

Secure und managed Web-to-any-Server Computing

HOBLink
 **J-Term**

1



HOB
SOFTWARE

Inhaltsübersicht

- Warum neue Technologien einsetzen?
- Funktionsweise der HOB Web-to-any-Server-Lösung
- Management der HOB Lösung
- Die Sicherheitskonzepte von HOB

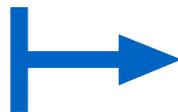
2



HOB
SOFTWARE

Warum eine neue Software/Technologie?

- Kostensenkung



Einsparpotentiale

- Vereinfachung von Unternehmensprozessen

3



HOB
SOFTWARE

Kosten senken durch ...

- Leitungskosten
 - Nutzung des Internet
 - Die Nutzung des Internet ist billiger als angemietete Standleitungen. Die Erfahrung zeigt, dass trotz erheblicher Störungen die Verfügbarkeit des Internets erhalten bleibt.
- Neue Technologien/
Vereinfachung von Unternehmensprozessen
 - Mobile Anbindung (u.a. UMTS)
Durch die mobile Anbindung an die Firmenzentrale ergeben sich Vorteile:
 - Kurze Reaktionszeit
 - Schneller Datenabgleich mit der Zentrale
 - Unabhängigkeit vom Standort

4



HOB
SOFTWARE

Kosten senken durch ...

- Anbindung von Außenstellen
(die man vorher nur schwer anbinden konnte)
- Zentrale Administration
 - Benutzeradministration (keine Turnschuh-Administration)
 - User-Help-Desk
 - Flexibilität
Die Administration ist unabhängig vom momentanen Standort möglich. Der Netzwerkzugang zur zentralen Komponente ist völlig ausreichend
 - Software Verteilung/Update (web basiert) bzw. Server Based Computing verringern die Ausfallzeiten beim Benutzer
 - Server Based Computing erhöht die Standzeiten der Clienthardware

5



HOB
SOFTWARE

Kosten senken durch ...

- Integration
 - Zahlreiche Integrationsoptionen und Plattformunabhängigkeit bietet einen wichtigen Beitrag zum Investitionsschutz und für zukünftige Investitionen
- Erleichterungen für die Benutzer
 - zentrale Zugangssoftware
 - einheitliche Benutzeroberfläche
 - reduzierte Ausfallzeiten
 - schnellere Hilfe

6



HOB
SOFTWARE

Lösungen von HOB...

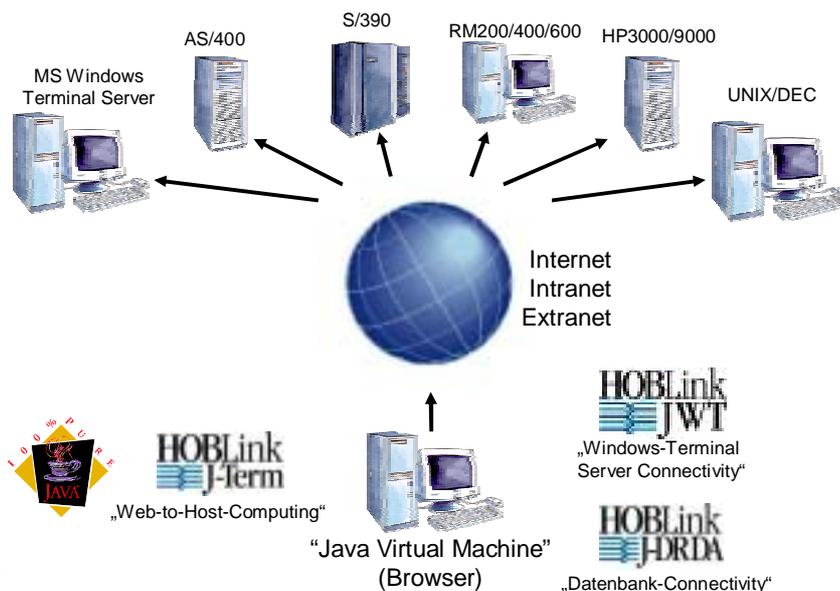
- HOB Enterprise Access
 - Web to any Server
 - Eine einzige Lösung zum Zugriff auf alle Unternehmensserver
 - Plattformunabhängig
 - Minimale Belastung vorhandener Netzwerk-Ressourcen
 - Softwareverteilung steckt in der Technologie
 - Server based Computing
 - Schlanke Lösung mit wenig Overhead (technisch wie administrativ)
 - Plattformunabhängig

7



HOB
SOFTWARE

Web-to-any-Server-Computing



8



HOB
SOFTWARE

Lösungen im Bereich ...

- Sicherheit
 - sicherer & performanter Zugriff aus dem Internet
 - Hohe Flexibilität
 - SSL Standard
 - Kompatibilität zu anderen SSL-Gegenstellen
 - Aufbau einer eigenen PKI
 - SmartCard Unterstützung nach Windows Standard
 - SSH2 mit VT
 - Hohe Flexibilität
 - VPN
 - Kompatibilität zu Cisco und Checkpoint

9



HOB
SOFTWARE

HOBLink J-Term - Konzept

HOBLink Gesamtkonzept

Connectivity

Benutzerfreundliche
Emulation von 3270-,
5250-, VT-, HP700- und
SINIX 97801-Terminals
Anbindung an Windows
Terminal Server

Administration

HOB Enterprise
Access zur
zentralen
Administration und
Konfiguration

Sicherheit

HOBLink Secure zur Verschlüsselung und
Authentifikation auf SSL-Basis (v 3.0) und SSH2

10



HOB
SOFTWARE

HOBLink J-Term - Interessant weil...

- Nur **ein modulares** Softwareprodukt
- **Unabhängig** von
 - den gängigen Host/Servern Systemen
 - den gängigen Client-Plattformen
- Für den Zugriff auf **alle** wichtigen Unternehmens-Server ist HOBLink J-Term die moderne, leistungsfähige und sichere Lösung
- **Zentrale** Installation, Konfiguration und Administration mit dem HOB Enterprise Access

11



HOB
SOFTWARE

HOBLink J-Term ... prinzipielle Funktionsweise



12



HOB
SOFTWARE

HOBLink J-Term ... prinzipielle Funktionsweise

HOBLink J-Term Version 3.2

Session Manager

Name	Typ	Status	Inhaber	Info	Abmelden
4330 - VM	Windows-Browser	Geschlossen	algeme		
4330 - J2D	Windows-Browser	Geschlossen	algeme		
437801	Windows-Browser	Geschlossen	algeme		
Taschenrechner	JVT Session	Geschlossen	algeme		
437801	Windows-Browser	Geschlossen	algeme		
IP_prof	JVT Session	Geschlossen	algeme		

Auswahl aus den verfügbaren Verbindungen/Applications im Webbrowser

13

HOBLink J-Term ... prinzipielle Funktion

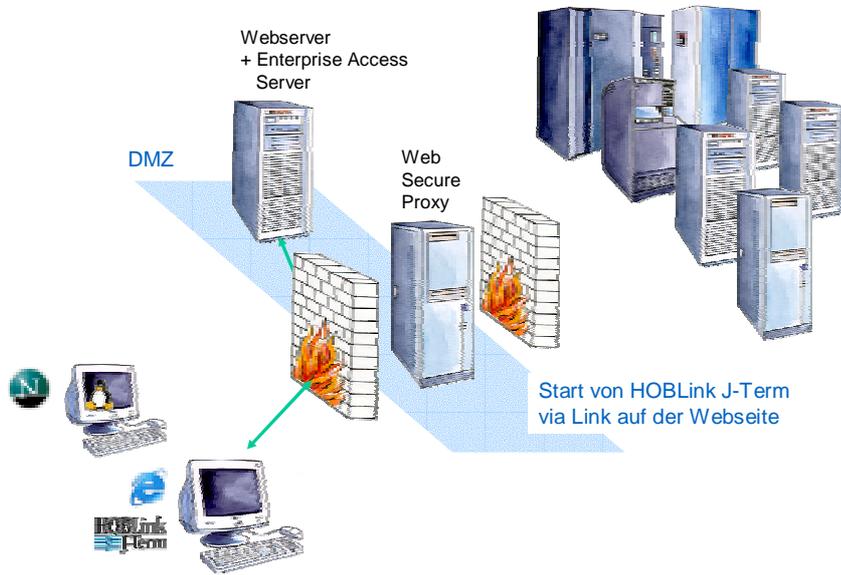
Webserver + Enterprise Access Server

z.B. Port 13270

Verbindung zum EA-Server (Änderung der Konfiguration durch den Benutzer, Metering)

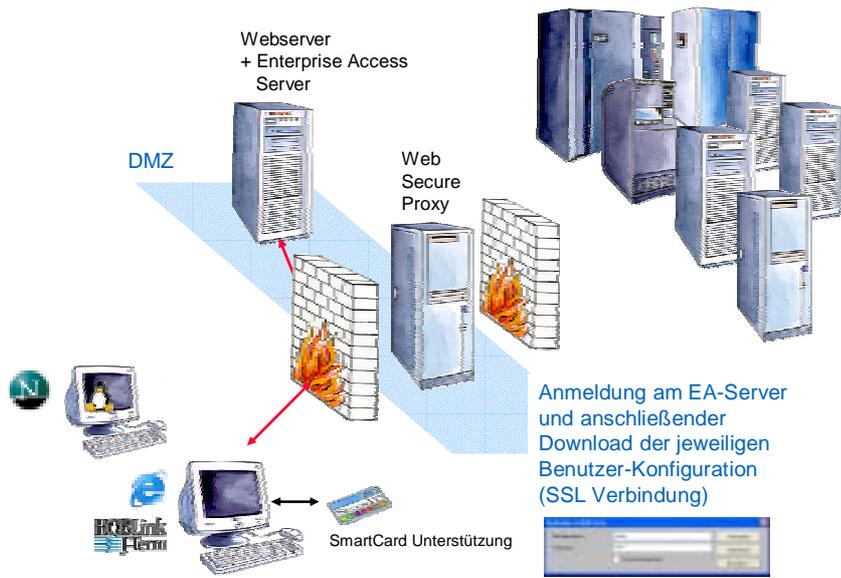
14

HOBLink J-Term ... über Internet



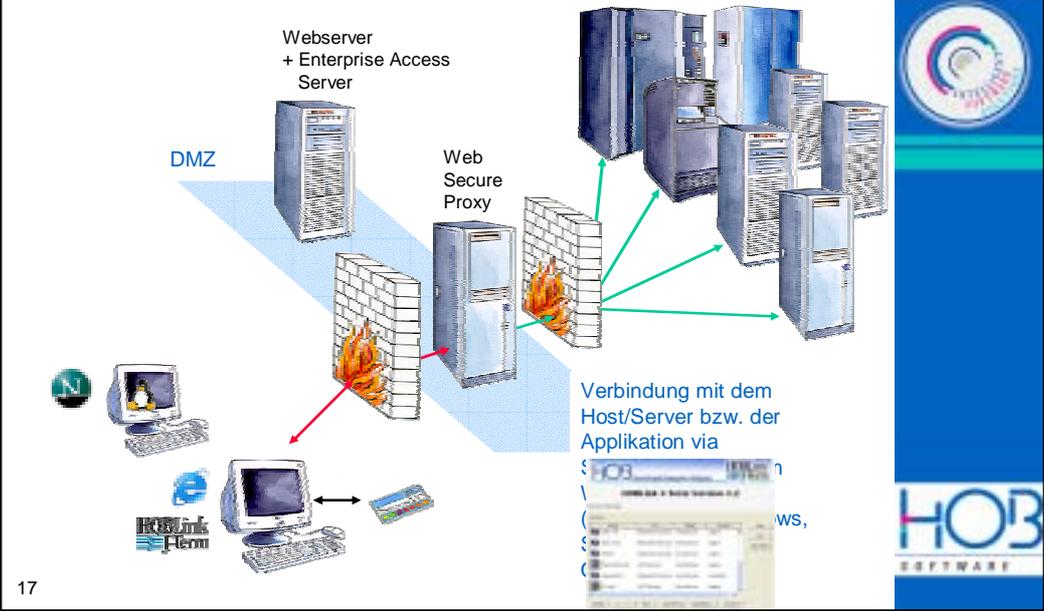
15

HOBLink J-Term ... über Internet

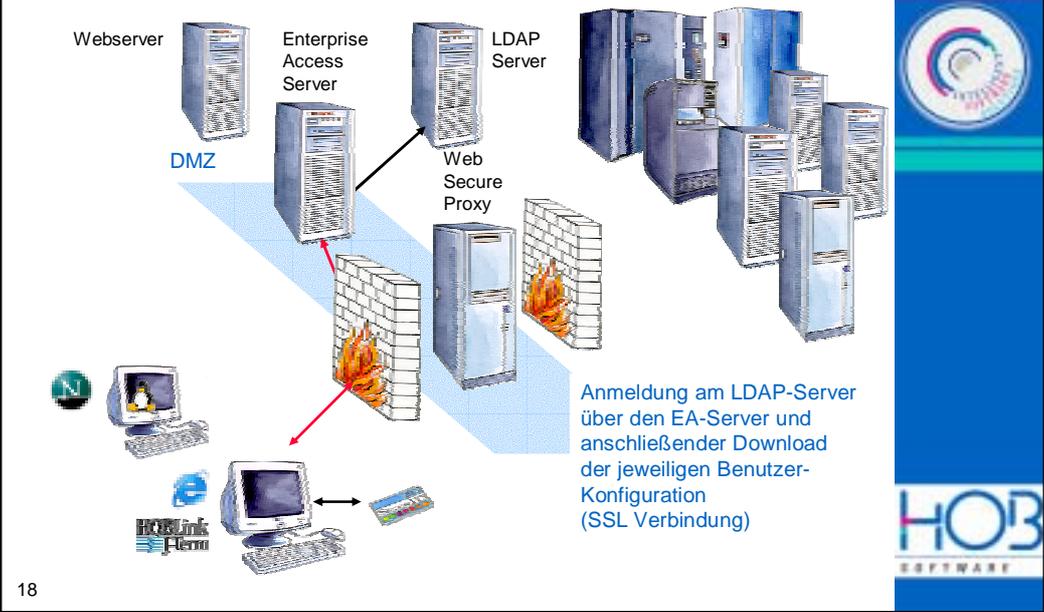


16

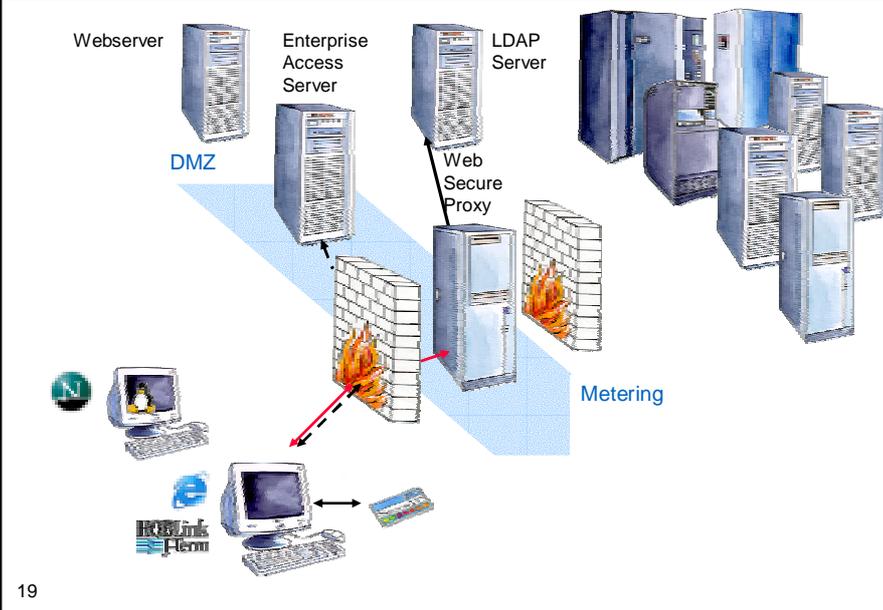
HOBLink J-Term ... über Internet



HOBLink J-Term ... und LDAP



HOBLink J-Term ... und LDAP

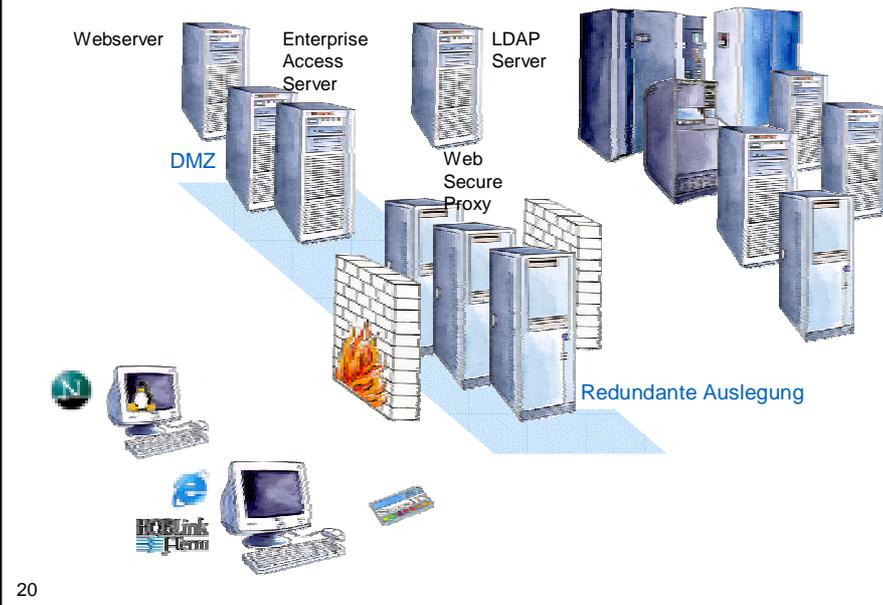


19



HOBLINK
SOFTWARE

HOBLink J-Term ... Erhöhung der Ausfallsicherheit



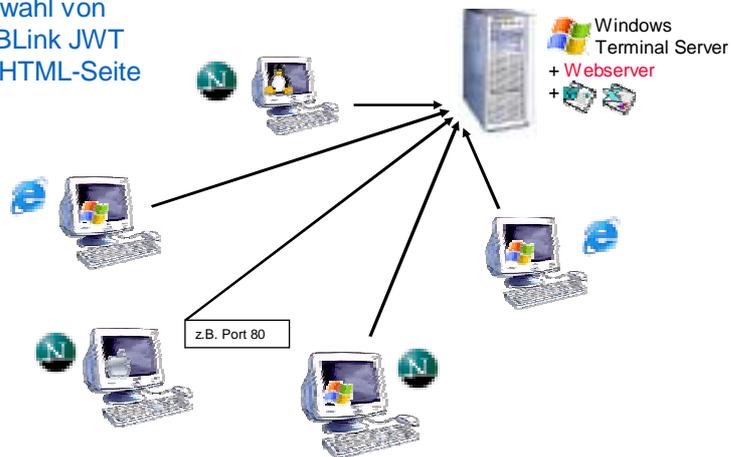
20



HOBLINK
SOFTWARE

HOBLink JWT ... in der Arbeitsgruppe

Auswahl von
HOBLink JWT
auf HTML-Seite



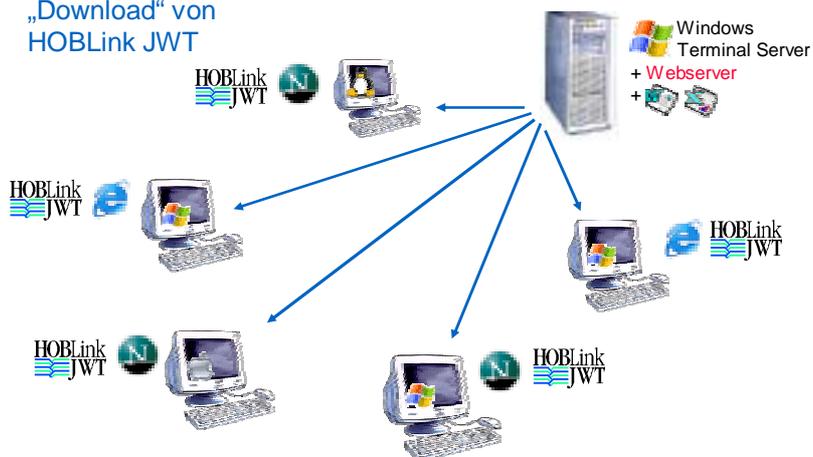
21



HOBLINK
SOFTWARE

HOBLink JWT ... in der Arbeitsgruppe

„Download“ von
HOBLink JWT



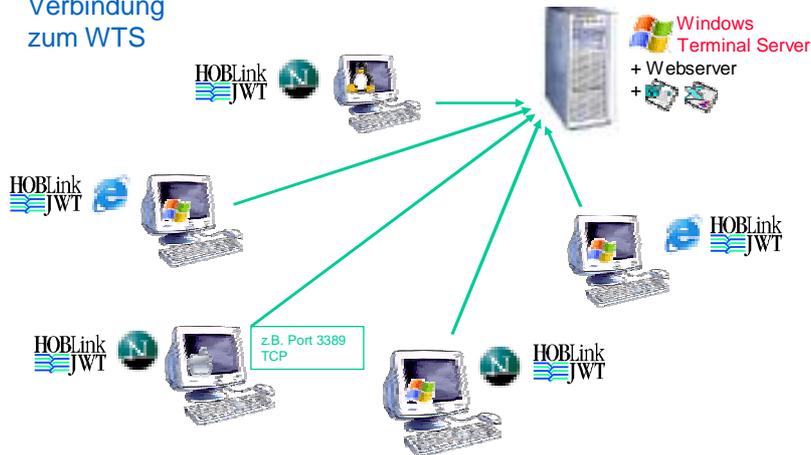
22



HOBLINK
SOFTWARE

HOBLink JWT ... in der Arbeitsgruppe

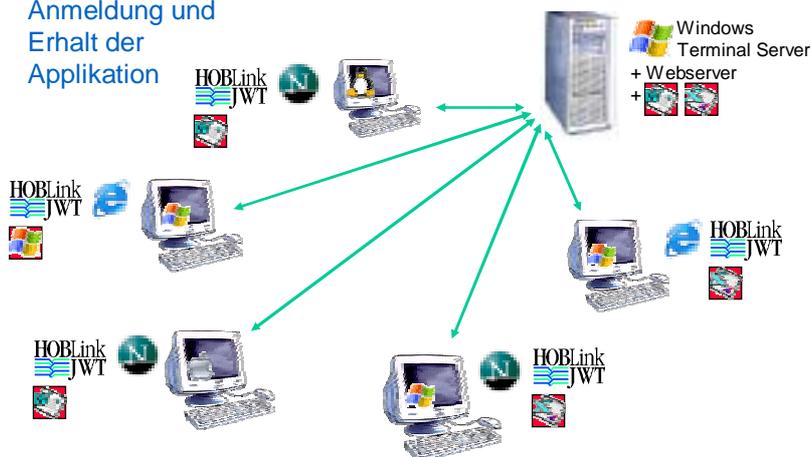
Verbindung
zum WTS



23

HOBLink JWT ... in der Arbeitsgruppe

Anmeldung und
Erhalt der
Applikation



24

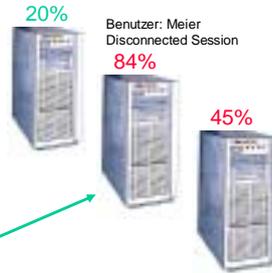
HOBLink JWT ... und eine Terminalserver-Farm

Terminalserver-Farm
mit unterschiedlich
installierten WTS

HOBLink
JWT



Benutzer: Meier



Gezielte Verbindung zu einer
Disconnected Session.

Gleiches Verfahren für
Application Publishing

25



HOBLINK
SOFTWARE

HOBLink JWT ... im Einsatz über Internet

Terminalserver-Farm
hinter einer Firewall

HOBLink
JWT



z.B. Port 80
TCP

öffentliche IP
z.B. 217.12.3.11

private IP
z.B. 10.0.1.100

private IP
z.B. 10.0.1.101

private IP
z.B. 10.0.1.102

z.B. Port 4095
UDP

Auswahl des WTS mit Hilfe
des HOB Load Balancing

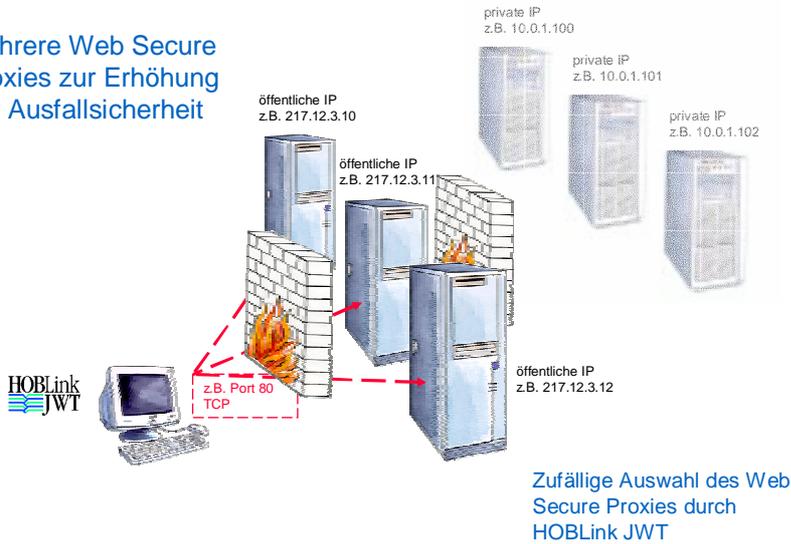
26



HOBLINK
SOFTWARE

HOBLink JWT ... im Einsatz über Internet

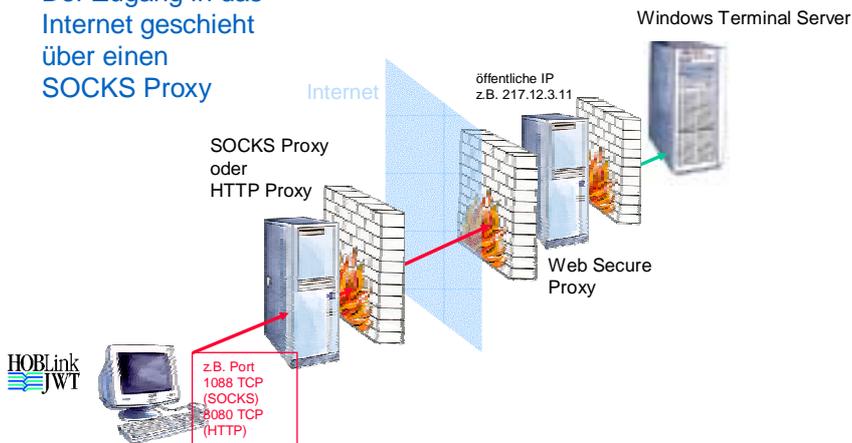
Mehrere Web Secure Proxies zur Erhöhung der Ausfallsicherheit



27

HOBLink JWT ... in Kombination mit SOCKS Proxies+SSL

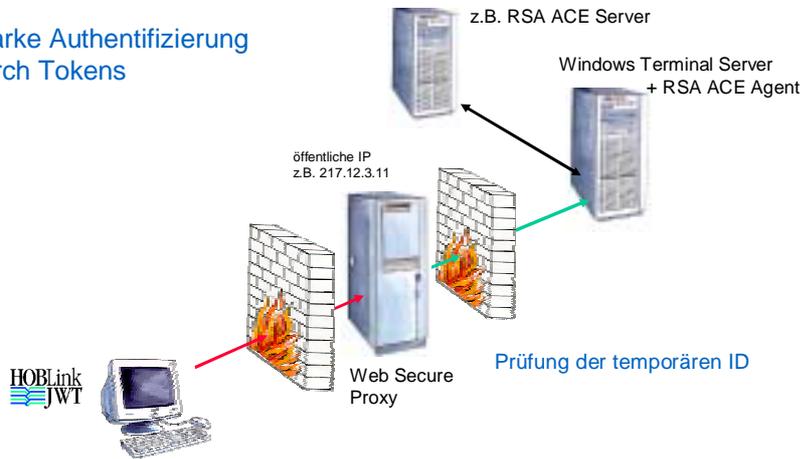
Der Zugang in das Internet geschieht über einen SOCKS Proxy



28

HOBLink JWT ... und Authentifizierungs-Token

Starke Authentifizierung
durch Tokens



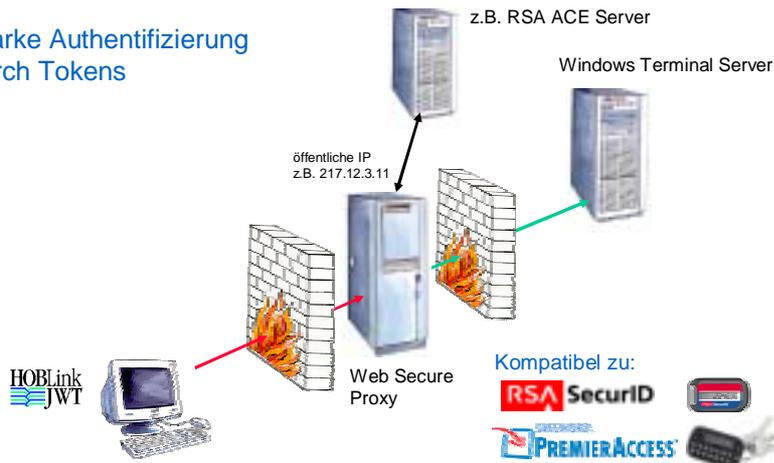
29



HOBLINK
SOFTWARE

HOBLink JWT ... und Authentifizierungs-Token

Starke Authentifizierung
durch Tokens



30



HOBLINK
SOFTWARE

HOBLink J-Term - Integration

- einfache Integration
 - durch frei wählbare Ports
 - angepasst wird nur die Software und nicht die bestehende Infrastruktur
- Sicherheit bleibt erhalten
 - Vorhandene Zugänge können genutzt werden

31



HOBLINK
SOFTWARE

HOBLink J-Term - Potentiale

- **Investitionsschutz** durch Nutzung der bestehenden Infrastruktur
- **Kostensenkungspotentiale** durch Einsatz der Java Technologie, die eine **zentrale** Durchführung von Installations-, Konfigurations- und Administrationsaufgaben ermöglicht
- die **effiziente** und **sichere** Anbindung aller Client-Plattformen an zentrale Daten und Applikationen

32



HOBLINK
SOFTWARE

Details zu HOB Enterprise Access

Auf einen Blick:

- Zentrale und plattformübergreifende Benutzerverwaltung
- Zentrale und plattformübergreifende Applikationsverwaltung
- Universelle Clientsoftware
(in Verb. mit HOBLink J-Term)

33



HOB
SOFTWARE

HOB Enterprise Access - Grundgedanke

- Ausgangssituation
 - Benutzerverzeichnis zum Login
 - Telefonnummern-Verzeichnis
 - E-Mail-Verzeichnis
 - Verzeichnis installierter Software
 - Konfigurationsdaten der Hardware
 - benutzerabhängige Konfigurationsdaten verschiedener Applikationen
 - ... Personaldaten ... Organigramm ... PKI ... DNS ... NIS
- Eine Studie von Forrester Res. aus den USA besagt, daß große Unternehmen **im Mittel 180 verschiedene Verzeichnisse** parallel betreiben!

34



HOB
SOFTWARE

HOB Enterprise Access - Grundgedanke

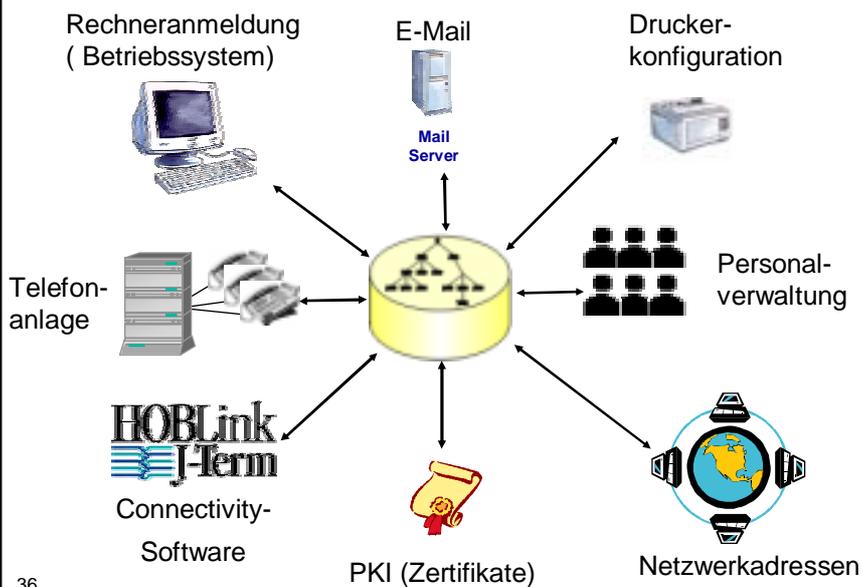
- Nachteile vieler Verzeichnisdienste
 - Mehrfachaufwand zur Pflege der Daten
 - Inkonsistenz der Daten
 - Redundanz in den Daten
 - veraltete Daten
 - aufwendige Synchronisations-Mechanismen
 - "Insel-Denken"
(ICH und MEINE Daten)

35



HOB
SOFTWARE

HOB Enterprise Access - Grundgedanke



36



HOB
SOFTWARE

HOB Enterprise Access - Zentrale Administration

- Zentrale Userverwaltung
- Vererbung von Einstellungen und Rechten
 - über Gruppenzugehörigkeit
 - über Organisationsstruktur
- Zentrale Sessionkonfiguration
- Konfiguration aller Enterprise Access-fähigen HOB Produkte
- Automatische Benutzerstatistiken

37



HOB
SOFTWARE

HOB Enterprise Access - LDAP Unterstützung

- Zugriff auf LDAP-Verzeichnisse (LDAP v3)
 - IBM SecureWay Directory Server
 - MS Active Directory Server
 - iPlanet Directory Server
 - Novell eDirectory
 - Siemens DirX
 - Manuelle Anpassung an jeden anderen LDAP Server
- **Schemaerweiterung** zur Integration der HOB Benutzerdaten in LDAP-Verzeichnis
- LDAP-Benutzer stehen im Enterprise Access zur Verfügung
- **Keine mehrfache** Benutzerverwaltung

38



HOB
SOFTWARE

HOB Enterprise Access - Zentrale Administration

- Zentrales und übersichtliches Konfigurationsmenü für den Administrator

In diesem Fenster werden die jeweiligen Mitglieder aus dem entsprechenden Ordner (Anwender, Gruppe, Container oder Objekt) angezeigt.

Über dieses Fenster bestimmt der Anwender, welche Applikation konfiguriert bzw. zugeordnet werden soll.

Hier wird die Organisationsstruktur abgebildet. Diese besteht aus Anwendern, Gruppen, Containern und Objekten.

Dieses Konfigurationsbutton öffnet das Tor zur eigentlichen Vorkonfiguration der Anwendung (Session Editor).

39

HOB Enterprise Access - Zentrale Administration

- Vererbung und Einstellung von Rechten

40

HOB Enterprise Access - Vorteile

- Administration und Konfiguration an einem zentralen Punkt
- Optimale Kontrolle der Benutzerrechte
- Zero Day Employee - Anlegen eines neuen Mitarbeiters in zwei Schritten:
 - Vergeben eines Usernamens
 - Zuordnen zu einer Gruppe; entsprechende Rechte werden automatisch vererbt
- Minimaler Administrationsaufwand
- Senkung der TCO

43



HOB
SOFTWARE

Enterprise Access fähige Produkte

- HOBLink J-Term
inkl. HOB Proxy Server
(SSL fähiger Proxy in Java)
- HOBLink Terminal Edition
- HOBLink JWT
- HOBLink X11

zukünftig:

- HOBLink VPN

44



HOB
SOFTWARE

Warum brauchen Sie Kryptographie?

- Sie nutzen öffentliche Netze
 - für die Zusammenarbeit verschiedener Betriebsteile (Entwicklung u. Produktion)
 - zum Datenaustausch mit Filialen
 - für Beziehungen zu Lieferanten
 - für Bestellungen von Kunden
 - zur Darstellung in der Öffentlichkeit
- Kommunikation im Internet entspricht heute meist dem Senden einer Postkarte - nicht eines verschlossenen Briefes!

45



HOB
SOFTWARE

Was erwarten Sie von „sicherer“ Kommunikation?

- Vertraulichkeit
 - Daten sind nur vom vorgesehenen Empfänger lesbar
- Integrität
 - Daten können nicht unbemerkt von Dritten verändert werden
- Echtheit (Authentizität)
 - Daten stammen vom genannten Absender
- Praktikabilität
 - Datenaustausch wird durch Sicherheitsmaßnahmen nicht unzumutbar behindert

46



HOB
SOFTWARE

Sicherheit - womit und wogegen

wogegen?	womit?
Spionage, Fälschung bei der Datenkommunikation	SSL: HOBLink Secure (ähnlich auch mit VPN)
unautorisierte Zugriffe über das Netzwerk	Firewall, Intrusion Detection System
kompromittierende Kanäle anzapfen	Abschirmung, Datenträgervernichtung
Password cracking	Beachtung von Regeln
Viren, Trojanische Pferde, Würmer etc.	Anti-Viren-Software, "diskless systems"
Ausfall, Datenverlust	USV, Backup-Strategie
Bedienungsfehler	Schulung, Administration
Sicherheitslücken	Software-Pflege
Einbruch, Diebstahl	klass. Sicherheitstechnik
klassischer Verrat	Mitarbeiterbindung

47



HOB
SOFTWARE

Was ist Sicherheit?

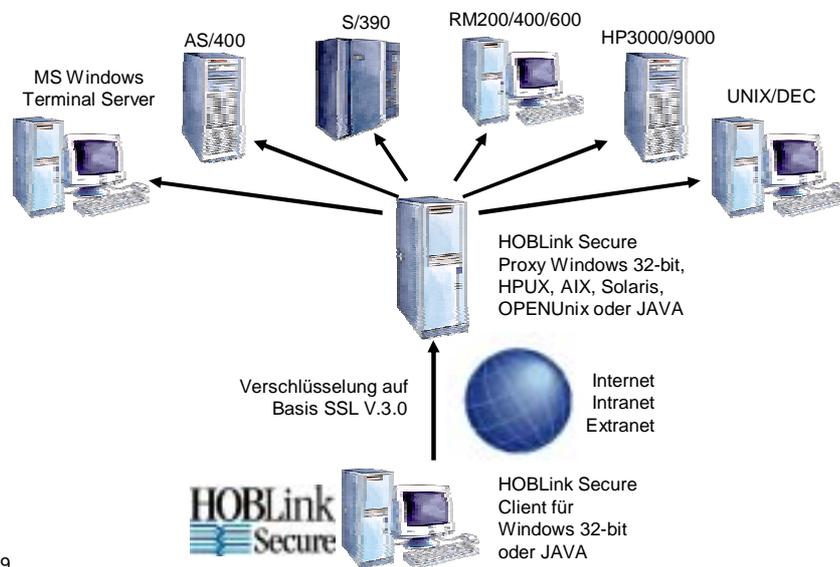
- Sicherheit ist dann gegeben, wenn der Angreifer erkennt, daß der Aufwand für das Überwinden der Sicherheitsmaßnahmen den zu erwartenden Nutzen übersteigt.
- „Das Ziel von Sicherheitsmaßnahmen kann nur sein, zwischen dem Aufwand zur Sicherung und dem Aufwand zum Durchbrechen dieser Sicherung ein Ungleichgewicht zu Ungunsten des Angreifers herzustellen.“

48



HOB
SOFTWARE

Security mit HOBLink Secure



49

„Strong Encryption“ von HOB

- für die Web-to-any-Server-Connectivity mit HOBLink Secure auf Basis von SSL V. 3
 - für HOBLink J-Term und HOBLink JWT
 - für HOBLink Terminal Edition
 - für HOBLink SNA Router
 - für HOBLink DRDA und J-DRDA
- in Deutschland entwickelt
- unterliegt keinen Exportbeschränkungen
- von HOB, einem bekannten Hersteller aus dem Connectivity-Bereich

50

Was bietet HOB an?

- **HOBLink Secure**
 - ist eine Verschlüsselungssoftware
 - mit starker Kryptographie aus Deutschland
 - ohne Schlüssel hinterlegung bei der NSA,
 - die zwischen Transport- und Sitzungsschicht (im OSI-Modell)
 - auf Basis von SSL V.3 bzw. TLS arbeitet.

51



HOB
SOFTWARE

Was zu HOBLink Secure gehört:

- **SSL-Client (bzw. -Server) in C**
 - für Anwender mit Windows-Rechnern,
- **SSL-Client (bzw. -Server) als Java-Applet**
 - für Anwender mit einer JVM (ab 1.1.4)
- **Administrator-Werkzeuge**
 - Java-Programm zur Konfiguration und Zertifikatverwaltung (Security Manager)
 - SSL-Proxy für Anwendungen, die nicht direkt mit unserem SSL-Client arbeiten, sowohl als Windows-, Solaris- als auch als Java-Version erhältlich (in J-Term / Portal)
 - Testwerkzeuge und Hilfsprogramme

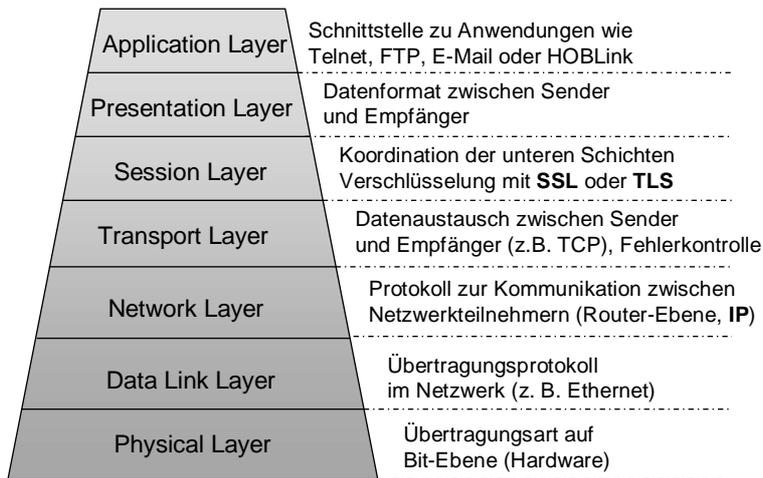
52



HOB
SOFTWARE

OSI-Schichtenmodell

- SSL versus IPsec (VPN)



53

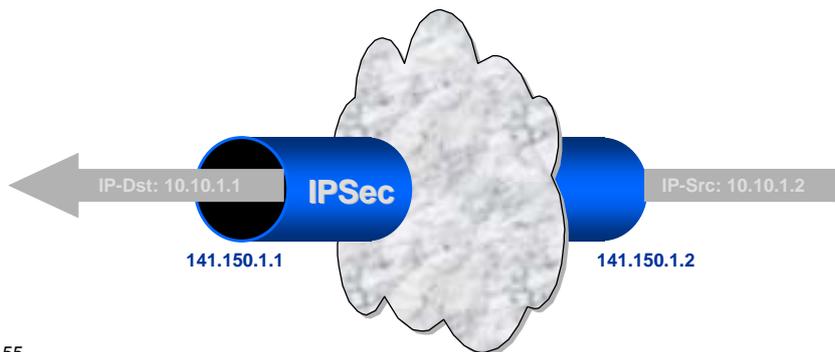
Was ist SSL / TLS?

- Secure Sockets Layer / Transport Layer Security
- Protokolle zum Zugriff auf Applikationen (Client-Server-Modell)
- arbeiten oberhalb der Transportschicht
- Sicherung des Datenaustausches durch Authentifizierung und Verschlüsselung
- Authentifizierung durch Zertifikate (PKI)
- Entwicklung durch einen Hersteller
- einheitliche Implementation

54

VPN

- "Tunneln" von verschlüsselten Datenpaketen mit privaten, nicht registrierten IP-Adressen durch das öffentliche Netzwerk (Internet)



55

Vergleich von SSL und IPsec

SSL/TLS	IPsec/IPv6 (VPN)
zwischen Schicht 4 und 5	Schicht 3 im OSI-Modell
sichert den Datenaustausch mit einzelnen Anwendungen	sichert den IP-Datenstrom; bringt entfernte PCs ins Firmennetz
folgt Client/Server-Modell	Hardware-näher (auf Treiberebene)
sehr flexibel	für feste Verbindungen
PKI mit Zertifikaten	Authentifizierung uneinheitlich
transparent für Netzwerk	IPv6 benötigt kompatibles Netzwerk
optimal für den sicheren Zugriff von Benutzern auf einzelne Anwendungen	optimal zur Verbindung von LANs über das Internet zum Intranet

56

Wann benutze ich was?

- VPN
 - Verbinden zweier Rechnernetze
 - Einbinden von Einzel-PCs in ein Netz
 - Nutzung vieler verschiedener Anwendungen
 - feste Verbindungen (z. B. Router - Router)
- SSL
 - Zugriff auf einzelne Anwendungen auf einem Host-Rechner
 - Zusammenarbeit von einander völlig unbekanntem Gegenstellen
 - wechselnde Verbindungen (Internet-Café)

57



HOB
SOFTWARE

www.Tolly.com

- Zertifiziert bei der Tolly Group
(*independent test lab*)



58



HOB
SOFTWARE