

Single-Sign-On und weiter ?

Dipl. Ing. (FH) Manfred Meise

IBM Certified Advanced Developer - Lotus Notes and Domino R3 – R8

IBM Certified Advanced Administrator - Lotus Notes and Domino R3 – R8, R8.5

IBM Certified Advanced Instructor – Lotus Notes and Domino R3- R8, R8.5



zu meiner Person: Manfred Meise

- Studium Elektrotechnik
- Arbeit als Softwareingenieur seit mehr als 30 Jahren bei verschiedenen Computerherstellern und Softwarehäusern
- Gründer und Geschäftsführer der mmi consult gmbh
- Erfahrungen mit Lotus Notes/Domino seit 2002 - Markteinführung in Europa (als Leiter Strategische Projekte bei Lotus Development Deutschland)
- IBM Zertifizierungen als Anwendungsentwickler, Systemadministrator, Trainer für die Produktversionen R3 bis R8.5
- Tätigkeitsschwerpunkte im Entwicklungsbereich:
CRM, Workflow, Objektorientierte Anwendungsarchitekturen
- Tätigkeitsschwerpunkte als Systemadministrator:
Domänenzusammenführungen und –trennungen, Betriebshandbücher und Administrationsstandards, Versionswechsel, Infrastruktur-Audits, Client-Rollouts
- Erreichbar unter:
 - ***manfred.meise@mmi-consult.de***
 - ***<http://www.mmi-consult.de>***
 - ***<http://www.mmi-consult.de/faq>***



Meine Themen heute ...

- Die aktuelle Situation und Herausforderung an User
- Single Signon bei Lotus Notes / Lotus Domino
- Single Signon für Webuser
- Single Signon in IBM Multiserver Umgebungen
- Unterstützung durch Produkte von Drittanbietern
- Trends und mögliche Entwicklungsrichtungen

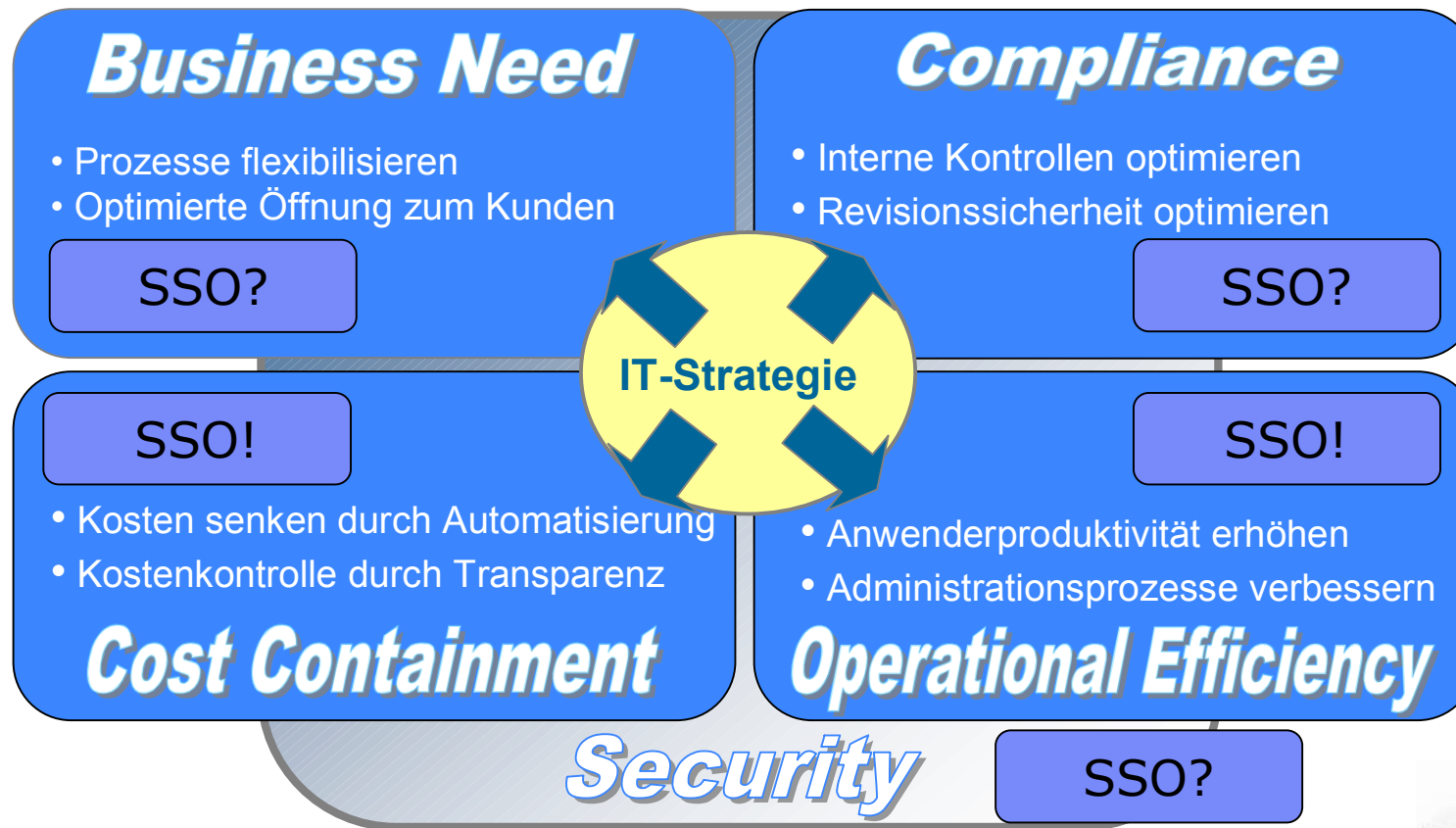


Die aktuelle Situation eines Business Users

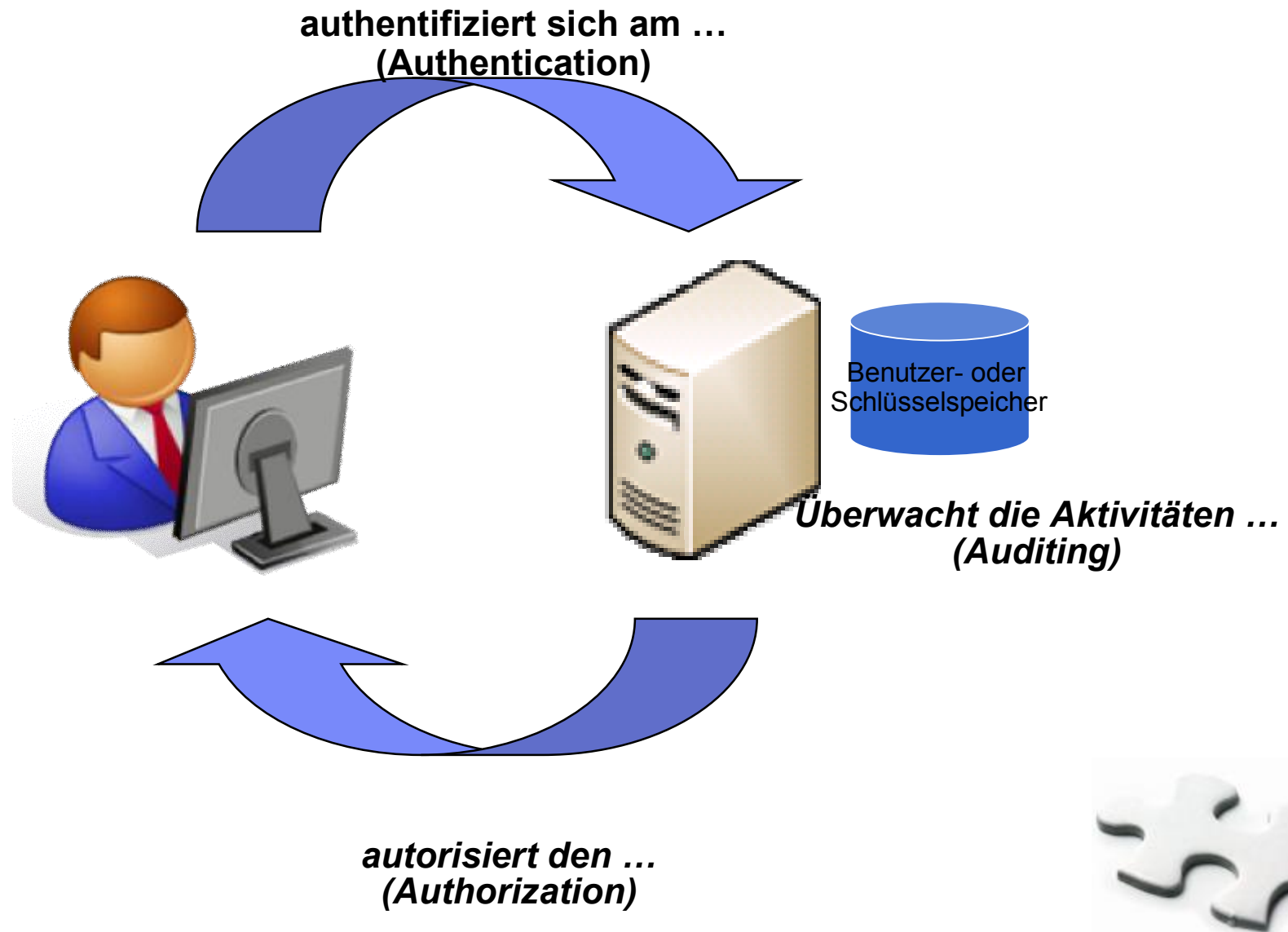
- User haben für zahlreiche Systeme zahlreiche Kennwörter für Ihre Anmeldung
- User werden regelmäßig gezwungen, neue Kennwörter zu vergeben (Vorgabe des Datenschutzbeauftragten)
- User können nur komplexe Kennwörter verwenden, um sich anzumelden (um die Vertraulichkeit zu erhöhen)
- User können sich die zahlreichen Kennwörter nicht merken und benötigen Hilfestellung bei UHD
- Um nicht ständig den UHD zu bemühen schreiben User ihre Kennwörter auf (oder legen die Liste unter die Tastatur)
- Somit hoher betrieblicher Aufwand mit dem Ziel Datenschutz zu erhöhen, doch die Praxis macht es zunichte



Die IT im Wandel: Business-Treiber für SSO



Authentifizierung, Autorisierung und Auditing



Methoden der Authentifizierung

- Die Authentifizierung (Nachweisen der eigenen Identität) kann ein Subjekt auf drei verschiedenen Wegen erreichen:

1. Nachweis der Kenntnis einer Information (Das Subjekt weiß etwas); Beispiel: Passwort.

- Passwort
- PIN
- Antwort auf eine bestimmte Frage

This is my secret

2. Benutzung eines Besitzes (Das Subjekt hat etwas)

- Schlüssel
- Zertifikat
- TAN
- Token



3. Anwesenheit des Subjektes selbst (Das Subjekt ist etwas)

- Fingerabdruck
- Gesichtserkennung
- Stimme



- Die Authentisierungsmethoden haben je nach Anwendungsgebiet verschiedene Vor- und Nachteile in ihrer Betrachtung einer speziellen Eigenschaft des Subjektes.



Lösungsansätze für SSO

- Lokale Lösung
 - ▶ Benutzername/Kennwort werden lokal gespeichert und jedes Mal übertragen

- Portal
 - ▶ Einloggen auf einem zentralen Portal
 - ▶ Portal etabliert Sitzung und steuert weitere Zugriffe

- Ticketing System
 - ▶ Ticket mit Identitätsnachweis wird bei erster Authentifizierung erstellt
 - ▶ Weitere Authentifizierungen werden über dieses Ticket abgewickelt



Klingt doch ganz einfach?!

Connectors

Kerberos

Notes Single Logon

Web SSO

LTPA

SPNEGO

Notes Shared Login

LDAP

Active Directory

Domino Directory
Independance



Single Signon bei Lotus Notes / Lotus Domino



Notes Single Logon (Notes 6+)

- Benutzer starten Lotus Notes ohne Kennworteingabe
- Lotus Notes und Windows Kennwörter werden synchronisiert
- Notes Single Logon Service ist eine optionale Installationskomponente
 - ▶ Verwendet Netzwerk- und Windowsdienst um Kennworteingabe abzufangen
 - ▶ Erfordert eine Synchronisation zwischen Notes und Windows-Kennwort
- Aktivierung über den Sicherheitsdialog
- Übliche Schwierigkeiten:
 - ▶ Kennwortrichtlinien zwischen Windows und Notes erlauben kein gemeinsam gültiges Kennwort
 - ▶ Synchronisiert lediglich Kennwörter auf der aktuellen Maschine
 - ▶ In Kombination mit Domino Roaming und gewechselten Kennwörtern beliebig verwirrend für Benutz
- Nur auf Windows Plattformen unterstützt



Notes Shared Login (NSL) In Notes 8.5

- Keine Synchronisation von Kennwörtern, sondern Verwendung der Windows-Anmeldung, um ID File zu entsperren
- Die Funktion des ID Files bleibt unverändert erhalten
 - ▶ Der Client authentifiziert sich weiterhin mit einer zertifikatsbasierten Client/Server Authentifizierung
 - ▶ ID File enthält weiterhin Internetzertifikate
 - ▶ ID File enthält weiterhin Dokumentenschlüssel
- Kennwortverwaltung wird ausschließlich von Windows Mechanismen und Richtlinien gesteuert
- Nur auf Windows Plattformen unterstützt



Aktivierung durch Richtlinien

Sicherheitseinstellungen : -Default-

[Allgemein](#) |
 [Kennwortverwaltung](#) |
 [Ausführungskontrollliste \(ACL\)](#) |
 [Schlüssel und Zertifikate](#) |
 [Sicherheitseinstellungen](#)

[Kennwortverwaltung - Allgemein](#) |
 [Gemeinsame Notes-Anmeldung](#)

Gemeinsame Notes-Anmeldung

Gemeinsame Notes-Anmeldung mit dem Betriebssystem aktivieren:

Benutzer dürfen Änderungen vornehmen?
 ☐ Ja
 ☒ Nein

Aktivierungsbenachrichtigung

Benachrichtigungsart bei Aktivierung:

Benutzerdefinierter Nachrichtentext:

Deaktivierungsbenachrichtigung

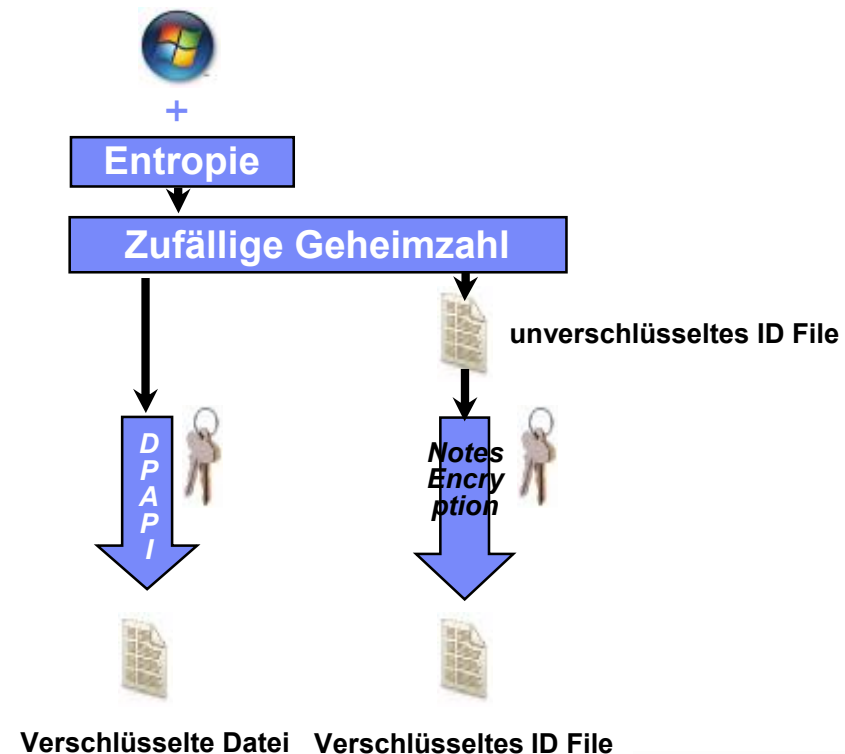
Benachrichtigungsart bei Deaktivierung:

- Direkte Steuerung über Richtlinien
- Verriegelungsmöglichkeit für Benutzer
- Anpassbare Dialoge für
 - ▶ Aktivierung
 - ▶ Deaktivierung



Aktivierung von NSL am Client

- Benutzer meldet sich an Windows an
- Bei Notes Start: Erkennen von NSL Aktivierung durch Richtlinie
- Notes generiert einen neuen komplexen Zufallsstring mit nicht druckbaren Zeichen
- Notes verwendet die MS-DPAPI um den Zufallsstring mit Maschinenkennung/Benutzerkennung zu verschlüsseln
- Notes speichert den Schlüssel im Windowsprofil
- Notes verschlüsselt das ID File mit einem Schlüssel, der vom generierten Schlüssel abgeleitet wurde



Benutzerdialoge bei aktiviertem NSL

- Benutzerhinweis nach Aktivierung (wenn „System-Dialog“ konfiguriert)

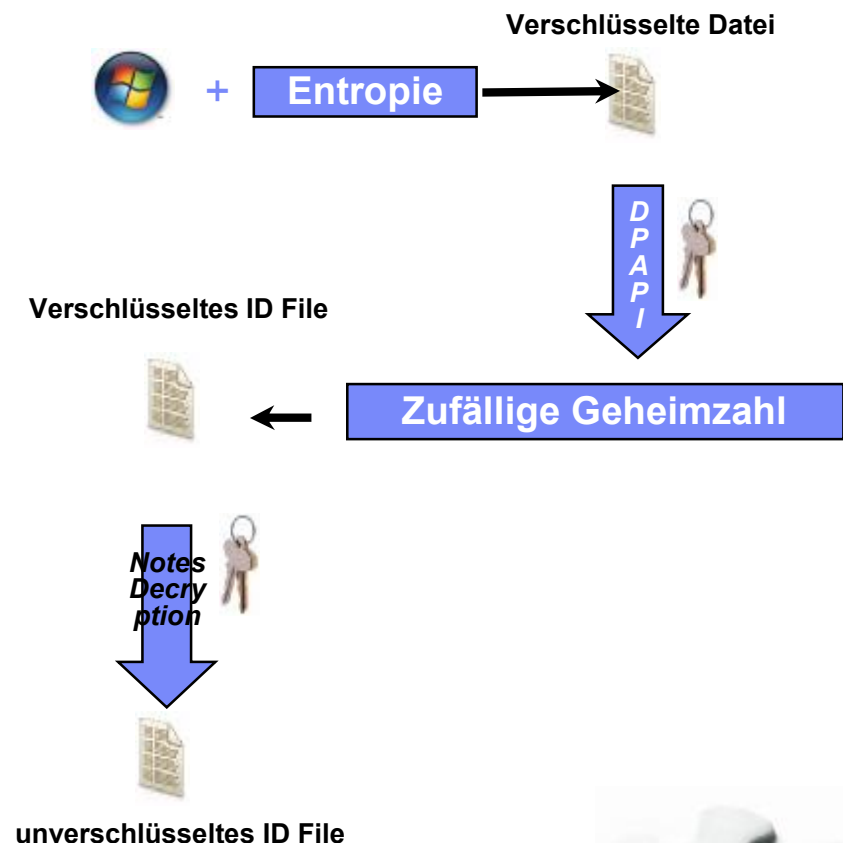


- Zugriff auf Sicherheitsdialog ist durch Windows geschützt



Wie NSL am Client verwendet wird

- Benutzer meldet sich an Windows an
- Benutzer startet Notes
- Das ID File zeigt an, das es NSL aktiv ist
- Notes lokalisiert den Schlüssel im Windowsprofil, um diesen über die MS-DPAPI mittels der Benutzer-/Maschineninformation zu entschlüsseln
- Notes Client verwendet den Schlüssel um das ID File zu entsperren
- Notes läuft ohne einen Kennwortdialog



8.5



NSL aktivierte Datei am falschen Gerät



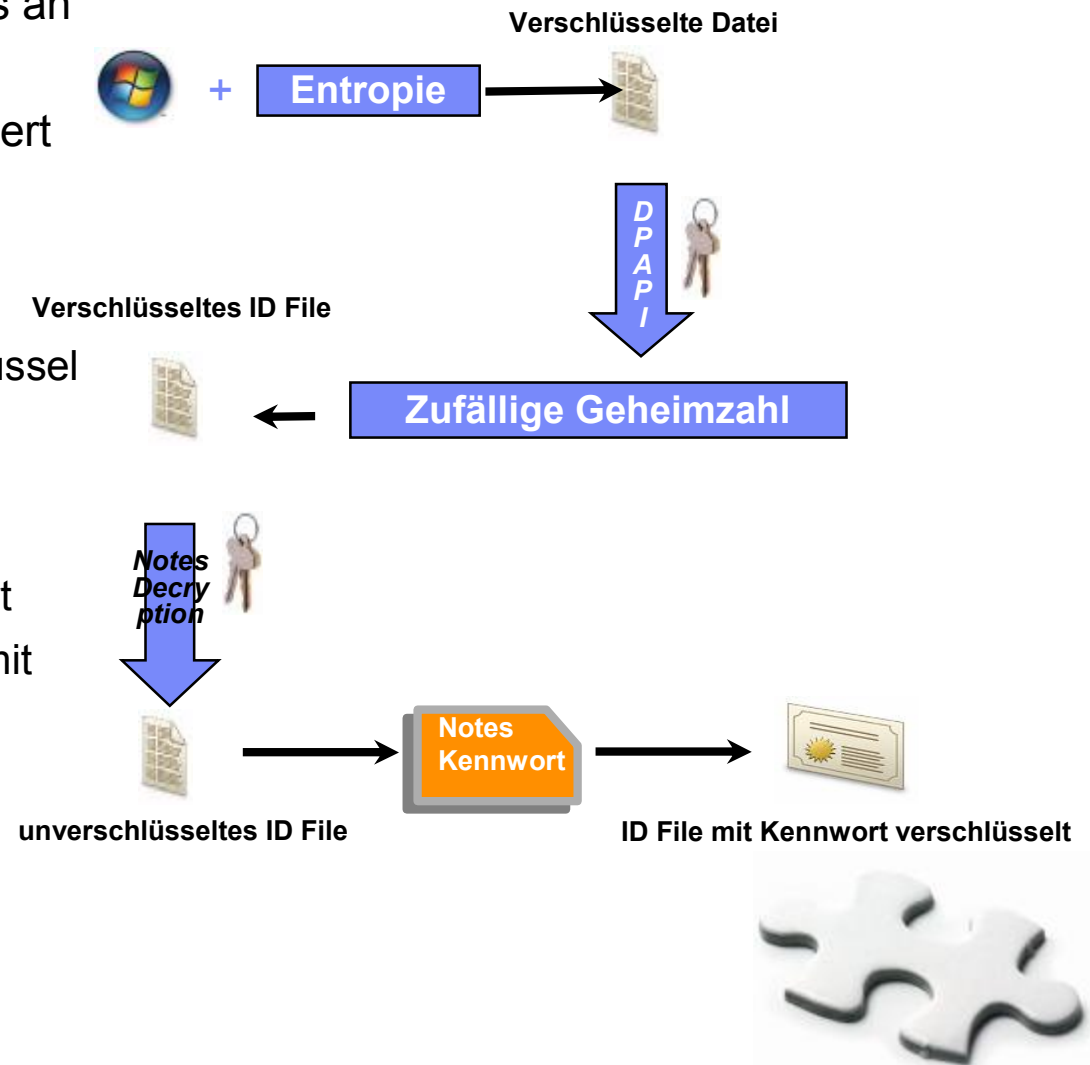
- Pech gehabt



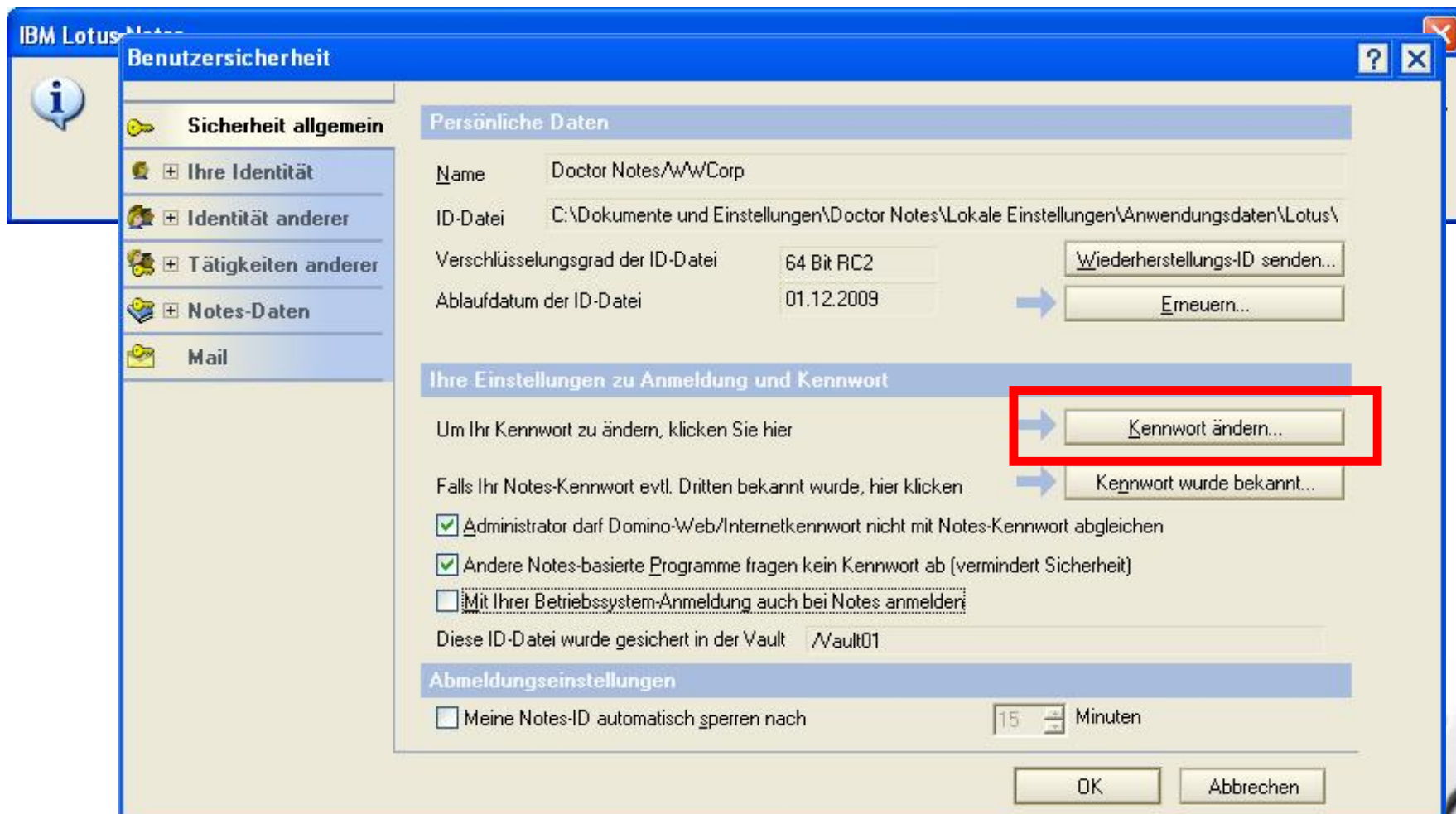
Deaktivierung von NSL am Client

- Benutzer meldet sich an Windows an
- Beim Notes Start wird durch eine Policy erkannt, dass NSL deaktiviert werden soll

- ▶ Notes ermittelt den geheimen Windows Schlüssel
- ▶ Notes entschlüsselt diesen Schlüssel mit den aktuellen Maschinen-/Benutzerdaten
- ▶ Notes entschlüsselt das ID File
- ▶ Notes fragt nach einem Kennwort
- ▶ Notes verschlüsselt das ID File mit dem eingegebenen Kennwort



Benutzerdialoge bei deaktiviertem NSL



NSL Einsatzüberlegungen

- Synchronisation zwischen Notes- und Internetkennwort kann nicht genutzt werden
 - ▶ NSL ID Files haben kein Kennwort – keine Daten für die Synchronisation
 - ▶ Neue Verfahren notwendig, um Windows Kennwörter mit dem Notes Internet Kennwort zu synchronisieren
- Da der geheime Windows Schlüssel zum entschlüsseln des ID Files Benutzer- und Maschinenspezifisch ist, kann
 - ▶ ein NSL ID File nicht in das Mailfile importiert werden (iNotes/Blackberry) – erfordert eine separate Kennwort geschützte Kopie des ID Files
 - ▶ ein NSL ID File kann nicht auf eine andere Maschine kopiert werden
 - Unkritisch in Verbindung mit dem ID Vault
 - Unkritisch, wenn auf weiteren Maschinen eine kennwortgeschützte Kopie eingesetzt wird
- Jegliche Sicherheit wird nunmehr durch Windows kontrolliert !??!
- ID Sicherungen notwendig, um vor Verlust geschützt zu sein
- Domino Kennwortüberprüfung muss deaktiviert sein



Notes Single Logon wird aus Gründen der Abwärtskompatibilität weiterhin unterstützt (ACHTUNG bei Client-Updates unbedingt deinstallieren!)



NSL im Einsatz



Live-Demonstration



Was mir **nicht** gefällt ...


- Immer noch keine sinnvolle Roaming Unterstützung
 - ▶ Kennwortwechsel machen IDs an anderen Rechnern unbrauchbar
 - ▶ Lösbar nur durch ID-Vault und löschen des lokalen ID Files
- Bei Wechsel des Arbeitsrechners in eine andere Domäne oder bei lokaler Anmeldung ist ID File nicht zu öffnen



Single Signon für WebUser



Web SSO für Web Benutzer

- Windows Benutzer 
 - ▶ Windows Benutzer sind mit Ihrer Betriebssystemanmeldung bereits authentifiziert
 - ▶ Moderne Browser können diese Authentifizierung übernehmen und an Server weitergeben
 - ▶ Ergebnis: Kein erneute Authentifizierung an Webservern (Beispiel: IE an IIS)
 - ▶ Erfordert: SPNEGO mit Keberos Protokoll
 - ▶ Einschränkung
 - Funktioniert nur im Intranet
 - Benötigt Unterstützung auf der Seite der Anwendungsserver
- Alternative für alle anderen Konfigurationen und Fälle
 - ▶ Verwendung von LTPA Tokens (IBM Entwicklung für Domino / Websphere)
 - ▶ Unterstützt von allen IBM Webservern
 - ▶ Ergebnis: Einmalige Anmeldung innerhalb der Domäne
 - ▶ Erfordert: Directory mit Session Tokens





Wer oder was ist Kerberos?

- Ist der Torwächter der Unterwelt in der griechischen Mythologie
- Ist aber auch der Name eines Authentifizierungs-Protokolls 1978 von Steve Miller/Clifford Neuman entwickelt
- Wird bis heute am M.I.T. weiterentwickelt (Version 5)
- Kerberos in der IT...
 - ▶ ... ist ein verteilter Authentifizierungsdienst
 - ▶ ... ist konzipiert für offene und unsichere Netze
 - ▶ ... ermöglicht Single Sign-On
 - ▶ ... ist Plattform- und Systemunabhängig
 - ▶ ... verwendet symmetrische Verschlüsselung
 - ▶ ... ist in RFC 1510 beschrieben
 - ▶ ... ist in den meisten Betriebssystemen implementiert
 - ▶ ... ist das Standard-Protokoll im Active Directory
 - ▶ ... basiert auf einer vertrauenswürdigen Instanz und einem Ticketing-System

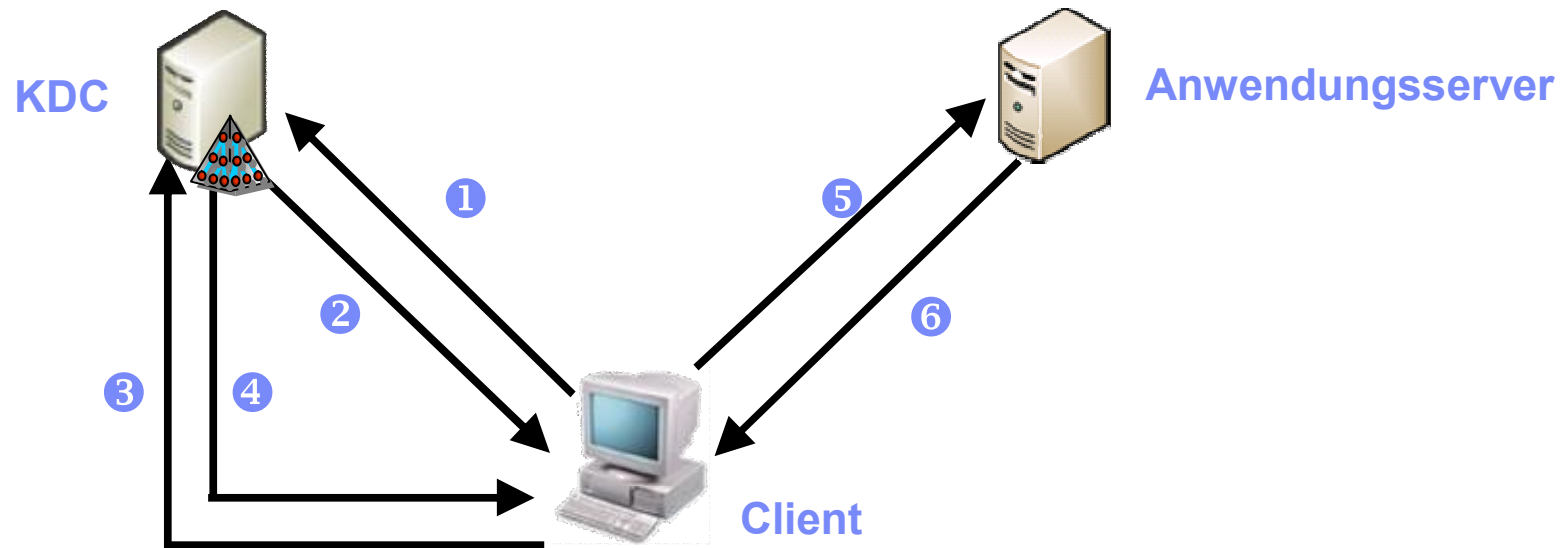


Key Distribution Center (KDC)

- Key Distribution Center (KDC) bestehent aus:
 - ▶ Principal Database (z.B. Active Directory)
 - Speichert Principals und Keys
 - ▶ Authentication Server (AS)
 - Erstellt das Ticket Granting Ticket (TGT)
 - ▶ Ticket Granting Server (TGS)
 - Erstellt Service Tickets für ein TGT
- Alle beteiligten Principles müssen in Principle Database aufgeführt sein
 - ▶ (Windows Clients) sind automatisch Mitglied
 - ▶ Anwendungsserver müssen Konfiguration und Teilnahme unterstützen



Ablauf einer Kerberos Authentifizierung



1. Ein Principal (hier der Client) startet einen ersten Authentication Service Request an das KDC, um ein Ticket Granting Ticket (TGT) zu erhalten.
2. Das KDC antwortet dem Client mit einem TGT. Dieses enthält einen key (ticket session key) und ist mit dem Passwort des Clients verschlüsselt.
3. Der Client verwendet das TGT um ein Ticket Granting Service (TGS) ticket anzufordern, das für einen anderen Principal (hier ein weiterer Server) notwendig ist.
4. Das KDC vergibt ein Ticket Granting Service (TGS) ticket an den Client, das vom Server verwendet werden kann.
5. Der Client weist das TGS als Anfrage an den Server
6. Der Server authentifiziert den Client durch Quittierung des TGS. Wenn gegenseitige Authentifizierung erforderlich ist, erwidert der Client die Serverauthentifizierung.



Weitere Protokolle und Standards

- Generic Security Services API (GSSAPI):
 - ▶ generisches Interface zur Unterstützung von „strong Authentication“, wie z.B. Kerberos
 - ▶ wird oft von Services verwendet um Kerberos zu unterstützen
- Security Support Provider Interface (SSPI):
 - ▶ Microsoft Pendant zu GSSAPI
- Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO):
 - ▶ Übermittlung eines Kerberos-Tickets per HTTP



SPNEGO Konfiguration im Browser

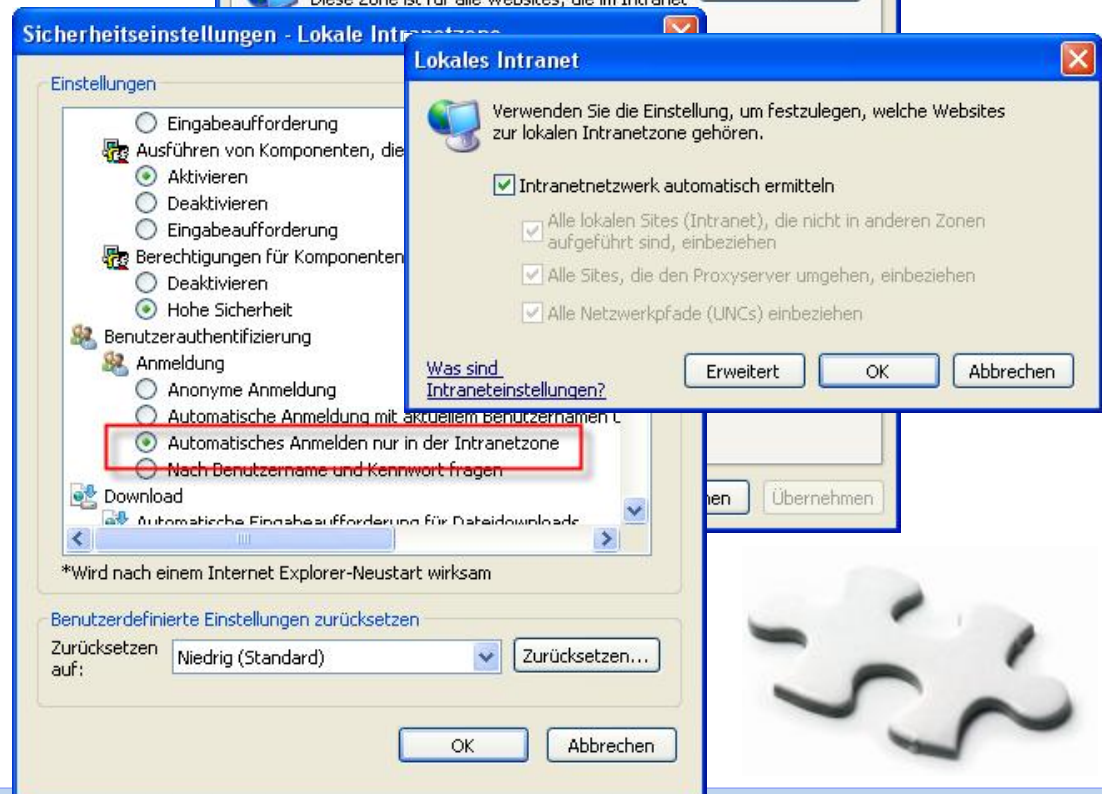
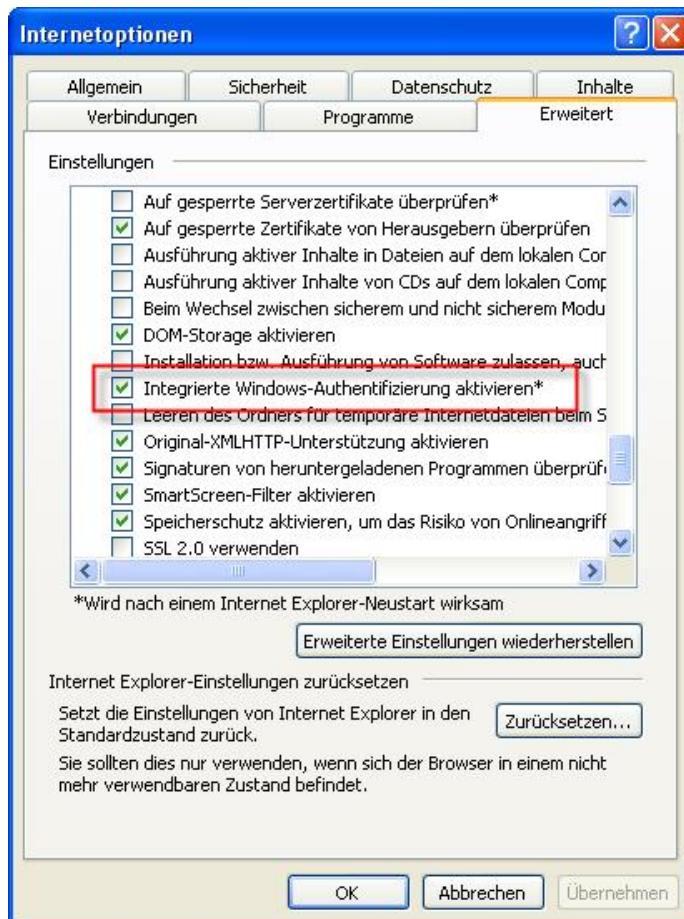
- Firefox: „about:config“ in die Adressenzeile eingeben



SPNEGO Konfiguration im Browser



Internet Explorer: Extras - Internetoptionen

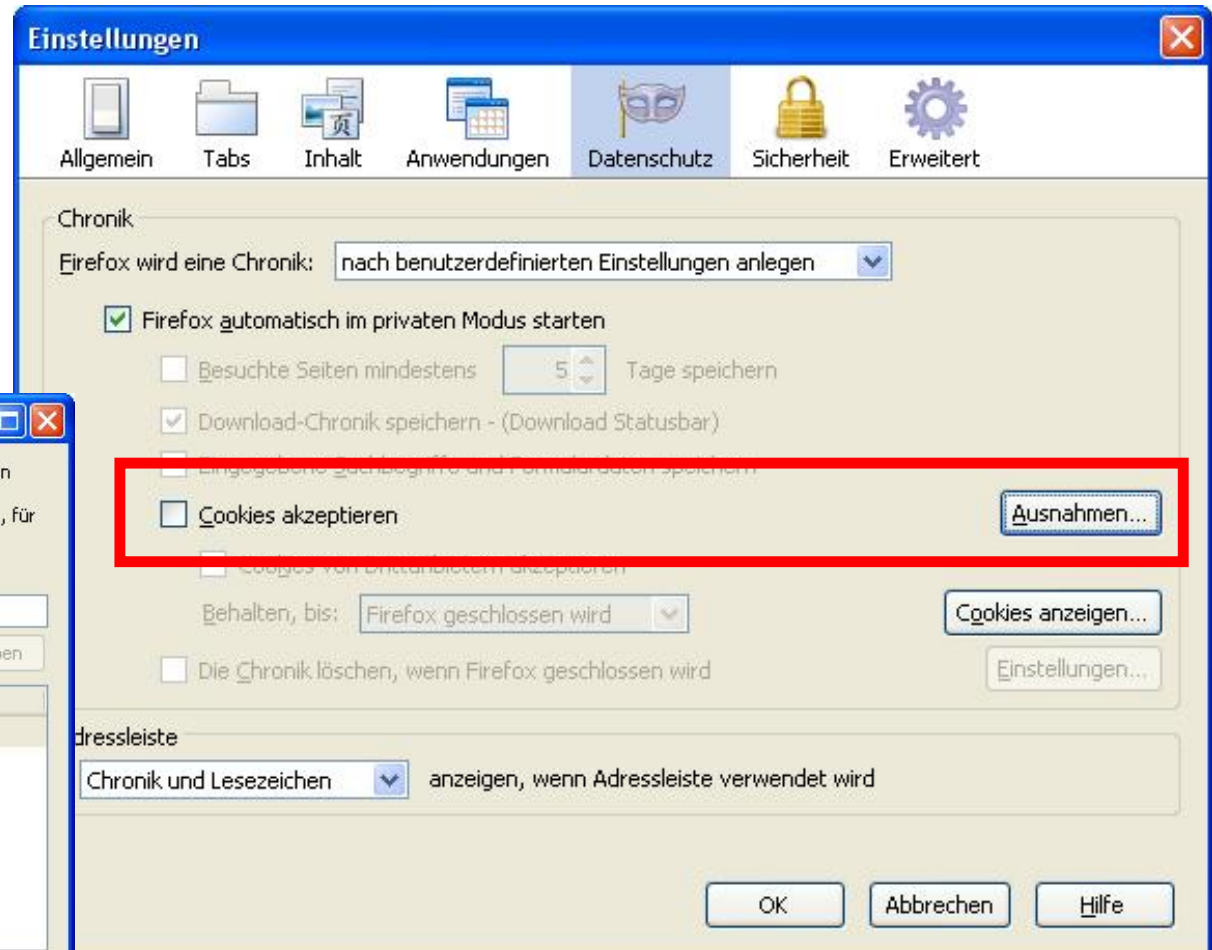
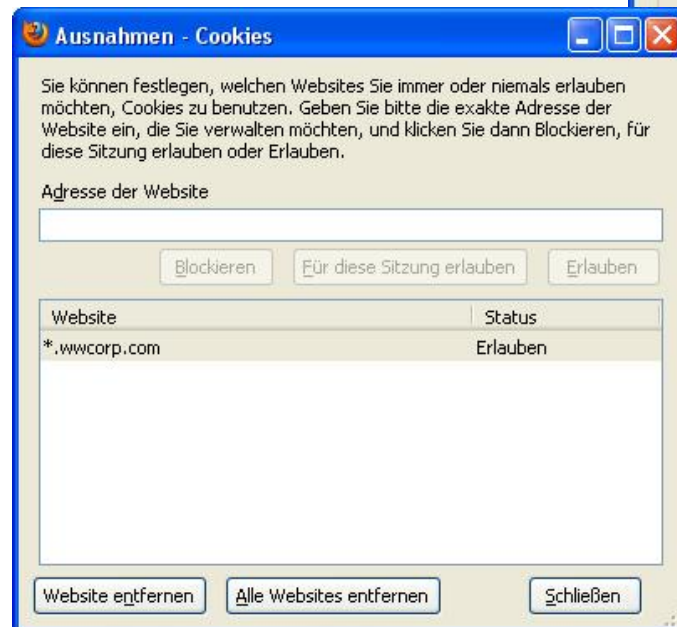


Browser Konfiguration zur Verwendung von LTPA




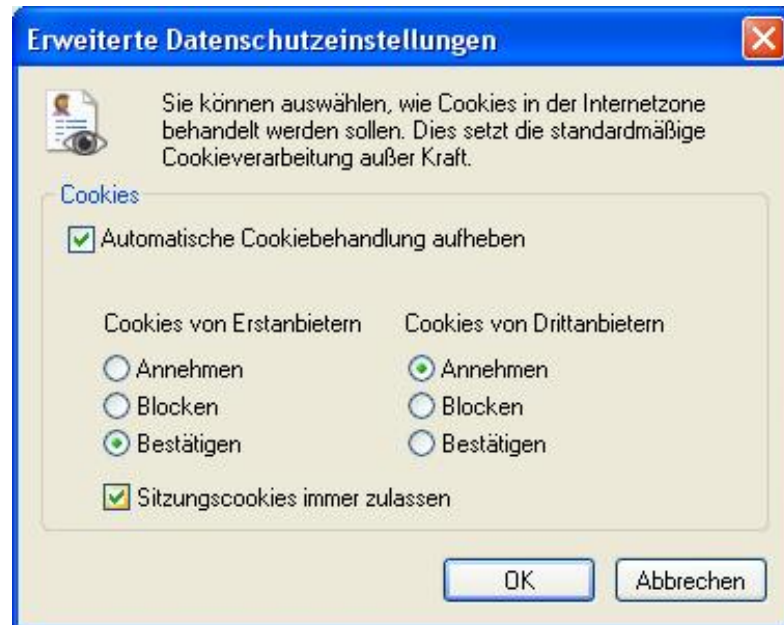
▪ Erlaubnis für Cookies erforderlich

- ▶ Generell
- oder
- ▶ über Ausnahmen

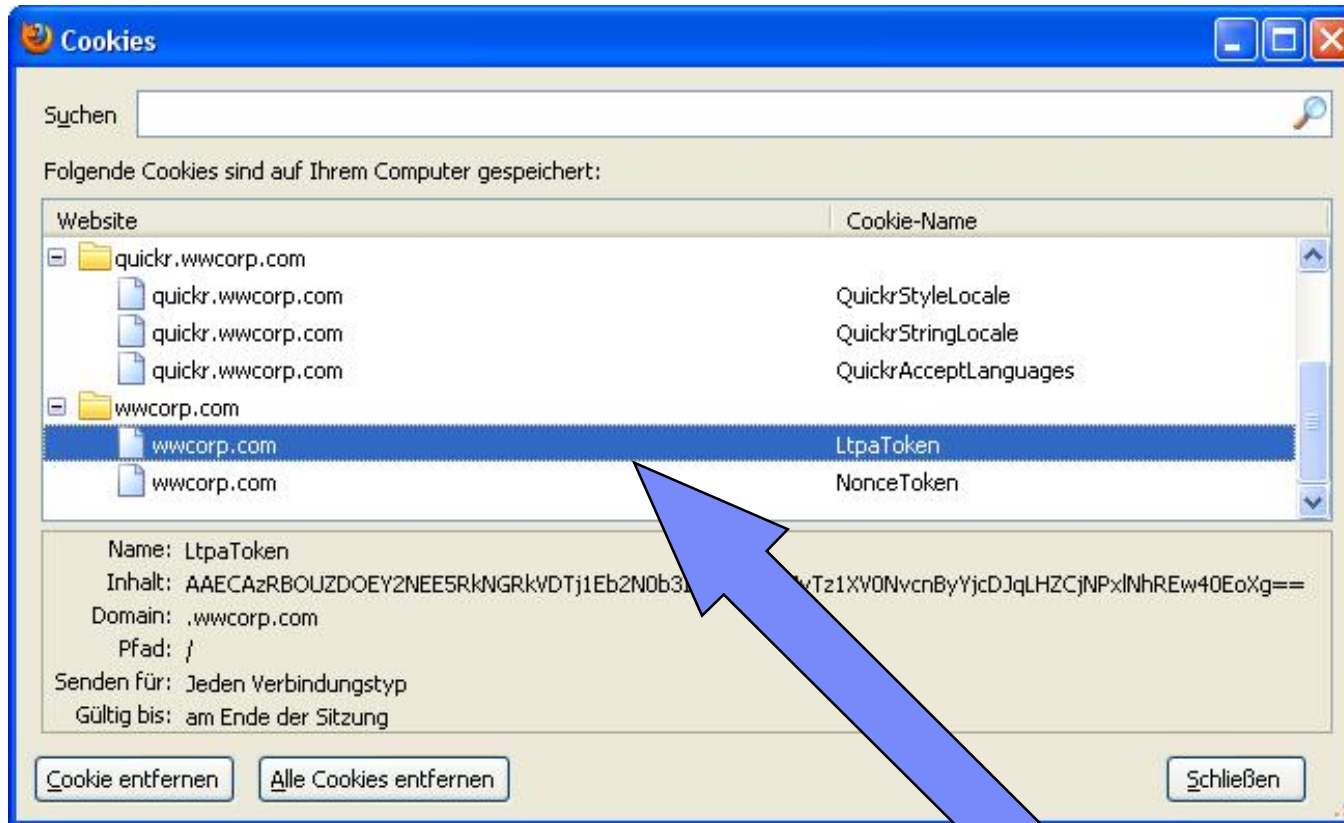


Browser Konfiguration zur Verwendung von LTPA

- 
 Erlaubnis für Cookies erforderlich
 - ▶ Generell oder
 - ▶ über Ausnahmen

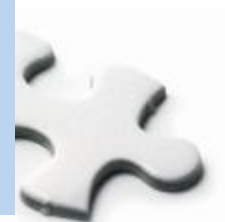


Wie funktioniert ein LTPA Token?



Cookie enthält

- Benutzer
 - Authentifizierter Realm
 - Zeitstempel
- mit 3DES verschlüsselt



Kann ich SPNEGO und LTPA kombinieren?

- Authentifizierung an einem Server, der SPNEGO und LTPA Support besitzt (z.B. WebSphere Portal oder IIS)
- SPNEGO-unterstützenden Browser einsetzen
- Authentifizierung an WebSphere und Umleitung an Domino Ressource



Single Signon für Domino und WebSphere WebUser



Authentifizierung von Domino Web-Benutzern

- Personendokument mit Domino Directory erforderlich
 - ▶ Alternativ auch über vertrauenswürdiges LDAP Verzeichnis
- Authentifizierung mit Benutzername und Internetkennwort
- Internetkennwort kann bereits bei Benutzerregistrierung gesetzt werden
- Änderung von Internetkennwörtern durch den Benutzer:
 - ▶ Bearbeitung des **eigenen** Personendokumentes
(ACHTUNG: Autorenberechtigung auf das Domino Directory erforderlich)
 - ▶ Synchronisation mit Lotus Notes Kennwörtern
(ACHTUNG: Nur möglich, wenn **kein** NSL verwendet wird)
 - ▶ Verwendung von Lotus iNotes
(ACHTUNG: Nur für Änderungen möglich; erfordert vorherige Authentifizierung)
- Authentifizierungsmöglichkeiten
 - ▶ Einmalig
 - ▶ Sitzungsbasiert
 - ▶ Sitzungsbasiert (Serverübergreifend)



Single Signon für Webuser (SSO)

- Aktuell erreichbar mit sitzungsbasierter Anmeldung (verfügbar seit R5)
- Die Aktivierung der sitzungsbasierten Anmeldung eröffnet folgende Vorteile:
 - ▶ Vermeidung erneuter und ständiger Anmeldevorgänge, wenn Benutzer den Realm (Links zu unterschiedlichen Zielen) wechseln
 - ▶ Benutzersitzungen können serverseitig durch ein Konsolenkommando verfolgt werden
 - ▶ Benutzer können Sitzungen beenden, ohne den Browser neu zu starten (indem sie einfach „?logout“ an die URL hängen)
 - ▶ Die verwendeten Anmeldemasken können angepaßt werden
 - ▶ Benutzer nach einmaliger Anmeldung jeden Domino Server oder WebSphere server in der gleichen Domäne nutzen, ohne sich erneut authentifizieren zu müssen



Der LTPA Token

- Ein SSO Token ist der Schlüssel zum Erfolg, um eine serverübergreifende Anmeldungen zu erreichen
- Sametime verwendet SSO, und erzeugt bereits bei der Installation einen Token
 - ▶ Dieser Token wird mit dem Namen 'LTPAToken, gekennzeichnet
- Der Token wird bei der Anmeldung mit dem Browser heruntergeladen
 - ▶ als Session based cookie beim User gespeichert
- Der Browser überträgt den Token zusammen mit jeder neuen Anforderung
 - ▶ Solange der Token gültig ist, wird der Server die Anfrage akzeptieren



Einrichten von SSO auf Domino Servern (1)

- Prüfen Sie den „Vollständig qualifizierten Internet-Hostnamen“ aller beteiligten Server (müssen zur gleichen Internet-Domäne gehören)
- Entscheiden/prüfen Sie, wie die Internetkonfigurationen erfolgen soll
 - ▶ aus dem Serverdokument
 - ▶ aus Web-Internetsite-Dokumenten
(**ACHTUNG:** nicht alle Lotus Companion Products unterstützen Internetsite-Dokumente!!!)



The screenshot shows the 'Allgemein' (General) tab of the Domino Server Configuration window for the server 'Hub/SVR/WWCorp'. The 'Vollständig qualifizierter Internet-Hostname' (Fully qualified Internet hostname) is set to 'hub.wwwcorp.com' and is highlighted with a red box. The 'Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden' (Load Internet configurations from Server-Internet-Site documents) checkbox is checked, and the 'Deaktiviert' (Deactivated) status is highlighted with a red box.

Allgemein	
Servename:	Hub/SVR/WWCorp
Servertitel:	Worldwide's Hub server
Domänenname:	WWCorp
Vollständig qualifizierter Internet-Hostname:	hub.wwwcorp.com
Clustername:	
Internet-Konfigurationen aus Server-Internet-Site-Dokumenten laden:	Deaktiviert



Einrichten von SSO auf Domino Servern (2)

- Erstellen Sie einen LTPA Token für alle am SSO teilnehmenden Server

- ▶ Über die Maskenaktion



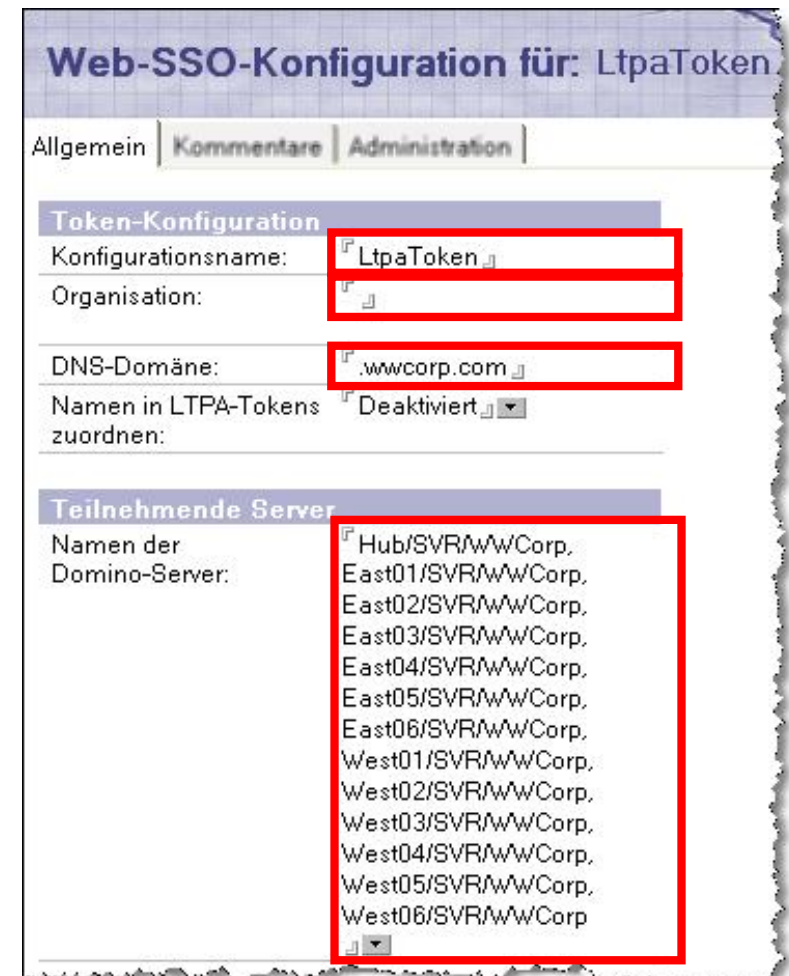
des Serverdokumentes

- ▶ oder die Ansichtsaktion
der Ansicht „Web – Internet-Sites“



Einrichten von SSO auf Domino Servern (3)

- Legen Sie die LPTA Token Eigenschaften fest
- Konfigurationsname:
 - ▶ (wenn möglich) nicht ändern, da nicht von allen Produkten unterstützt
- Organisation:
 - ▶ Unbedingt leer lassen, bei Internetkonfiguration über Serverdokument
 - ▶ Unbedingt füllen, bei Internetsite-Dokumente
- DNS-Domäne:
 - ▶ Name (beginnend mit „.“ in Bezug auf Internet-Hostnamen aus Serverdokument
- Namen der Domino-Server
 - ▶ Alle am SSO teilnehmenden Server



Web-SSO-Konfiguration für: LtpaToken

Allgemein | Kommentare | Administration

Token-Konfiguration

Konfigurationsname: LtpaToken

Organisation:

DNS-Domäne: .wwcorp.com

Namen in LTPA-Tokens zuordnen: Deaktiviert

Teilnehmende Server

Namen der Domino-Server:

- Hub/SVR/WWCorp,
- East01/SVR/WWCorp,
- East02/SVR/WWCorp,
- East03/SVR/WWCorp,
- East04/SVR/WWCorp,
- East05/SVR/WWCorp,
- East06/SVR/WWCorp,
- West01/SVR/WWCorp,
- West02/SVR/WWCorp,
- West03/SVR/WWCorp,
- West04/SVR/WWCorp,
- West05/SVR/WWCorp,
- West06/SVR/WWCorp

Einrichten von SSO auf Domino Servern (4)

- Verweisen Sie darauf, welcher zuvor erstellte LTPA Token verwendet werden soll
- Bei Konfiguration über Serverdokumente



Server: **Hub/SVR/WWCorp** hub.wwcorp.com

Allgemein | Sicherheit | Ports... | Server-Tasks... | Internetprotokolle... | MTA

HTTP | Domino-Web-Server | **DIOP** | LDAP

HTTP-Sitzungen

Sitzungsauthentifizierung:	Serverübergreifend (SSO)
Web-SSO-Konfiguration:	LtpaToken
Anmeldung mit SSL erzwingen:	Nein
Maximale Anzahl aktiver Sitzungen:	1000

- Bei Konfiguration über Internetsite-Dokumente



Website WWcorp

Allgemein | Konfiguration | Domino-Web-Server | Sicherheit

HTTP-Sitzungen

Sitzungsauthentifizierung:	Serverübergreifend (SSO) ▾
Web-SSO-Konfiguration:	LtpaToken ▾
Anmeldung mit SSL erzwingen:	Nein ▾
Beim Überschreiben der Sitzungsauthentifizierung Sitzungs-Cookie generieren:	Ja ▾

Verwendung verschiedener Server einer Domäne



Live-Demonstration



SSO in IBM Umgebungen



Besonderheiten bei Sametime und QuickR

- Sametime und QuickR unterstützen KEINE Internet Site Dokumente
- Der verwendete Token **muss** 'LTPAToken, heissen
- Der Token darf **keinen** Organisationsnamen enthalten
- Es sind stets FQDNs zu verwenden – nur so weiss der Browser, dass er den Token zusammen mit einer Anfrage senden muss

- Die vollständige funktionale Integration von Sametime und QuickR erfordert zusätzliche Integrationsschritte (hier nicht weiter thematisiert)

- Unterschiedliche SSO Funktionalitäten bei Sametime-Clients
 - ▶ Embedded Client: LTPA
 - ▶ Sametime Connect: SPNEGO



Sametime - Anmeldeoptionen

1. Standard Sametime Login mit LDAP/HTTP Password (entweder Sametime Connect oder Notes embedded Sametime)
 - ▶ LDAP oder HTTP Password wird über Sametime Option lokal gespeichert
 - ▶ Sametime-Start ---> gespeichertes LDAP/HTTP Password wird an Sametime Server übertragen. Benutzer werden nicht nach Kennwort gefragt, solange LDAP/HTTP Password nicht anderweitig geändert wird.
2. Notes Authentifizierung mit Sametime (Notes embedded Sametime)
 - ▶ User.id des Benutzers wird (nach Kennworteingabe) für die Notes Authentifizierung verwendet. Sametime ist konfiguriert, um diese Credentials zu verwenden.
 - ▶ Wenn Sametime (mit Notes) gestartet wird, verwendet Sametime (ohne, dass der User es bemerkt) die Notes Credentials für die Authentifizierung am Domino Server über das Notes Protokoll. Der erhaltene LTPA Token wird dann verwendet, um eine Authentifizierung am Sametime Server durchzuführen.



Sametime – Anmeldeoptionen (*Forts.*)

3. Notes Authentifizierung für Sametime kombiniert mit Notes Shared Login (Notes embedded Sametime)
 - ▶ Benutzer authentifizieren sich an Windows, ---> Notes startet ohne Kennworteingabe (durch NSL). Weitere Authentifizierungsschritte wie unter 2.
4. Authentifizierung an Sametime über SPNEGO (nur Sametime Connect)
 - ▶ Verwendung der Windows Anmeldung durch Einsatz von SPNEGO
 - ▶ Benutzer meldet sich an Windows an → Sametime Connect Client kann mit den Windows Credentials verwendet werden (Verwendung der Active Directory / LDAP Namen)



Embedded-Sametime (mit Internet-Kennwort)

- Voraussetzungen:
 - ▶ keine
- Anwendung:
 - ▶ Basic Client
 - ▶ Standard Client
- Abhängigkeiten:
 - ▶ keine

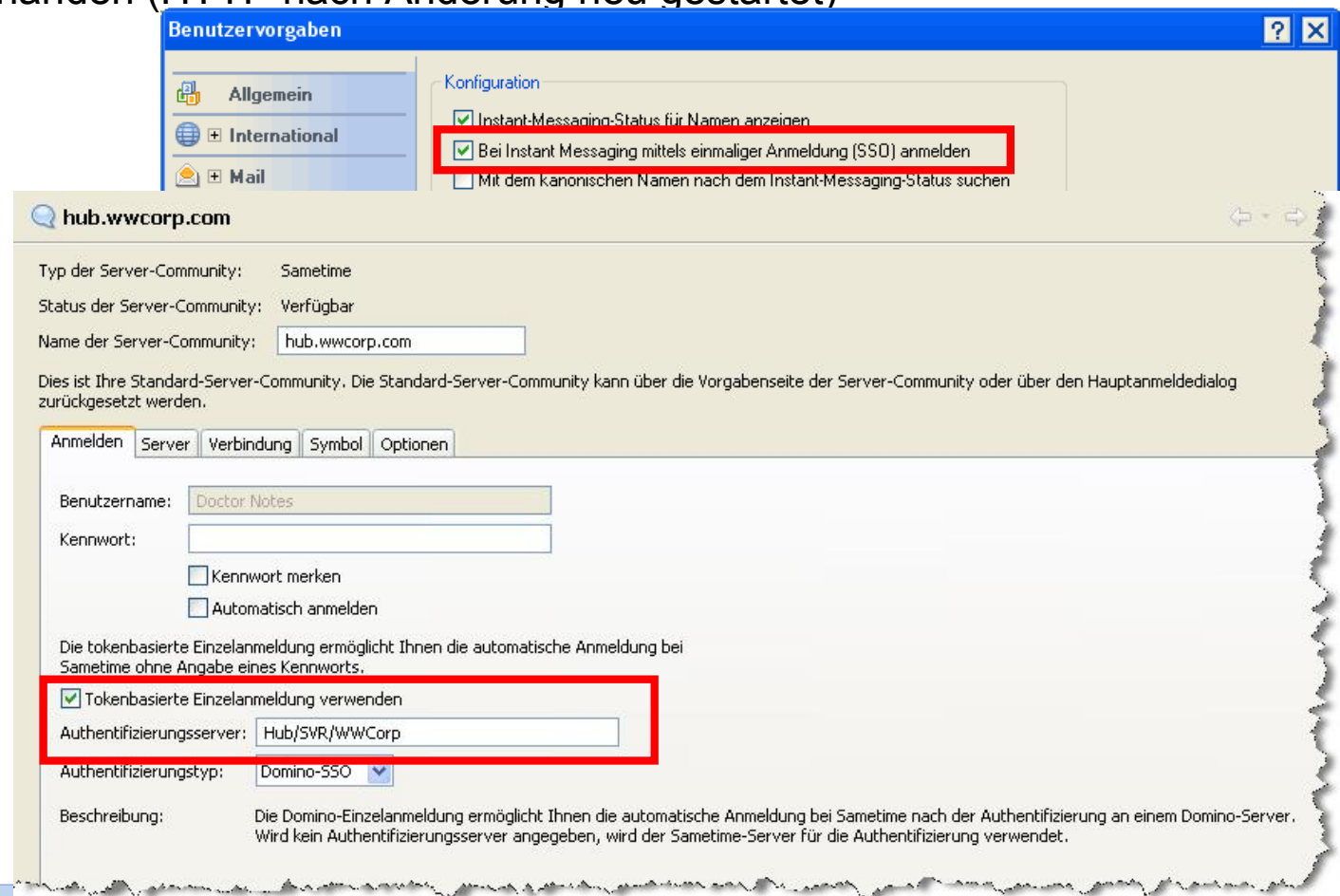


The screenshot shows a login window for Sametime. At the top, it says 'Typ der Server-Community: Sametime'. Below that, 'Name der Server-Community:' is followed by a text box containing 'hub.wwwcorp.com:Doctor Notes'. A message states 'Dies ist Ihre Standard-Server-Community'. There are four tabs: 'Anmelden' (selected), 'Server', 'Verbindung', and 'Optionen'. Under the 'Anmelden' tab, there is a 'Benutzername:' field with 'Doctor Notes' and a 'Kennwort:' field with '*****'. Below the password field are two checkboxes: 'Kennwort merken' (checked) and 'Automatisch anmelden' (unchecked).



Embedded-Sametime (mit LTPA Token)

- Voraussetzungen:
 - ▶ Domino mit Internet-Konfiguration über Serverdokument
 - ▶ SSO Token vorhanden (HTTP nach Änderung neu gestartet)
- Anwendung:
 - ▶ Basic Client
 - ▶ Standard Client
- Abhängigkeiten:
 - ▶ arbeitet sehr gut mit NSL zusammen



The screenshot shows the 'Benutzervorgaben' (User Settings) window for a Domino Sametime client. The window is divided into two main sections: 'Allgemein' (General) and 'Konfiguration' (Configuration).

In the 'Konfiguration' section, the following options are visible:

- ☒ Instant-Messaging-Status für Namen anzeigen
- ☒ Bei Instant Messaging mittels einmaliger Anmeldung (SSO) anmelden
- ☐ Mit dem kanonischen Namen nach dem Instant-Messaging-Status suchen

The 'Anmelden' (Login) section is also visible, showing the following fields and options:

- Typ der Server-Community: Sametime
- Status der Server-Community: Verfügbar
- Name der Server-Community: hub.wwcorp.com
- Benutzername: Doctor Notes
- Kennwort: (empty field)
- ☐ Kennwort merken
- ☐ Automatisch anmelden
- ☒ Tokenbasierte Einzelanmeldung verwenden
- Authentifizierungsserver: Hub/SVR/WWCorp
- Authentifizierungstyp: Domino-SSO

Red boxes highlight the 'Bei Instant Messaging mittels einmaliger Anmeldung (SSO) anmelden' checkbox in the configuration section and the 'Tokenbasierte Einzelanmeldung verwenden' checkbox in the login section.

Sametime – Desktop-Richtlinien unterstützen

- Um Benutzern die Konfigurationsarbeit abzunehmen sollten Administratoren Desktop-Richtlinien einsetzen

Desktopeinstellungen : -Default-

Allgemein | Smart Upgrade | Anwendungen | Widgets | Wählverbindungen | Konten | Namensserver | SSL | Appletsicherheit | Proxies | Mail | Vorgaben | K...

Allgemein | Verschiedenes | Fensterverwaltung | Ländereinstellungen | Internet | Mail | Instant Messaging | Replizierung | Netzwerkports |

Einstellungen für Instant-Messaging für Benutzer von Notes 8 Basic, Notes 7 und früher	Wie diese Einstellung angewendet wird:	Übernehmen von übergeordneter Richtlinie:	Zwingend in untergeordnet Richtlinien:
Instant-Messaging-Status für Namen anzeigen: <input type="checkbox"/> Aktivieren <input type="button" value="v"/>	Wert festlegen und Änderungen verhindern <input type="button" value="v"/>	<input type="checkbox"/> Übernehmen	<input type="checkbox"/> Zwingend
Bei IBM Lotus Instant Messaging mittels einmaliger Anmeldung (SSO) anmelden: <input type="checkbox"/> Aktivieren <input type="button" value="v"/>	Wert festlegen und Änderungen verhindern <input type="button" value="v"/>	<input type="checkbox"/> Übernehmen	<input type="checkbox"/> Zwingend
Kanonischen Namen zum Suchen nach dem Instant-Messaging-Status verwenden: <input type="checkbox"/> Deaktivieren <input type="button" value="v"/>	Wert festlegen und Änderungen verhindern <input type="button" value="v"/>	<input type="checkbox"/> Übernehmen	<input type="checkbox"/> Zwingend
Chatmitschriften: <input type="checkbox"/> Nachfragen, ob Mitschriften gespeichert werden sollen <input type="button" value="v"/>	Wert festlegen und Änderungen verhindern <input type="button" value="v"/>	<input type="checkbox"/> Übernehmen	<input type="checkbox"/> Zwingend

Einstellungen für Instant-Messaging für Benutzer des Notes Standard-Clients	Wie diese Einstellung angewendet wird:	Übernehmen von übergeordneter Richtlinie:	Zwingend in untergeordnet Richtlinien:
Instant-Messaging-Server: <input type="text" value="Hub/SVR/WWCorp"/>	Wert festlegen und Änderungen verhindern <input type="button" value="v"/>	<input type="checkbox"/> Übernehmen	<input type="checkbox"/> Zwingend
Bei IBM Lotus Instant Messaging mittels einmaliger Anmeldung (SSO) anmelden: <input type="checkbox"/> Aktivieren <input type="button" value="v"/>	Wert festlegen und Änderungen verhindern <input type="button" value="v"/>	<input type="checkbox"/> Übernehmen	<input type="checkbox"/> Zwingend

Sametime-Connect (mit SPNEGO)

- Notwendige Konfigurationsentscheidung für Anmeldeverfahren
 - ▶ Verwendung von LTPA Tokens aus einem LDAP Verzeichnis
 - ▶ Verwendung von SPNEGO (zur Zeit nicht vom Embedded Client unterstützt)
- Einrichtung des Sametime Servers und Sametime Connect mit SPNEGO ist im Infocenter dokumentiert
 - ▶ Sametime Connect Client erforderlich
 - ▶ Sametime Server muss auf einen Microsoft® Active Directory LDAP Server verweisen
 - ▶ IBM WebSphere Server für die erste Authentifizierung erforderlich
 - ▶ Microsoft Windows® Active Directory Domain Controller und entsprechendes Kerberos Key Distribution Center (KDC)
 - ▶ Aktueller Rechner muss Mitglied der Microsoft Windows Domäne sein
- Detaillierte Info unter:
 - ▶ http://publib.boulder.ibm.com/infocenter/sametime/v8r0/topic/com.ibm.help.same.time.802.doc/IMLU/st_adm_security_sso_spnego_t.html



Besonderheiten bei Lotus QuickR

- Zwei Edition für Lotus QuickR verfügbar
 - ▶ Lotus Domino
 - ▶ J2EE (Websphere)
- QuickR Clients sind zahlreich
 - ▶ Sidebar Plugin in Lotus Notes
 - ▶ Connectoren für Windows Anwendungen
 - ▶ Web Browser

Aufgabenstellung kann beliebig umfangreich und spezifisch sein.



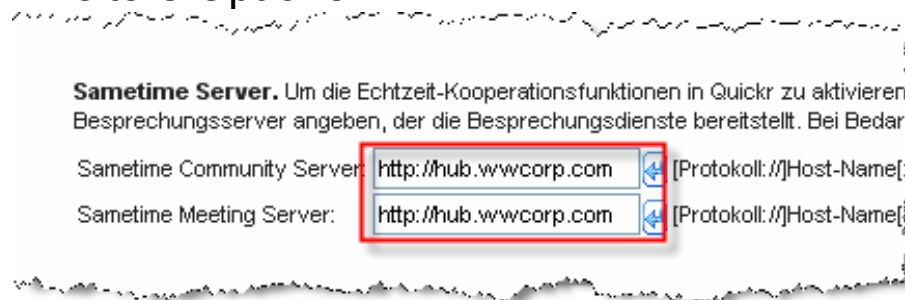
Anwesenheitsanzeige und Instant Messaging für QuickR aktivieren

1. Dateien auf den Lotus Sametime Server kopieren

Dateiname	Kopieren aus	Kopieren nach
STComm.jar	Sametime SDK client\stjava\bin\	<DominoData>\Domino\html\QuickPlace\peopleonline
CommRes.jar	Sametime SDK client\stjava\bin\	<DominoData>\Domino\html\QuickPlace\peopleonline
PeopleOnline31.jar	Lotus Quickr Server <DominoData>LotusQuickr\	<DominoData>\Domino\html\QuickPlace\peopleonline

2. Lotus Sametime Server in Lotus QuickR konfigurieren

- Anmelden
- Site-Administration
- Weitere Optionen



3. Testen



Die IBM SSO Landschaft (SPNEGO)

Clients



Lotus Sametime.



SPNEGO

Lotus Sametime.



SPNEGO

Server



SPNEGO*

Lotus Domino.



SPNEGO*

Lotus Quickr.



SPNEGO

Lotus Connections



SPNEGO*

Lotus Sametime.



SPNEGO

WebSphere Portal



SPNEGO

Tivoli software



Verwendung verschiedener Server einer Domäne



Live-Demonstration



Unterstützung durch Produkte von Drittanbietern



Unterstützung durch Produkte von Drittanbietern

- IBM Tivoli Access Manager for Enterprise SSO (WebSeal)
 - ▶ Portal für ESSO
- CA SiteMinder
 - ▶ Portal für ESSO
- Pistolstar
 - ▶ „Password-Power“Plugins für SSO (Notes und Web)
- Northern Collaborative Technologies
 - ▶ „NCT Simple Signon“



Fazit und weitere mögliche Entwicklungsrichtungen



Wo steht SSO Im Domino Umfeld?

- Notes Clients SSO mit NSL einfach und elegant zu betreiben
 - ▶ Regelmäßige Kennwortwechsel und Roaming User bleiben immer noch ein Problem
- Web SSO gegen Domino-Server
 - ▶ **Ein** Kennwort erforderlich mit LTPA Token
 - ▶ **Ein** Kennwort erforderlich durch SPNEGO Support (ab 8.5.1 auf Windows Servern)
 - ▶ Manche Plugins / Clients speichern Kennwörter lokal und rufen diese nur ab
 - ▶ Eine Durchgängige Lösung ist abhängig von der Kombination der installierten Domino-Companionproducts
- Umfangreiche Lösungen (ohne Domino 8.5.1) erfordern zusätzliche Server
 - ▶ WebSphere
 - ▶ Tivoli Access Manager
 - ▶ Microsoft IIS (siehe Anhang C)
 - ▶ etc.



und umfangreiche Konfigurationen / Tests



Fazit und weitere mögliche Entwicklungsrichtungen

- SPNEGO Support für alle Anwendungen
- SPNEGO Anbindung für Linux Systeme
- Domino Directory Independance (Domino 8.5.x ?) bringt zusätzlichen Komfort für Web SSO
- Zusatzprodukte erforderlich, für Domino (<8.5.1) SPNEGO Support, und wenn Domino nicht auf Windows läuft
- Authentifizierung heisst noch nicht Autorisierung
 - ▶ ggf. Name Mapping bei Mult-Directory Ansätzen erforderlich (hier nicht behandelt)
- Enterprize SSO (ESSO)
 - ▶ Authentifiziert Benutzer einmalig
 - ▶ Anwendungen welche Authentifizierungen benötigen, bedienen sich einer zentralen Instanz (Umsetzung durch die spezifischen Systeme)
 - ▶ Ermöglicht einen zentralen Single-Sign-Off



Weniger oder kein Kennwort erforderlich?

- Zugriffe auf Domino Daten erfordern (i.d.R.) Authentifizierungen
 - ▶ Im Intranet ist zukünftig eine Authentifizierung über SPNEGO/Kerberos möglich (kein Domino HTTP Kennwort erforderlich)
 - ▶ Internet Zugriff auf Domino erfordert auch zukünftig ein Kennwort (weil z.B. SPNEGO nicht genutzt werden kann).
- Lösungsansätze für Internet Kennwörter:
 - ▶ Domino HTTP für jeden Benutzer oder
 - ▶ Verwendung von Windows Kennwörtern
 - Wenn das Domino HTTP Kennwort im Personendokument **nicht** gesetzt ist (und zukünftig Domino Directory Independence Konfiguration verwendet wird)
 - Verzeichnisunterstützung auf ein Active Directory verweist, oder Domino Directory Independence in Verbindung mit Active Directory verwendet wird
 - Kein Bedarf mehr für Domino Kennwort Richtlinien, da Benutzer gegen das Active Directory authentifiziert werden
 - Kennwortrücksetzung erfolgt ggf. durch andere Help-Desk Instanzen



Noch Fragen offen geblieben?



<http://www.mmi-consult.de>
<http://www.mmi-consult.de/faq>
<mailto:manfred.meise@mmi-consult.de>



Anhang A: Referenzen (und weitere Informationen)

- **Notes Shared Login:**
 - ▶ <http://www-10.lotus.com/ldd/dominowiki.nsf/dx/id-vault-and-notes-shared-login-faq>
- **QuickR SSO:**
 - ▶ http://publib.boulder.ibm.com/infocenter/lqkrhelp/v8r0/index.jsp?topic=/com.ibm.lotus.quickr.admin.dom.doc/admin/qp_adm_sec_s_s_t.html
- **Sametime und QuickR Integration:**
 - ▶ <http://www.ibm.com/developerworks/lotus/library/connections-integrating/>
- **SameTime SSO/SPNEGO:**
 - ▶ http://www-01.ibm.com/support/docview.wss?rs=477&context=SSKTXQ&q1=Domino+Single+Sign-On+Connect&uid=swg21297954&loc=en_US&cs=utf-8&lang=en
 - ▶ <http://www.ibm.com/developerworks/lotus/documentation/sametime/d-ls-integratingspnego/>
- **SPNEGO**
 - ▶ <http://en.wikipedia.org/wiki/SPNEGO>
- **Konfiguration Sametime Server und Sametime Connect für Anmeldung über SPNEGO:**
 - ▶ http://publib.boulder.ibm.com/infocenter/sametime/v8r0/topic/com.ibm.help.sametime.802.doc/IMLU/st_adm_security_sso_spnego_t.html
- **Domino Integration mit IIS**
 - ▶ <http://www-01.ibm.com/support/docview.wss?uid=swg21105816>
- **Northern Collaborative Technologies „Simple Signon“**
 - ▶ <http://www.thenorth.com/ncthome.nsf/html/nctssso>
- **Pistolstar „Password Power“**
 - ▶ <http://pistolstar.com/password-plugin-products/password-power-8.html>
- **CA SiteMinder**
 - ▶ <http://www.ca.com/de/products/product.aspx?id=5262>
- **Tivoli Access Manager for Enterprise Single Sign-on**
 - ▶ <http://www-01.ibm.com/software/tivoli/products/access-mgr-esso/>



Anhang B: Begriffsdefinitionen im SSO Umfeld

- **Enterprise SSO**
 - ▶ Nach Erst-Authentifizierung werden Zugangsdaten zu verschiedenen Systemen an einem sicheren Ort abgespeichert.
 - ▶ Zugangsdaten werden jeweils von einem „Interceptor“ vom sicheren Ort ausgelesen und der fremden Anwendung zur Verfügung gestellt
- **Web based SSO**
 - ▶ Verwaltet SSO innerhalb der Organisation über Grenzen von SITES und Anwendungen hinweg
- **Kerberos based SSO**
 - ▶ Nach Erst-Authentifizierung erhält der Benutzer ein Ticket-Granting Ticket, das weiteren Anwendungen im Rahmen zusätzlicher Authentifizierung vorgelegt wird, um diesen eine Authentifizierung am TGT Server zu ermöglichen
- **Password synchronisation**
 - ▶ Verwaltung eines Passwortes, dass zwischen verschiedenen Anwendungen identisch gehalten wird, um dem Benutzer die Authentifizierung mit stets dem gleichen Passwort zu ermöglichen
- **Cross Domain SSO**
 - ▶ Benutzer authentifizieren sich einer einer Domäne und verwendet Anwendungen in weiteren Domänen. Vertrauensstellungen erfolgen hierbei jeweils auf Domänenebene
- **Federated SSO**
 - ▶ Erweiterung von Web based SSO über Unternehmensgrenzen hinaus. Setzt Vertrauensstellungen zwischen Unternehmen und einen gemeinsamen Austausch/Akzeptanz von Security Tokens voraus.
- **Smart Card SSO**
 - ▶ Benutzer besitzt ein Device vor, auf dem Zertifikate oder Passwörter gespeichert sind, die im Rahmen von SSO benötigt werden.



Anhang C: Integration Domino 8 mit IIS

1. WAS Plugin installieren
2. WAS Plugin in IIS einbinden
3. WAS Plugin konfigurieren
4. Sicherheitseinstellungen für IIS
5. Konfiguration des Domino Server
6. (optional)SPNEGO Authentifizierung verwenden
7. (optional)Name Mapping für Benutzer



Schritt 1: WASPlugin installieren

- Verzeichnisstruktur auf IIS Server anlegen

C:\Programme\IBM\WebSphere\AppServer\bin

C:\Programme\IBM\WebSphere\AppServer\config

C:\Programme\IBM\WebSphere\AppServer\etc

C:\Programme\IBM\WebSphere\AppServer\logs

- Plug-in Dateien kopieren

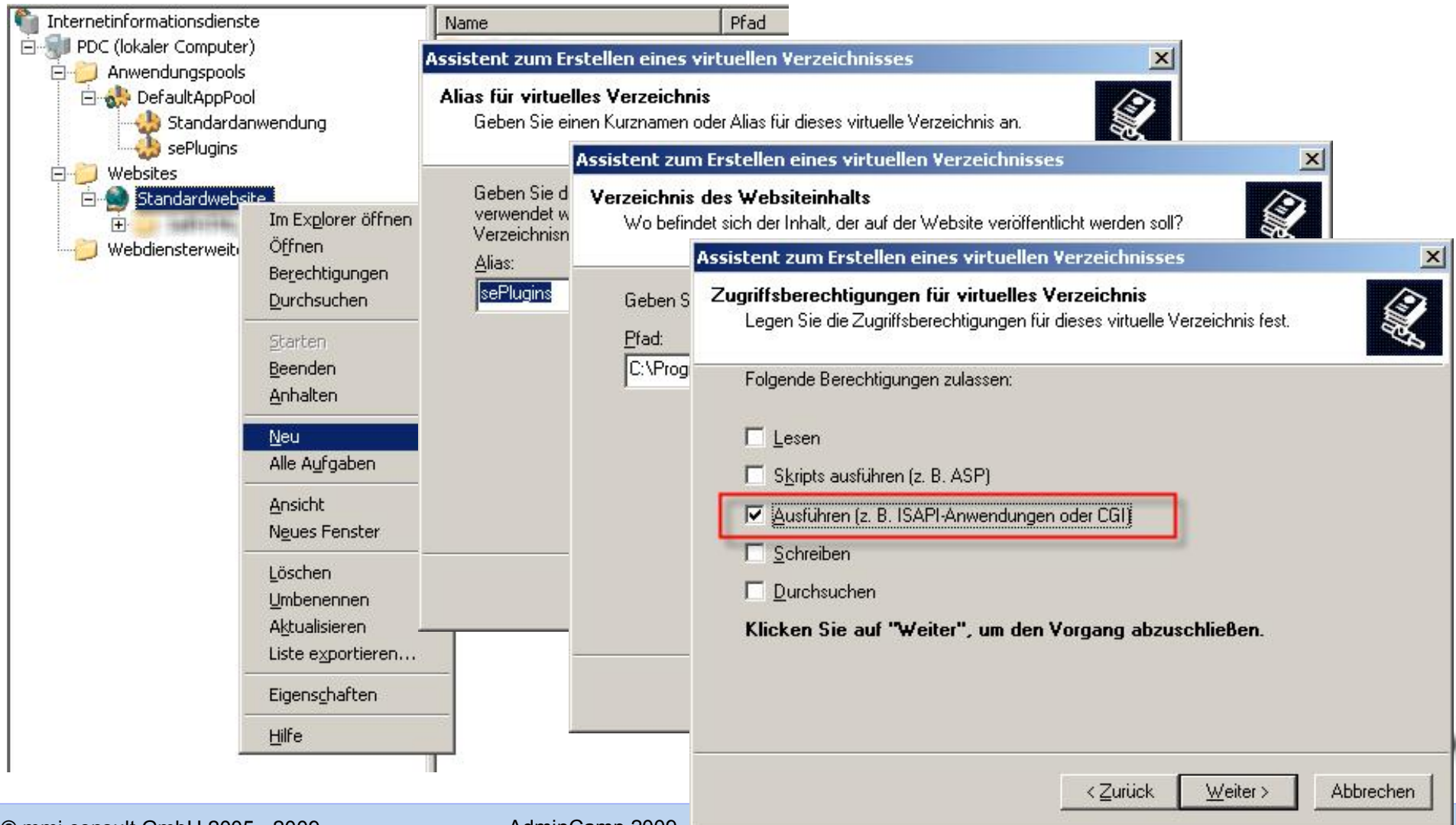
"plugin\plg.webserverplugins.pak\repository\plugins.http\bin\iisWASPlugin_http.dll
nach "C:\Programme\IBM\WebSphere\AppServer\bin,,

"plugin\plg.webserverplugins.pak\repository\plugins.http\config\templates\plugin-
cfg.xml" nach "C:\Programme\IBM\WebSphere\AppServer\config"



Schritt 2: WAS Plugin einbinden

- Virtuelles Verzeichnis „sePlugins“ mit Referenz auf Plug-in DLL



Schritt 3: Was Plug-in konfigurieren

- Im DLL Verzeichnis „C:\Programme\IBM\WebSphere\AppServer“ eine Verweisdatei „plugin-cfg.loc“ mit Pfad zur Konfigurationsdatei anlegen

C:\Programme\IBM\WebSphere\AppServer\config\plugin-cfg.xml

- Konfigurationsdatei "C:\Programme\IBM\WebSphere\AppServer\config\plugin-cfg.xml,, mit Editor anpassen:

```
<Log LogLevel="Error"
  Name="C:\Programme\IBM\WebSphere\AppServer\logs\http_plugin.log"/>
```

...

```
<Transport Hostname="west06.wwcorp.com" Port="8080" Protocol="http"/>
```

...

```
<Uri Name="/* .nsf*" />
```

```
<Uri Name="/* .NSF*" />
```

```
<Uri Name="*/icons/*" />
```

```
<Uri Name="*/domjava/*" />
```

```
<Uri Name="*/domjs/*" />
```

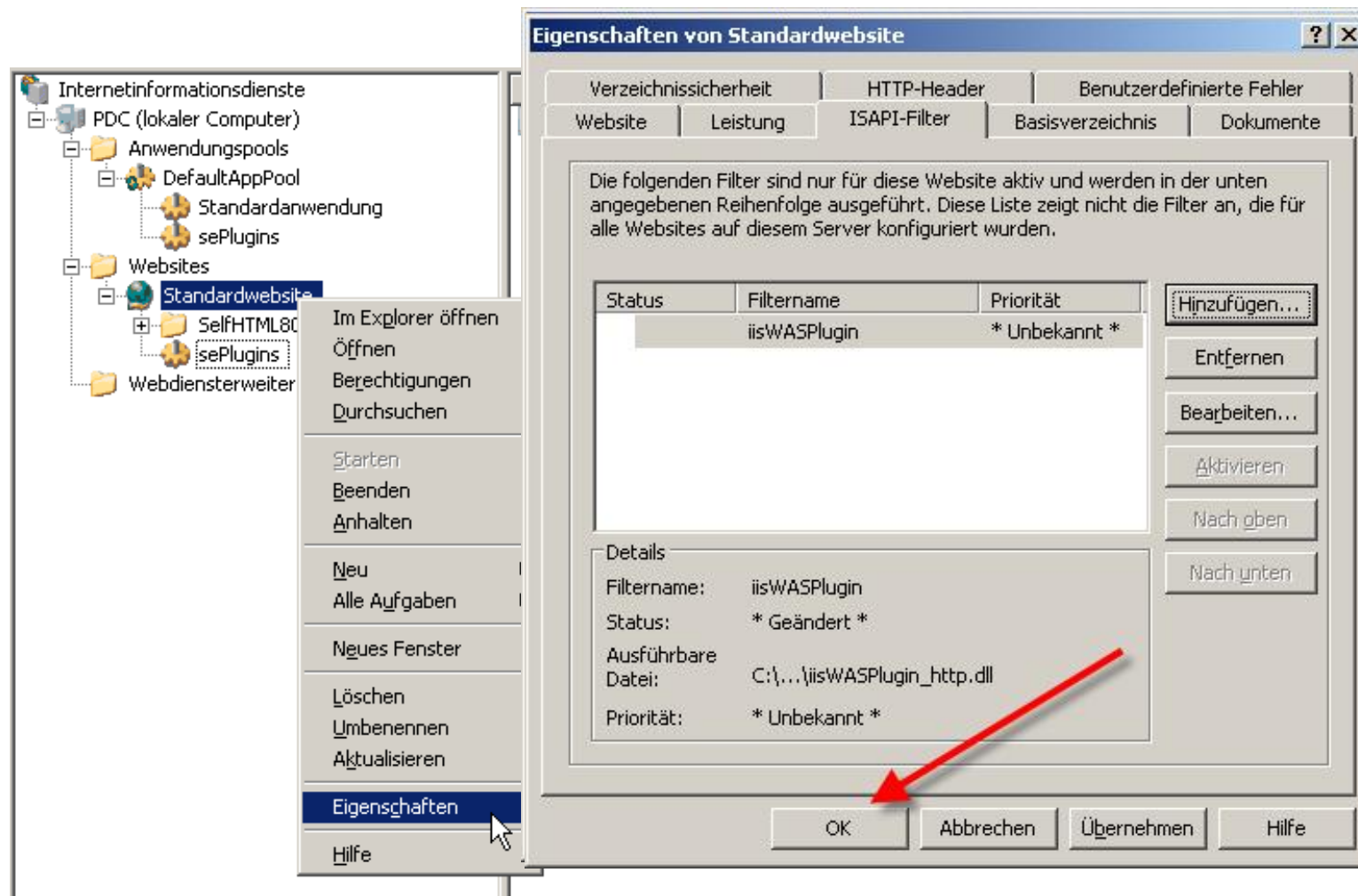
```
<Uri Name="*/domino/*" />
```

...



Schritt 4. Sicherheitseinstellungen für IIS

- ISAPI Filter (WAS Plug-in) in IIS einbinden



Eigenschaften von Standardwebsite

Verzeichnissicherheit | HTTP-Header | Benutzerdefinierte Fehler
Website | Leistung | **ISAPI-Filter** | Basisverzeichnis | Dokumente

Die folgenden Filter sind nur für diese Website aktiv und werden in der unten angegebenen Reihenfolge ausgeführt. Diese Liste zeigt nicht die Filter an, die für alle Websites auf diesem Server konfiguriert wurden.

Status	Filtername	Priorität
	iisWASPlugin	* Unbekannt *

Hinzufügen...
Entfernen
Bearbeiten...
Aktivieren
Nach oben
Nach unten

Details

Filtername: iisWASPlugin
Status: * Geändert *
Ausführbare Datei: C:\...\iisWASPlugin_http.dll
Priorität: * Unbekannt *

OK | Abbrechen | Übernehmen | Hilfe



Schritt 5: Konfiguration des Domino Servers

- Integration mit IIS konfigurieren
- Bindung an den in Plug-in Konfiguration konfigurierten Port
- Notes.ini:

HTTPEnableConnectorHeaders=1

Server: **West06/SVR/WWCorp** pdc.wwcorp.com

Allgemein | Sicherheit | Ports... | Server-Tasks... | Internetprotokolle... | MTA... | Ver...

HTTP | Domino-Web-Server | DIIOP | LDAP

HTTP-Sitzungen

Sitzungsauthentifizierung:

Maximale Anzahl aktiver Sitzungen:

URL-Referenzen für diesen Server generieren

Verwendet dieser Server IIS?

Protokoll:

Hostname:

Portnummer:

Allgemein | Sicherheit | Ports... | Server-Tasks... | Internetprotokolle...

Notes-Netzwerkports | Internet-Ports... | Proxies

SSL-Einstellungen

Name der SSL-Schlüsseldatei:

SSL-Protokollversion (für alle Protokolle außer HTTP):

SSL-Sitezertifikate annehmen: ☐ Ja ☒ Nein

Abgelaufene SSL-Zertifikate annehmen: ☒ Ja ☐ Nein

SSL-Verschlüsselungscodes: RC4-Verschlüsselung mit 128
RC4-Verschlüsselung mit 128
Triple-DES-Verschlüsselung mit 128
DES-Verschlüsselung mit 56
RC4-Verschlüsselung mit 40

SSL V2 aktivieren: ☐ Ja
(SSL V3 ist immer aktiviert)

Web | Verzeichnis | Mail | DIIOP | Remote-Debug-Manager

Web (HTTP/HTTPS)

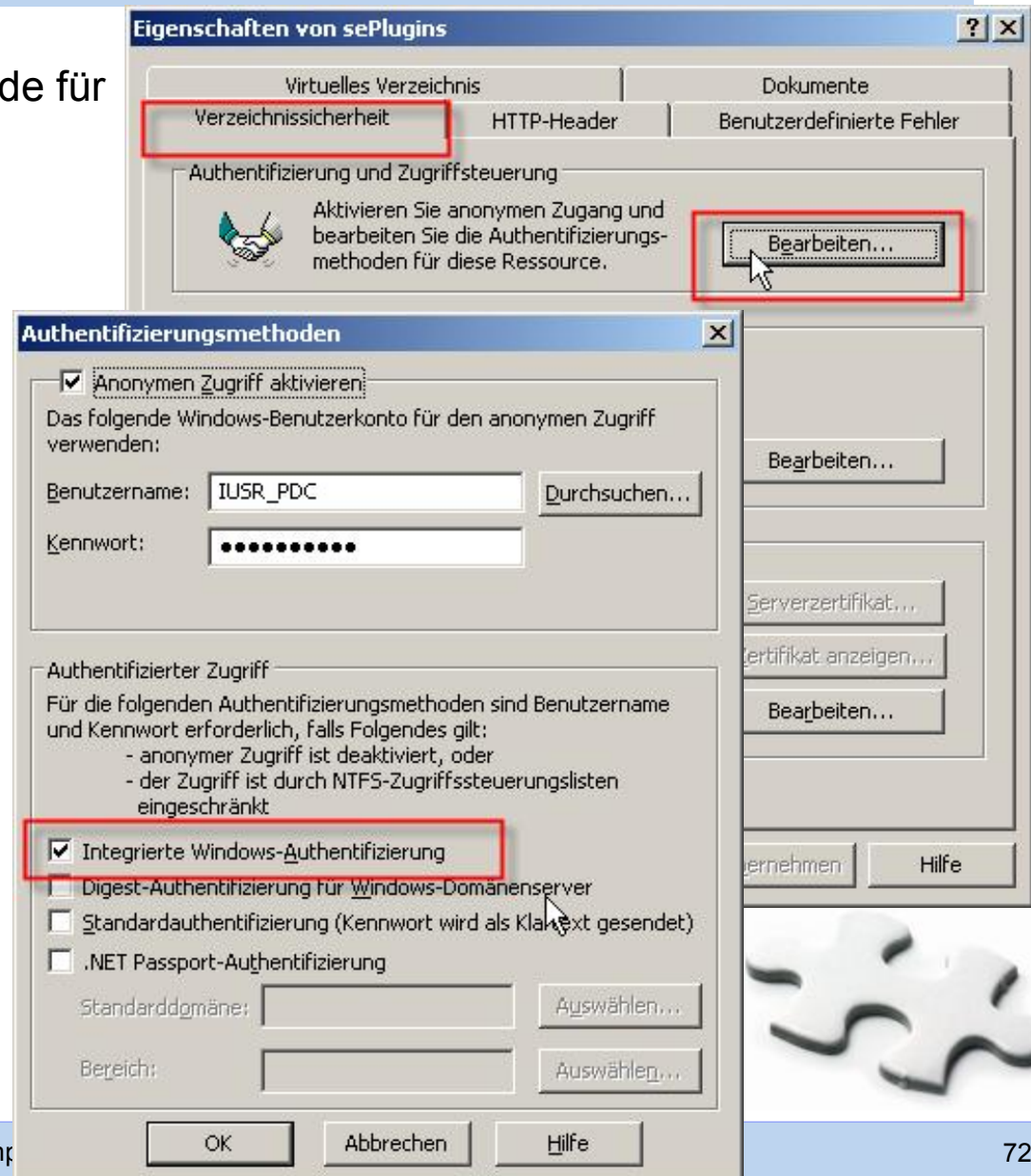
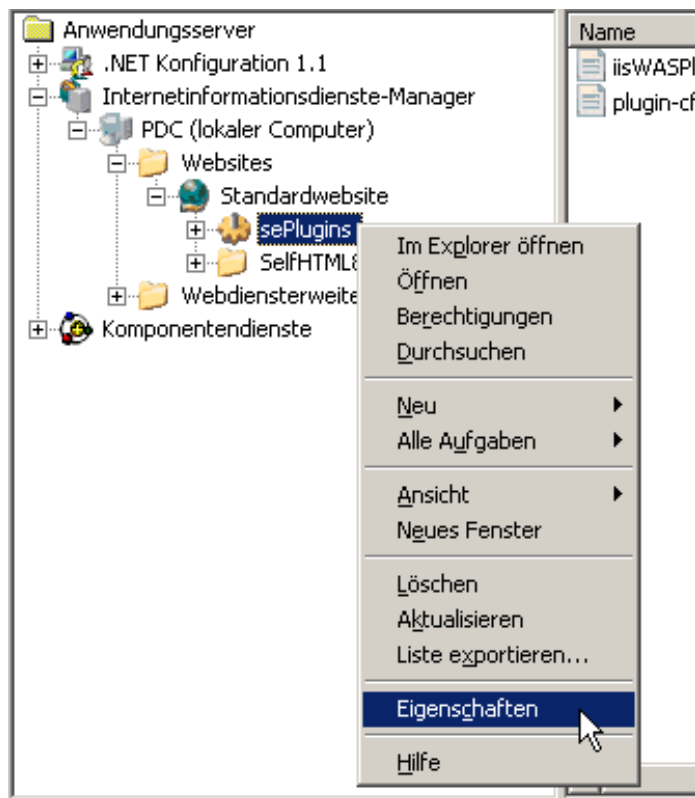
TCP/IP-Portnummer:

TCP/IP-Portstatus:

Einstellungen zum Serverzugriff erzwingen:

Schritt 6: SPNEGO Authentifizierung verwenden

- weitere Authentifizierungsmethode für IIS hinzufügen



Schritt 7: Name Mapping für Benutzer

- Verschiedene Integrationsalternativen möglich
 - ▶ Domino Directory Independance (ab Domino 8.5.1)
 - ▶ Active Directory über Verzeichnisuntersützung als LDAP Verzeichnis
 - Erfordert Schema Erweiterung in AD
 - Domino Benutzernamen werden in AD abgelegt
 - ▶ DN aus Active Directory als AliasName in Domino abgelegt

