MÜNCHNER KREIS

18. September 2003

Chipkarten-basierte Datensicherheit im Wireless LAN

Franz Haniel

Geschäftsführer
Giesecke & Devrient

Giesecke & Devrient

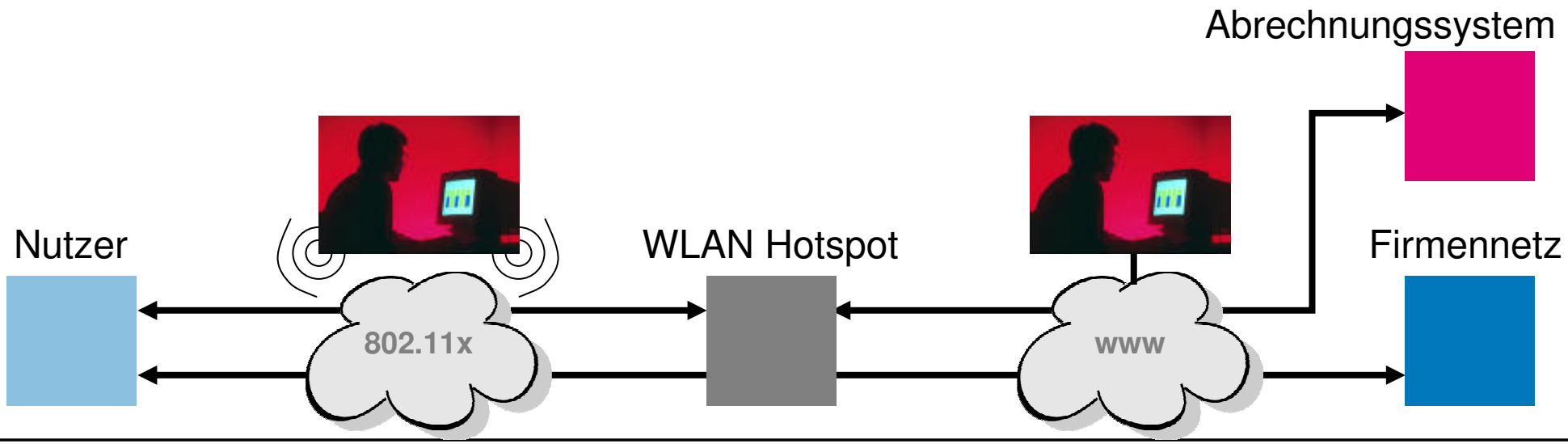
Es bestehen verschiedene Anforderungen an die Datensicherheit, abhängig vom Systemteilnehmer

Datensicherheit aus Nutzersicht

- Anonymität der Abrechnungsdaten für durchreichende Instanzen
- Vertraulichkeit der Daten, auf die z.B. im Firmennetz zugegriffen wird, gegenüber dem Betreiber des Netzwerkes und potentiellen Angreifern.

Datensicherheit aus Betreibersicht

- Zuverlässigkeit der Basisdaten für die Abrechnung:
  - Identität des Benutzers
  - Start und Ende der Verbindung
- Schutz der internen Daten gegenüber weiteren Service-Providern und potenziellen Angreifern.



Sicherheitsrelevante Faktoren in WLAN-Infrastrukturen

Sichere Authentifizierung als Basis erfolgreichen Billings

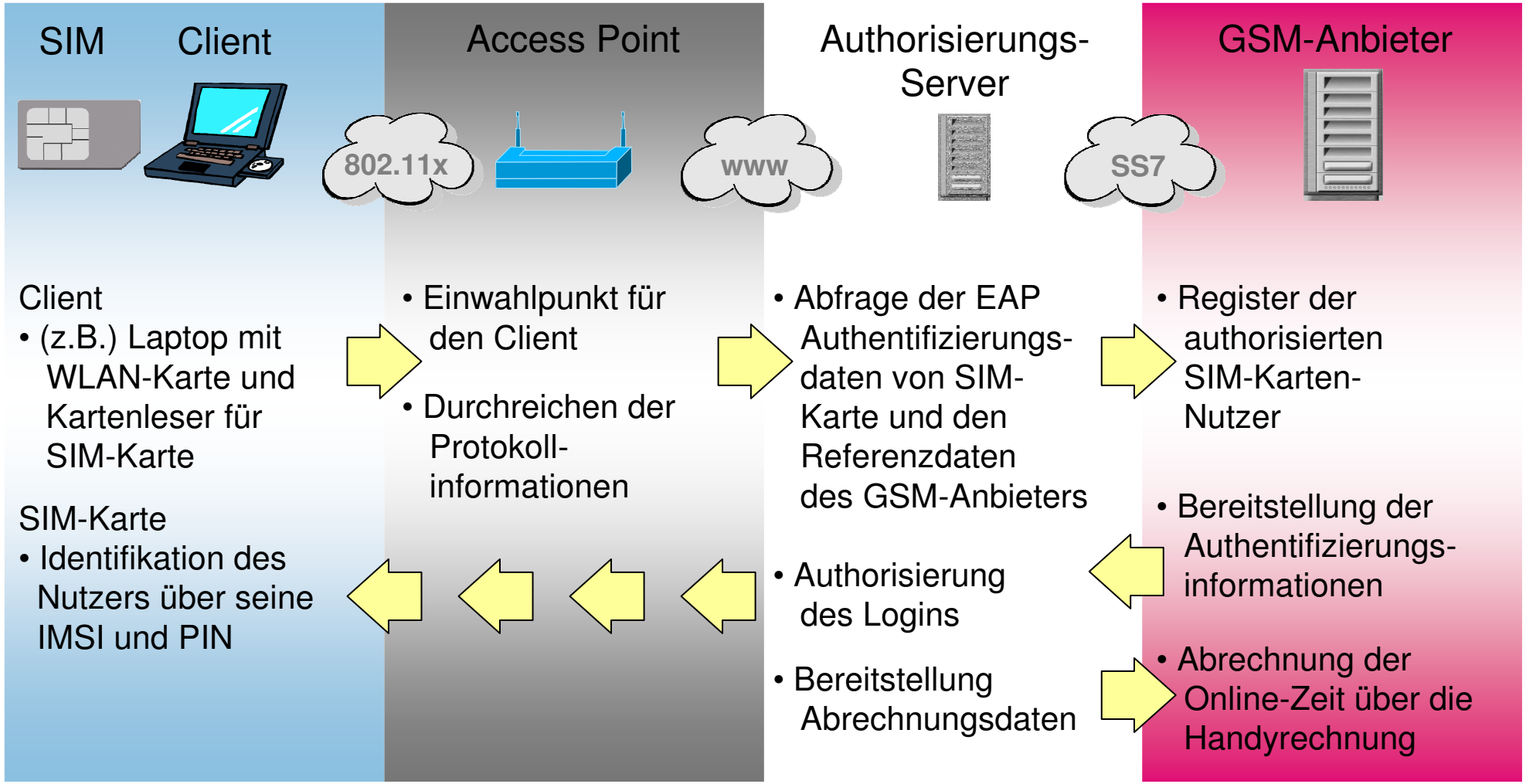
Einsicht nach dem Internet-Hype:

- Eine große Anzahl potentieller Kunden garantiert kein funktionierendes Geschäftsmodell.
- Auch digitale Dienste brauchen den zahlenden Nutzer.

- Systeme, die auf „Cyber Dollars“ basieren, d.h. anonymer Bezahlung, haben sich bis heute nicht durchgesetzt.
- Erfolgreicher sind bisher Lösungen, die auf bestehende Zahlungsmittel der Nutzer zurückgreifen.
  - Konto
  - Kreditkarten
  - Handyrechnung
- Diese Systeme bedingen eine eindeutige Identifikation des Nutzers in der virtuellen Welt.

Authentifizierung und Abrechnung im Wireless LAN über EAP SIM

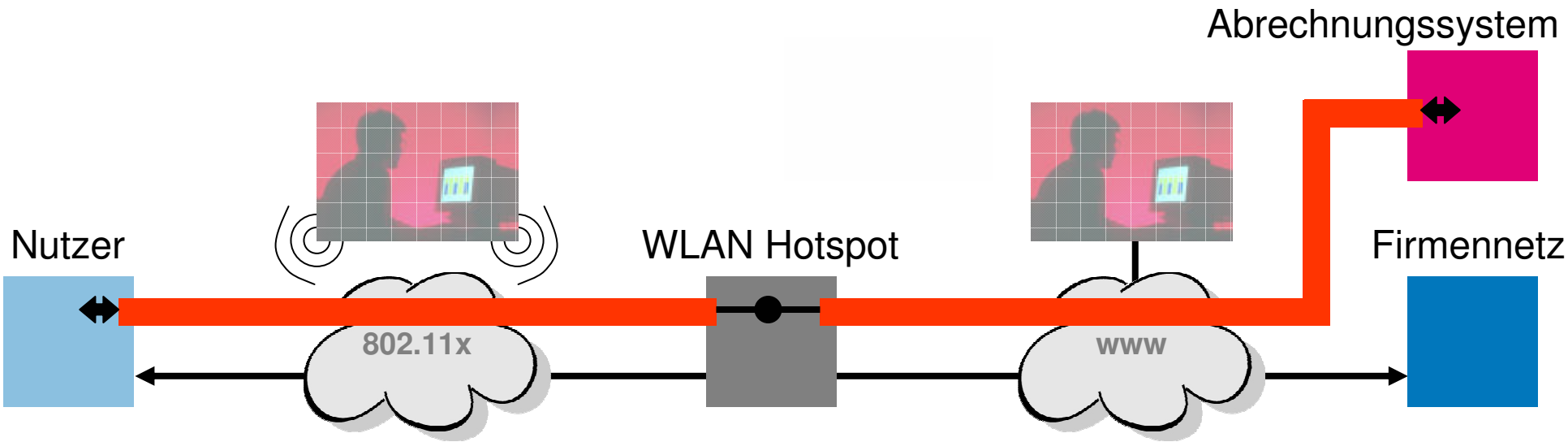
EAP SIM - Authentifizierungs-Protokoll unter Verwendung der Standard-Sicherheitsalgorithmen einer SIM-Karte



Sicherheit durch EAP SIM im WLAN

Eine EAP SIM basierte Authentifizierung des Nutzers sichert die Abrechnung der Nutzungszeiten

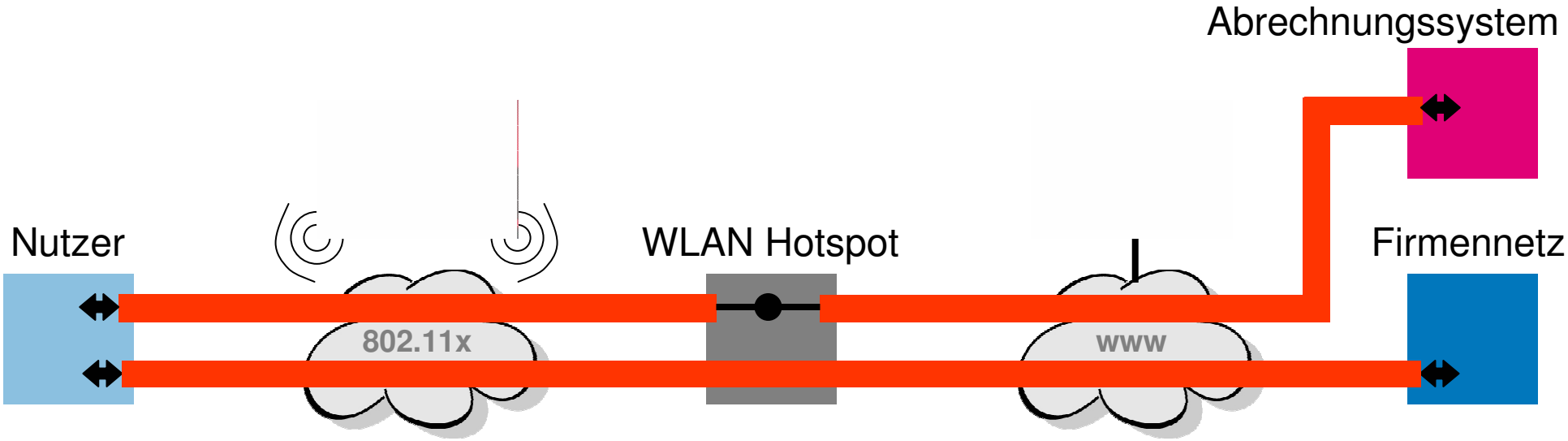
- Authentifizierung: Nutzer ist eindeutig identifiziert
- Sicherheit : Kommunikation ist kryptografisch abgesichert
  - Manipulation der Abrechnungsdaten (Start/Stop) nicht möglich
  - Abrechnung ist einem Nutzer zuzuordnen
  - Verbindung kann nicht unbefugt übernommen werden („hijacking“)



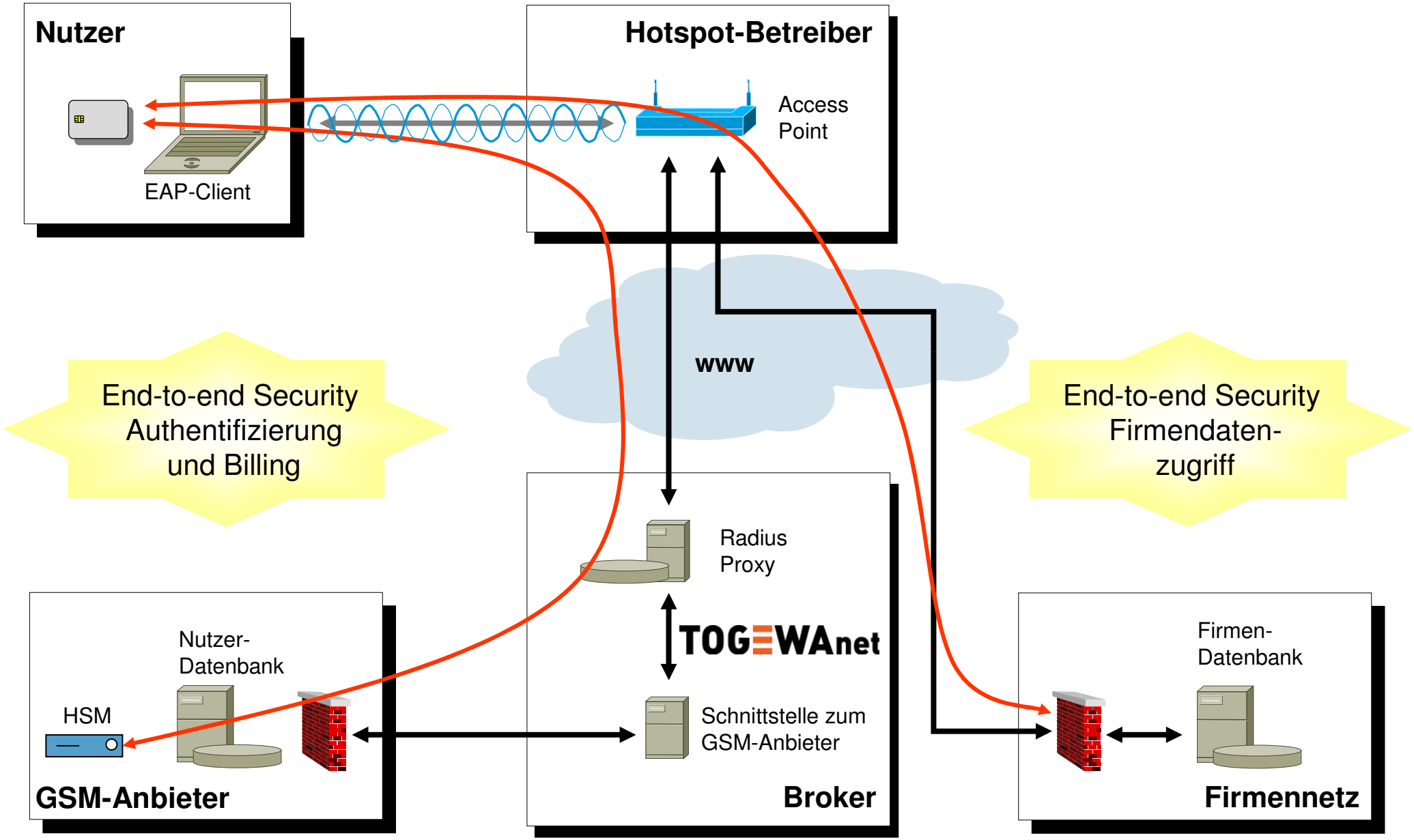
Datenschutz durch Erweiterung der EAP SIM-Lösung um VPN-Komponenten

Eine VPN-Lösung auf dem Client, z.B. mit einer erweiterten SIM-Karte als Sicherheits-Token, verschlüsselt die Kommunikation zum Firmennetz.

- Voraussetzung:
  Der VPN-Tunnel muß sich ohne Einschränkungen durch alle Systemkomponenten hindurch aufbauen können.
- Weder Hotspot-Betreiber noch potenzielle Angreifer haben dann Zugriff auf die übertragenen Daten



Realisierung: WERoam® Authentifizierungs- und Roaming-Plattform



Zusammenfassung: Vorteile einer EAP SIM-Lösung im WLAN

- **Sicherheitsmodell “State of the Art”**
- **Die Lösung ist effizient, ökonomisch und schnell zu realisieren, da bestehende Infrastrukturen und Komponenten genutzt werden.**

- **Subscriber**
  - Ein Authorisierungsprozess (über die vorhandene SIM-Karte)
  - Einfache und übersichtliche Abrechnung (über Betreiber)
  - Vereinfachtes Roaming (zu anderen EAP SIM-ausgestatteten W-LANs)
- **Hotspot-Betreiber**
  - Minimierter Betrug (verbesserte Sicherheit und zuverlässige Abrechnung)
  - Standardisiertes Billing (keine eigene Abrechnungsinfrastruktur)
- **Betreiber des Handynetzes**
  - Bestehendes Geschäftsmodell (SIM)
  - Bestehende Authentifizierungs- und Abrechnungsinfrastruktur
  - Vereinfachtes Roaming zwischen WLAN-Netzwerken
  - Einfache Integration in 2.5G/3G Netzwerke

MÜNCHNER KREIS

18. September 2003

Chipkarten-basierte Datensicherheit im Wireless LAN

Franz Haniel

Geschäftsführer
Giesecke & Devrient

Giesecke & Devrient