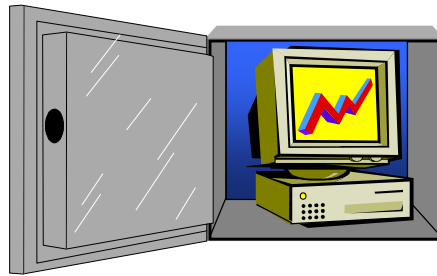




System-Sicherung und System-Konfiguration



j.meissburger@fz-juelich.de



Was tun, um die Sicherheit zu erhöhen ?

(ZAM-TKI-0354)

- Aktuelle Betriebssysteme und Patches einspielen (Microsoft MBSA für NT/2K/XP, Patches von <http://v4.windowsupdate.microsoft.com/de/default.asp>)
- Regelmäßiges Sichern des Betriebssystems und wichtiger Benutzerdaten, Start/Notfalldiskette erstellen und testen (**PowerQuest ImageCenter 5.01**)
- Abschalten nicht benutzter Dienste und Protokolle (nur TCP/IP verwenden!)
- Paßwortgeschützte (verschlüsselte) Benutzerauthentisierung. **Keine anonymen Accounts**. Paßwortschutz für Freigaben („Shares“)
- Nutzung eingebauter Sicherheitsmechanismen in Windows-Applikationen (Internet-Explorer, Makroviruschutz, EFS)
- Die **Einrichtung eines aktuellen Virenschutzprogramms** vor allem für E-Mail und File Download (**F-Prot und NAI Virusscan**)
- Einrichtung eines **persönlichen Firewalls** (**@Guard** oder **Norton Personal Firewall 2002**) zur Steuerung des IP-Verkehrs (**ZAM-TKI-0349** und **IB-9916**)



Updates für Betriebssystem & Komponenten

- Neue Betriebssystemversionen und Patches, Konfiguration:
 - [\\zelcds](#)
 - <http://support.microsoft.com/support/downloads>
- Office- und Explorer-Updates:
 - [\\zelcds.zel.kfa-juelich.de\Off97](#), [\\zelcds\Off2k](#)
 - [\\zelcds.zel.kfa-juelich.de\public\ie](#)
- Antiviren-Software:
 - [\\pcsrv.zam.kfa-juelich.de\public\nai\viruscan](#)
 - [\\pcsrv.zam.kfa-juelich.de\public\f-prot](#)
 - <http://www.fz-juelich.de/zam/net/security/software>
- AtGuard Firewall bzw. Norton Personal Firewall 2002
 - [\\zelcds.zel.kfa-juelich.de\atguard](#) [Symantec Live Update](#)
- Backup:
 - [\\pcsrv.zam.kfa-juelich.de\public\adsm](#) (Datensicherung)
 - 2 Disketten oder CD für PowerQuest [DeployCenter V5.01](#) (ZAM-Dispatch)



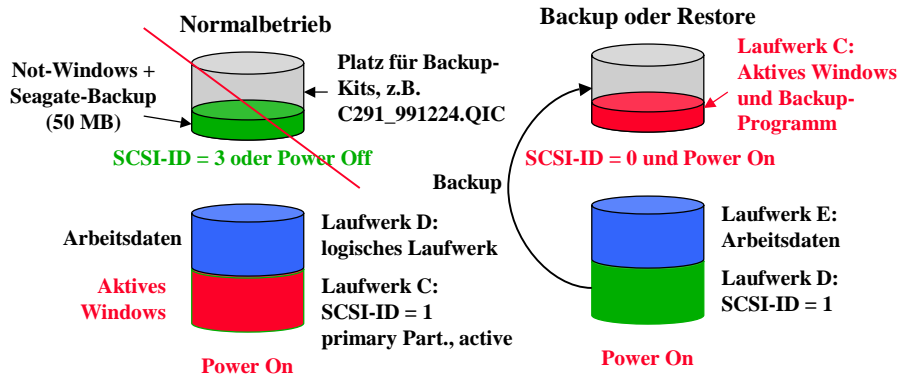
Säubern, Testen, Sichern des Betriebssystems

- Ordner, auf den die Variable „TEMP“ zeigt:
 - C:\TEMP
- Ordner, auf den die Variable „TMP“ zeigt:
 - C:\%WINDIR%\TEMP
- Temporäre Internet-Dateien (Cache):
 - C:\%WINDIR%\Temporary Internet Files
- Aus dem Web geladene Hilfsprogramme (ActiveX, Java):
 - C:\%WINDIR%\Downloaded Program Files
- Cookies:
 - C:\%WINDIR%\Cookies
- Temporäre Disk-Images für CD-Brenner
- **Verifizieren mit „ScanDisk“:** Standard mit automatischer Korrektur



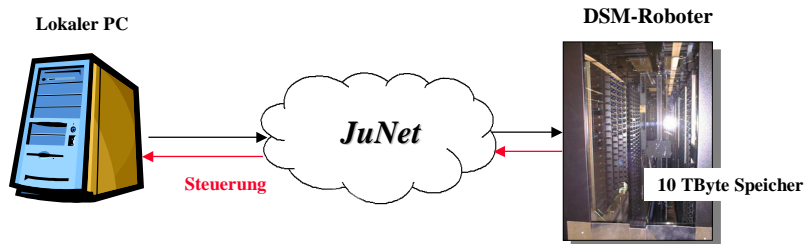
Dual Disk-Backup für Standalone-Systeme

- Schnell, preiswert (<30 Min für 2 GB Betriebssystem), sicher
- Bit-für-Bit-Image des gesamten Betriebssystems inklusive Registry
- unabhängig von der Festplattenstruktur



ADSM inkrementelles Backup

- ADSM (Tivoli) zur regelmäßigen Sicherung von Betriebssystem-Dateien (Konfigurationsdateien) und der Benutzerdaten (incremental backup)
- Backup-Start von Hand, durch lokalen Taskplaner oder fremdgesteuert vom ADSM-Server (L.Wollschläger, 6420)
- **Achtung bei 10 Mb Thinwire-Netzanschluß: Unbedingt mit lokaler Kompression arbeiten, sonst Netzüberlastung!!**

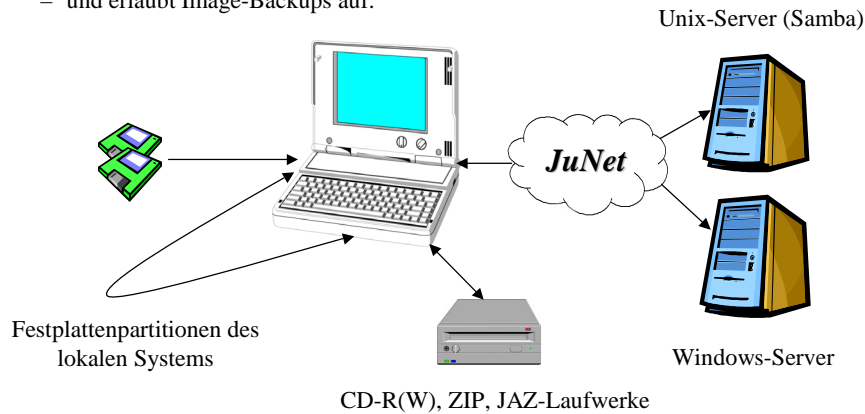




DeployCenter/ImageCenter V5.01

ZAM-IB-2001-02

- Disk-Imaging-Software
 - läuft vollständig von zwei Disketten unter einem stand-alone-Betriebssystem (DOS)
 - und erlaubt Image-Backups auf:



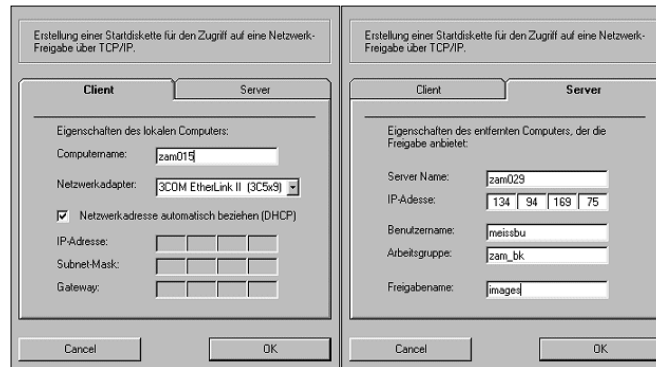
ImageCenter V5.01

- Stand-alone-Betriebssystem erlaubt das bitgenaue Sichern und Restaurieren von Windows- und Linux-Systempartitionen
- Erlaubt „Klonen“ ganzer Festplatten oder einzelner Partitionen.
- Enthält Grundfunktionen zur Repartitionierung mit Datenerhalt und Partitionsverwaltung unter Windows (auch Windows-ME).
- Ermöglicht das Ablegen von Systemkopien als Image-Dateien
 - unterteilt in kleinere Dateien für ZIP, JAZ oder CD/R(W)-Laufwerke
 - mit Schreibprüfung und automatischen Vergleich
 - mit **Paßwortschutz**
- Unterstützt zuverlässig alle gängigen Dateisysteme wie FAT, FAT32(X), NTFS und F-ext 2 auch für große Festplatten (>32 GB)
- Bietet Partitionsverwaltung und Restauration einzelner Dateien unter Windows

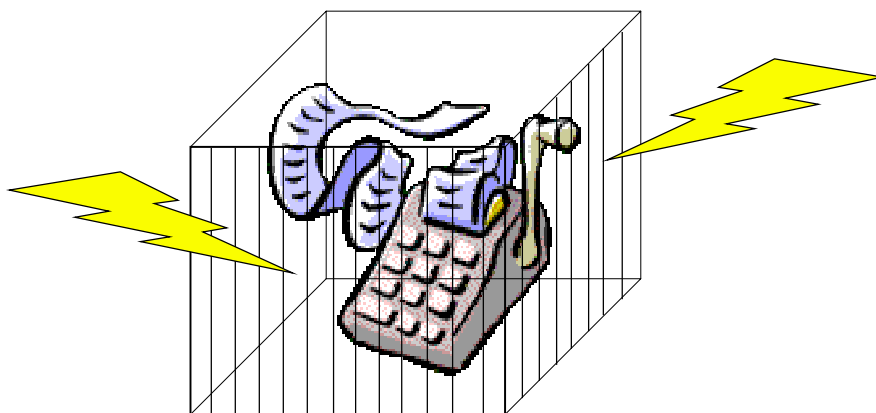


Einrichten der Disketten für Netzwerk-Backup

- Basierend auf einer leeren, DOS-622-formatierten Boot-Diskette und der DriveImagePro-Programmdiskette (beim ZAM-Dispatch erhältlich)
- Halbautomatisches Einrichten der Netzwerk-Startdiskette unter Windows mit Hilfe des Programms „MS_Lan“ ([ZAM-TKI-0366](#))



Schutzfunktionen des Betriebssystems





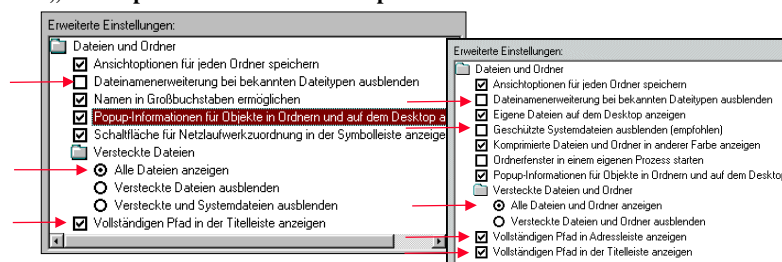
Paßwortschutz

- BIOS-Paßwort verhindert unbefugtes Booten des Systems:
 - Administratives Paßwort zum Schutz der BIOS-Konfiguration
 - Benutzerpaßwort zum Schutz des Windows-Betriebssystems
- Benutzer individuell mit eigenen Profilen einrichten:
 - NT/2k: „Programme - Verwaltung – Benutzermanager/Computerverwaltung“
 - Win95/98: „Start - Einstellungen - Systemsteuerung - Benutzer bzw. Kennwörter“
- Anonyme oder wohlbekannte Benutzernamen vermeiden:
 - Gast / Guest / USR_ *Computername* für anonymen Webzugang, Anonymous FTP
 - Administrator
- Paßwortverschlüsselung für Shares (Windows 98+ und NT+):
 - Paßwort geht bei jedem „Laufwerk verbinden“ über das Netz
 - Paßwortverschlüsselung auch bei Zugriff auf Samba-Server benutzen
 - Bei Windows 9x/ME Security-Patch einspielen:
<http://www.microsoft.com/technet/security/bulletin/MS00-072.asp>
 - **Achtung:** Paßwörter werden gespeichert und können für unauthorisierten Zugriff wiederverwendet werden (kann ggf. durch Editieren der Registry geändert werden)
- Bildschirmschoner mit Paßwortschutz aktivieren (10 Minuten)



Konfiguration des Desktop

- Mit
 - „Arbeitsplatz - Ansicht - Ordneroptionen - Ansicht“



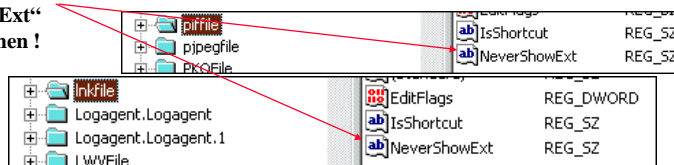
- Alle Dateien anzeigen, versteckte, Systemdateien und dem System „bekannte“ Dateien nicht ausblenden, alle Dateien mit vollem Pfad anzeigen
- Evtl. auch weitere, ausführbaren Dateien wie PIF oder Linkdateien anzeigen durch Ändern mit dem Registrieditor:
 - HKEY_CLASSES-ROOT\xxxxxfile NeverShowExt ändern in AlwaysShowExt



Endungen aller Dateien anzeigen

- Endungen auch für registrierte Dateien anzeigen. Beispiele:
 - `macrotest1.txt.rtf` → Word-Makro, angezeigt als `macrotest1.txt`
 - `Messung.gif.vbs` → Visual Basic Script, angezeigt als `Messung.gif`
- Grundsätzlich interpretiert beispielsweise Office eine Datei beim Öffnen nach ihrem Inhalt, nicht nach ihrer Endung !
 - Ein Makro in `macrotest1.doc`, umbenannt in `macrotest1.txt` wird beim Öffnen mit Word ausgeführt !
- Erweiterungen für bestimmte Dateien wie PIF, LNK etc. immer anzeigen:

„NeverShowExt“ in
„AlwaysShowExt“
ändern oder löschen !



- Vorsicht beim Ausführen MIME-codierter EXE-Dateien (MHTML)



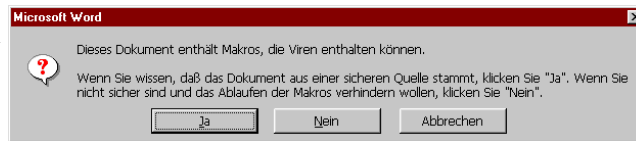
Ausführbare Dateien

- Mit „Arbeitsplatz - Extras – Ordneroptionen – Dateitypen“ wird in der Aktion „Öffnen“ oder „Open“ bzw. der Default-Aktion das Programm angezeigt, das diesen Dateityp öffnet (ausführt)
- Die gängigsten ausführbaren Dateitypen:
BAT, CHM, CMD, COM, CPL, EXE, HLP, HTA, INF, JS, JSE, LNK, MSI, PIF, REG, SCR, SCT, SHS, URL, VB, VBS, VBE, WSC, WSF, WSH
- Die üblichen makrofähigen Dokumenttypen:
XL..., DO..., RTF, PP..., MD...
- Unter Umständen in der Aktion „Öffnen“ (Default) einen Viewer wie <http://office.microsoft.com/downloads/2000/wd97vwr32.aspx> oder QuickViewPlus (http://www.jasc.com/download_4.asp) eintragen



Makrovirus-Schutz

- Microsoft Word, Excel, Access, PowerPoint können Makro-Programme enthalten, die beim Öffnen des Dokuments automatisch gestartet werden
- Solche Programme haben vollen Zugriff auf alle Systemressourcen wie Laufwerke, Dateien, Programme, Registry, Benutzerdaten
- Deshalb mit “Extras - Optionen... - Allgemein - Makrovirus-Schutz “ (Off97) bzw. „Extras - Macro - Sicherheit - Mittel“ (Off2k) den Makroviruschutz einschalten
- Auch beim Öffnen eines Dokuments im Webbrowser (Plugin) funktioniert der Makroviruschutz:
- Vorsicht vor allem beim Öffnen von Dokumenten in der Anlage von E-Mails !!!
Solche Dokumente niemals ohne vorherigen Virenschutz öffnen!!!



Netzwerkconfiguration für JuNet „Netzwerkumgebung - Eigenschaften“

- **Nur TCP/IP-Protokolle benutzen** (der Transport anderer Protokolle wird in JuNet nicht unterstützt bzw. unterbunden)
- NetBEUI und IPX/SPX (Novell) abschalten
- Keine Bindung für „Client für Microsoft Netzwerk“ oder „Datei- und Druckerfreigabe für Microsoft-Netzwerk“ über DFÜ einrichten bzw. entfernen, falls vorhanden
- Netzwerk-Monitoragent, falls installiert, nicht aktivieren
- Kein IP-Forwarding einschalten
- DNS für Windows-Auflösung (IP-Namensauflösung) und DHCP für Adreßkonfiguration benutzen



Freigabe von Systemressourcen

- Laufwerk oder Ordner freigeben

Mit „Laufwerk - RM - Eigenschaften - Freigabe“

Freigabe für den Zugriff durch einen aktiven Webserver

Mit angehängtem „\$“ beim „Browsen“ nicht sichtbar !

Schreib/Leschutz durch Paßwort.

Achtung: Ohne Paßwort kann jeder zugreifen!

„NetWatch“ aus dem NT-Resourcekit zeigt aktuell benutzte Shares

- Drucker freigeben:



Mit „Start - Einstellungen - Drucker - RM - Eigenschaften - Freigabe“



Aktivieren der Paßwortverschlüsselung für Windows 98 / NT (nicht Win95!)

- Windows 98:
 - REGEDIT4


```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNetsup]
"EnablePlainTextPassword"=dword:00000000
```
- Windows NT 4.0
 - REGEDIT4


```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]
"EnablePlainTextPassword"=dword:00000000
```
- Windows 2000
 - REGEDIT4


```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"EnablePlainTextPassword"=dword:00000000
```



Freigabe von Shares und Webordnern

- Share-Freigabe für den Zugriff aus dem Netz (Netzlaufwerk) mit Hilfe der „NETBIOS -Dienste“ (über IP) im Microsoft Netzwerk
- Shares werden automatisch bei Systeminstallation (NT) eingerichtet
 - Windows NT: ADMIN\$, IPC\$, C\$, D\$,..... Für administrativen Zugriff
 - aber auch: Taskplaner (Outlook), Drucker, Webseiten (IIS oder Peer Web Server)
- Überprüfen mit
 - „net share“ bzw.
 - „net view **rechnername**“
 - „Server - Freigaben“ in der NT/2k-Sytemsteuerung
- Web-Freigaben:
 - mit dem Internet-Dienst-Manager überprüfen (anonym/NT-Anmeldung)
 - Aliasnamen benutzen: C:\InetPub\wwwroot\cgi-bin → http://webserver/bin
 - Zugriffsrechte „Lesen“, und „Scripting“ setzen (normalerweise nicht „Ausführen“)
 - Anonymen Zugriff erlauben oder Benutzeranmeldung (NT) verlangen

```
C:\>net share

Name           Ressource           Beschreibung
-----
ADMIN$         C:\WINNT            Remote-Admin
IPC$           C:\                 Remote-IPC
C$             C:\                 Standardfreigabe
D$             D:\                 Standardfreigabe
P$            P:\                 Standardfreigabe

Der Befehl wurde erfolgreich ausgeführt.
```

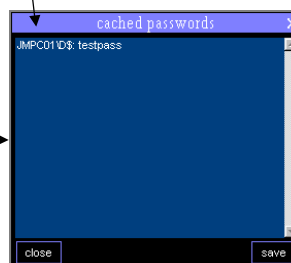
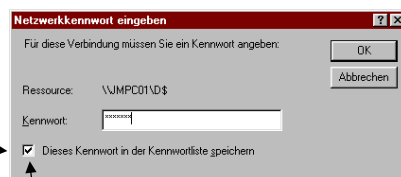


Speichern von NETBIOS-Paßwörtern

- Keine Kennwörter in der Kennwortliste

C:\%WINDIR%\{userid}.pwl

abspeichern !

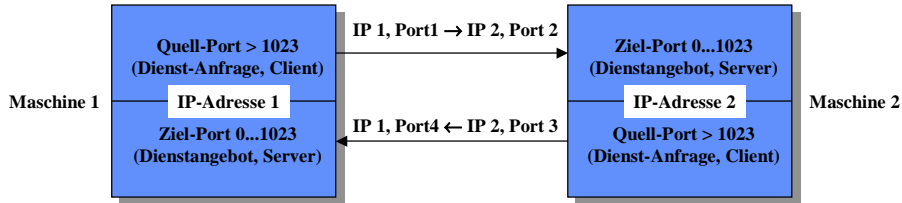


- Ein Trojaner könnte sie ganz leicht auslesen und mißbrauchen!



Das Prinzip der IP-Kommunikation

- Ein IP-Verbindung zwischen zwei Maschinen wird über "IP-Sockets" mit Hilfe der WinSock-Schnittstelle (WINSOCK.DLL) hergestellt:



- Ein Server bietet Dienste im Netz an, indem ein Programm (ein "Dienst") auf einem ganz bestimmten IP-Port (TCP oder UDP) "lauscht"

PortNumbers

- Ein Client versucht
 - sich mit diesem Port zu verbinden ("SYNC") und dann über die stehende Verbindung Daten auszutauschen (verbindungsorientiert, TCP)
 - oder einfach Pakete an den Port zu senden und zu hoffen, daß diese ankommen (verbindungslos, UDP)



Welche Dienste biete ich an und wer ist mit meinem System verbunden ?

- Mit "netstat -a | more" in einer DOS-Box werden die auf zam125 aktiven Ports und Verbindungen angezeigt:



Dienste (Daemons) unter Windows NT

- „Netzwerk - Eigenschaften - Dienste“
- „Start - Einstellungen - Systemsteuerung - Dienste“

3Com dRMON SmartAgent PC Software: Zur Fernüberwachung des Systems mit SNMP

Arbeitsstationsdienst: Erlaubt dem Rechner, als Client im Microsoft-Netzwerk zu arbeiten

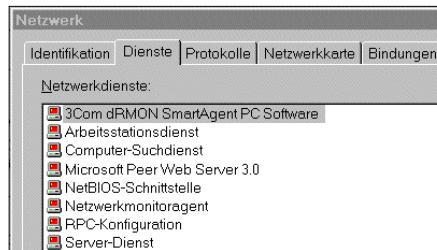
Computersuchdienst: Durchsucht ein Microsoft-Netzwerk nach freigegebenen Ressourcen.

Microsoft Peer Web Server (PWS): Ein einfacher Webserver für das Web-Publishing

NETBIOS über IP (PC) = Samba (Unix)

Dienste:

•nbname:	Port 137
•nbdatagram:	Port 138
•nbssession:	Port 139
•microsoft-ds	Port 445



NetBIOS-Schnittstelle: Erlaubt die Ausführung von NETBIOS-Applikationen auf dem Rechner

Netzwerkmonitoragent: Erlaubt die Fernüberwachung des Rechners und des Netzes

RPC-Konfiguration: Remote Procedure Call, auch lokal (COM/DCOM) benutzt

Serverdienst: Erlaubt die Freigabe von Laufwerken, Ordnern und Druckern



Dienste unter Windows 2k (Server)

- Unter „Systemsteuerung – Software – Windows-Komponenten“
- Internet-Informationdienste nur installieren, wenn ein Webserver (IIS) betrieben werden soll! Zusatzdienste nur, falls unbedingt erforderlich!
 - Dokumentation
 - Ggf. Frontpage 2000 Servererweiterungen nur bei Site-Management mit FrontPage
 - Gemeinsame Dateien
 - Ggf. Internetdienste-Manager (HTML) nur bei Remote-Management über Web
 - WWW-Server
 - Kein NNTP, SMTP, FTP, VisualInterDev
- Nicht benötigt:
 - Netzwerkdienste
 - Remoteinstallationsdienste
- **Auf keinen Fall Netzwerkdienste** (außer vielleicht einfache TCP/IP-Dienste für Testzwecke) **installieren ! Kein DHCP, DNS, WINS!!!**



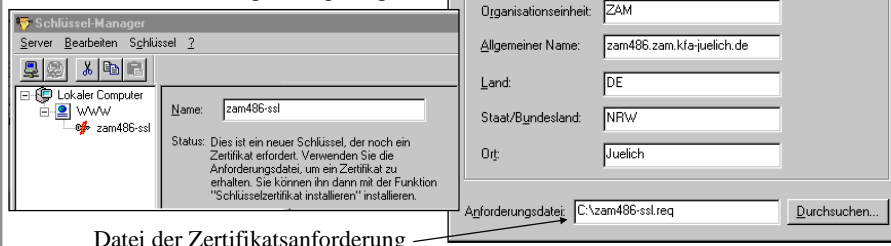
IIS und PWS: Sicherheit von Webservern

- Auf gängigen Ports (80, 8080 etc.) nur aktivieren, wenn unbedingt erforderlich
- Standarddokument definieren, Durchsuchen von Verzeichnissen nicht zulassen
- PWS nur in Verbindung mit einer Personal Firewall betreiben
- Default-Scripte und Remote Management abschalten
- Gopher-, FTP-Dienste abschalten
- Server-Scripts (CGI, PHP, ASP) nur von Alias-Verzeichnissen ausführen, Scripting nur in dafür bestimmten Verzeichnissen zulassen
- Keine Interpreter (Perl, TCL, PHP) in cgi-bin-Verzeichnissen ablegen
- Logging aller Zugriffe aktivieren
- Bei FrontPage Server-Extensions (_vti_*) auf Zugriffsrechte achten
- SSL-Verschlüsselung mit FZJ-Zertifikat einrichten



IIS und PWS für SSL einrichten

1. Im Schlüssel-Managers des Internet-Dienste-Managers für den WWW-Server die Funktion „Schlüssel - Neuen Schlüssel erstellen“ ausführen
2. Menü ausfüllen, verwendetes Paßwort für eigenen Schlüssel gut merken!
3. Der neue, noch nicht zertifizierte Schlüssel (1024 bit Default) wird im Dienste-Manager eingetragen





FZJ-CA-Zertifikat anfordern

4. Funktion „Serverzertifikat anfordern“ auf dem CA-Server des FZJ <http://www.fz-juelich.de/CA/x509/ca-home.htm> ausführen Zertifikatsrequest
5. Den Text aus **zam486-ssl.req** mit cut&paste in das Feld „PKCS“ einfügen. Formular ausfüllen und abschicken
6. Beim ZAM-Dispatch mit Personalausweis Formular unterzeichnen
7. Den Text des per E-Mail oder Web erhaltenen „Base 64 encoded certificate“ zwischen BEGIN und END etwa als **zam486-servercert.txt** auf dem Desktop ablegen
8. Im Schlüssel-Manager des Internet-Dienste-Managers den noch nicht zertifizierten Schlüssel auswählen und „Schlüssel - Schlüsselzertifikat installieren“ ausführen
9. **zam486-servercert.txt** angeben und mit Kennwort bestätigen. Damit ist das Zertifikat im Webserver registriert.



Webserver für SSL-Zugang einrichten

10. Serververbindung "Standard" mit OK bestätigen
11. Internet-Dienste-Manager starten, Eigenschaften des WWW-Dienstes anzeigen
12. Verzeichnis für Zugriff über SSL auswählen, z.B. das Stammverzeichnis, falls nur SSL-Zugang erlaubt sein soll
13. "Sicherer SSL-Kanal erforderlich" aktivieren →
14. Damit ist der Webserver für SSL-Zugang (https://, Port 443) eingerichtet

Eigenschaften des Verzeichnisses

Verzeichnis:

Basisverzeichnis

Virtuelles Verzeichnis

Alias:

Konteninformationen

Benutzername:

Kennwort:

Virtueller Server

IP-Adresse des virtuellen Servers:

Zugriff

Lesen Ausführen

Sicherer SSL-Kanal erforderlich

Client-Zertifikate aktiviert Client-Zertifikate erforderlich

Beispiel PWS



Wer sich im Web bewegt



Windows-Basistechnologien

- Alle Windows-Systeme implementieren das „**D**istributed **C**ommon **O**bject **M**odel (COM/DCOM)“, mit dem Applikationen (DLL 's oder EXE 's) über eindeutige Class-Identifiers (CLSIDs) ihre Eigenschaften und Methoden mit Hilfe von RPC im Netz anbieten
- **ActiveX**-Steuerelemente (OLE-Controls) sind COM-Objekte zur Entwicklung modularer, wiederverwendbarer Softwarekomponenten in OLE-Technik (**O**bject **L**inking and **E**embedding-Technik)
- Microsoft's **J**ava **V**irtual **M**achine (VM) ist beispielsweise ein solches ActiveX-Control, das mit Hilfe von COM scriptfähig gemacht wurde
- **Active Scripting** basiert auf COM-Interfaces, mit deren Hilfe viele Applikationen ihre Objekte als programmierbare Variable an Scripting-Engines wie VBScript oder JavaScript exportieren. Damit sind diese Programme durch Scriptsprachen (Interpreter) steuerbar



Warum gefährlich ?

- Ein Programm, das einmal auf dem eigenen PC läuft, kann auf jede Systemkomponente und auf das Netz zugreifen. Ebenso kann es aus dem Netz ferngesteuert werden. Deshalb Vorsicht beim Ausführen fremder Programme (z.B. aus **Email-Attachments oder Download von Webseiten**)
- Viele Applikationen wie beispielsweise der Internet-Explorer, Outlook (Express) oder der Windows Scripting Host können durch Scripting andere Programme starten oder bereits laufende Programme steuern
- Office-Applikationen können **beim Öffnen von Dokumenten aller unterstützten Dateitypen (!) automatisch Makro-Programme ausführen**, die ihrerseits weitere Programme starten und steuern können
- Durch Scripting und dynamisches HTML auf Webseiten und in HTML-formatiierten Emails sind Zugriffe auf Systemkomponenten und Benutzerdaten möglich



Was kann der Internet-Explorer ?

- Der Internet-Explorer interpretiert die von einem Webserver heruntergeladenen HTML-Dateien (Webseiten) und stellt sie dar
- Er liefert auf Anfrage des Servers Informationen über den Benutzer und dessen Browsingprofile („privacy“)
- Er führt die in der HTML-Seite eingebetteten Scripts (JavaScript oder VBScript) in einer abgesicherten (?) Umgebung aus (Scripting Host)
- Er lädt automatisch ActiveX-Steuerelemente vom Webserver und führt diese lokal auf dem PC aus (C:\%WINDIR%\Downloaded program files)
- Er lädt bei Bedarf (gesteuert durch den MIME-Typ des angeforderten Dokuments) Plugin-Programme und zeigt deren Ergebnisse als integralen Bestandteil der gerade dargestellten Webseite an
- Er läßt sich als Automation Object beliebig neu instanzieren (erzeugen) und durch Scripting fernsteuern (auch völlig unsichtbar im Hintergrund)



Windows Script Host

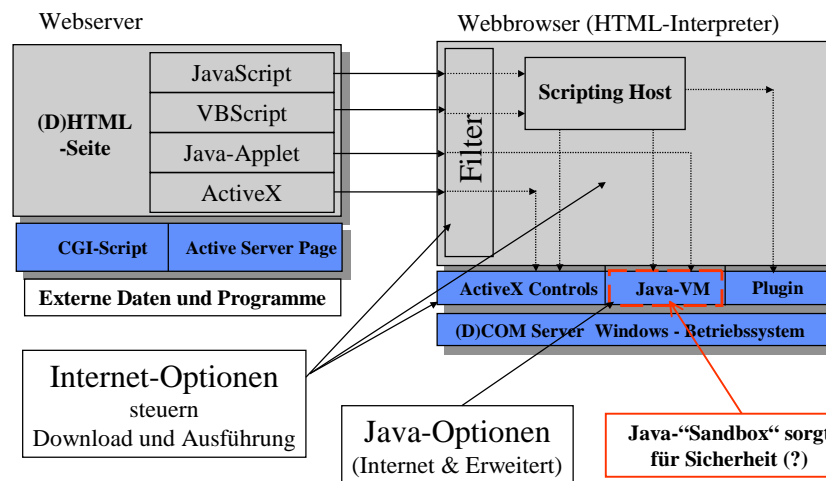
- Derzeit unterstützte Scriptsprachen
 - „JavaScript“ (*.js)
 - „VBScript“ (*.vbs)
 - „VBScript encoded“ (*.vbe)
- Werden unter Windows interpretiert durch
 - C:\% WINDIR%\WSCRIPT.EXE
 - C:\% WINDIR%\COMMAND\CSCRIPT.EXE
- Wer ganz sicher gehen möchte, kann diese beiden umbenennen (etwa in „wscript_exe.sav“) oder durch einen harmlosen Texteditor ersetzen
- Script-Beispiel: Unbemerkttes Öffnen einer fremden Website im Hintergrund:



msie2.vbs



Zusammenspiel verschiedener Webtechniken





„Internetoptionen - Sicherheit - Stufe anpassen“ (1)

- Auch sichere ActiveX-Controls sind nicht wirklich sicher!
- Das auf jeden Fall verhindern!
- Manchmal braucht man die einfach (z.B. Acrobat-Reader)
- Hängt vom Vertrauen in den Serverbetreiber ab!
- Auf keinen Fall, zu gefährlich!
- Entweder immer fragen oder nur im Intranet den aktuellen Namen und Paßwort benutzen

The screenshot shows the 'ActiveX-Steuerelemente und Plugins' section of the Internet Options dialog. It lists several categories with their respective security settings:

- ActiveX-Steuerelemente ausführen, die für Scripting sicher sind:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- ActiveX-Steuerelemente und Plugins ausführen:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Vom Administrator genehmigt
- Download von signierten ActiveX-Steuerelementen:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Download von unsignierten ActiveX-Steuerelementen:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Benutzerauthentifizierung:**
 - Anmeldung
 - Anonyme Anmeldung
 - Automatische Anmeldung mit aktuellem Benutzernamen
 - Automatisches Anmelden nur in der Intranetzone
 - Nach Benutzername und Kennwort fragen



„Internetoptionen - Sicherheit - Stufe anpassen“ (2)

- Cookies sind harmlos (können aber vom Serverbetreiber zum Erstellen von Nutzerprofilen benutzt werden)
- Ab und zu muß man mal eine Datei herunterladen.
- Schriftarten (Fonts) sind wohl unproblematisch und sorgen für korrekte Darstellung
- Java sollte mit hoher Sicherheit immer gut genug funktionieren. Individuelle Einstellungen sind aber mit „Benutzerdefiniert“ möglich

The screenshot shows the 'Content Advisor' section of the Internet Options dialog. It lists several categories with their respective security settings:

- Cookies:**
 - Cookies annehmen, die gespeichert sind:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Cookies pro Sitzung annehmen (nicht gespeichert):**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Download:**
 - Dateidownload:**
 - Aktivieren
 - Deaktivieren
 - Schriftartdownload:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung 1g
- Microsoft VM:**
 - Java-Einstellungen:**
 - Benutzerdefiniert
 - Hohe Sicherheit
 - Java deaktivieren
 - Mittlere Sicherheit
 - Niedrige Sicherheit



„Internetoptionen - Sicherheit - Stufe anpassen“ (3)

- **Active Scripting ist nicht sicher.**
Aber ohne kann man kaum auskommen. Das ist sicher!
- Kaum gebraucht, daher nachfragen!
- Kaum benutzt, nachfragen!
- Sollte eigentlich kein Server tun, also abschalten!
- Wird auch von Microsoft immer abgeschaltet!
- Nur wenn man sich sicher ist, deshalb nachfragen!

The screenshot shows the 'Content Advisor' tab in Internet Options. It lists several categories with their respective settings:

- Scripting**
 - Active Scripting
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Einfügeoperationen über ein Skript zulassen
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Scripting von Java-Applets
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Verschiedenes**
 - Auf Datenquellen über Domänengrenzen hinweg zugreifen
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Dauerhaftigkeit der Benutzerdaten
 - Aktivieren
 - Deaktivieren
 - Installation von Desktopobjekten
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung

Blue arrows point from the text on the left to the corresponding settings in the screenshot. A red box with the text "Im Zweifelsfalle besser aktivieren!" has a red arrow pointing to the 'Active Scripting' setting.



„Internetoptionen - Sicherheit - Stufe anpassen“ (4)

- Nur, wenn man dem Server vertraut. Deshalb fragen!
- Unbedingt nachfragen, damit man es überhaupt merkt!
- Da kann zwar jeder mitlesen, aber ohne geht's kaum (besser wäre natürlich SSL)!
- Unkritisch, deshalb aktiviert!
- Was immer das heißt!

The screenshot shows the 'Content Advisor' tab in Internet Options. It lists several categories with their respective settings:

- Programme und Dateien in einem IFRAME starten
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Subframes zwischen verschiedenen Domänen bewegen
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Unverschlüsselte Formular Daten übermitteln
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Ziehen und Ablegen oder Kopieren und Einfügen von Dateien
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Zugriffsrechte für Softwarechannel
 - Hohe Sicherheit
 - Mittlere Sicherheit
 - Niedrige Sicherheit

Blue arrows point from the text on the left to the corresponding settings in the screenshot.



„Internetoptionen - Erweitert“

- Einige Einstellungen in den Optionen „Erweitert“ haben indirekt Einfluß auf die Sicherheit beim Browser im Internet.

- Wer nicht alleine auf seinem PC ist, sollte auch dies noch aktivieren!

Browsing	
<input type="checkbox"/>	Automatische Überprüfung auf Aktualisierungen von Internet Explorer
<input checked="" type="checkbox"/>	Benachrichtigen, wenn Download beendet ist
<input checked="" type="checkbox"/>	Browserfenster in einem eigenen Prozess öffnen
<input type="checkbox"/>	Channelleiste beim Start anzeigen (falls der Active Desktop deaktiviert)
<input checked="" type="checkbox"/>	Die Schaltfläche "Wechseln zu" in der Adressleiste anzeigen
<input checked="" type="checkbox"/>	Installation auf Anfrage aktivieren

Sicherheit	
<input checked="" type="checkbox"/>	Auf zurückgezogene Serverzertifikate überprüfen (Neustart erforderlich)
<input checked="" type="checkbox"/>	Auf zurückgezogene Zertifikate von Herausgebern überprüfen
<input checked="" type="checkbox"/>	Bei ungültigen Site-Zertifikaten warnen
<input checked="" type="checkbox"/>	Beim Wechsel zwischen sicherem und nicht sicherem Modus warnen
<input checked="" type="checkbox"/>	Fortezza verwenden
<input type="checkbox"/>	Leeren des Ordners "Temporary Internet Files" beim Schließen des Br
<input type="checkbox"/>	PCT 1.0 verwenden
<input checked="" type="checkbox"/>	Profil-Assistent aktivieren
<input checked="" type="checkbox"/>	SSL 2.0 verwenden
<input checked="" type="checkbox"/>	SSL 3.0 verwenden
<input type="checkbox"/>	TLS 1.0 verwenden
<input type="checkbox"/>	Verschlüsselte Seiten nicht auf der Festplatte speichern
<input checked="" type="checkbox"/>	Warnen, falls Formulardaten umgelenkt werden



Speichern von Formulardaten vermeiden

- Internetoptionen - Inhalt

Internetoptionen

Algemein | Sicherheit | Inhalt | Verbindungen | Programme | Erweitert

Inhaltsanbieter
Filter helfen Ihnen bei der Kontrolle der Internetinhalte, die auf diesem Computer angezeigt werden können.
Aktivieren... Einstellungen...

Zertifikate
Verwenden Sie Zertifikate, um sich selbst, Zertifizierungsagenturen und Herausgeber zuverlässig zu identifizieren.
Zertifikate... Herausgeber...

Persönliche Informationen
Mit AutoVervollständigen werden Ihre Eingaben gespeichert und Übereinstimmungen vorgeschlagen.
AutoVervollständigen...

Microsoft Profil-Assistent speichert Ihre persönlichen Informationen.
Profil...

OK Abbrechen Übernehmen

- keine Formulardaten und
- keine Kennwörter speichern

Einstellungen für AutoVervollständigen

Mit AutoVervollständigen können Übereinstimmungen mit früheren Eingaben angezeigt werden.

AutoVervollständigen verwenden für:

Webadressen

Formulare

Benutzernamen und Kennwörter für Formulare

Nachfragen, ob Kennwörter gespeichert werden sollen

Verlauf in AutoVervollständigen löschen:

Formulare löschen Kennwörter löschen

Öffnen Sie "Internetoptionen" und wählen Sie "Verlauf leeren" auf der Registerkarte "Allgemein", um Webadressen-Einträge zu löschen.

OK Abbrechen



Datenverschlüsselung: Windows 2000 EFS

- Einfach durchzuführende Verschlüsselung von Ordnern und Dateien
 - Ordner – Rechte Maustaste – Eigenschaften – Erweitert – Inhalt verschlüsseln, um Daten zu schützen
- Zugriff auf verschlüsselte Dateien im EFS

Zugriff durch:	Ordnerinhalt anzeigen	Datei öffnen
Benutzer	Ja	Ja
Anderer Benutzer	Nein	Nein
Anderer Benutzer mit Administrator-Rechten	Ja	Nein
Administrator	Ja	Ja

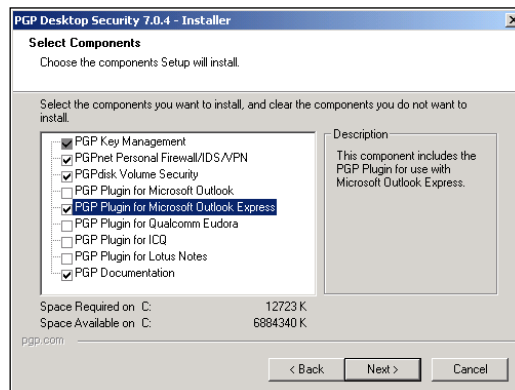
Festlegung der Administrator-Zugriffsrechte durch Eintrag des Administrators in „Agenten für Wiederherstellung von verschlüsselten Daten“ in der lokalen Sicherheitsrichtlinie:

```
OU = EFS File Encryption Certificate
L = EFS
CN = Administrator
```



PGP Desktop Security für Windows V7+

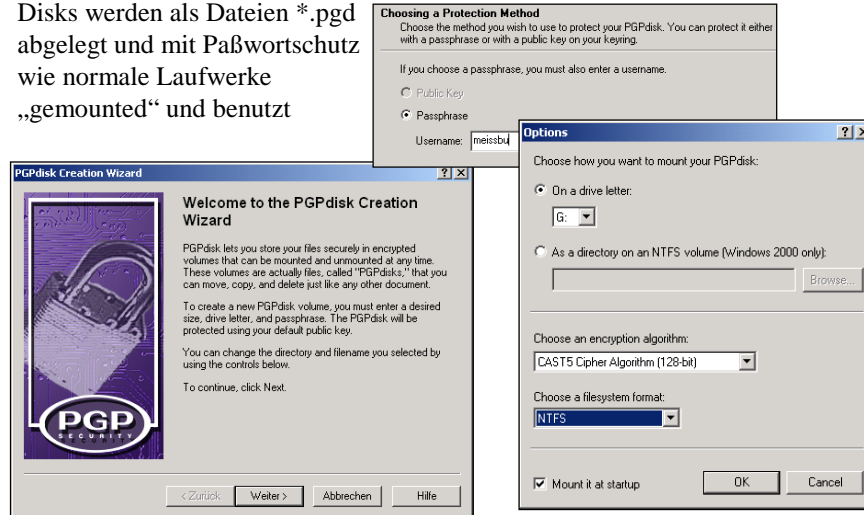
- Verschlüsselung von Dateien
- Erstellen verschlüsselter Container-Disks
- Erstellen und Verwalten von Schlüsselringen und Generierung von Schlüsselpaaren
- Veröffentlichen öffentlicher Schlüssel
- Signieren und Verschlüsseln von E-Mail (Plugin's)





PGP-verschlüsselte Container-Disks

- Disks werden als Dateien *.pgd abgelegt und mit Paßwortschutz „gemountet“ und benutzt



J.Meißburger, FZI- ZAM

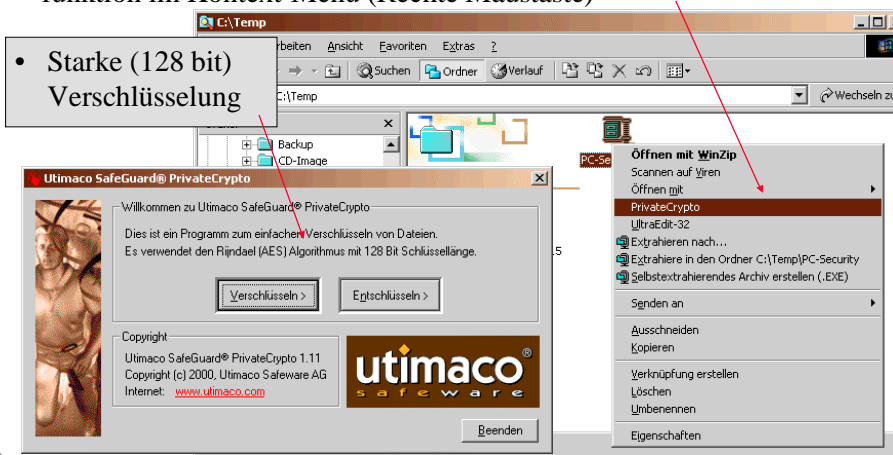
Seite 46



Dateiverschlüsselung mit Utimaco SafeGuard® PrivateCrypto

- Einfach zu benutzende Verschlüsselung von Dateien durch Zusatzfunktion im Kontext-Menü (Rechte Maustaste)

- Starke (128 bit) Verschlüsselung



J.Meißburger, FZI- ZAM

Seite 47



Secure Shell: Sicherer Zugang zu Unix-Systemen

❖ Frei verfügbare Software:

- **TeraTermPro**
VT- und TEK-kompatibler Klient mit ssh V1 für Windows
- **Ssh-Win**
VT-kompatibler Terminalzugang mit ssh V1 für Windows
- **Ssh-Dos**
VT-kompatibler Terminalzugang mit ssh V1 für DOS

❖ Lizenzierte Software:

- **F-Secure**
VT-kompatibler Terminalzugang mit ssh und Schlüsselmanagement, ssh-Versionen 1 und 2 verfügbar
- **ssh-win**
Terminalprogramm **und Server** mit ssh-Verschlüsselung Version 2 (über DFN für das Forschungszentrum lizenziert)



<http://www.fz-juelich.de/zam/net/security/software/ssh/pc>



Zusammenfassung

- Mit Verstand surfen, dubiose Quellen vermeiden, zweifelhafte Mails (auch „Hoaxes“) löschen
- Fremdsoftware und Disketten vor Gebrauch scannen, nicht anbooten !
- Keine Programme (ActiveX controls, Desktop-add-ons etc...) aus dem Netz ausführen ohne sie vorher mit dem Virenschanner zu überprüfen
- Antivirensoftware und Firewall bei Systemstart mitstarten
- Keine Mails automatisch downloaden und öffnen (Vorschau !), Attachments nicht ungeprüft öffnen
- System- und Antivirensoftware regelmäßig auf neuesten Stand bringen
- Auf jeden Fall Image-Backup (mit Paßwortschutz) erstellen
- Alle sensitiven Daten verschlüsselt ablegen und wenn möglich verschlüsselt kommunizieren (ssh, ssl)