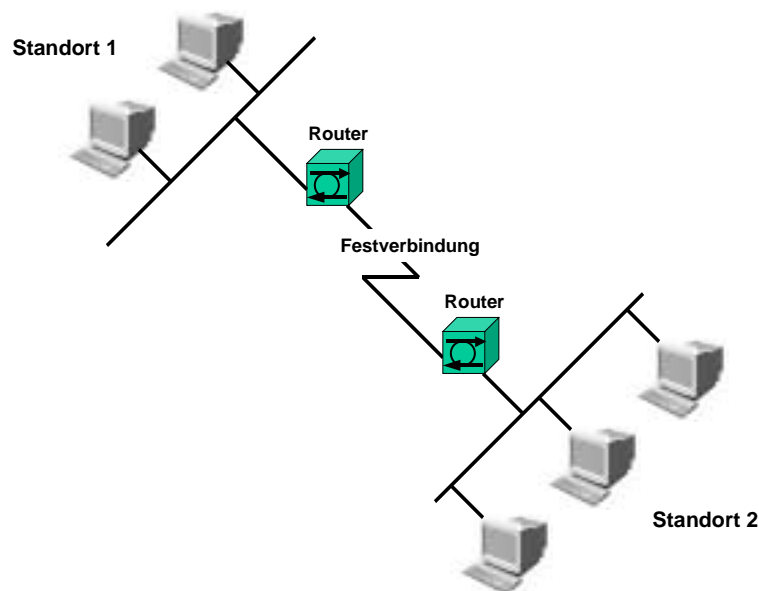


## ***IT-Sicherheit und Virtuelle Private Netze***

*Von Dr. Bernd Kuhlmann*

Die zunehmende Dezentralisierung und Globalisierung von Organisationseinheiten z.B. in der Industrie, der öffentlichen Verwaltung und der Bundeswehr macht den Einsatz modernster Kommunikationstechnologien unabdingbar. Gleiche Anforderungen ergeben sich aus den Schnittstellenbeziehungen zu Geschäftspartnern und/oder Kunden. Voraussetzungen sind flexible und sichere Netze, welche die Grundlage einer lokationsübergreifenden Informationsübermittlung bilden. Der Aufbau oder die Nutzung spezieller Strukturen, die einen hohen Sicherheitsstandard gewährleisten können, verbietet sich in vielen Fällen schon aus Kostengründen. Abbildung 1 zeigt ein solches Szenario mit einer Punkt-zu-Punkt Festverbindung.



*Abb. 1: Festverbindung*

Eine Lösung des Problems der hohen Kosten wäre die Nutzung des Internets. Es ist weltweit verfügbar, ausserordentlich flexibel, kann aber in seiner originären Form nicht einmal ein Minimum an Sicherheit bieten.

Unter Sicherheit verstehen wir dabei das Einhalten der Kriterien:

- Vertraulichkeit: Zugriff auf Informationen nur für die beteiligten Partner.
- Integrität: Unverfälschbarkeit der übermittelten Daten.
- Authentizität: Feststellung der Identität der Kommunikationspartner.
- Beweisbarkeit: Nichtabstreitbarkeit der Kommunikation
- Verfügbarkeit: Bereitstellung der erforderlichen Kommunikationsmittel.

Die in den vergangenen Monaten berichteten Angriffe auf das Internet in Form von Denial-Of-Service Attacks haben das Kriterium der 'Verfügbarkeit' in den Vordergrund treten lassen, obwohl die isolierte Betrachtung lediglich eines Aspektes den Fragestellungen im Bereich IT-Sicherheit nicht gerecht werden kann. Sicherheit kann stets nur durch eine enge Verflechtung von technischen, administrativen und organisatorischen Maßnahmen erreicht werden.

Da sich die Kosten organisationseigener Netzinfrastrukturen nur in einem sehr begrenzten Umfang reduzieren lassen, und zudem die Flexibilität dieser Architekturen den heutigen Anforderungen der Dezentralisierung und Globalisierung nicht mehr gerecht werden kann, bieten sich Lösungen an - beispielhaft dargestellt in Abbildung 2 -, die über Verschlüsselungstechnologien eine abgesicherte Kommunikation auch über das Internet zulassen (Bildung von Tunnels).

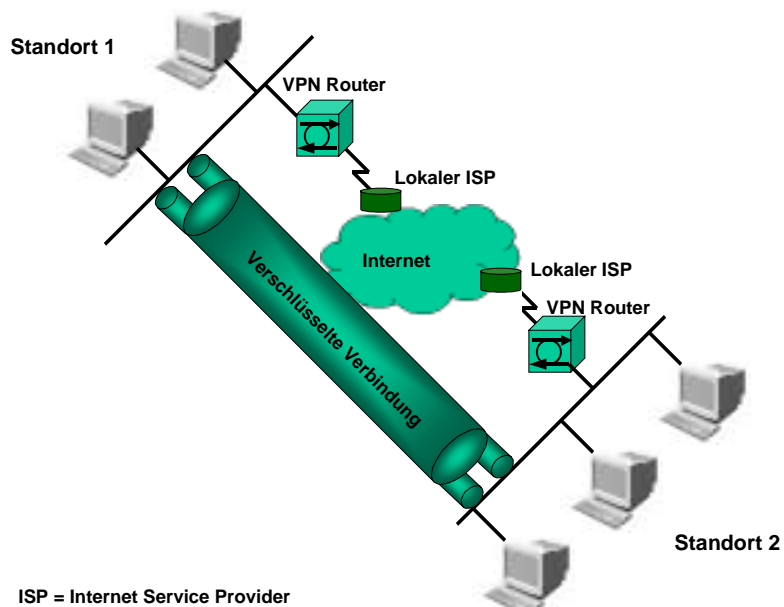


Abb. 2: verschlüsselte Verbindung

Ein ausserordentlich vielversprechender und zukunftssträchtiger Ansatz ist der Aufbau und die Verwendung von sogenannten 'Virtuellen Privaten Netzen' (VPN's). Dabei geht es nicht ausschliesslich um die Vertraulichkeit von Informationen, sondern es können, z.B. in Verbindung mit digitalen Unterschriften und der Nutzung von Smartcards, alle oben genannten Aspekte der IT-Sicherheit erfasst werden.

## Virtuelle Private Netze

Ein Virtuelles Privates Netz verhält sich gegenüber einem Anwender oder einem Informationssystem genauso wie ein unternehmenseigenes, privates und lokales Netzwerk. In Wirklichkeit jedoch werden die Daten verschlüsselt, zum Beispiel über ein öffentliches Netz wie das Internet, zum Kommunikationspartner übertragen (Abbildung 3).

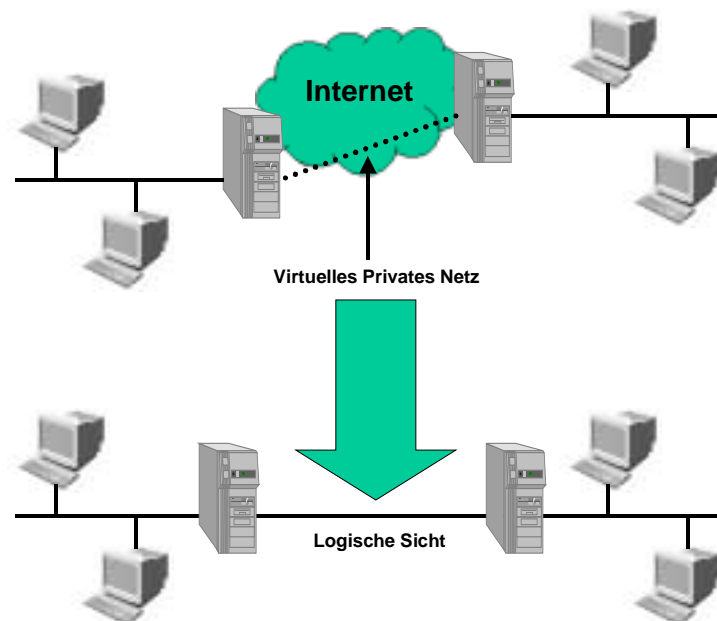


Abb. 3: logistische Sicht

Aus dieser Transparenz ergeben sich diverse Vorteile. So wird zum Beispiel die Akzeptanz eines Benutzers nicht durch zusätzliche Lernaufwände bzw. durch die Einführung neuer Komplexitäten in Geschäftsprozesse geschmälert. Des Weiteren ist der Betrieb bestehender Anwendungssysteme ohne Modifikationen und damit ohne Zusatzkosten auch in einem VPN sichergestellt.

VPN Infrastrukturen können unter Nutzung spezieller Hardware- und/oder Softwarekomponenten realisiert werden. Wegen der zunehmenden Leistungsfähigkeit der zur Verfügung stehenden Rechnersysteme geht der Trend eindeutig in Richtung von Software basierten Lösungen. Gründe dafür sind:

- größere Herstellerunabhängigkeit durch die Nutzung von standardisierten Protokollen (z.B. IPSec),
- Unterstützung diverser Übertragungsprotokolle wie TCP/IP, IPX/SPX, SNA, NetBEUI und NetBIOS,
- höhere Flexibilität zum Beispiel bei dem Einsatz von starken Verschlüsselungsverfahren,
- vielfältigere Einsatzmöglichkeiten,
- die bestehende IT-Infrastruktur kann unverändert beibehalten werden,
- vollständige Transparenz zu bestehenden Netzwerken und Anwendungen,
- Ende-zu-Ende Absicherung durch die Nutzung von VPN Client-Komponenten,
- VPN Clients können zentral administriert werden,

- Verknüpfung mit unternehmensinternen PKI's für die zentrale Kontrolle der Zugriffsrechte, die Verteilung von Schlüsseln und Zertifikaten für die in einem VPN genutzten Krypto-Verfahren und den Einsatz von digitalen Signaturen.

## Einsatz von VPNs

### 1. Anbindung von Telearbeitsplätzen

Ein Anwender wählt sich von seinem Telearbeitsplatz bei einem lokalen Internet Service Provider (ISP) ein. Im Vergleich zu einer Lösung mit zentralen Zugangsknoten werden sich die Telefonkosten auf dieser Basis erheblich reduzieren. Um eine vollständige Ende-zu-Ende Sicherheit zu erreichen, kann auf dem Rechnersystem des 'Telearbeiters' eine VPN Client Software installiert werden, die sicherstellt, dass sich das VPN wirklich bis zum Telearbeitsplatz erstreckt und nicht erst an einem zentralen VPN Gateway beginnt (Abbildung 4). Der Grad der Sicherheit ist beliebig skalierbar. So können zum Beispiel für eine weiter optimierte Absicherung Smartcard basierte Authentifizierungs- und Verschlüsselungsverfahren integriert werden. Die Prinzipien Besitz (Smartcard) und Wissen (PIN) oder auch Besitz und Sein (biometrische Erkennungsmerkmale) stellen insbesondere auch die Beweisbarkeit einer Kommunikation sicher.

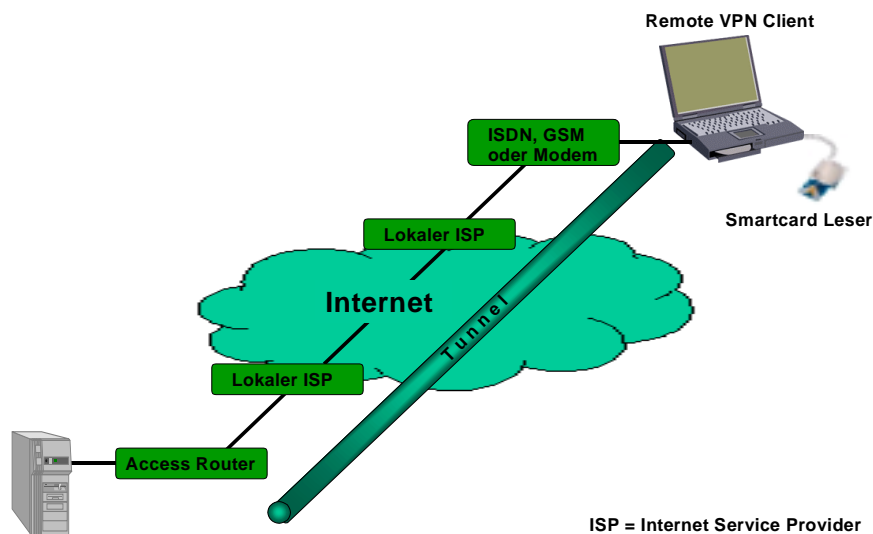


Abb. 4: VPN-Telearbeit

### 2. Anbindung eines lokalen Netzwerkes (LAN) an eine zentrale IT-Infrastruktur

Auch in diesem Szenario kommt für die Herstellung der Ende-zu-Ende Sicherheit eine VPN Client Software zum Einsatz. Dies hat den weiteren Vorteil, dass der dem LAN zugeordnete Router, der die korrekte Verteilung der Kommunikationsdatenströme übernimmt, nicht mit VPN Fähigkeiten ausgestattet sein muss (Abbildung 5).

Ist eine echte Ende-zu-Ende Absicherung nicht erforderlich, so kann in Abwandlung auf die VPN Clients verzichtet werden und statt dessen ein Router mit VPN Funktionalitäten zum Einsatz kommen.

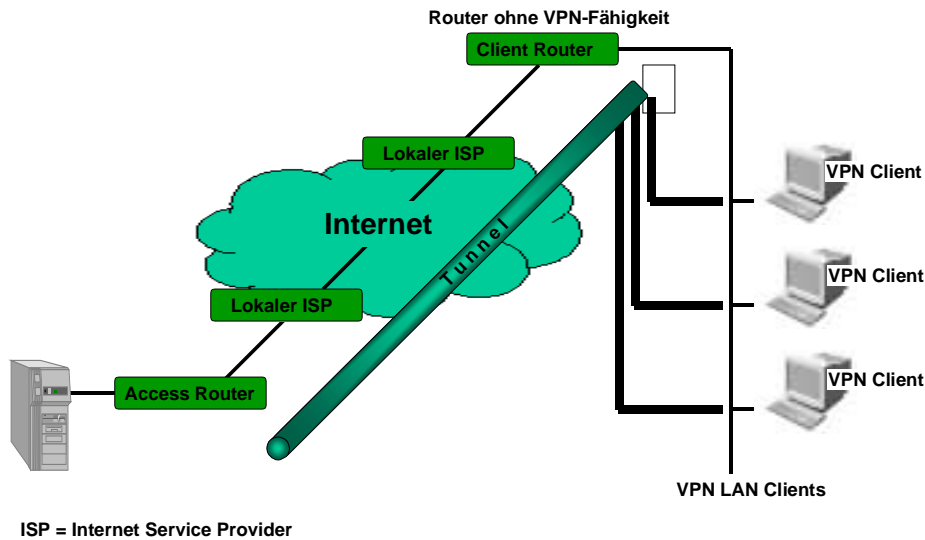


Abb. 5: LAN  
(Local Area Network)

## **Virtuelle Private Netze, Schlüssel und zentrale Verzeichnisdienste**

Das Konzept asymmetrischer Verschlüsselungsverfahren basiert auf der Existenz von zwei komplementären Schlüsseln, einem öffentlichen und einem privaten. Ist mit dem privaten Schlüssel eine Kodierung von Informationen erfolgt, so liefert das Anwenden des öffentlichen Schlüssels auf diese Daten wieder das Original. Entsprechendes gilt auch bei einer Vertauschung der Reihenfolge des Schlüsseleinsatzes. Die zuletzt genannte Vorgehensweise wird für allgemeine Verschlüsselungsaufgaben genutzt, während die zuerst genannte für die Realisierung von digitalen Signaturen herangezogen wird.

Nur der Besitzer des privaten Schlüssels kann eine Unterschrift leisten, die durch Verwendung des öffentlichen Schlüssels des Unterschreibers geprüft und diesem zugeordnet werden kann. Für diese nicht fälschbare und eindeutige Zuordnung zwischen einem öffentlichen Schlüssel und seinem Besitzer nutzt man das Konzept der Zertifikate. Diese werden von 'neutralen' dritten Instanzen, den Trustcentern ausgestellt.

Der private Schlüssel sollte sicher auf einer Smartcard abgelegt sein, damit ausschließlich der Eigner der Karte und damit des Schlüssels einen Zugriff auf diesen besitzt. Im Gegensatz dazu kann der öffentliche Schlüssel in Form eines Zertifikates frei verteilt werden. Dies geschieht in den meisten Fällen über globale Verzeichnisdienste.

Die Kombination von digitalen Signaturen und Zertifikaten definiert einen sicheren Weg, um Anwender in einem Virtuellen Privaten Netz eindeutig zu authentifizieren. Was liegt also näher, als die für VPN's und elektronische Unterschriften jeweils erforderlichen Infrastrukturen miteinander zu kombinieren und damit die Abdeckung der genannten Kriterien der IT-Sicherheit zu garantieren?

Kommen globale Verzeichnisdienste zum Einsatz, so eignen sich diese auch hervorragend für eine zentralisierte Administration der Virtuellen Privaten Netze, wie zum Beispiel die Vergabe von Zugriffsberechtigungen.

Ein solcher Ansatz ist in Abbildung 6 dargestellt. Die Verwaltung erfolgt über den zentralen Verzeichnisdienst, der auf den Standards X.500 und/oder LDAP basiert. Auch das CA-System, welches für das Erzeugen von Zertifikaten und das Personalisieren von Smartcards verantwortlich ist, nutzt diesen zentralen Dienst. Innerhalb des Virtuellen Privaten Netzes des Unternehmens existieren Subnetze, die wiederum als VPN's ausgebildet sind. Auch die entsprechenden Server-Systeme können das zentrale Verzeichnis nutzen.

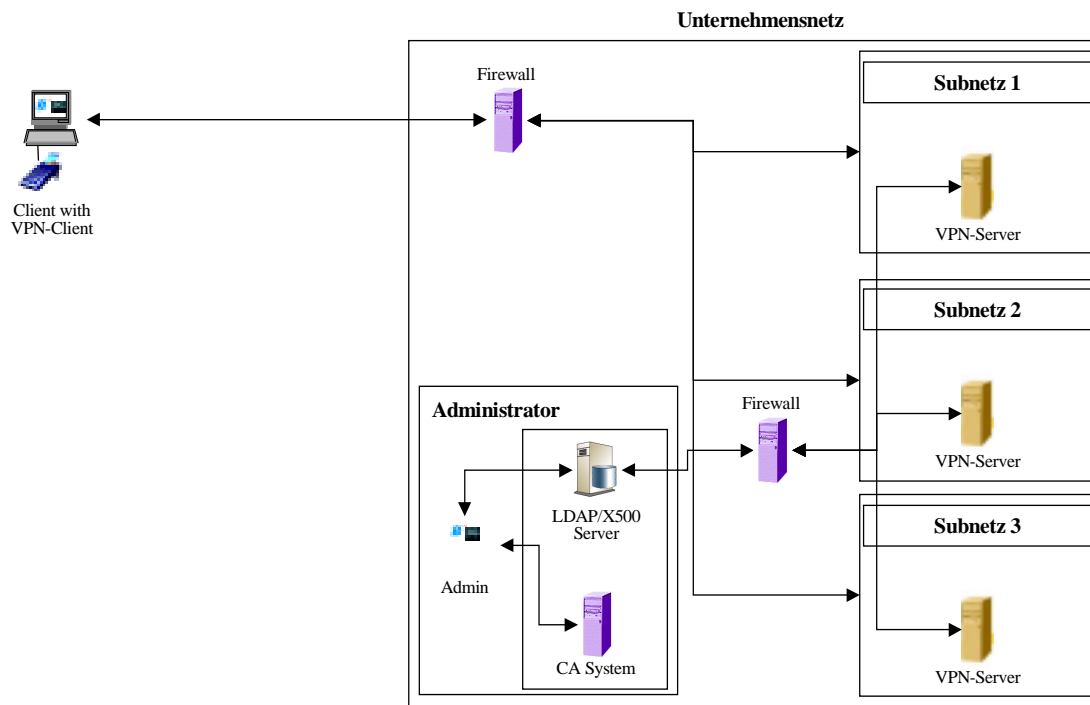


Abb. 6: PKI  
(Public Key Infrastructure)

## Schlussfolgerungen

Die Vorteile des Einsatzes von Virtuellen Privaten Netzen sind überzeugend:

- Erfüllen der Kriterien der IT-Sicherheit auch in öffentlichen Netzen,
- Transparenz für Anwender und Informationssysteme,
- Reduktion der Kosten,
- Skalierbarkeit,
- zentrale Administrierbarkeit,

- Beibehaltung der vorhandenen IT-Infrastrukturen bei Software basierten VPN Lösungen,
- Integration von Infrastrukturen für das Bereitstellen und Nutzen digitaler Signaturen (Public Key Infrastrukturen - PKI).

Zur Zeit können Virtuelle Private Netze mit Integration von PKI's als das Optimum einer kostenbewussten und alle Aspekte der IT-Sicherheit berücksichtigenden Lösung für die Kommunikationsanforderungen in einer dezentral und global agierenden Umwelt angesehen werden.

**Dipl.-Informatiker Dr, Bernd Kuhlmann**

Jahrgang 1960, diplomierte im Fach Informatik an der Christian-Albrechts-Universität in Kiel.

Nach seiner Promotion 1991 war er zunächst für die Deutsche Bank in Eschborn tätig und wechselte 1993 zur BGS Systemplanung AG, wo er heute die Technologieprojekte mit Schwerpunkt IT-Sicherheit leitet.

**Anschrift:**

BGS Systemplanung AG  
Robert-Koch-Str. 41  
51129 Mainz  
Tel.: 06131/914-143  
Fax: 06131/914-400