

# BremSec-Forum



## Das SIMOIT-Projekt *Sichere mobile Anbindung*

**SIMOIT** Sicherer Zugriff  
Mobile Mitarbeiter  
IT-Infrastrukturen



*Dr.-Ing. Kai-Oliver Detken*

Business URL: <http://www.decoit.de>

Private URL: <http://www.detken.net>

E-Mail: [detken@decoit.de](mailto:detken@decoit.de)

*Consultancy & Internet Technologies*

## Portfolio der DECOIT GmbH

- ◆ **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



## Agenda

- ◆ Netzwerksicherheit: Stand heute
- ◆ Ziel und Aufgabe des SIMOIT-Projekts
- ◆ Der TNC-Ansatz – die Quarantänezone
- ◆ Schnittstellen im SIMOIT-Projekt
- ◆ Markt Betrachtung
- ◆ Ausblick und Fazit
- ◆ Zusammenfassung

## Netzwerksicherheit: Stand heute

- ◆ Zunehmende Vernetzung und verteilte Systeme
- ◆ Stark zunehmende Gefahr durch Malware (insbesondere Trojaner, Viren und Rootkit-Werkzeuge)
- ◆ Die Absicherung von Netzwerkzugriffen erfolgt meist nur über eine reine Benutzerauthentifizierung
- ◆ Es findet keine Integritätsprüfung der verwendeten Rechnersysteme statt und damit keine Unterscheidung zwischen vertrauenswürdigen/nicht vertrauenswürdigen Rechnersystemen
- ◆ Immer mehr mobile Endgeräte werden im normalen Unternehmensalltag ungeschützt verwendet
- ◆ Fazit:
  - Das Netzwerk ist durch Malware und Eindringlinge gefährdet
  - Netze besitzen keine Vertrauenswürdigkeit
  - Es ist kein ausreichend vertrauenswürdiger Datenaustausch möglich

## Ziel und Aufgabe des SIMOIT-Projekts

**SIMOIT** Sicherer Zugriff  
Mobile Mitarbeiter  
IT-Infrastrukturen

- ◆ SIMOIT = Sicherer Zugriff von MObilen Mitarbeitern auf die IT-Infrastruktur von mittelständisch geprägten Unternehmen
- ◆ Es sollen Konzepte und auch technische Lösungen entwickelt werden, um die neu entstehenden mobilen Anwendungen und mobilen IT-Infrastrukturen von mittelständisch geprägten Unternehmen auf jetzige und zukünftige IT-Sicherheitsanforderungen vorzubereiten
- ◆ Ziel ist es, eine auf Standards basierende mobile IT-Sicherheitslösung herstellerunabhängig für den Bereich hochmobiler Mitarbeiter zu entwickeln

## Eigene Webseite: [www.simoit.de](http://www.simoit.de)

- ◆ Programm: InnoVision2010 von Bremen
- ◆ Partner:
  - TZI – Uni Bremen
  - IIA – HS Bremen
  - DECOIT GmbH
  - ThyssenKrupp Krause GmbH (Pilot)
  - Pan Dacom Networking AG (Kooperation)
- ◆ Laufzeit: 12 Monate
- ◆ Aktuellen Termine und Arbeiten werden veröffentlicht



**SIMOIT** Sicherer Zugriff  
Mobile Mitarbeiter  
IT-Infrastrukturen

HOME | AKTUELLES | TERMINE | SIMOIT | PARTNER | KONTAKT | IMPRESSUM

### IMPRESSUM

IM IMPRESSUM WERDEN DIE RELEVANTEN PROJEKTDATEN SOWIE DIE TECHNISCHEN VORRAUSSETZUNGEN ZUR NUTZUNG DIESER WEBSEITEN KURZ DARGESTELLT. BEI FRAGEN SPRECHEN SIE UNS BITTE DIREKT AN.

**Herausgeber und Verantwortlicher - © SIMOIT-Konsortium**

Das verantwortliche SIMOIT-Konsortium besteht aus den folgenden Instituten und Unternehmen:

- » DECOIT GmbH
- » Technologie-Zentrum Informatik (TZI), Universität Bremen
- » Institut für Informatik und Automation (IIA), Hochschule Bremen
- » ThyssenKrupp Krause GmbH

**Design, Text, Grafik und Software - © SIMOIT-Konsortium**

Kopieren oder Reproduktion oder jede andere Art der Wiedergabe oder Verwendung der in diesem Internet-Auftritt verfügbaren Materialien bzw. Informationen nur mit schriftlicher Genehmigung des SIMOIT-Konsortiums. Verantwortlich für den Inhalt dieses Internet-Auftritts ist das SIMOIT-Konsortium. Für Inhalte, die aus Weiterleitungen zu anderen Anbietern von Inhalten resultieren, übernimmt das SIMOIT-Konsortium keine Verantwortung oder Haftung.

**Technische Voraussetzungen:**

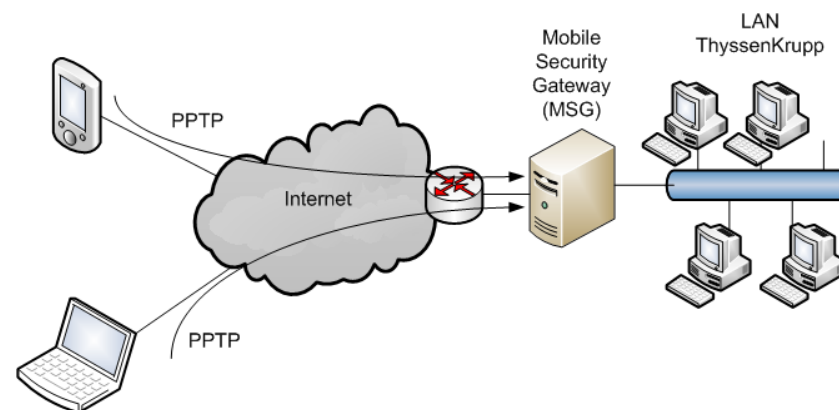
Diese Website ist optimiert für Internet-Explorer ab 5.5 und Mozilla ab 1.5 auf Windows 9x/2000/XP/Linux/MAC bei einer Bildschirmauflösung von 1024x768 Pixel. Empfohlen wird allerdings eine Auflösung von 1280x1024. Für eine optimale Darstellung sollte Javascript aktiviert sein. Zum Betrachten einiger Inhalte benötigen Sie zusätzliche Software wie zum Beispiel den Adobe Acrobat Reader von Adobe, den Flash Player von Macromedia oder den Real-Player. An entsprechender Stelle wird Ihnen die Möglichkeit zum Download angeboten.

Die Umsetzung und das Design erfolgte durch die Firma **DECOIT GmbH** (<http://www.decoit.de>).

## Aspekte der mobilen Sicherheit

- ◆ Zentrale Fernadministration von Netzen mobiler Endgeräte
- ◆ Identität durch starke Authentisierungsmethoden
- ◆ Absicherung der mobilen Kommunikation durch starke Verschlüsselung
- ◆ Absicherung des entfernten (remote) Zugriffs auf mobile Endgeräte
- ◆ Datenverschlüsselung
- ◆ Firewall-, Viren- und allgemein Malwareschutz-Funktionalität
- ◆ Trusted Network Connect (TNC) Funktionalität
- ◆ Herstellerunabhängigkeit und modularer Aufbau

- ◆ Arbeitsschwerpunkte:
  - Softwareverteilung
  - TNC-Anbindung
  - Administrationsoberfläche
- ◆ Mobile Security Gateway
  - TNC (Trusted Network Connect) Erweiterung
  - Wert auf Herstellerneutralität legen (Offenheit/Modularität)
- ◆ Mobile Endgeräte
  - PDAs (Windows Mobile mit .NET Framework, Symbian OS)
  - Laptops (Windows XP, Vista)





## Notwendige Dienste der MSG-Servers

- ◆ Betriebssystem: Debian Linux Plattform, inkl. Samba
- ◆ Verzeichnisdienst: OpenLDAP mit AD-Anbindungsmöglichkeit
- ◆ RADIUS-Dienst zur Authentifizierung: FreeRADIUS
- ◆ Firewall-Funktionalität: iptables
- ◆ VPN-Funktionalität: IPsec/IKE mittels Openswan
- ◆ SSL Root CA und Server/Client-Zertifikate

## Der TNC-Ansatz

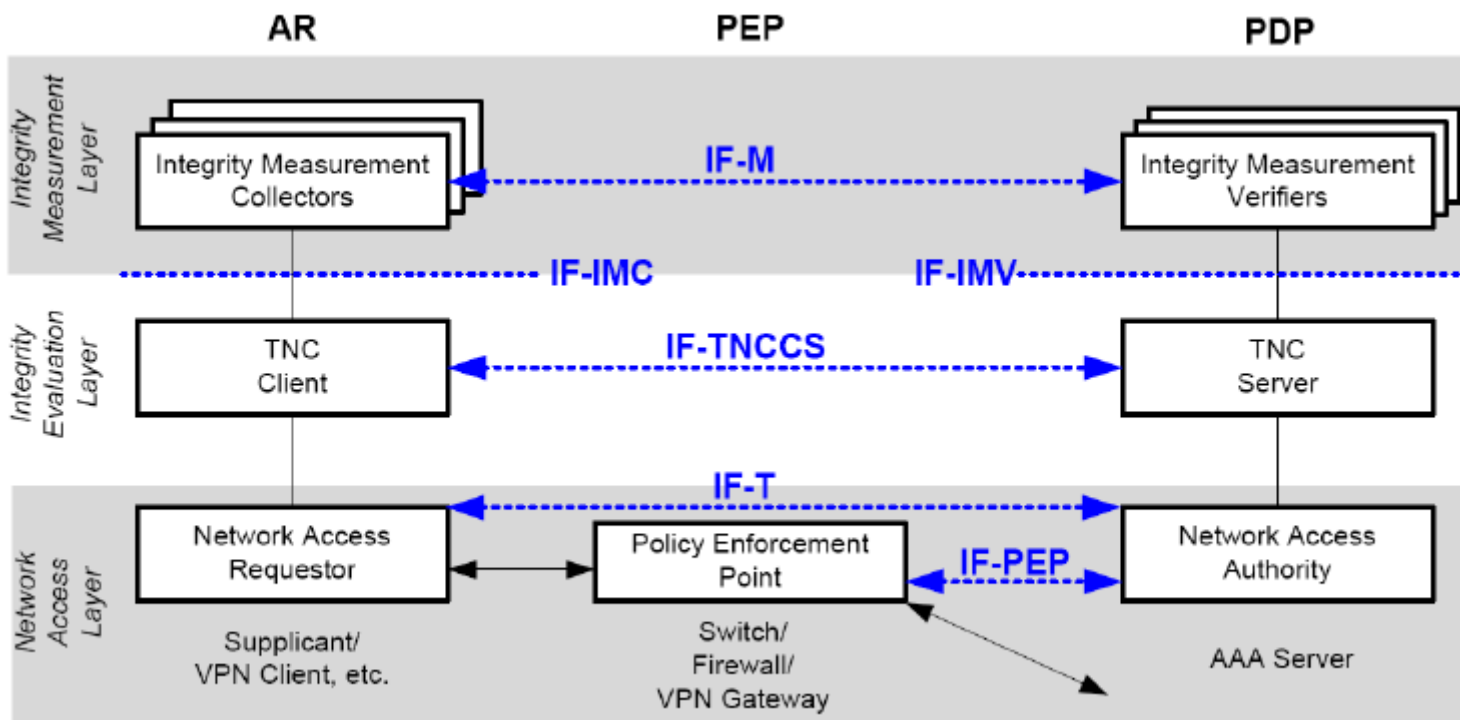


- ◆ Mit der Trusted Network Connect-Spezifikation (TNC) entwickelt die Trusted Computing Group (TCG) einen eigenen NAC-Ansatz
- ◆ Die Entwicklung findet durch die Trusted Network Connect-Subgroup mit über 75 vertretenen Firmen statt und liegt aktuell (Mai 2007) in der Version 1.2 vor
- ◆ Ziel ist die Entwicklung einer offenen, herstellerunabhängigen Spezifikation zur Überprüfung der Endpunkt-Integrität
- ◆ TNC baut auf vorhandene Technologien auf, wodurch eine einfachere Integration in bestehende Infrastrukturen möglich ist
  - Netzwerkzugriff: 802.1x, VPN, PPP
  - Nachrichtentransport: EAP, TLS & HTTPS
  - Authentifizierung: Radius Server, Diameter

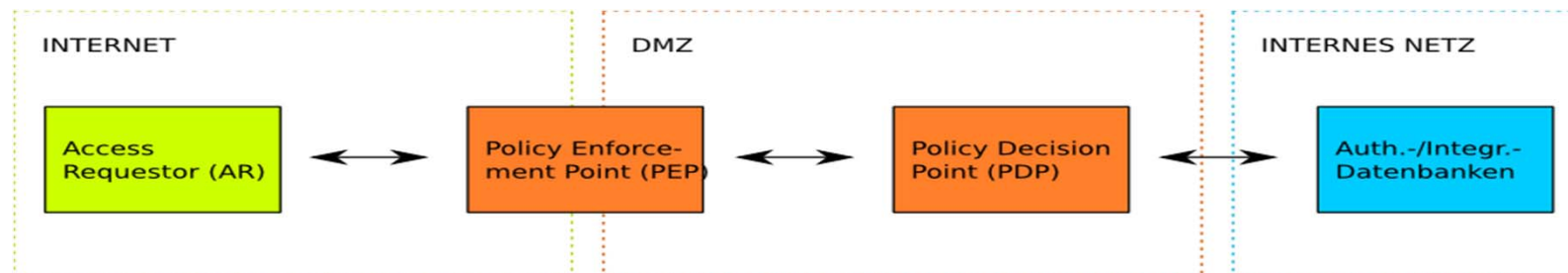
## TNC-Basisfunktionalität

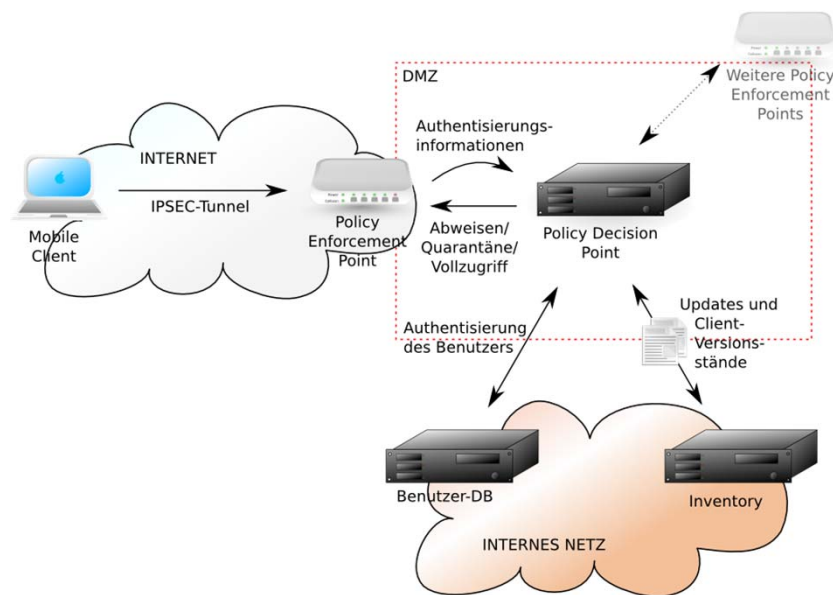
- ◆ Überprüfung der Vertrauenswürdigkeit:
  - Richtlinien-abhängige Zugriffssteuerung für Netzwerke
  - Integritätsprüfung: Messen des Systemzustands (Konfiguration der Endgeräte) und Überprüfung dieser Zustände gemäß Richtlinien (Assessment-Phase)
  - Isolation von potentiell gefährlichen Rechnersystemen 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 Framework



- ◆ Umsetzung des TNC-Ansatzes auf das Projektzenario
- ◆ Die TNC-Architektur definiert drei verschiedene Komponenten:
  - Access Requestor (AR)
  - Policy Enforcement Point (PEP)
  - Policy Decision Point (PDP)





- ◆ Mobiler Client baut IPsec-Tunnel zum PEP auf
- ◆ PEP fragt Authentifizierungsinfos vom PDP ab
- ◆ Client wird abgewiesen oder zugelassen
- ◆ Benutzer-Datenbank und Inventory Infos werden mit PDP synchronisiert
- ◆ Weitere PEP Server können einbezogen werden

## Marktbetrachtung

- ◆ Alternativen
  - Microsoft NAP (proprietär und Softwareabhängig): voraussichtlich Anfang 2008 verfügbar
  - Cisco NAC (proprietär und Hardware-/Softwareabhängig): verfügbar. Benötigt die Hardware von Cisco.
  - Checkpoint Interspect-Appliance (proprietär und Softwareabhängig): verfügbar. Benötigt Checkpoint-NG-Software.
  - Weitere Ansätze (proprietär): teils verfügbar (u.a. von McAfee, Juniper)

## Ausblick und Fazit

- ◆ Administration
  - Erhöhter Aufwand bei Verwendung unterschiedlicher Hard- und Softwarelösungen (heterogenes Netz)
  - Jede einzelne Konfiguration muss durch Richtlinien abgedeckt werden
  - Gefahr zu restriktiver Richtlinien
  - Mitarbeit der Hardware-/Softwarehersteller nötig
- ◆ Sicherheit
  - Bei Agenten-basierten Systemen (Client/Server) besteht die Gefahr gezielter Angriffe zur Veränderung von Messwerten
  - TNC bietet durch offene Standards eine mögliche Integration in andere Plattformen
- ◆ Standardisierung
  - Alle bisherigen Lösungen inkompatibel zueinander (erste Bestrebungen der Standardisierung durch die IETF)
  - Eine (offene) Standardisierung ermöglicht auch eine einfachere Portierung auf neue Plattformen (z.B. Sicherheitsplattformen)



## Zusammenfassung

- ◆ Vorhandene VPN-Lösungen sind nicht ausreichend für vertrauenswürdige Netzwerkverbindungen
- ◆ Mit einer Integritätsprüfung werden vertrauenswürdige Netzwerkverbindungen möglich
- ◆ Vorhandene Lösungen sind nicht kompatibel zueinander
- ◆ Standardisierungsbedarf ist vorhanden
- ◆ Das TNC Framework ist ein offener Lösungsansatz; es fehlt hier aber noch an abschließenden Standards
- ◆ SIMOIT-Projekt greift TNC auf und wird die Entwicklung auch weiterhin verfolgen
- ◆ Mobile Endgeräte müssen in das Sicherheitskonzept eines Unternehmens einbezogen werden

**Ende**

**SIMOIT URL:**  
**<http://www.simoit.de>**



**DECOIT GmbH**  
**Fahrenheitstraße 9**  
**D-28359 Bremen**  
**<http://www.decoit.de>**  
**Tel.: 0421-596064-0**  
**Fax: 0421-596064-09**

*Consultancy & Internet Technologies*