SSL VPNs

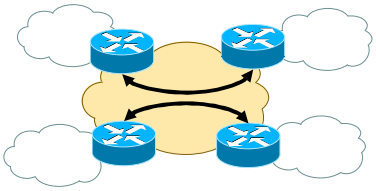
2G06

Andreas Aurand
Network Consultant NWCC, HP

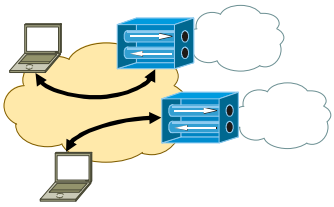
VPNs – eine Übersicht

VPNs – *Virtual Private Network*

- Aufbau eines privaten Netzwerks über eine gemeinsam genutzte Infrastruktur (z.B. über das Internet)
- **Site-to-Site VPNs**
  - IPSec VPNs
  - MPLS VPNs
  - VPLS und EoMPLS

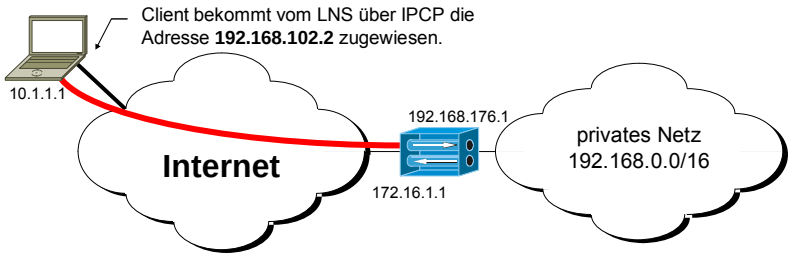


- **Remote Access VPNs**
  - PPTP VPNs
  - L2TP VPNs
  - IPSec VPNs
  - **SSL VPNs**



L2TP – Layer 2 Tunneling Protocol

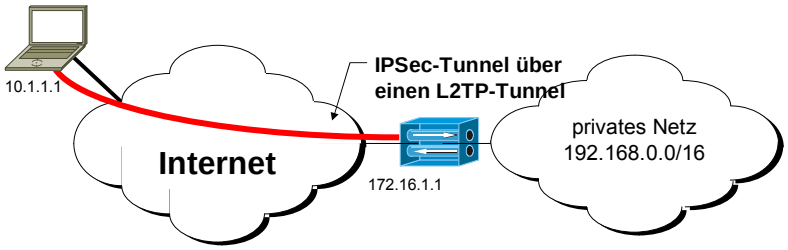
- Aufbau eines PPP-Tunnels über ein IP-Netzwerk
  - unterstützt **alle Netzwerkprotokolle** (IP, DECnet, IPX …)
  - IP Multicasts und IP Broadcasts
- **keine Verschlüsselung** der Daten



Outer IP Header 10.1.1.1 172.16.1.1	UDP Header Port 1701	L2TP Header	PPP Header	Inner IP Header 192.168.102.2 192.168.x.x	End-to-End (IP) Packet

L2TP mit IPSec-Verschlüsselung

- zusätzliche Verschlüsselung und Authentifizierung
  - Möglichkeit, nicht-IP Protokolle zu verschlüsseln

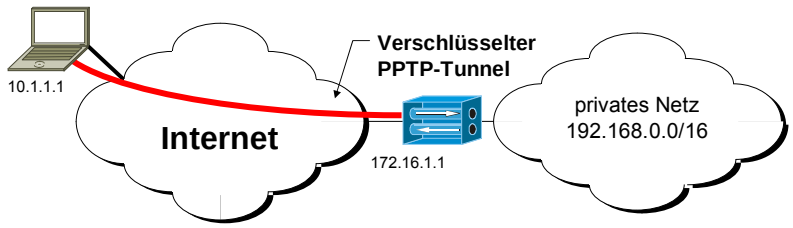


Outer IP Header 10.1.1.1 172.16.1.1	ESP Header	UDP Header Port 1701	L2TP Header	PPP Header	Inner IP Header 192.168.102.2 192.168.x.x	End-to-End (IP) Packet

verschlüsselt durch IPSec-Protokoll

PPTP – Point-to-Point Tunneling Protocol

- ***Tunnel Protocol***: Übertragung der Daten
  - modifiziertes IP-Protokoll 47 (GRE, Generic Routing Encapsulation)
  - unterstützt **alle Netzwerkprotokolle** (IP, DECnet, IPX usw.)
  - optionale Verschlüsselung mit **MPPE** (*Microsoft Point-to-Point Encryption*)
- ***Control Connection Protocol***: Aufbau des Tunnels (TCP Port 1723)

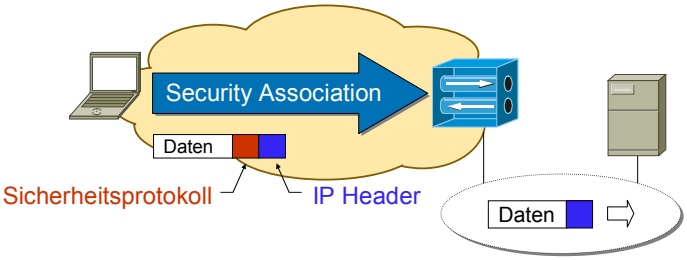


Outer IP Header 10.1.1.1 172.16.1.1	GRE Header	PPP Header	Inner IP Header 192.168.102.2 192.168.x.x	End-to-End (IP) Packet

verschlüsseltes MPPE-Paket (PPP-Protokoll 0x00FD)

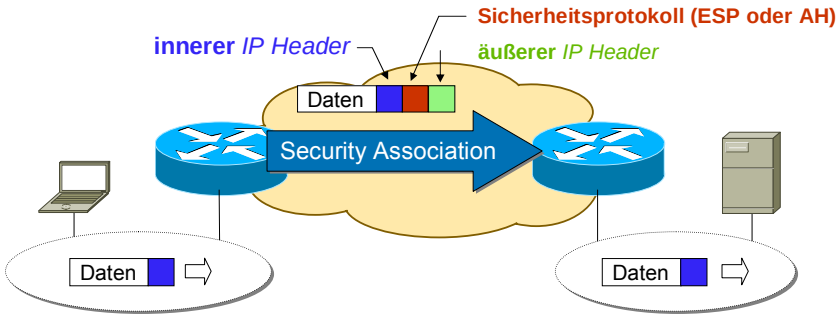
IPSec VPNs – Transport Mode

- **Direkte Verbindung** zwischen zwei Systemen
  - z.B. bei L2TP- oder GRE-Tunnel mit IPSec
  - Konfiguration auf Endsystemen notwendig
- Meistens für ***Remote Access VPNs*** eingesetzt



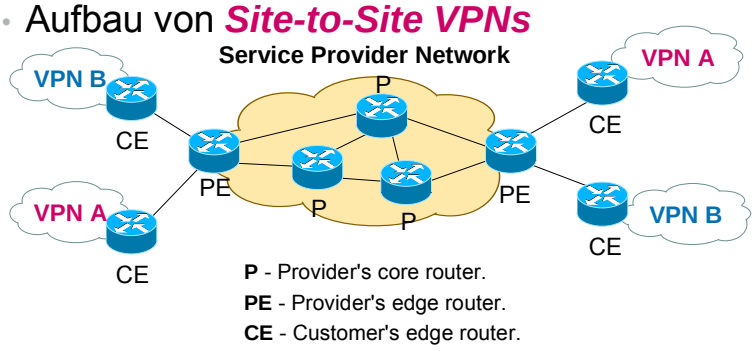
IPSec – Tunnel Mode

- Aufbau von ***Site-to-Site VPNs***
  - Verschlüsselung und Authentifizierung von ***IP Unicasts***
  - keine Konfiguration auf den Endsystemen notwendig



MPLS– Multiprotocol Label Switching

- Trennung auf **IP-Routing-Ebene**
  - im ISP-Bereich eingesetzt
  - keine Verschlüsselung bzw. Authentifizierung der Daten
- Aufbau von ***Site-to-Site VPNs***



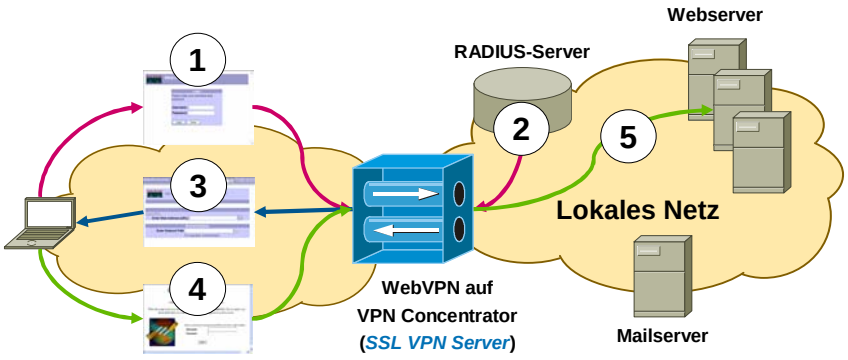
P - Provider's core router.
PE - Provider's edge router.
CE - Customer's edge router.

VPLS und **EoMPLS**

- **VPLS** – *Virtual Private LAN Service*
  - ***Multipoint Ethernet*** über ein MPLS Backbone
  - ***Layer 2 Broadcast Domain***
- **EoMPLS** – *Ethernet-over-MPLS Point-to-Point Services*
  - ***Point-to-Point Ethernet*** über ein *MPLS Backbone*
  - Keine *Layer 2 Broadcast Domain* möglich

SSL VPNs

SSL VPNs – Übersicht

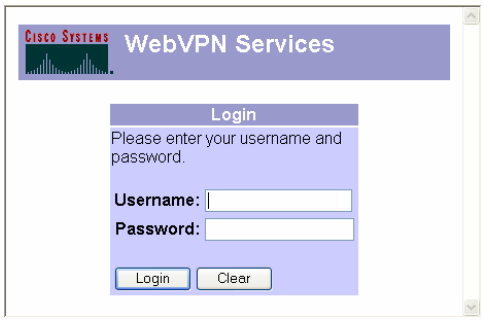


1. Aubau einer SSL-Verbindung zum *SSL VPN Server*; Angabe von Benutzername und Passv
2. Authentifizierung des Benutzers (lokal oder über einen RADIUS-Server)
3. Benutzer kommt ein **Web-Portal** mit den verfügbaren Applikationen angezeigt
4. Benutzer wählt Applikation aus und baut SSL-Tunnel zum *SSL VPN Server* auf
5. *SSL VPN Server* leitet die Daten an den richtigen Server weiter

April 22, 2004 Andreas Aurand, HP Network Competence Center 12

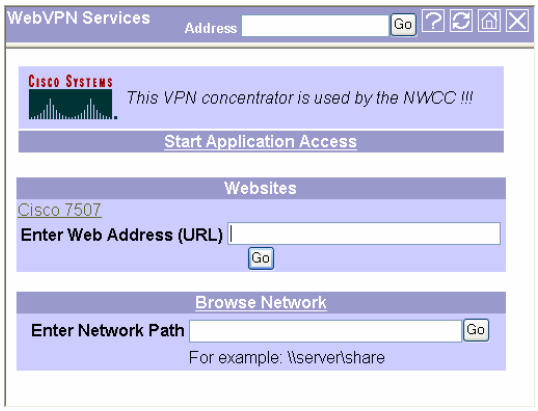
Cisco WebVPN

- VPN Concentrator ab Version V4.1
  - Benutzer muss sich über einen *Browser* auf dem *VPN Concentrator* authentifizieren
  - Anschließend sind Web-Verbindungen, Email, CIFS-Dateizugriff möglich



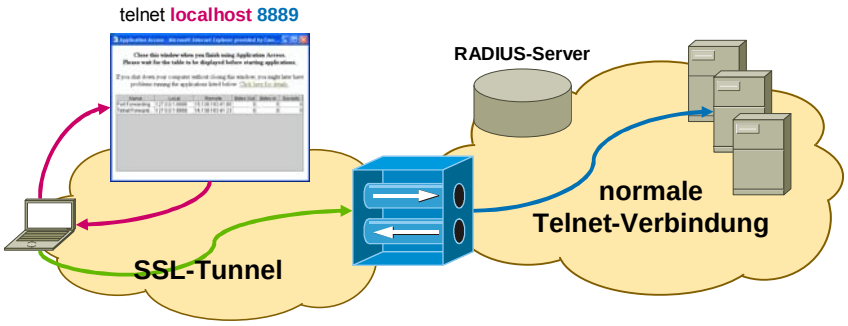
Cisco WebVPN

- Über *Web Portal* kann der Benutzer die angebotenen Services auswählen

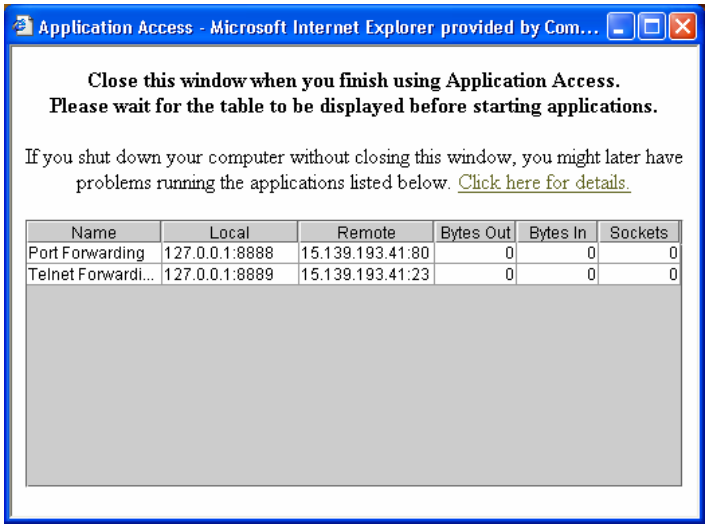


Cisco WebVPN – Port Forwarding

- Für Applikationen, die kein SSL unterstützen
  - **Java-Applikation** auf lokalem PC, die SSL-Tunnel zum Server aufbaut
  - Anstatt des Zielsystems wird spezieller Port auf dem lokalen PC angesprochen

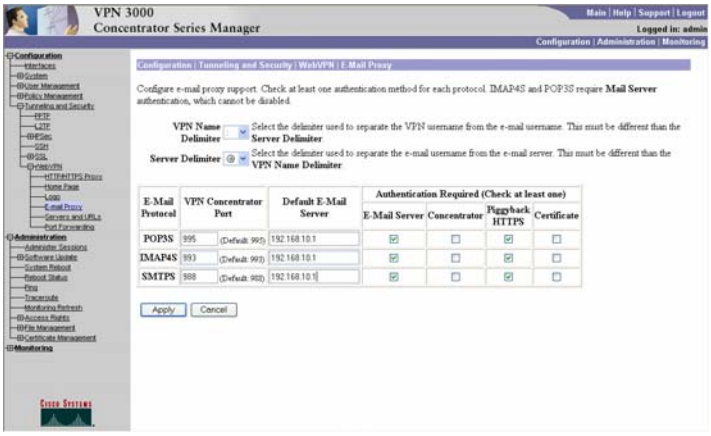


Cisco WebVPN – Port Forwarding

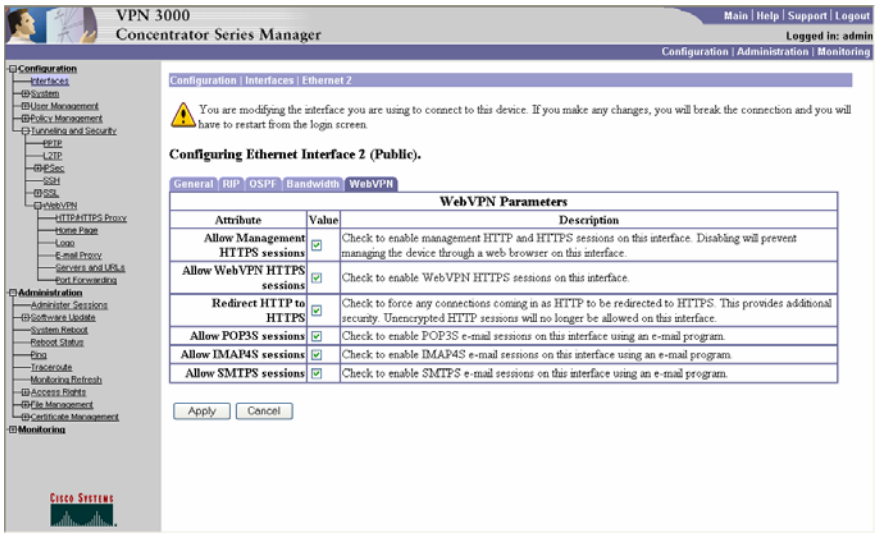


Cisco WebVPN – Email Services

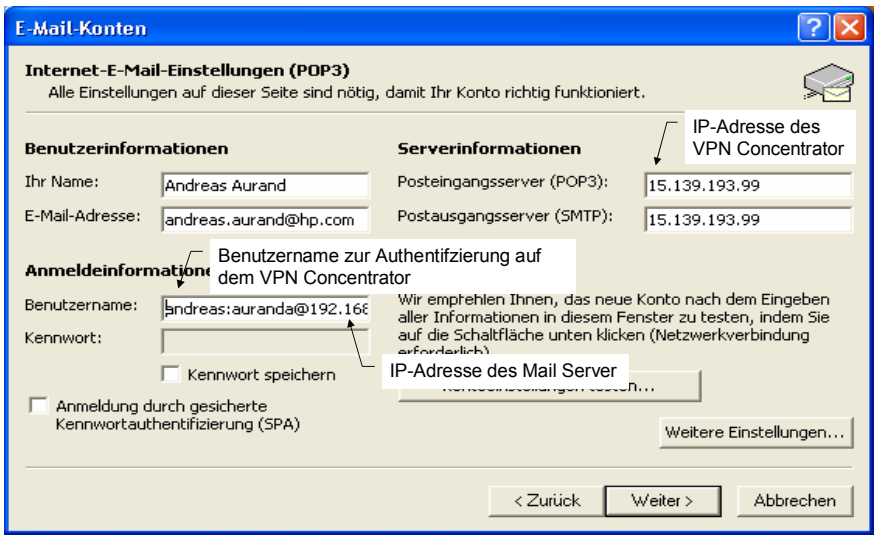
- **POP3S** und **IMAP4S** zum Empfangen von Mails
- **SMTPS** zum Senden von Mails



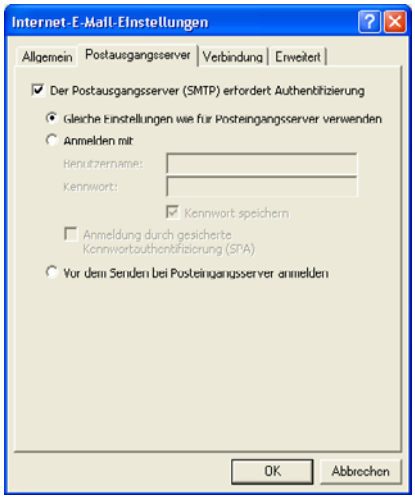
Cisco WebVPN – Email Services

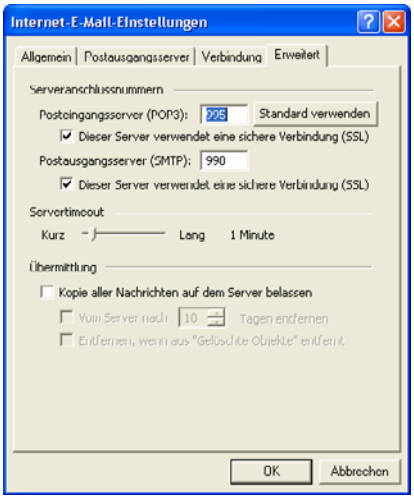


Cisco WebVPN – Outlook-Konfiguration



Cisco WebVPN – Outlook-Konfiguration





SSL VPNs – Vorteile

- ***Clientless Access***
  - Im Gegensatz zu IPSec ist keine spezielle Client-Software notwendig
- Weniger Probleme mit **Interoperabilität**
  - SSL VPNs benötigen für die gesicherte Verbindung lediglich einen SSL-kompatiblen Browser
  - Dadurch keine Änderungen in der unterliegenden Sicherheits-Infrastruktur notwendig

SSL VPNs – Nachteile

- Zugriff **nur für SSL-basierende Applikationen**
  - Web-Zugriff über HTTPS, Mail-Zugriff über POP3S, IMAP4S und SMTPS, Windows CIFS-Dateizugriff über Web-Schnittstelle
- Keine Möglichkeit, den **Zugriff auf interne Resourcen** zu beschränken
  - Client führt immer ***Split Tunneling*** durch
- Keine Unterstützung von **eingehenden Verbindungen**
  - z.B. XWindow, IP Telefonie, Netmeeting
- Sicherheit des SSL-Tunnels basiert auf ***Browser***
  - Normalerweise nur *Server-side TLS*; dadurch Sicherheitsprobleme (*The Compound Authentication Binding Problem – Draft RFC*)
  - Client beim Aufbau des SSL-Tunnels authentifizieren (*Client-side TLS*)

SSL-Protokoll – eine Übersicht

TLS Handshake

TLS Record

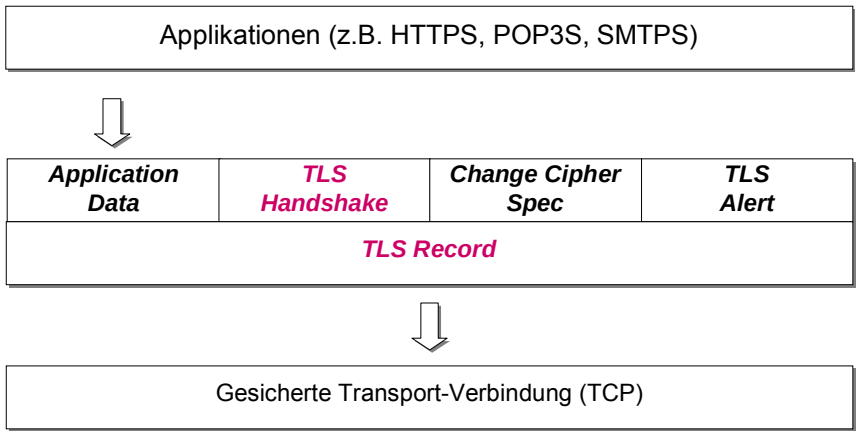
SSL – Secure Socket Layer

- verschlüsselte und authentisierte Client-Server-Kommunikation
  - Unabhängig von Applikation
  - benötigt aber andere Portnummern
- **TLS** (*Transport Layer Security*) ist die standardisierte Version

Applikation	TCP/UDP Portnummer
HTTP Protocol over TLS/SSL	443
NNTP Protocol over TLS/SSL	563
LDAP Protocol over TLS/SSL	636
FTP Protocol, data, over TLS/SSL	989
FTP Protocol, control, over TLS/S	990
TELNET Protocol over TLS/S	992
IMAP4 Protocol over TLS/SSL	993
SMTP Protocol over TLS/SSL	988
POP3 Protocol over TLS/SSL	995

April 22, 2004 Andreas Aurand, HP Network Competence Center 24

Aufbau des TLS-Protokolls



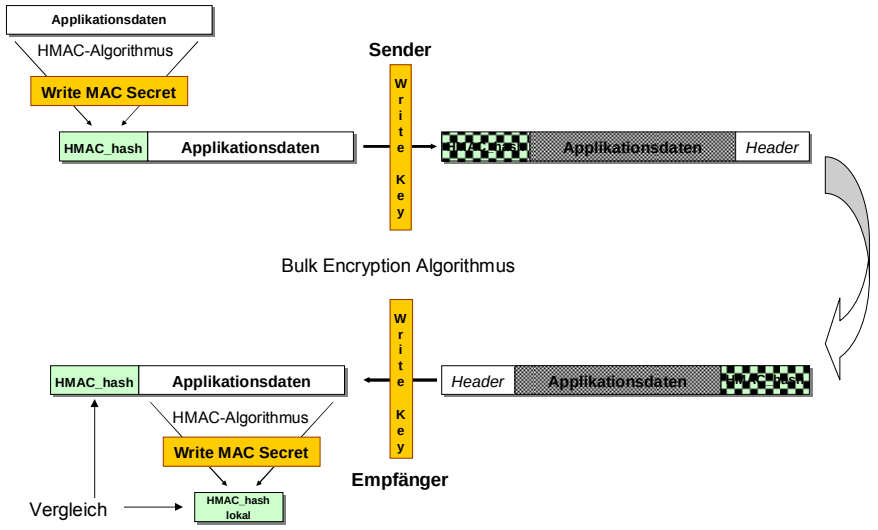
April 22, 2004 Andreas Aurand, HP Network Competence Center 25

TLS Record Protokoll

- Verschlüsselung der Daten
  - symmetrischer Algorithmus (z.B. AES, DES, 3DES)
- Integrität und Authentizität der Daten
  - *Message Authentication Code* (z.B. SHA1 oder MD5)
- Komprimierung der Daten (optional)
- Fragmentierung der Daten (optional)

April 22, 2004 Andreas Aurand, HP Network Competence Center 26

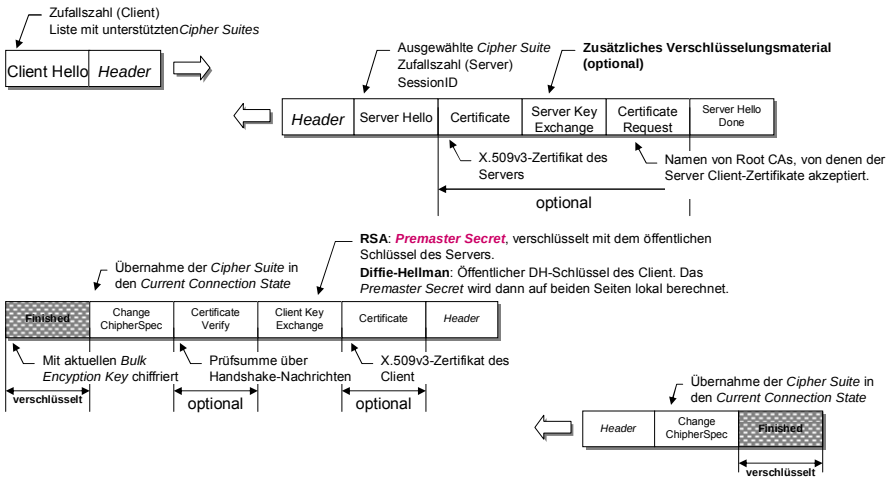
TLS Record Protokoll – **Verschlüsselung** und **Authentifizierung** der Daten



TLS Handshake Protokoll - Übersicht

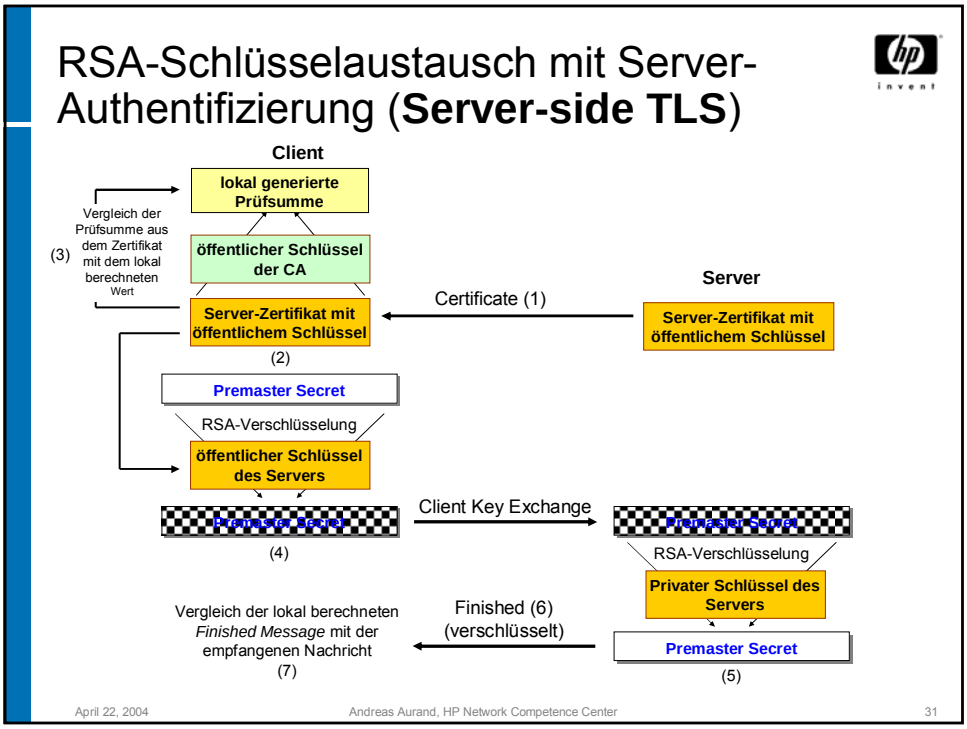
- Abstimmung der benötigten **kryptografischen Algorithmen** und **Schlüsselaustausch-Protokolle**.
- Austausch der kryptografischen Parametern, um sich auf ein ***Premaster Secret*** einigen zu können.
- Austausch von Zertifikaten und kryptografischen Informationen zur **gegenseitige Authentifizierung**.
- Verifikation, dass beide Partner die gleichen Sicherheits-Parameter generiert haben und dass keine Verfälschung erfolgt ist.

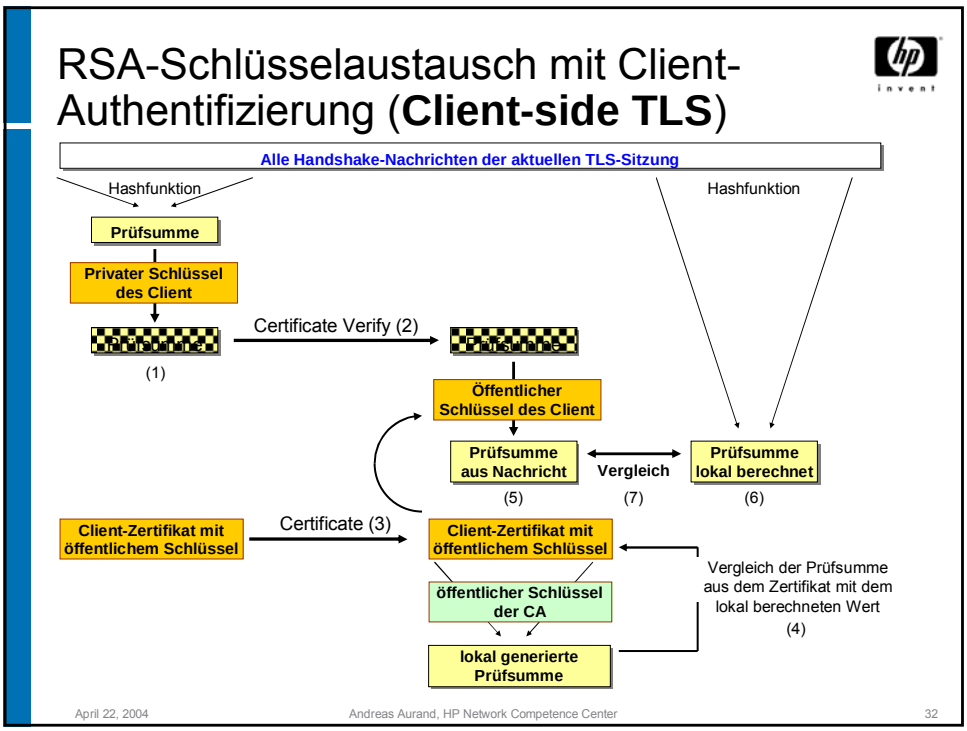
TLS Handshake Protokoll – Aufbau einer **TLS-Sitzung**



TLS Authentifizierung

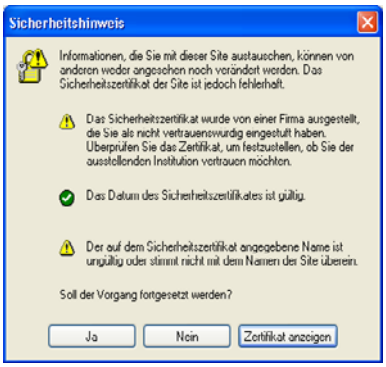
- **Anonymer Schlüsselaustausch**
  - Schlüsselaustausch über **RSA** oder **Diffie-Hellman**
  - **Keine Authentifizierung der Partner**
    - Gefahr von *Man-in-the-Middle*-Attacken
- **RSA Schlüsselaustausch**
  - Client überträgt ***Premaster Secret*** verschlüsselt
  - Server- und optionale Client-Authentifizierung
- **Diffie-Hellman Schlüsselaustausch**
  - Beide Seiten generieren das ***Premaster Secret*** lokal
  - Server- und optionale Client-Authentifizierung

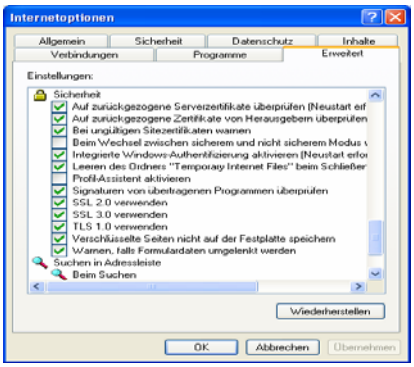

RSA-Schlüsselaustausch mit Server-Authentifizierung (Server-side TLS)
Client
lokal generierte Prüfsumme
Vergleich der Prüfsumme aus dem Zertifikat mit dem lokal berechneten Wert
(3)
öffentlicher Schlüssel der CA
Server
Certificate (1)
Server-Zertifikat mit öffentlichem Schlüssel
Server-Zertifikat mit öffentlichem Schlüssel
(2)
Premaster Secret
RSA-Verschlüsselung
öffentlicher Schlüssel des Servers
Premaster Secret
Client Key Exchange
Premaster Secret
(4)
RSA-Verschlüsselung
Privater Schlüssel des Servers
Vergleich der lokal berechneten Finished Message mit der empfangenen Nachricht
(7)
Finished (6) (verschlüsselt)
Premaster Secret
(5)
April 22, 2004
Andreas Aurand, HP Network Competence Center
31


RSA-Schlüsselaustausch mit Client-Authentifizierung (Client-side TLS)
Alle Handshake-Nachrichten der aktuellen TLS-Sitzung
Hashfunktion
Hashfunktion
Prüfsumme
Privater Schlüssel des Client
Certificate Verify (2)
(1)
Öffentlicher Schlüssel des Client
Prüfsumme aus Nachricht
Vergleich
Prüfsumme lokal berechnet
(5)
(7)
(6)
Client-Zertifikat mit öffentlichem Schlüssel
Certificate (3)
Client-Zertifikat mit öffentlichem Schlüssel
Vergleich der Prüfsumme aus dem Zertifikat mit dem lokal berechneten Wert
(4)
öffentlicher Schlüssel der CA
lokal generierte Prüfsumme
April 22, 2004
Andreas Aurand, HP Network Competence Center
32

Sicherheit der TLS Authentifizierung

- **Die Sicherheit des Protokolls hängt von der Sicherheit der verwendeten Zertifikate ab**
- Sicherheitshinweise des Browsers beachten
  - Auf zurückgerufene Zertifikate überprüfen





April 22, 2004 Andreas Aurand, HP Network Competence Center 33

Fragen