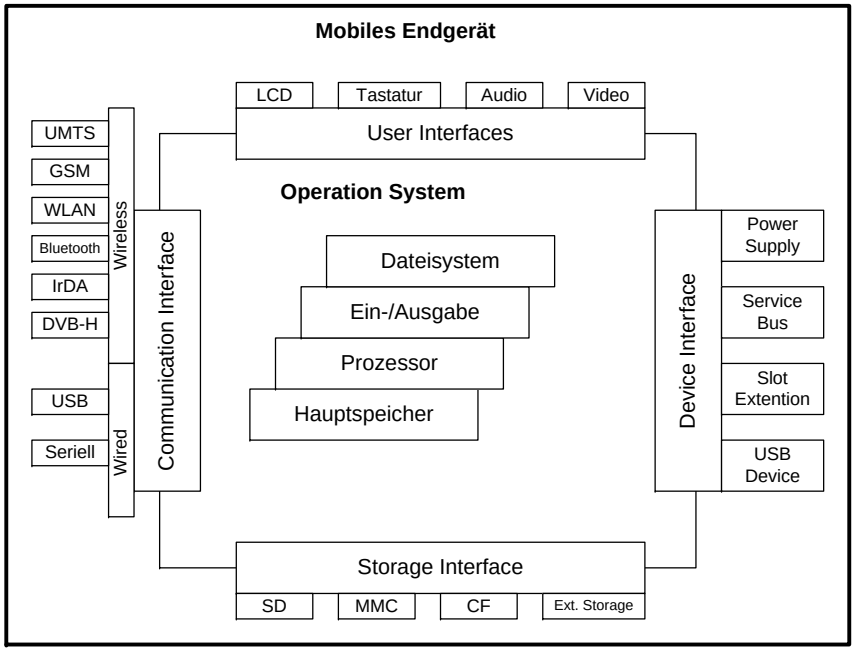
# Eigenschaften mobiler Endgeräte (1)

- **Mobiler Endgeräte:**
  - Zunehmende Integration von Funktionalitäten und Schnittstellen in mobile Endgeräte
  - Zusammenführung ursprünglich verschiedener Geräteklassen (Handy und PDA )
  - Leistungsfähigere Endgeräte
  - Mobile Endgeräte werden zudem als digitale Assistenten eingesetzt



# Eigenschaften mobiler Endgeräte (2)

- **Dienste:**
  - Verstärkte Verbreitung von echten mobilen Diensten
  - Spezifischen Eigenschaften und Fähigkeiten der mobilen Endgeräte werden genutzt
  - Neue Benutzungsparadigmen wie „Digital Lifestyle“ oder „Ubiquitous Computing“ verändern die Anforderungen an mobile Dienste
  - Bedienbarkeit und Kommunikationsfähigkeit ist wichtig
  - Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet



# Mobile Betriebssystemkonzepte (1)

- **Virtuelle Speicherverwaltung:**
  - Zuordnung von Speicherbereichen zu Applikationen und Diensten
  - Stellt sicher, dass mehrere aktive Anwendungen sich nicht gegenseitig negativ beeinflussen können
  - Dies betrifft z.B. die Daten anderer Programme oder deren Speicher
- **Java-Einsatz:**
  - Eigenes Java-Speicherschutzkonzept
  - Java sichert die Anwendungen zueinander ab, ohne auf die virtuelle Speicherverwaltung zurückgreifen zu müssen
- **Dateisysteme:**
  - Persistente Speicher werden verwaltet
  - Sind nach Neustart weiterhin verfügbar (Benutzerdaten)
  - Speicher wird durch Dateisysteme organisiert
  - Kontrolle von Dateizugriffen notwendig, um nur bestimmten Benutzern den Zugriff zu gestatten

# Mobile Betriebssystemkonzepte (2)

- **Kryptografische Verfahren:**
  - Verschiedene Verschlüsselungsverfahren sind im Einsatz je nach Gerät
  - Implementierung hängt davon ab, wie sicher diese Verfahren angewendet werden können
  - Handhabung kann Konfiguration erschweren, wodurch Sicherheitslücken entstehen
- **Zugangskontrollen:**
  - Authentifizieren des Benutzers für den Zugriff auf seine persönlichen Daten
  - Unterscheidung der Zugriffskontrolle bei verschiedenen Benutzern
- **Erweiterbarkeit:**
  - Hersteller haben Interesse an der kontrollierten Erweiterbarkeit vorhandener Gerätebasen
  - Ermöglicht eine höhere Flexibilität des Benutzers, der das Endgerät auch mit anderer Hardware nutzen möchte

VOGUE

# Neue Sicherheitsrisiken

- Fehlerhafte Konfiguration
  - Fehlkonfigurationen in Sicherheitskomponenten wie Firewalls, VPN-Gateways etc.
  - Betriebssystemfehler der Handys
- Offene mobile Endpunkte
  - Zugriff und Verwaltung von kritischen Geschäftsdaten
  - Keine Integritätsüberprüfung der Hardware ist möglich
  - Wachsender Malware-Markt für Smartphones
  - Verwendung von mobilen Endgeräten in unsicheren Netzen

# Vergleich mobiler Betriebssysteme

- Vorteile für Android:
  - Das Betriebssystem ist quelloffen und kann daher beliebig erweitert werden
  - Durch Open Source können die implementierten Sicherheitsmechanismen untersucht werden
  - Betriebssystem kann auch auf stationären Rechnern zum Einsatz kommen und eignet sich daher auch für andere mobile Endgeräte
  - Zusätzliche Applikationen (Apps) können jederzeit für Android entwickelt werden

| *Eigenschaften* | **SymbianOS** | **Windows Mobile** | **PalmOS** | **RIM** | **Android** | **Apple iOS** |
|---|---|---|---|---|---|---|
| Mehrbenutzersystem | Nein | Nein | Nein | Nein | Ja | Nein |
| Multitasking | Ja | Ja | Ja | Ja | Ja | Ja |
| Speicherverwaltung | Ja | Ja | Ja | Ja | Ja | Ja |
| Dateisysteme | Ja | Ja | Ja | Ja | Ja | Ja |
| Verschlüsselung | Ja | Ja | Ja | Ja | Ja | Ja |
| Zertifikate | Ja | Ja | Ja | Ja | Ja | Ja |
| Handhabung | Gut | Mittel | Gut | Gut | Gut | Sehr gut |
| Verbreitung | Gut | Gering | Gering | Gut | Gering | Sehr gut |
| Quelloffen | Nein | Nein | Nein | Nein | Ja | Nein |

# Trusted Network Connect (TNC)

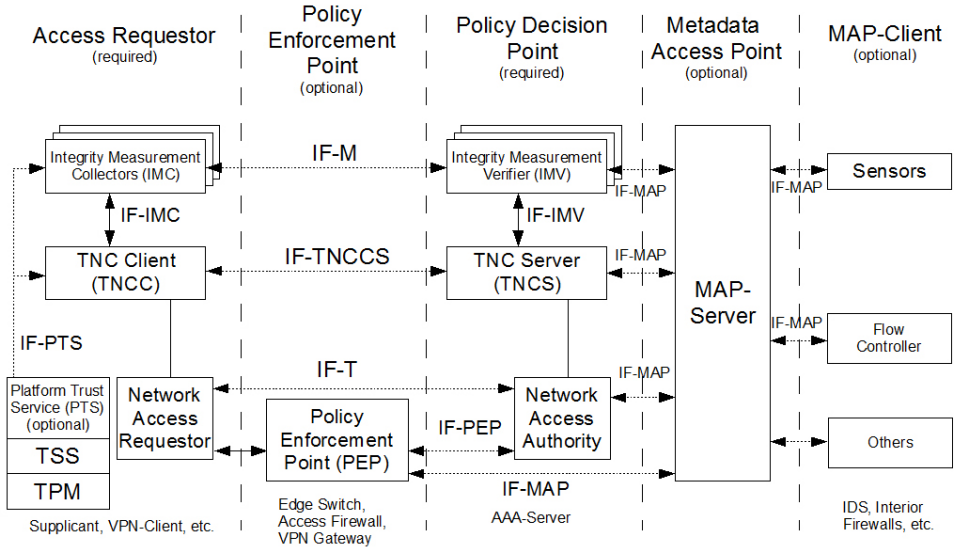
- TNC ist eine offene Architektur für Network Access Control (NAC), standardisiert durch die Trusted Network Connect Working Group (TNC-WG) von der Trusted Computing Group (TCG)
- Die Spezifikation stellt die „Reinheit“ von Endpunkten sicher: es kann durch Authentifizierungs- und Autorisierungsinformationen eine Zustandsprüfung („Health Check“) erfolgen, die sicherstellt, dass das Endgerät den IT-Sicherheitsregeln des Unternehmens entspricht
- Die TNC-Architektur ist somit die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten
- Die Architektur bezieht dabei schon bestehende Sicherheitsaspekte mit ein, wie Virtual Private Network (VPN), IEEE 802.1x (802.1x), Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), Hyper-Text Transfer Protocol Security (HTTPS)

VOGUE

TRUSTED COMPUTING GROUP™

# Architektur des TNC-Ansatzes

- Richtlinien-abhängige Zugriffssteuerung für Netzwerke
  - Integritätsprüfung: Messen des Systemzustands (Konfiguration der Endgeräte) und Überprüfung dieser Zustände gemäß Richtlinien (Assessment-Phase)
  - Isolation von potentiell gefährlichen Rechnersystemen bei Nichterfüllung der Richtlinien (Isolation-Phase)
  - Wiedereingliederung nach Wiederherstellung der Integrität (Remediation-Phase)
- Erweiterter Integritätscheck möglich (z.B. Binden von Zugangsdaten an ein bestimmtes Rechnersystem, Signierung von Messwerten)




TNC Architecture for Interoperability Version 1.4, Revision 4

VOGUE

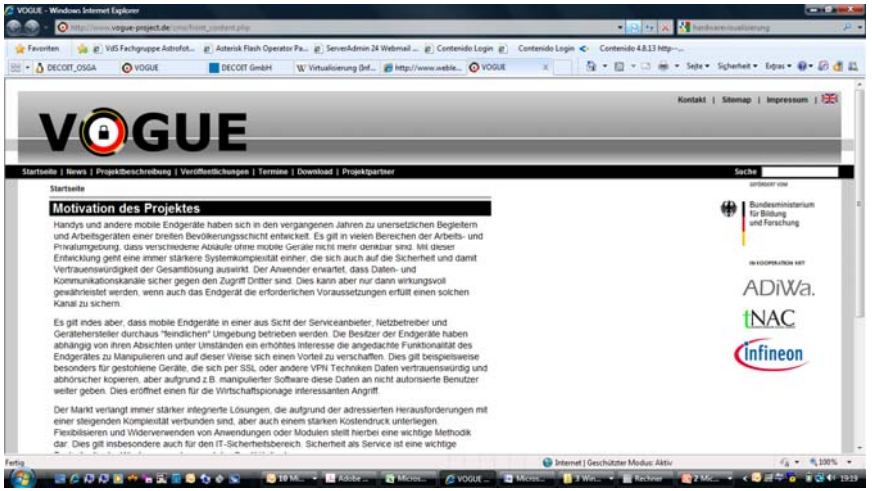
# Zusammenfassung der TNC-Aufgaben

- Eindeutige Erkennung von Zugangsversuchen und die Identifizierung der Endgeräte
- Vergleich mit den Policys und das Umsetzen von Sicherheitsrichtlinien
- Isolierung und im besten Fall die automatische Korrektur bei fest gestellten Richtlinienverletzungen
- Erstellung und Verwaltung der Richtlinien sowie die Auswertung der Ereignisse und gesammelten Daten

VOGUE

# Das VOGUE-Projekt

- Das VOGUE-Projekt ist ein nationales BMBF-Projekt (URL: http://www.vogue-project.de)
- VOGUE startete im Oktober 2009 und wird im September 2011 enden
- Folgende Partner sind in diesem Projekt involviert:
  - DECOIT GmbH (Konsortialführer)
  - Fraunhofer SIT (Darmstadt)
  - Mobile Research Center (Bremen)
  - NCP engineering GmbH (Nürnberg)
  - OTARIS (Bremen)



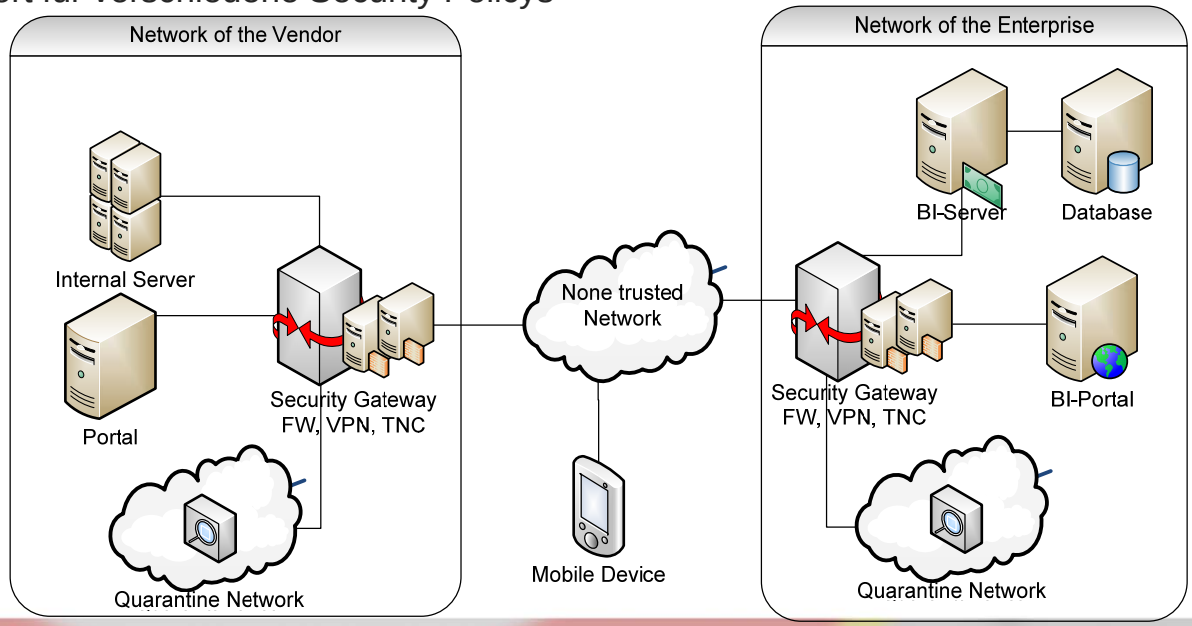
# Ziele des Projektes

- Erschließen des aufkommenden Marktes von TPM-basierten Lösungen im mobilen Bereich für die deutsche Wirtschaft
- Entwicklung einer Basis zur Erprobung von TPM-basierten Lösungen unter Verwendung eines Emulators der KMUs den Einstieg in dieses neue Geschäftsfeld ermöglicht
- Ermöglichen von sicherheitskritischen und mobilen Geschäftsprozessen durch die Etablierung einer vertrauenswürdigen Plattform für mobile Endgeräte. Hierdurch wird bereits möglichen Angriffen vorgebeugt bzw. deren Schaden drastisch reduziert
- Demonstration auf der Basis einer verbreiteten Plattform für mobile Endgeräte

VOGUE

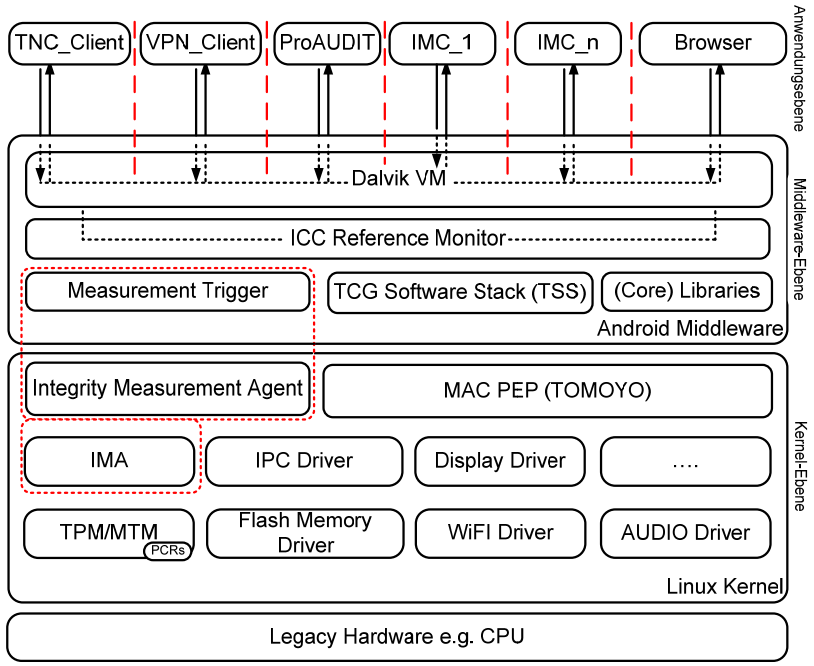
# Motivation und Hintergrund

- Es wurde im ersten Arbeitspaket ein generisches Szenario aus unterschiedlichen Anwendungsfällen entwickelt
- Zwei verschiedene Netze werden mit unterschiedlichen Sicherheitsrichtlinien verwendet
- Folgendes Sicherheitsniveau haben wir heute:
  - Keine Sicherheitsüberprüfung der Software (Patches)
  - Keine Hardware-Kontrolle verfügbar
  - Kein Support für verschiedene Security Policys



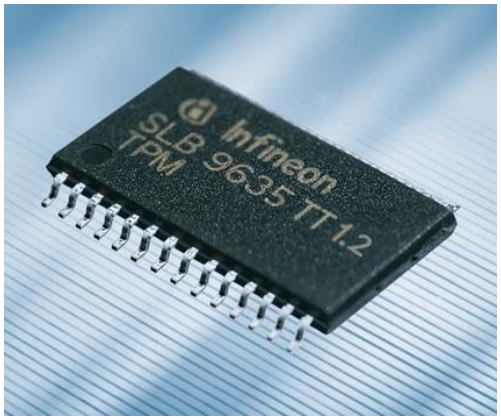
# Der VOGUE-Ansatz (1)

- Mobile Betriebssysteme wie Android ermöglichen die Entwicklung von Anwendungen (offene Plattform)
- Root-of-Trust Implementierung durch das Mobile Trusted Module (MTM) möglich
- MTM/TPM-Software- Emulation wird für die Entwicklung eingesetzt
- Es wird die Integrity Measurement Architektur (IMA) als Kernel-Erweiterung eingesetzt, um die Integrität weiterer Kernel-Module, Middleware mit ausführbaren Codes, Konfigurationsdateien, Skripte, dynamische Bibliotheken vor der Ausführung messen zu können
- TOMOYO wird als Referenzmonitor eingesetzt, der nicht erlaubte Interaktionen bzw. nicht autorisierte Zugriffe auf Gerätressourcen auf Kernel-Ebene unterbindet



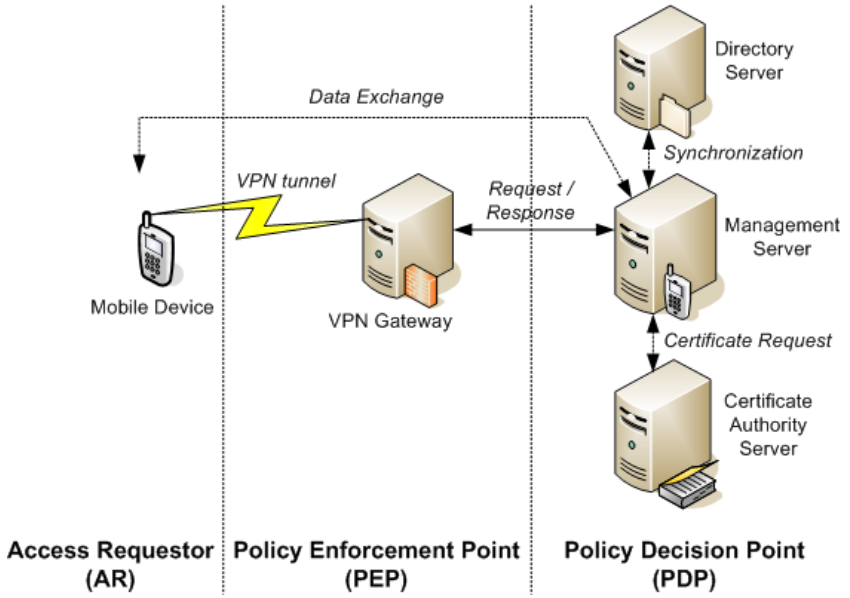
# TPM-/MTM-Chip

- Es wird ein Vertrauensanker empfohlen, der die Basis für die Plattformintegrität und weitere auf dem Gerät realisierte Sicherheitsfunktionalitäten bildet
- Von diesem Modul wird beim Gerätstart eine ununterbrochene Vertrauenskette aufgebaut, die bis hin zu den Android-Apps erweitert werden kann
- Der Vertrauensanker kann entweder ein Trusted Plattform Modul (TPM) oder ein oder mehrere Mobile Trusted Modules (MTMs) sein
- MTMs sind, im Gegensatz zu TPMs aus der Rechnerwelt, explizit für mobile und eingebettete Geräteplattformen unter Berücksichtigung der besonderen mobilen Anforderungen (z.B. Netzwerkbetreiber oder Gerätebesitzer, bzw. -Benutzer) entworfen worden
- Beide Technologien, MTM bzw. TPM, sind von der TCG spezifiziert worden



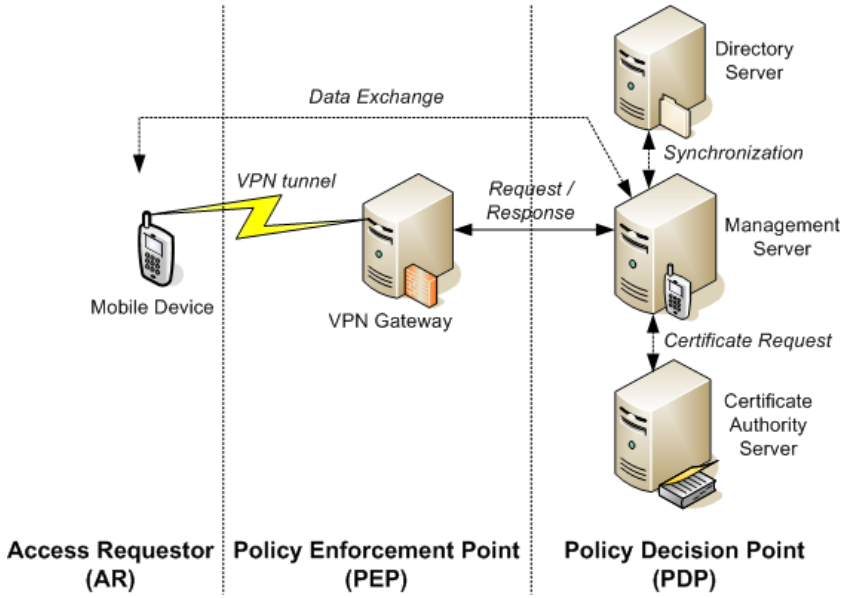
# Der VOGUE-Ansatz (2)

- Die Kernelements von VOGUE sind:
  - VPN Gateway
  - Management Server (z.B. RADIUS, TNC-Server)
  - Directory Server (z.B. LDAP)
  - CA-Server
  - TPM/MTM-Chip
  - TNC-Client auf Android



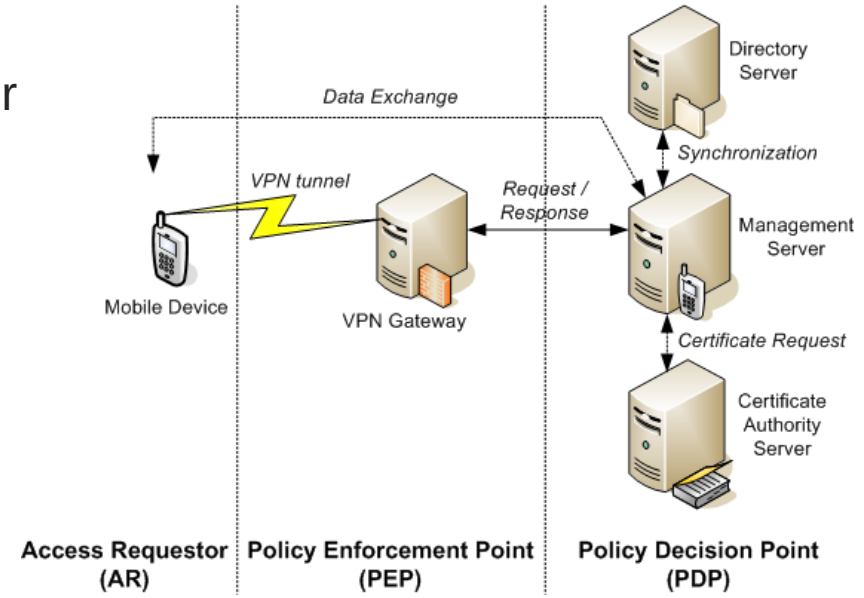
# VOGUE-Mechanismen (1)

- Jede Benutzergruppe besitzt verschiedene Sicherheitsrichtlinien für unterschiedliche Zugriffsrechte
- Das Managementsystem synchronisiert kontinuierlich in festgelegten Intervallen die Benutzerinformationen mit dem Verzeichnisdienstserver
- Das beinhaltet, das Benutzer des Verzeichnisdienstservers mit VPN-Zugriffsrechten, solange keinen Zugriff haben, solange keine Intervallsynchronisierung stattgefunden hat



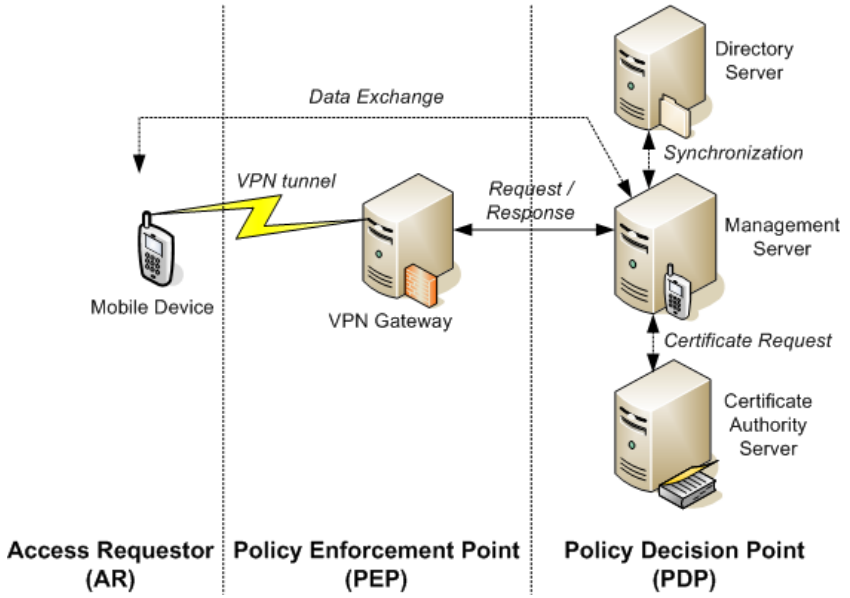
# VOGUE-Mechanismen (2)

- Optional kann eine Certification Authority (CA) in die Architektur integriert werden, um Zertifikate auf dem Management-Server für die Benutzer verwenden zu können
- Bei Verwendung einer CA, wäre der Management-Server eine Registration Authority (RA)
- Das VPN-Gateway wird so konfiguriert, dass alle eingehenden Client-Abfragen über den Management-Server autorisiert werden müssten
- Das VPN-Gateway muss dabei nicht separat die Teilnehmer enthalten, sondern gleicht sich automatisch mit dem Management-Server ab



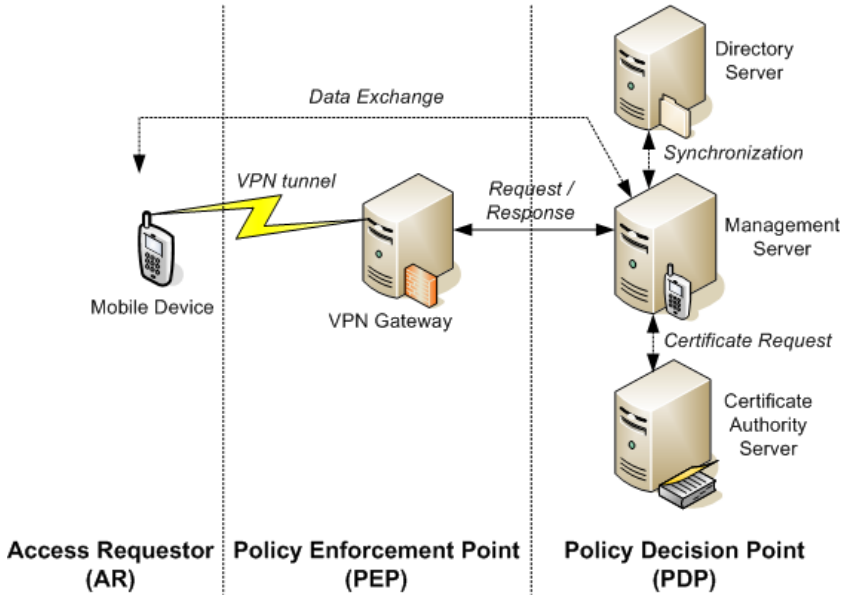
# VOGUE-Mechanismen (3)

- Nach der Authentifizierung des Benutzers wird sein Smartphone (Hardware- und Software-Konfiguration) überprüft, ob es den Anforderungen der TNC-Richtlinien entspricht
- Nach der Etablierung der VPN-Verbindung, wird der Zugriff des Smartphones auf die Quarantänezone begrenzt
- In dem Bereich der Quarantänezone ist es nur möglich Software-Updates vorzunehmen, wie z.B. Anti-Virus-Software oder Betriebssystem-Patches



# VOGUE-Mechanismen (4)

- Der Zugriff auf andere Netzwerkbereiche des Unternehmens ist bis dahin verboten
- Informationen über den Status der mobilen Geräte werden über den Access Requestor (AR) auf dem Smartphone sicher zur Verfügung gestellt
- Der AR beinhaltet:
  - Network Requestor (VPN-Client)
  - TNC-Client (Schnittstelle zwischen AR und Plugin-Software)
  - Integrity Measurement Collector (beschreibt Plugins, die mit dem TNC-Client kommunizieren dürfen)



# Projektstatus von VOGUE

- Die Definition der Anforderungen und mobiler Szenarien wurde beendet
- Die Analyse der mobilen Betriebssysteme ist abgeschlossen worden und wird auf Basis von Android weitergeführt
- Die Emulatoren für die Verwendung von TPM oder MTM stehen zur Verfügung; diese müssen in Zukunft auf die neue Android Version 3.0 angepasst werden
- Die Definition der VOGUE-Architektur wurde abgeschlossen
- Aktuell werden die verschiedenen Module der VOGUE-Plattform (OpenVPN, Funambol, FreeRADIUS, LDAP, libtnc) erweitert, zusammengeführt und getestet
- Die Softwarespezifikationen werden gerade im Detail beschrieben
- Ein erster Demonstrator wird im November fertiggestellt

# Fazit und Ausblick

- Der TNC-Ansatz in VOGUE erhöht den Sicherheitslevel in mobilen Netzen
- Verschiedene Herstellerlösungen sind bereits in der Vergangenheit etabliert worden (z.B. von Microsoft, Cisco Systems)
- Zusätzlich haben Forschungsprojekte das Thema Trusted Computing in den letzten Jahren immer mehr fokussiert:
  - **SIMOIT (http://www.simoit.de):** Das Projekt zielte auf die Entwicklung einer auf Standards basierenden mobilen IT-Sicherheitsplattform ab, die sich in heterogenen mobilen Umgebungen einsetzen lässt.
  - **TNC@FHH (http://trust.inform.fh-hannover.de/joomla/):** ist auch eine Open-Source-Implementierung der TNC-Architektur zur Integritätsprüfung von Endgeräten im Rahmen der Netzwerkzugangskontrolle 802.1x.
  - **tNAC (http://www.tnac-project.org):** ist ein vom BMBF gefördertes Projekt, welches eine vertrauenswürdige Network-Access-Lösung entwickelt. Durch die Integration von Turaya, einer Trusted-Computing-Plattform, soll ein signifikant höheres Sicherheitsniveau erreicht werden.
- Leider fehlen bislang TPM/MTM-Chips in den Endgeräten sowie TNC-Clients

# Vielen Dank für ihre Aufmerksamkeit

# Copyright 2009-2011

*The project VOGUE (http://www.vogue-project.de) is funded by the Federal Ministry of Education and Research (BMBF) of Germany. The project started in October 2009 and will end at September 2011. The authors would like to thank the BMBF for their support. We also wish to express our gratitude and appreciation to all VOGUE partners for their strong support and valuable contribution during the various activities presented in this paper.*

VOGUE