Single Sign On
mit
Active Directory

Andreas Artner
IBM Software Consultant

FRITZ & MACZIOL
Software, Systeme und Dienstleistungen

Agenda

- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

Alles ganz einfach ?

- SPNEGO
- Kerberos
- LTPA Token
- Directory Assistance
- Active Directory
- LDAP
- Name Mapping
- Sessionbased Authentication

Definition

- Was bedeutet Single Sign On ?
  - Single Sign On
    - Benutzer **authentifizieren** sich einmal z.b. bei der Anmeldung an Windows und dann nicht mehr !
  - Single Password
    - Benutzer verwenden zur Anmeldung an unterschiedlichen Systemen das **gleiche Passwort**
- Beide Verfahren haben Auswirkung auf die IT-Sicherheit

Definition

Verfahren, Begriffe die im Zusammenhang mit Single Sign On und Single Password stehen:

- Directory Assistance
  - Erlaubt das Einbinden zusätzlicher Verzeichnisse in Domino
  - Mächtig und sehr flexibel
- Session based Authentication
  - Bezieht sich auf Web-Sessions
  - Single oder Multi Server
  - Einmalige Anmeldung an einem Server oder einem Verbund von Servern

Definition

- LTPA Token
  - IBM Lightweight Third-Party Authentication
  - Browser Cookie um die Multi Server Session based Authentication zu ermöglichen
- SPNEGO
  - **S**imple and Protected GSSAPI **Nego**tiation Mechanism
  - SPNEGO wir verwendet wenn ein Client sich an einem Server anmelden will aber beide nicht sicher sind wie die Authentifizierung erfolgen soll
- Kerberos
  - Authentifizierungs Protokoll
  - Ticket basierte Authentifizierung
  - Seit Windows 2000 Standard in Windows Domänen

Single Password

Drei Optionen:

1. Logon wird gegen eine zentrales Verzeichnis validiert
   - Lösung: Directory Assistance
2. Passwörter werden gecached
   - Support intensiv
3. Passwörter werden zwischen den Systemen synchronisiert
   - Lösung: Tivoli Directory Integrator Password Plugins
   - Sehr Komplexes Setup
   - Auf jedem Active Directory Domaincontroller muss das Plugin installiert werden
   - Daher: nur in Ausnahmefällen und kleinen Umgebungen !

Single Sign On

- Die Lösung:
  - SPNEGO
  - (Session Based Authentication)
  - Tools wie:
    - TAM ESSO
    - SiteMinder
    - …

Die Qual der Wahl ?

- Single Sign On oder Single Password ?
- Sessionbased Authentication oder SPNEGO ?
- Oder ein Mix von allem ?

- Abhängig von Ihrer Umgebung
  - Active Directory vorhanden ?
  - Haben alle User Accounts im AD ?
- Abhängig von Ihren Anforderungen
  - Sollen sich Benutzer bewusst mehrmals anmelden ?

Die Grundlage

- Für alle Lösungen zwingend erforderlich:
  - Abgleich von Benutzernamen und Daten zwischen den Directories
  - Notes Fullname <-> AD Distinguished Name
    - Domino: CN=Johann Sametime/O=Admincamp
    - AD: CN= Johann Sametime,CN=Users,DC=Admincamp,DC=local
  - IBM stellt hierfür den Tivoli Directory Integrator zur Verfügung
    - Siehe hierzu auch Track 3 Session 1

Agenda

- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

AD Anbindung mit Directory Assistance

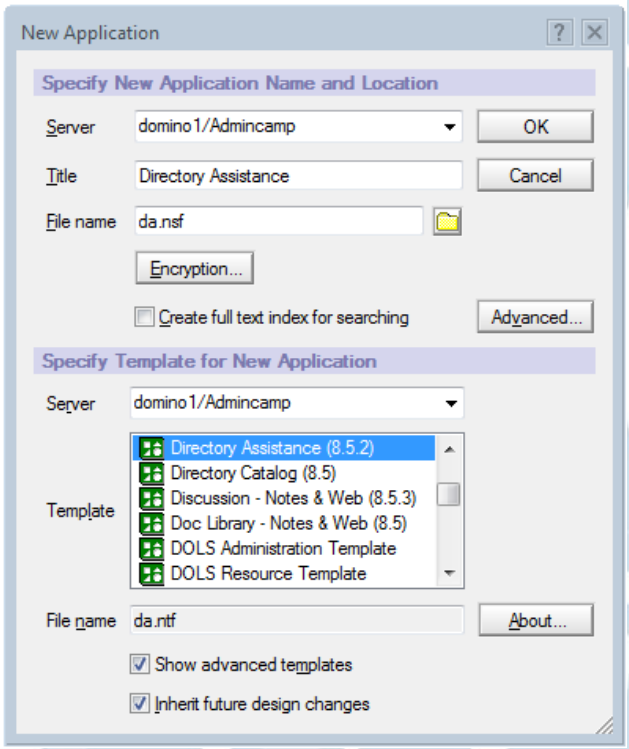
1. http://domino/names.nsf
2. Login Seite
3. Username und Passwort

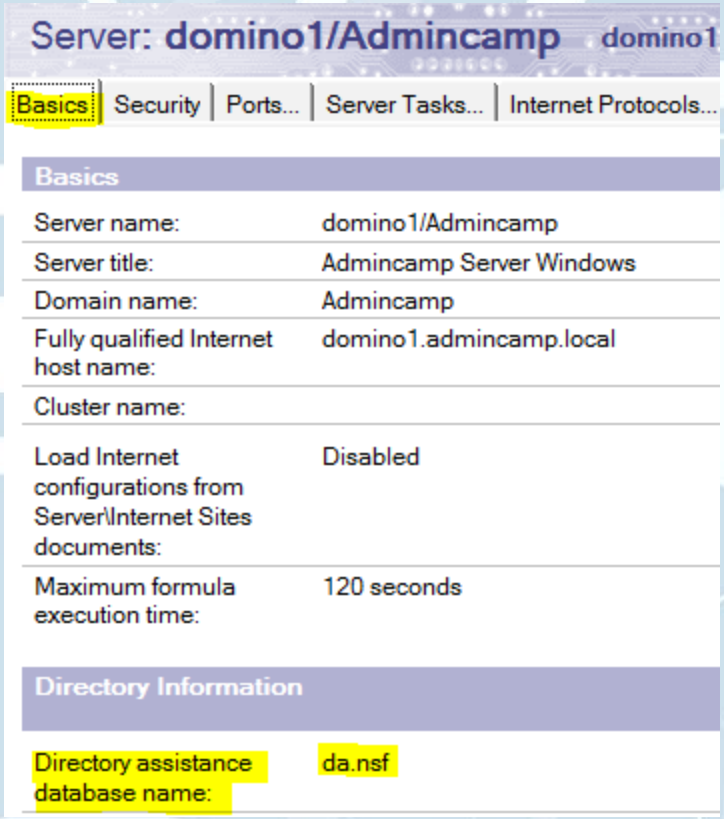
4. Prüft gegen Names.nsf

5. Prüft gegen Active Directory

Directory Assistance

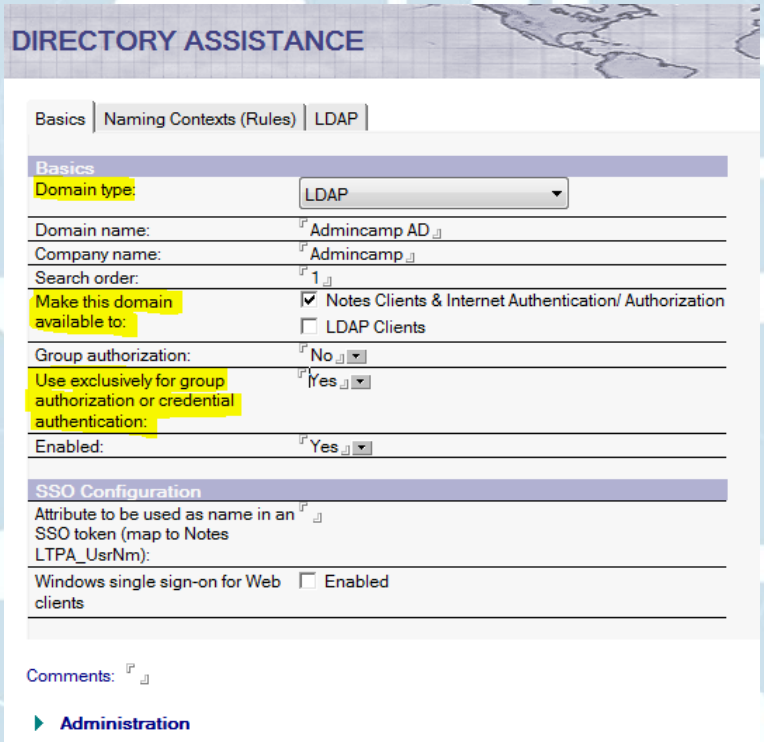
1. Directory Assistance DB erstellen und im Serverdokument konfigurieren

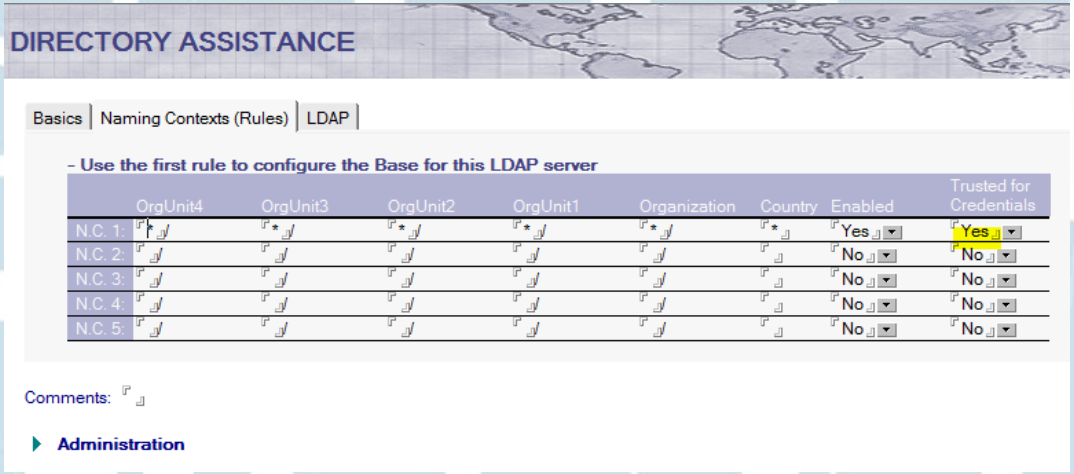




Directory Assistance

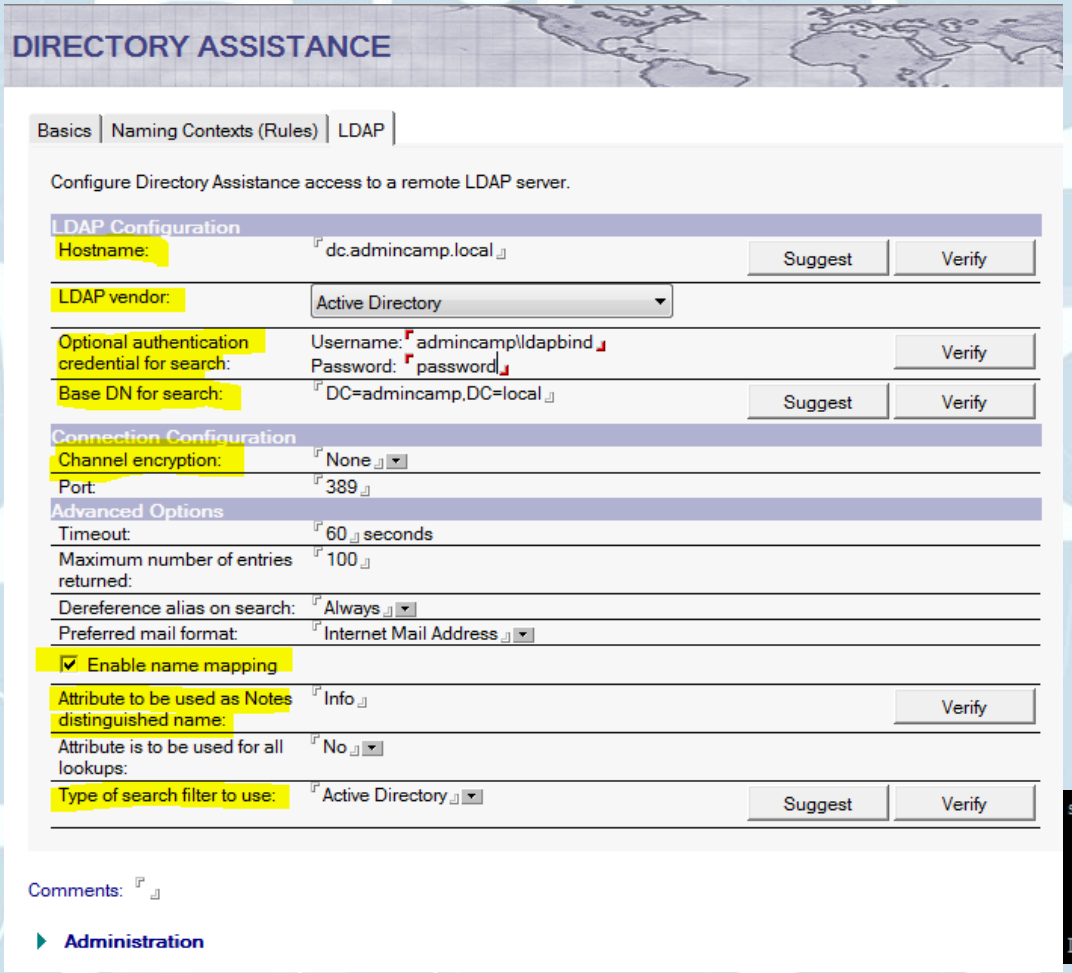
2. Directory Aissistance konfigurieren





Directory Assistance

2. Directory Aissistance konfigurieren …..




```
show xdir
  DomainName     DirectoryType       ClientProtocol Replica/LDAP Server
 ------------- --------------------- ------------- ----------------------
 1 ADMINCAMP      Primary-Notes       Notes & LDAP   names.nsf
 2 ADMINCAMP AD   Secondary-LDAP      Notes          DC.ADMINCAMP.LOCAL:389
Directory Assistance Database 'da.nsf' in use
```

Directory Assistance

Checkliste:

- Erstellen Sie einen LDAP-Bind Benutzer im Active Directory
- Installieren Sie einen LDAP-Browser (z.b. Softerra)
- Machen Sie sich mit der Active Directory Struktur vertraut
- Stellen Sie sicher das SSL aktiviert ist:
  - In Domino für http
  - In Active Directory für LDAP
- Wie soll das Name Mapping erfolgen
- Directory Assistance konfigurieren

Agenda

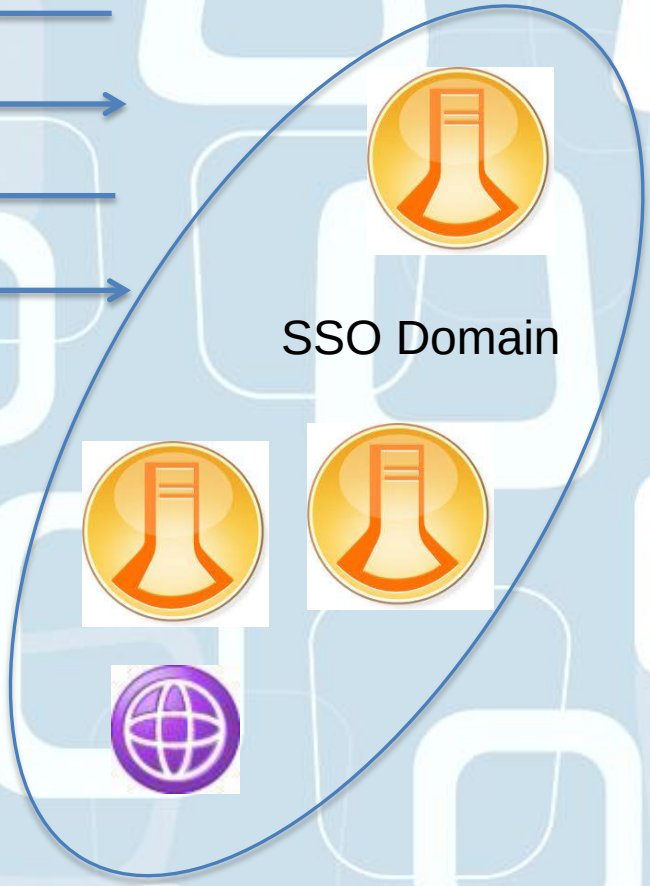
- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

Session based Authentication

- Einmalige Anmeldung in einer Web-Sitzung
- Browser muss Cookies zulassen (LTPA-Token)
- Zwischen mehreren Domino Servern
- Zwischen Domino und Websphere
- Vorteile:
  - Abmeldung möglich ohne den Browser zu schliessen über „?logout“
  - Anzeige der aktiven Sessions über „tell http show users“
  - Anmeldeseite kann in der domcfg.nsf anepasst werden

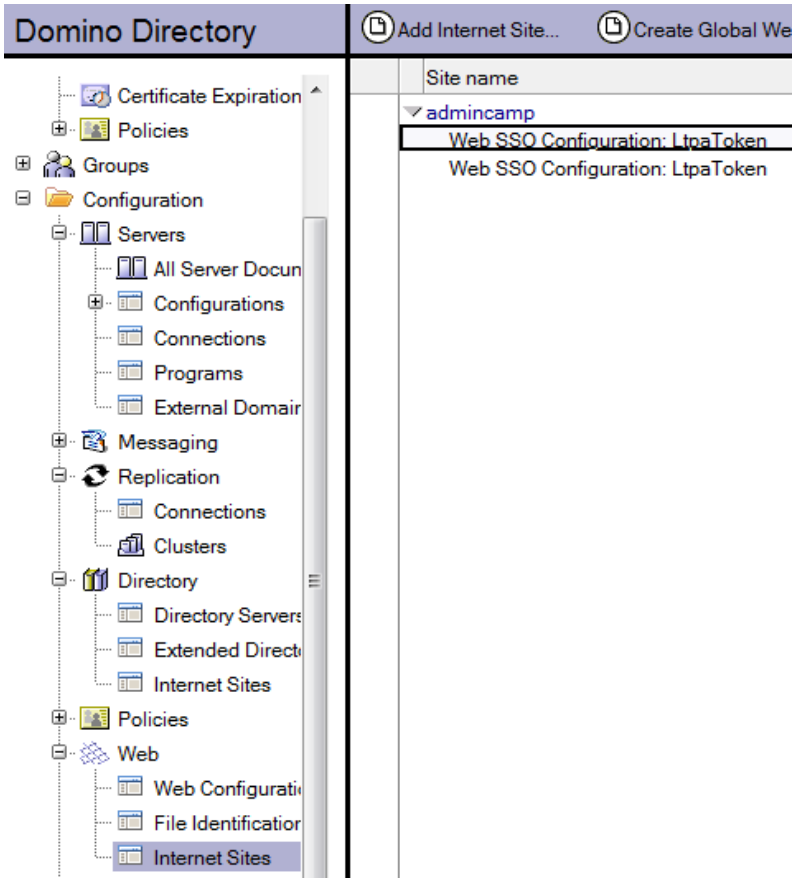
Session based Authentication

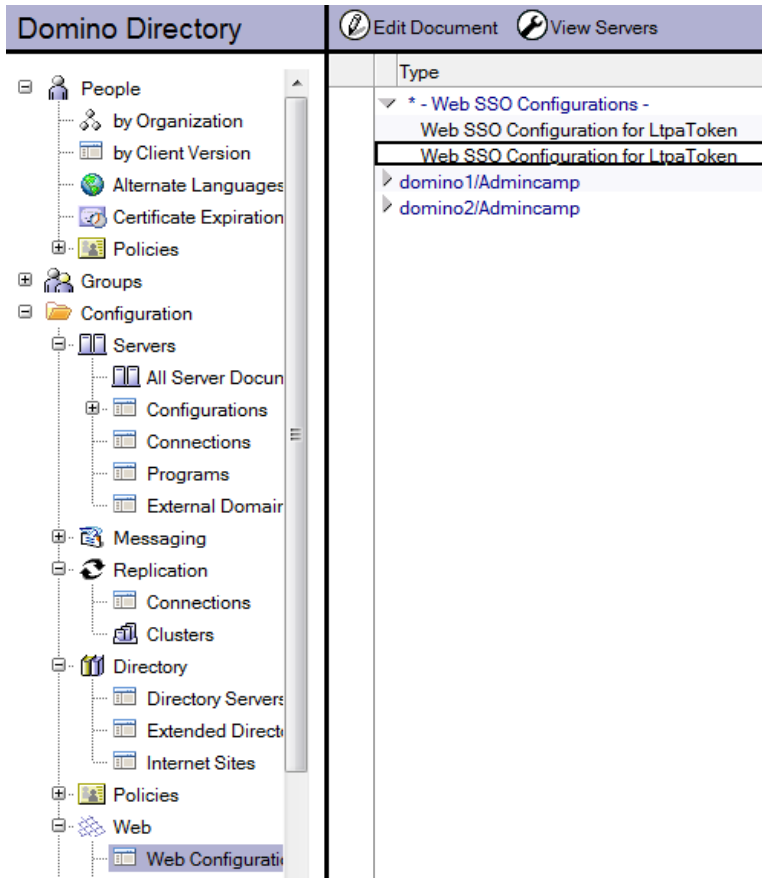
1. http://domino/names.nsf
2. Login Seite
3. Username und Passwort
4. LTPA Token
5. Zugriff auf weitere Server ohne erneute Anmeldung



LTPA einrichten

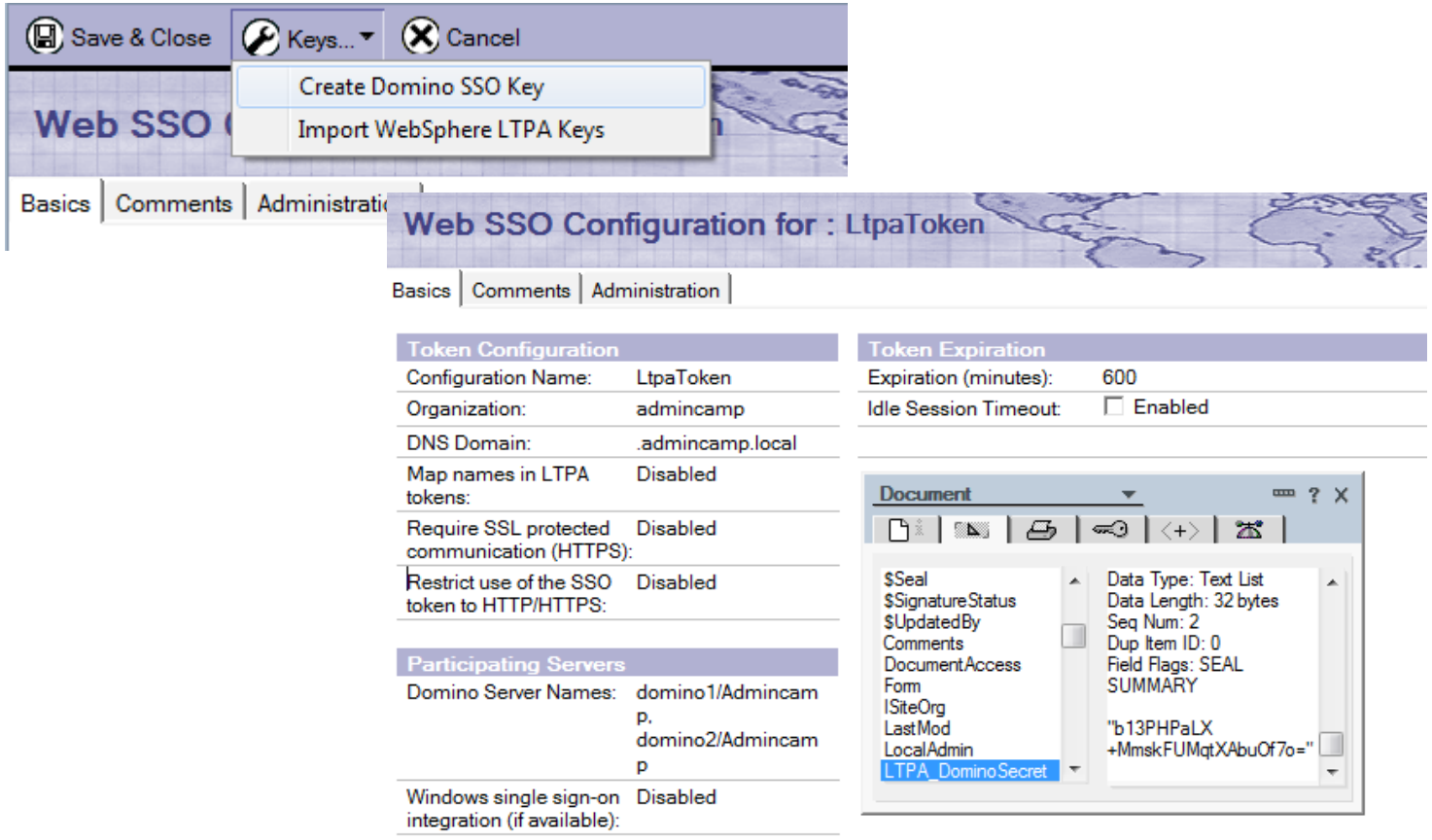
- Konfiguration über die „Web Configurations“ oder Internet Sites View je nachdem wie der Server eingerichtet ist





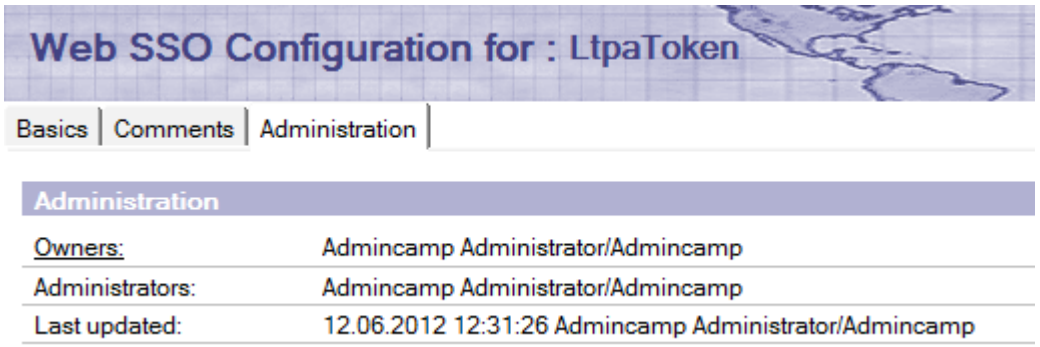
LTPA einrichten

- Neue Domino Keys generieren oder vorhandene WebSphere Keys importieren



LTPA einrichten

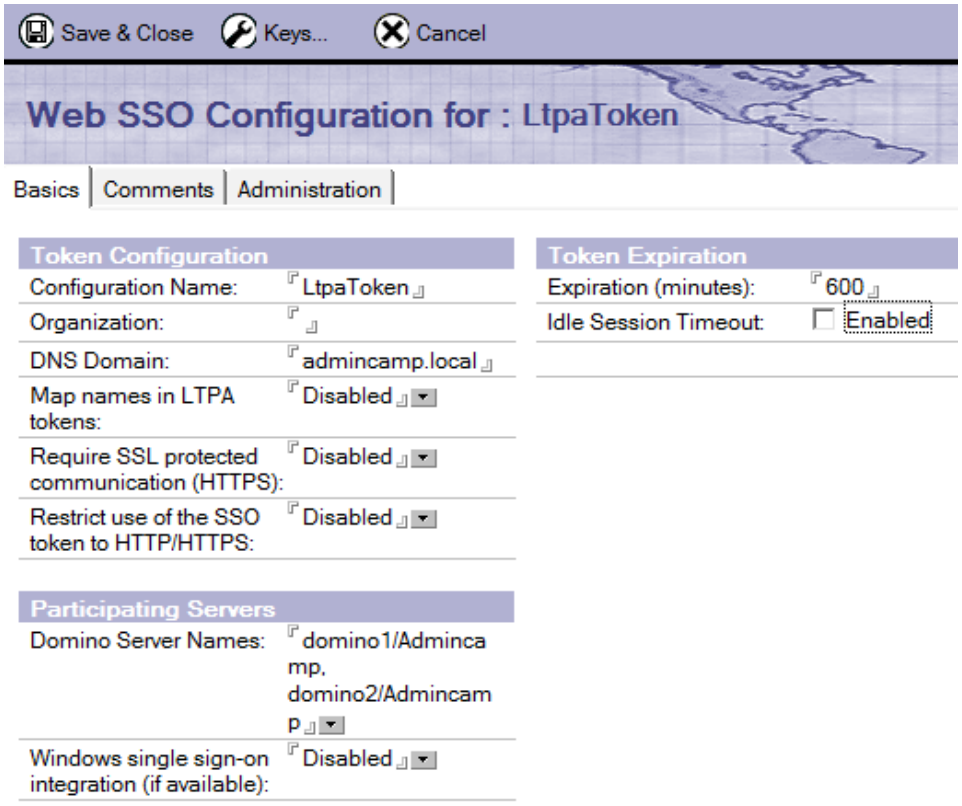
- Der Key wird für die teilnehmenden Server und Administratoren verschlüsselt. Nur Administratoren die angegeben sind können das Dokument bearbeiten



- Weitere Web SSO Konfigurationen einfach per copy & paste erstellen. Der vorhandene Key wird dann hierbei übernommen.

LTPA einrichten

- Organization nur angeben wenn Konfiguration über InternetSites erfolgt.
- DNS Domain der teilnehmende Server angeben

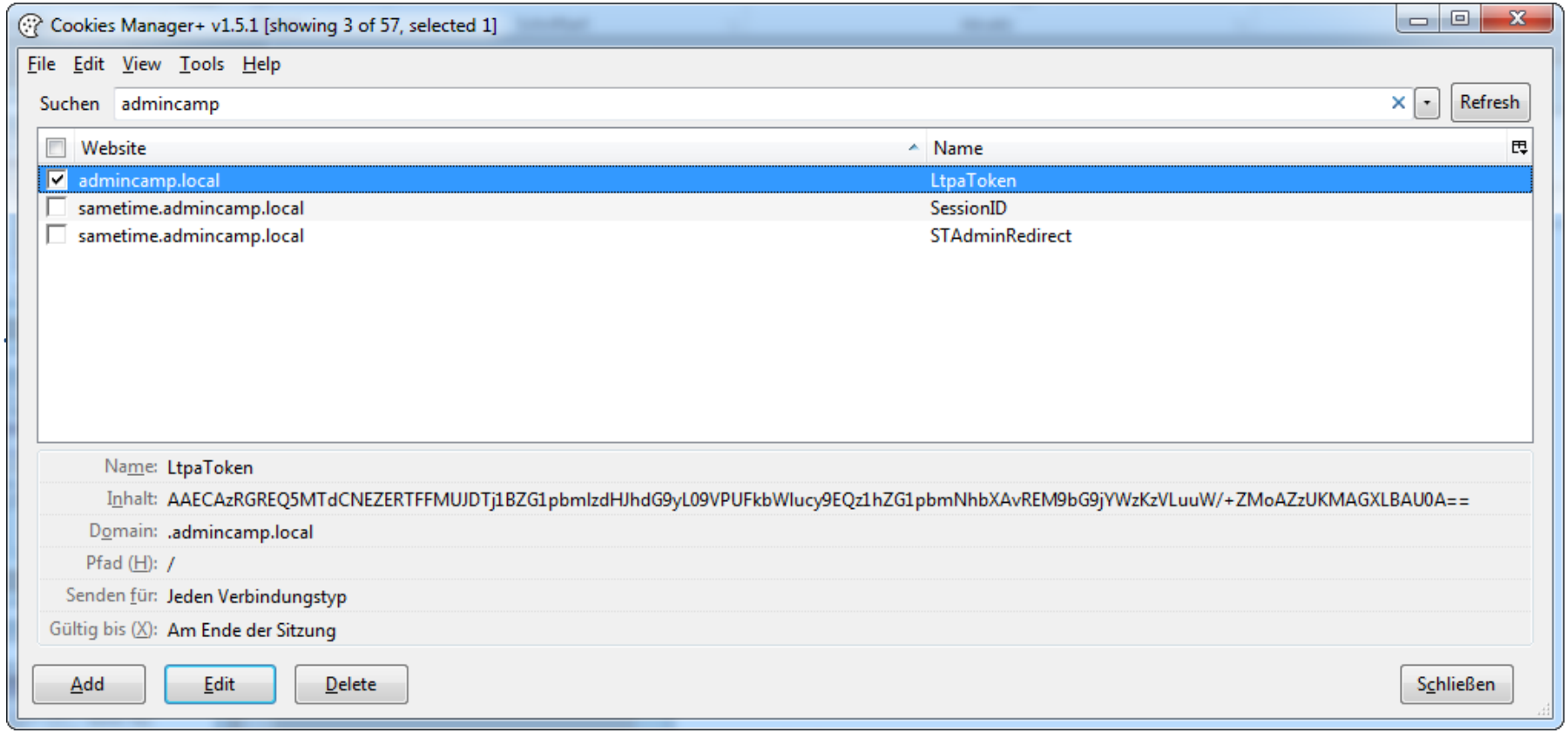


LTPA Token

- Das Token enthält:
  - Benutzernamen
  - Ablaufzeit
  - Gültigkeitsdomäne
- Tipps:
  - Uhrzeit der Server muss synchron sein
  - Bei mehreren WEB SSO Konfigurationen Ablaufzeit synchron halten
  - Debug über: DEBUG_SSO_TRACE_LEVEL=3

LTPA Token

LTPA Token im Browser:



Session based Authentication

Checkliste:

- Browser müssen Cookies zulassen
- Wird Name Mapping benötigt ?
  - Name Mapping konfigurieren
- Web SSO Konfiguration(en) erstellen
- Session based Authentication aktivieren

Agenda

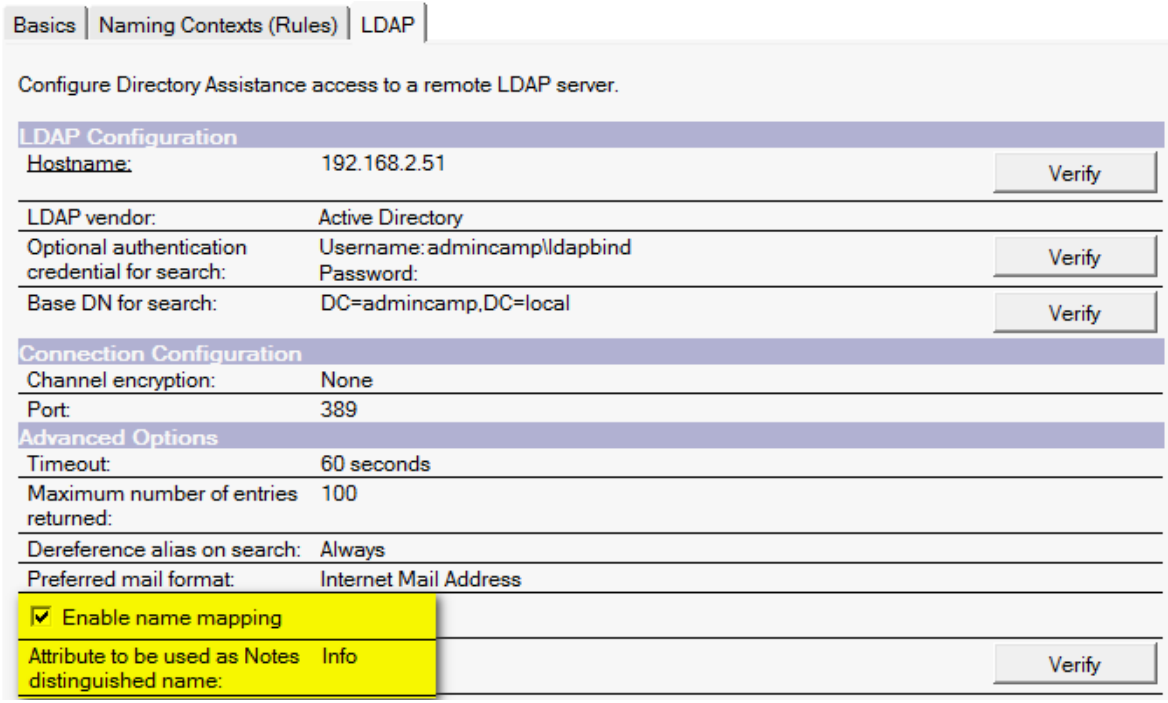
- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

Name Mapping

- Domino bietet durch seine „Name Mapping“ Möglichkeiten eine hohe Flexibilität
- Immer dann erforderlich wenn Systeme mit unterschiedliche Directories konfiguriert sind. Z.b.
  - Sametime -> Active Directory
  - iNotes -> Domino Directory

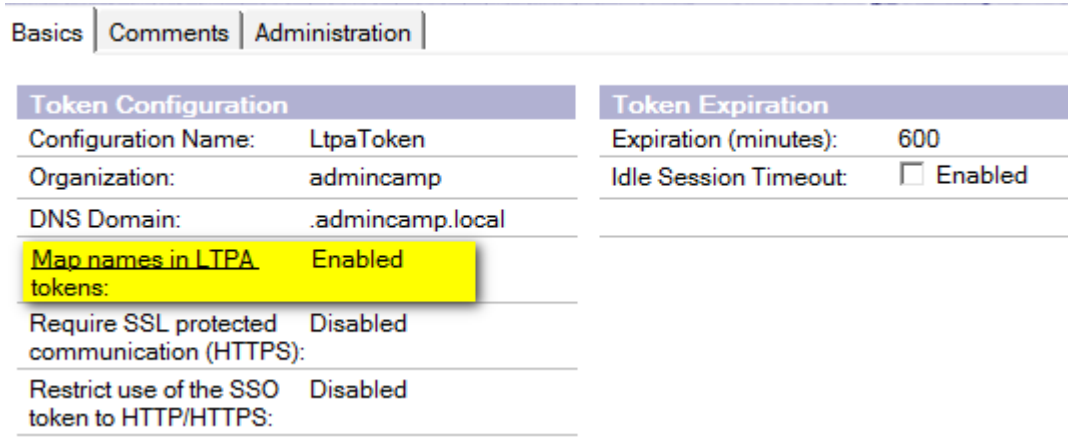
Name Mapping

- Name Mapping ist an den folgenden Stellen möglich:
  - Directory Assistance
    - Der im angegebenen Attribute gespeicherte Wert wird als Notes Distinguished Name verwendet.



Name Mapping

- LTPA Token
  - Der konfigurierte Username wird im LTPA-Token hinterlegt
  - Aktivieren der Funktion über die Web SSO Configuration



Name Mapping

- LTPA Username wird im Domino Directory hinterlegt.
  - Im Feld LTPA_UsrName

Client Information	
Name change request:	None
Network account name:	
LTPA user name:	CN=Johann Sametime/CN=Users/DC=admincamp/DC=local
DB2 account name:	
Active Directory (Kerberos) logon name:	Administrator@ADMINCAMP.LOCAL

  - Und als zusätzlicher Fullname

Basics | Work/Home | Other | Miscellaneous | Certificates | Roaming | Administration

Basics	
First name:	Admincamp
Middle name:	
Last name:	Administrator
User name:	Admincamp Administrator/Admincamp Admincamp Administrator CN=Johann Sametime/CN=Users/DC=admincamp/DC=local

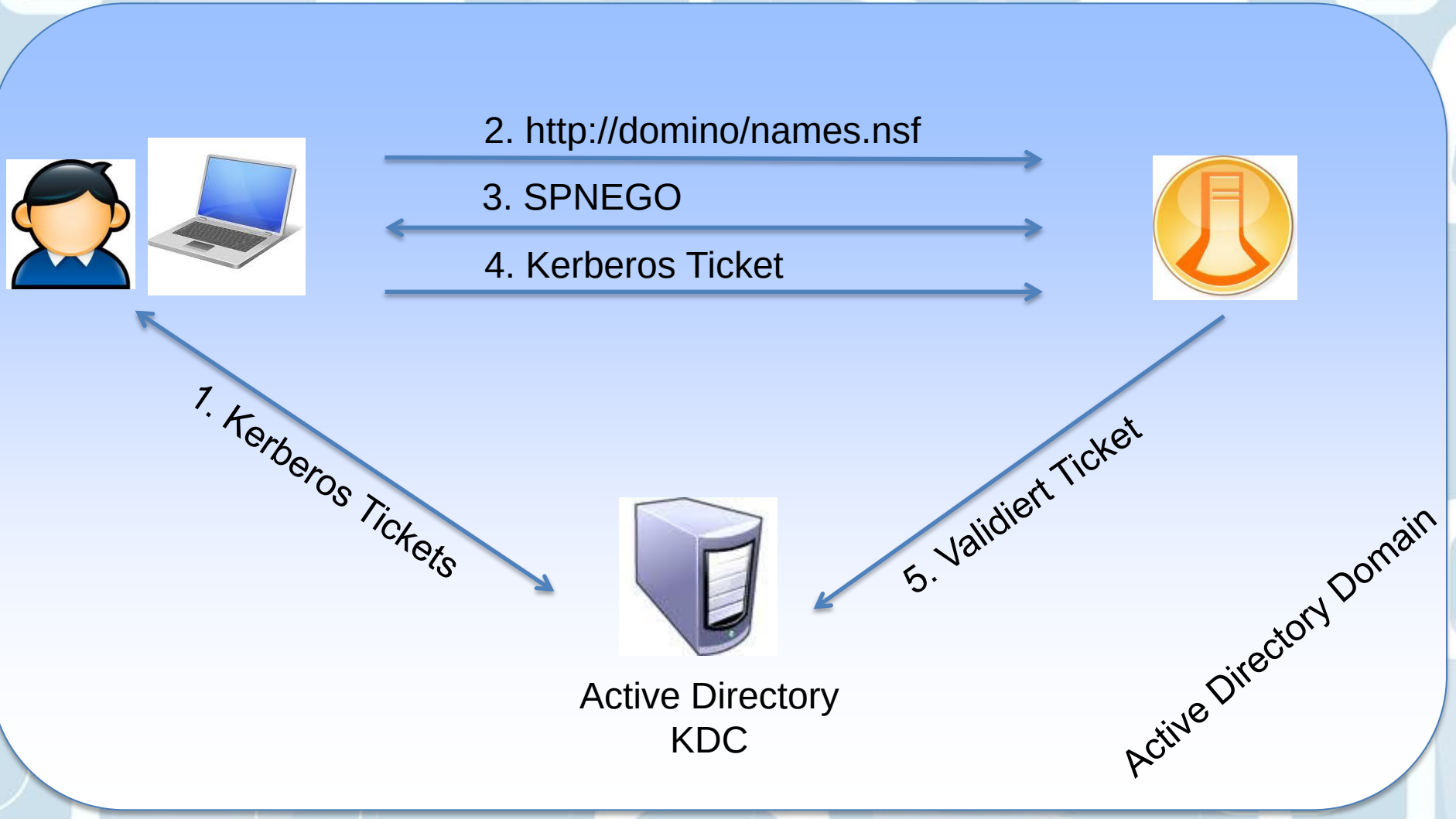
Agenda

- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

SPNEGO

- Echtes Single Sign On für Web User
- Windows Benutzer sind mit der Anmeldung am Betriebssystem bereits authentifiziert
- Über eine Kombination von SPNEGO und LTPA-Token könne auch Domino-Server per SSO erreichbar sein die nicht unter Windows laufen

SPNEGO – stark vereinfacht

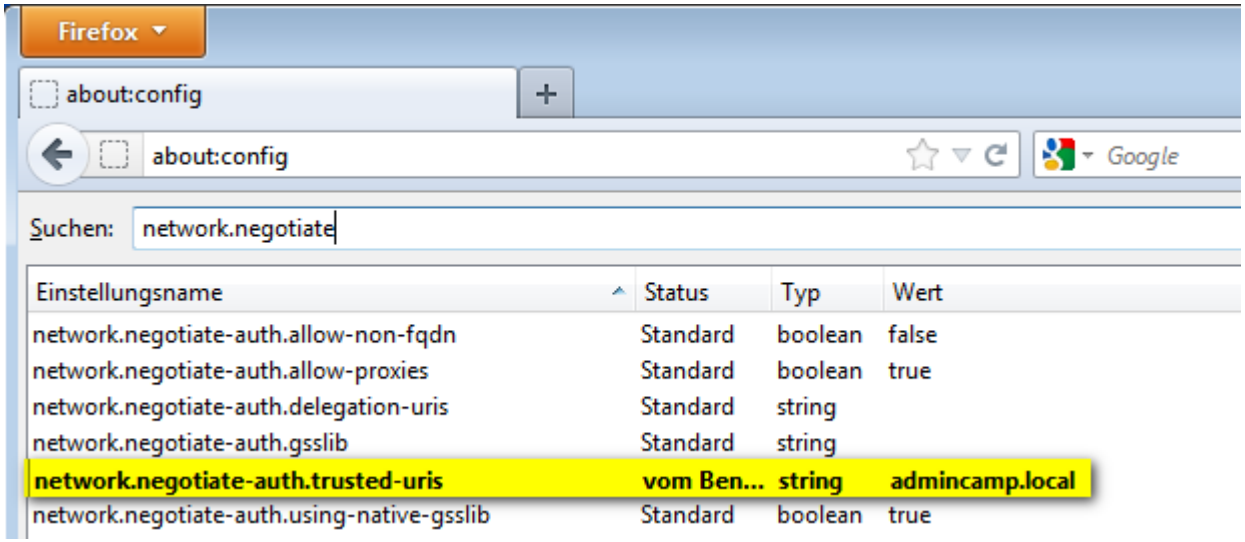


SPNEGO Voraussetzungen

- Kerberos Infrastruktur – Active Directory
- Active Directory Version > 2003
- Rechner der Benutzer und der Domino Server müssen Mitglied der Windows Domäne sein
- Domino Service muss mit einem Service Account laufen
- Browser müssen SPNEGO unterstützen und entsprechend konfiguriert sein

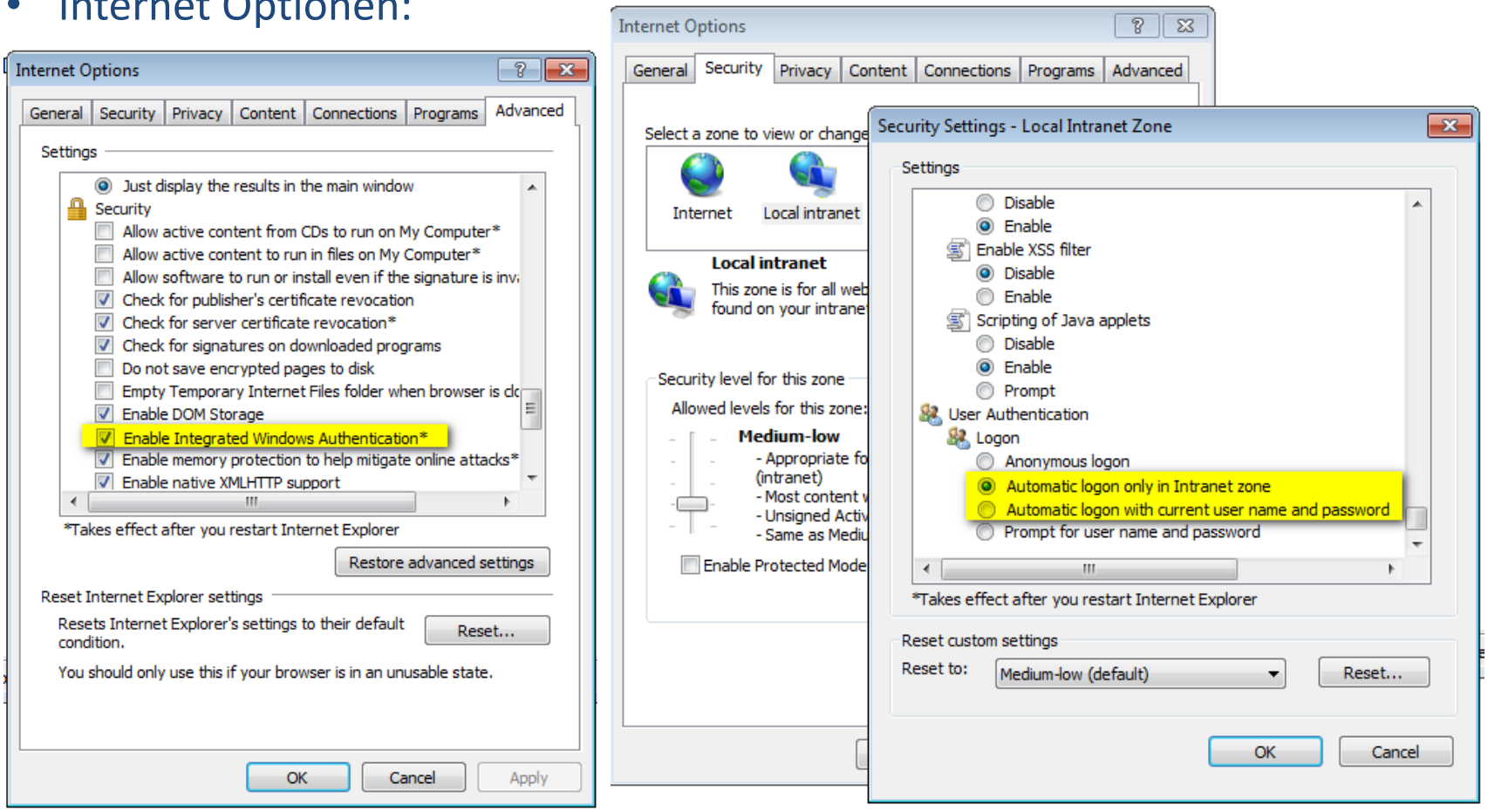
SPNEGO Browser Konfiguration

- Firefox
- about:config in die Adresszeile eingeben
  - network.negotiate-auth.trusted-uris konfigurieren



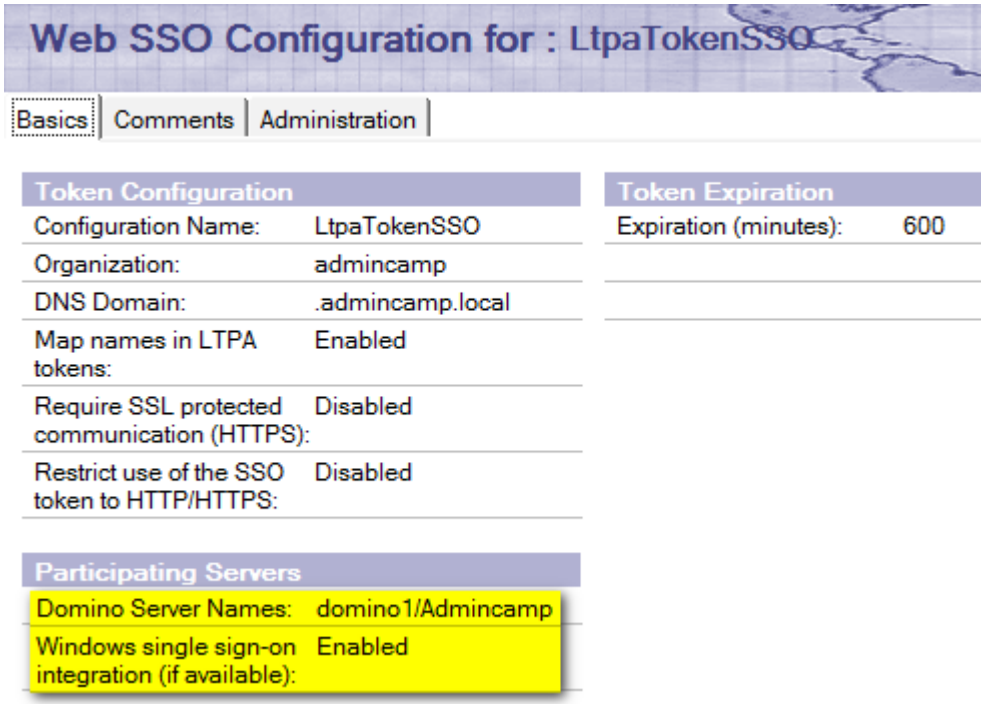
SPNEGO Browser Konfiguration

- Internet Explorer
  - Internet Optionen:



SPNEGO einrichten

- Web SSO Configuration erstellen und SPNEGO aktivieren

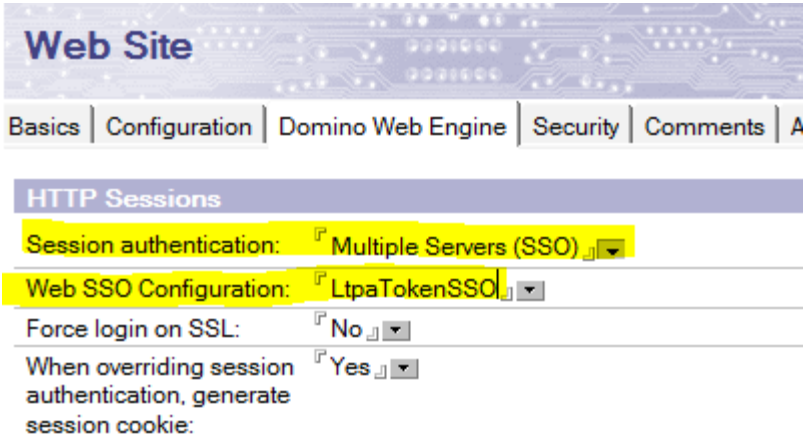


SPNEGO einrichten

- Internet Site für SSO einrichten

SPNEGO einrichten

- Session based Authentication aktivieren und die zuvor erstellte Web SSO Configuration zuweisen

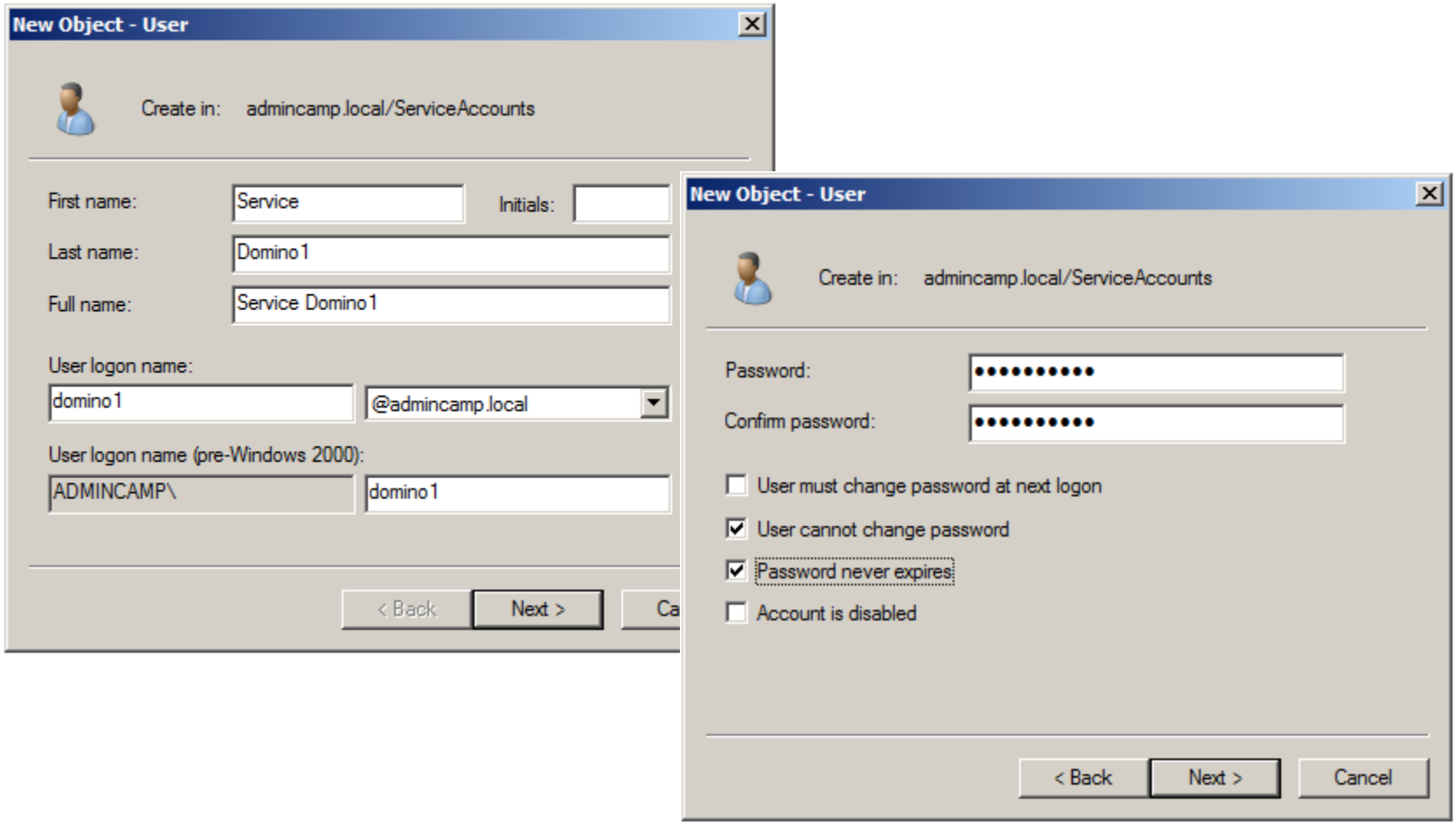


SPNEGO einrichten

- Weitere Web Sites entsprechend konfigurieren

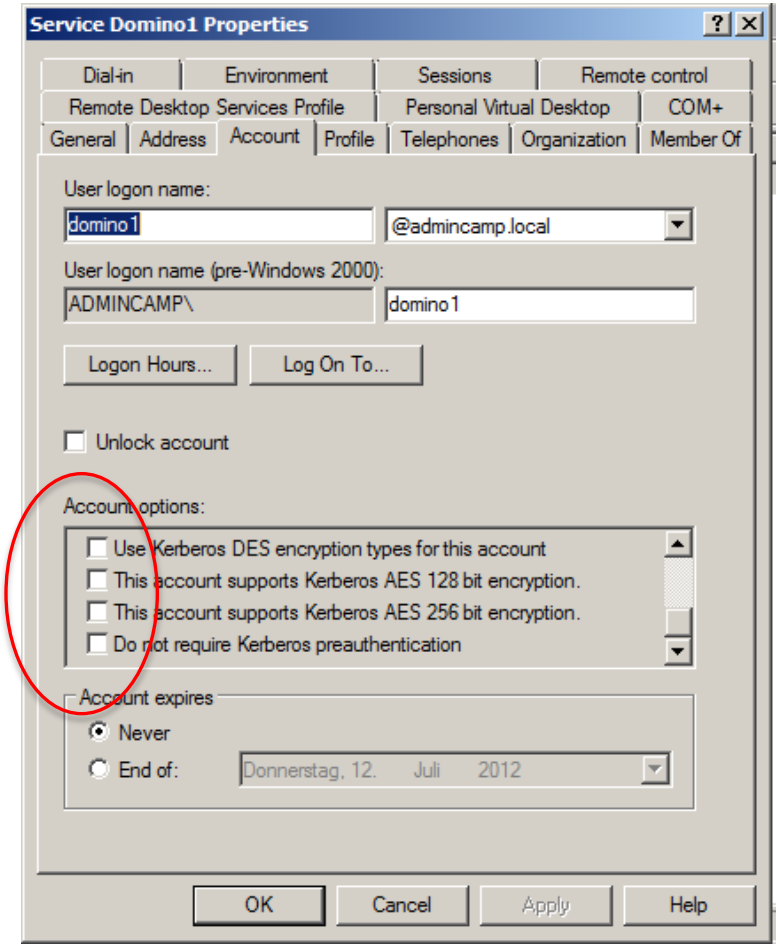
SPNEGO einrichten

- Service Account für Domino in Active Directory erstellen



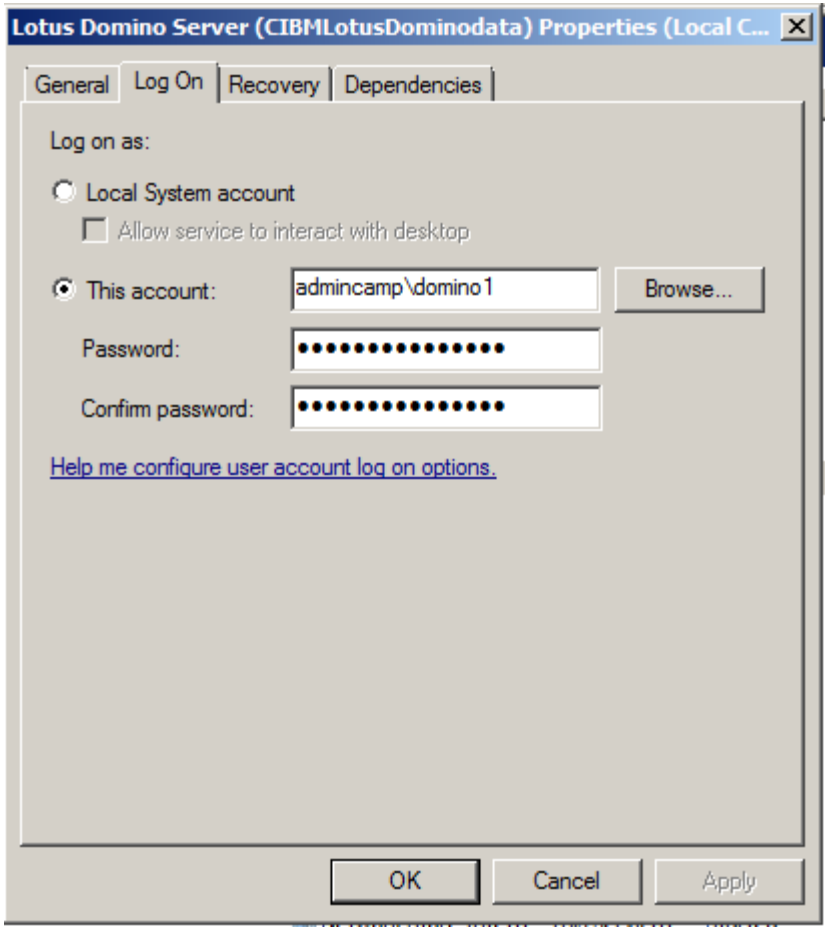
SPNEGO einrichten

- Service Account für Domino



SPNEGO einrichten

- Service Account beim Domino Service hinterlegen und Server neu starten



Service Principal Names

- Mindestens ein Service Principal Name (SPN) muss dem zuvor erstellen Domino Service Account zugewiesen werden
- SPN‘s entsprechen DNS-Namen in URL‘s mit denen Benutzer auf den Server zugreifen.
- Syntax der SPN‘s
  - HTTP/<DNS Name>@<Active Directery Kerberos Realm>
  - Z.b. HTTP/sso.admincamp.local@ADMINCAMP.LOCAL
- SPN‘s müssen eindeutig und dürfen nur einem Account zugeordnet sein
- SPN‘s müssen für alle DNS-Aliase definiert werden

Service Principal Names

- Die Zuweisung der SPN‘s erfolgt über das setspn Utility auf einem Domain Controller

```
Usage: setspn [modifiers switch] [accountname]
  Where "accountname" can be the name or domain\name
  of the target computer or user account

  Edit Mode Switches:
   -R = reset HOST ServicePrincipalName
    Usage:   setspn -R accountname
   -A = add arbitrary SPN
    Usage:   setspn -A SPN accountname
   -S = add arbitrary SPN after verifying no duplicates exist
    Usage:   setspn -S SPN accountname
   -D = delete arbitrary SPN
    Usage:   setspn -D SPN accountname
   -L = list SPNs registered to target account
    Usage:   setspn [-L] accountname
```

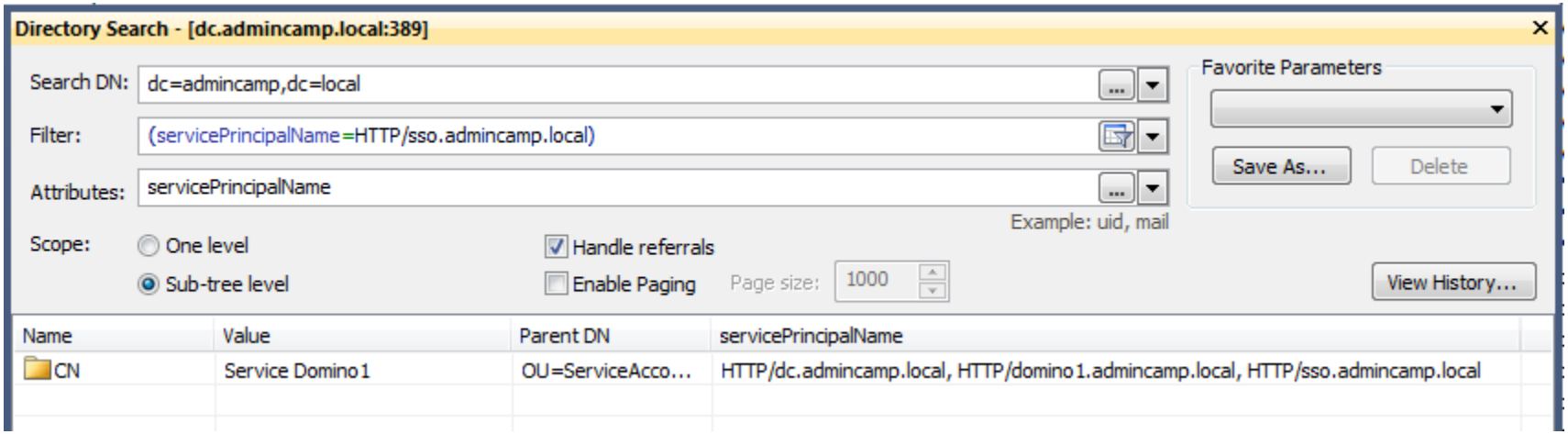
  - z.B.: setspn –A HTTP/sso.admincamp.local Domino1
  - Oder besser: setspn –F -S HTTP/sso.admincamp.local Domino1

```
C:\Windows\system32>setspn -F -S HTTP/domino85.admincamp.local domino1
Checking forest DC=admincamp,DC=local
Operation will be performed forestwide, it might take a while.

Registering ServicePrincipalNames for CN=Service Domino1,OU=ServiceAccounts,DC=admincamp,DC=local
        HTTP/domino85.admincamp.local
Updated object
```

Service Principal Names

- Die Eindeutigkeit der SPN‘s prüfen
  - Über das setspn Utility
  - Oder mit Hilfe eines LDAP Browsers



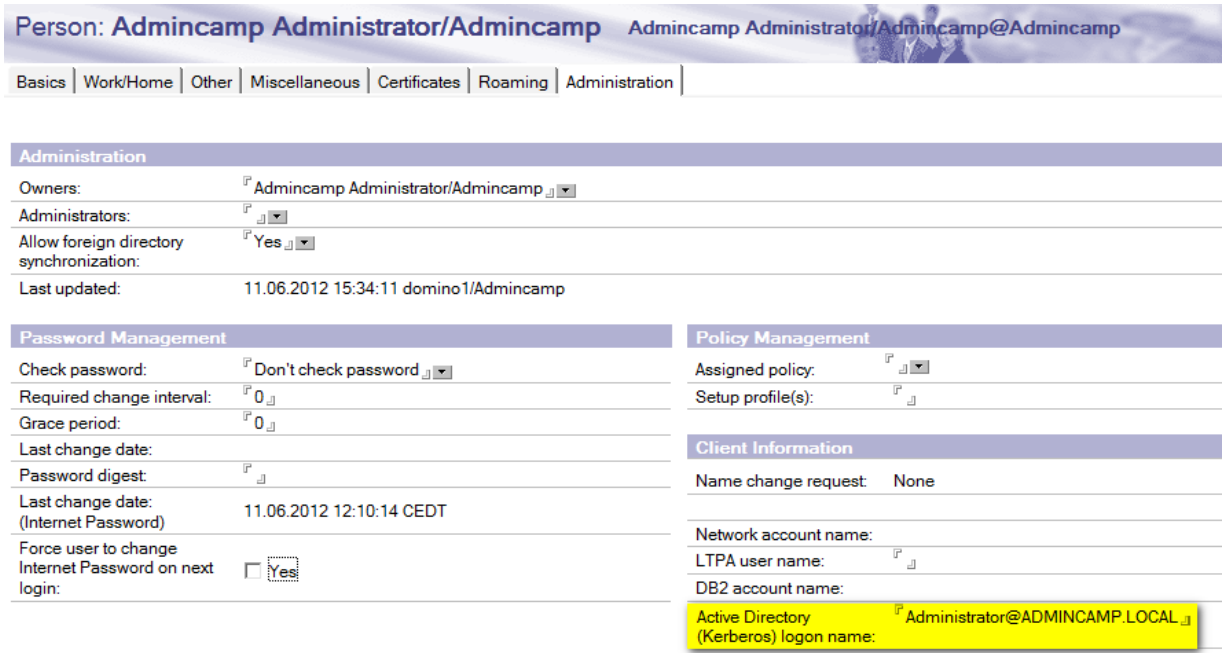
SPNEGO einrichten

- Test ob SPNEGO funktioniert:
  - DEBUG_HTTP_SERVER_SPNEGO=5 setzen
  - Zugriff auf eine Datenbank die eine Authentifizierung des Benutzers erfordert

```
Starting SPNEGO Negotiate - a properly configured HTTP client should send an Authorization: Negotiate header containing SPNEGO token when repeating the request /whoami.nsf
Success calling native routine AcquireCredentialsHandleW
Security token format received is SPNEGO NegTokenInit
Success calling native routine AcceptSecurityContext
SSPI security attributes received 0x20802, but requested 0x20014
Success calling native routine QueryContextAttributesW
Success calling native routine QueryContextAttributesW
Success calling native routine QueryContextAttributesW
User Administrator@ADMINCAMP.LOCAL authenticated by Kerberos service HTTP/dc.admincamp.local@ADMINCAMP.LOCAL
Success calling native routine QueryContextAttributesW
Authenticated user is Administrator@ADMINCAMP.LOCAL via Firefox/13.0
```

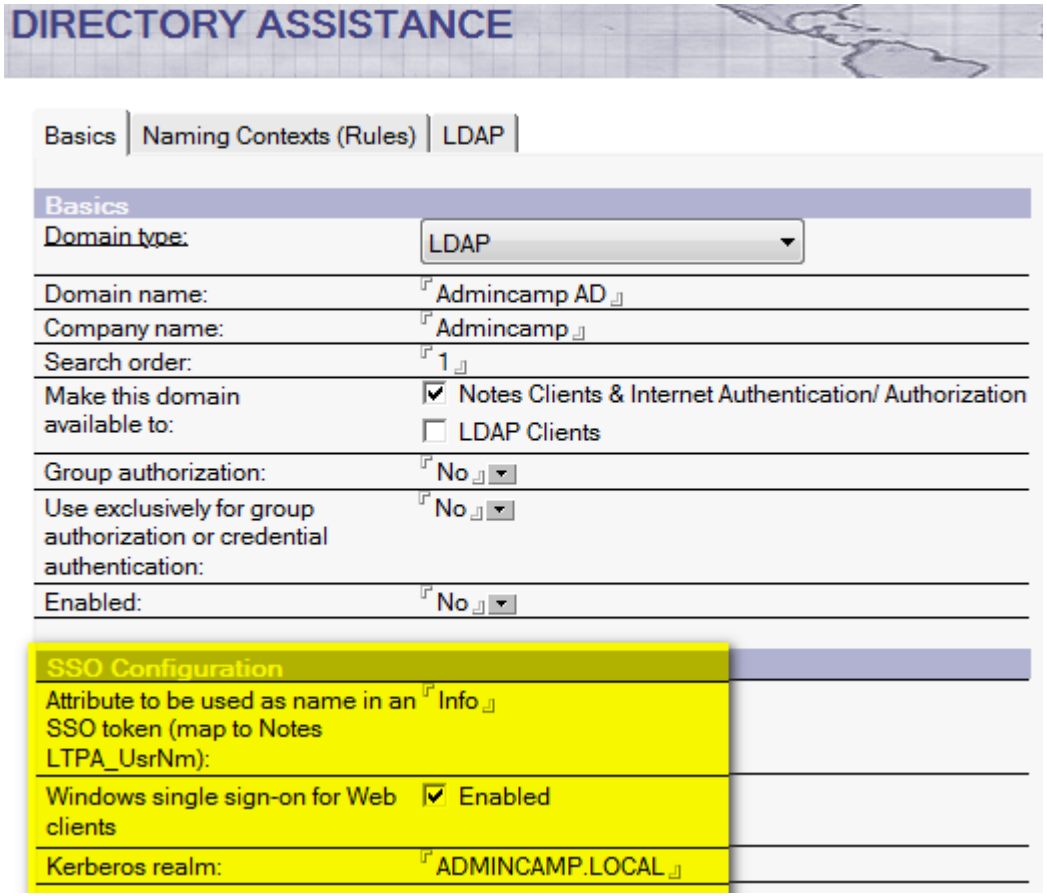
Name Mapping

- Auflösung des Kerberos UserPrincipalNames zu einem entsprechenden Domino Benutzer Namen
  - Zwei Optionen:
    1. Benutzer sind im Domino Directory
       - Notes.ini WIDE_SEARCH_FOR_KERBEROS_NAMES=1 aktivieren
       - UserPrincipalNames im Domino Personen Dokument hinterlegen (TDI)



Name Mapping

2. Benutzer befinden sich im Active Directory
   - Name Mapping über Direcotry Assistance konfigurieren:



SPNEGO Tips

- SPNEGO Debugging unter Domino
  - DEBUG_HTTP_SERVER_SPNEGO=5
- Troubleshooting SPNEGO
  - In 9 von 10 Fällen passt der SPN nicht
  - http://www-304.ibm.com/support/docview.wss?uid=swg21394592
- Windows Server 2003 benutzt UDP für Kerberos
  - http://support.microsoft.com/kb/244474
- Kerberos Infos, Debugging, Troubleshooting
  - http://technet.microsoft.com/en-us/library/cc753173(v=ws.10).aspx
- Kerberos verwendet Port 88 (TCP, UDP)

SPNEGO Checkliste

- Active Directory Version > 2003
- Domino SPNEGO Server definieren
- Clients und SPNEGO Server sind Mitglied der Domäne
- Browser unterstützen SPNEGO
- Browser Konfiguration angepasst
- Service Account in Active Directory erstellt
- Service Principal Name(s) zugewiesen
- Domino Service mit dem Service Account starten
- Name Mapping definieren
  - Über Directory Assistance
  - Über Domino Directory

Agenda

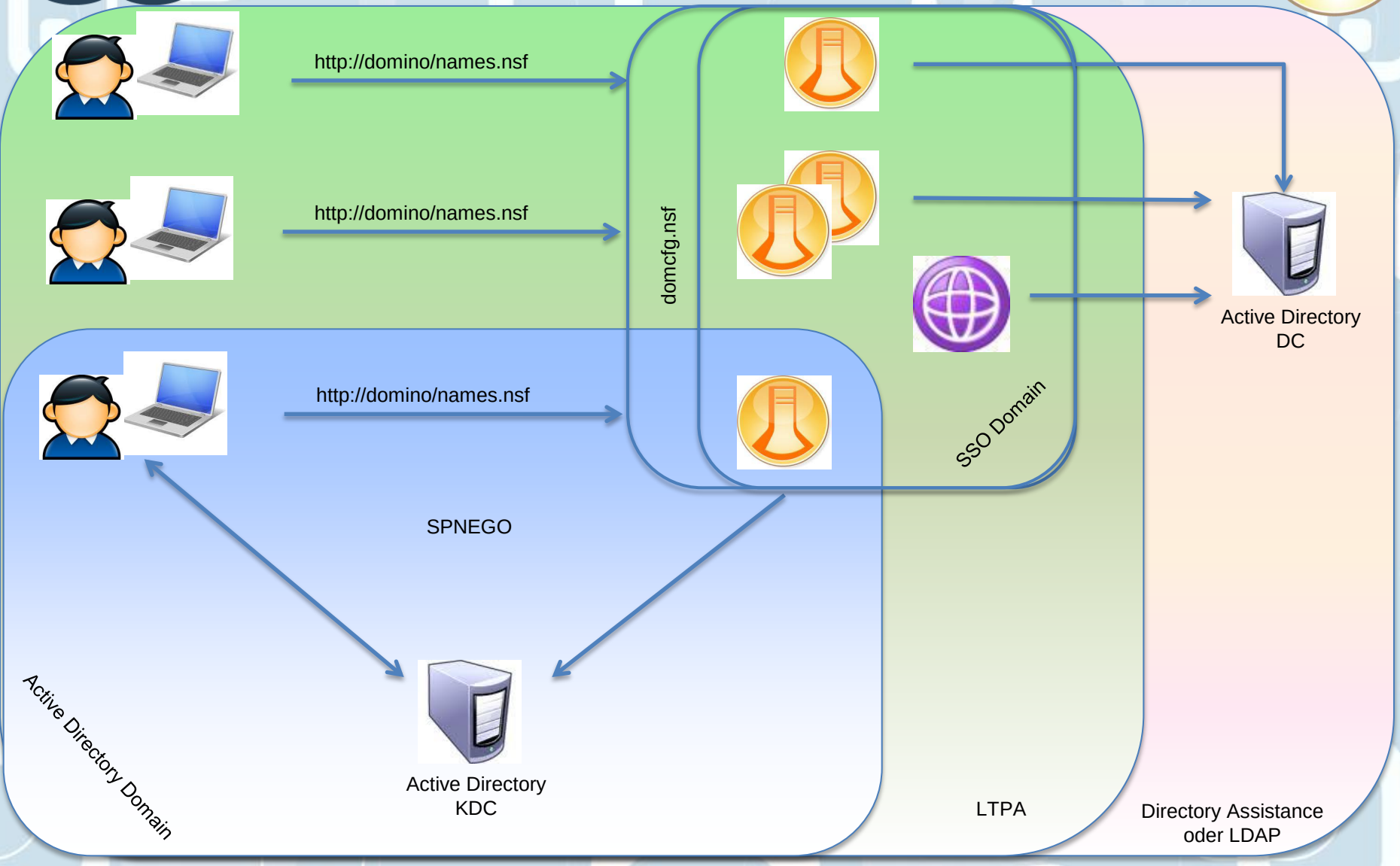
- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

Alles zusammen….

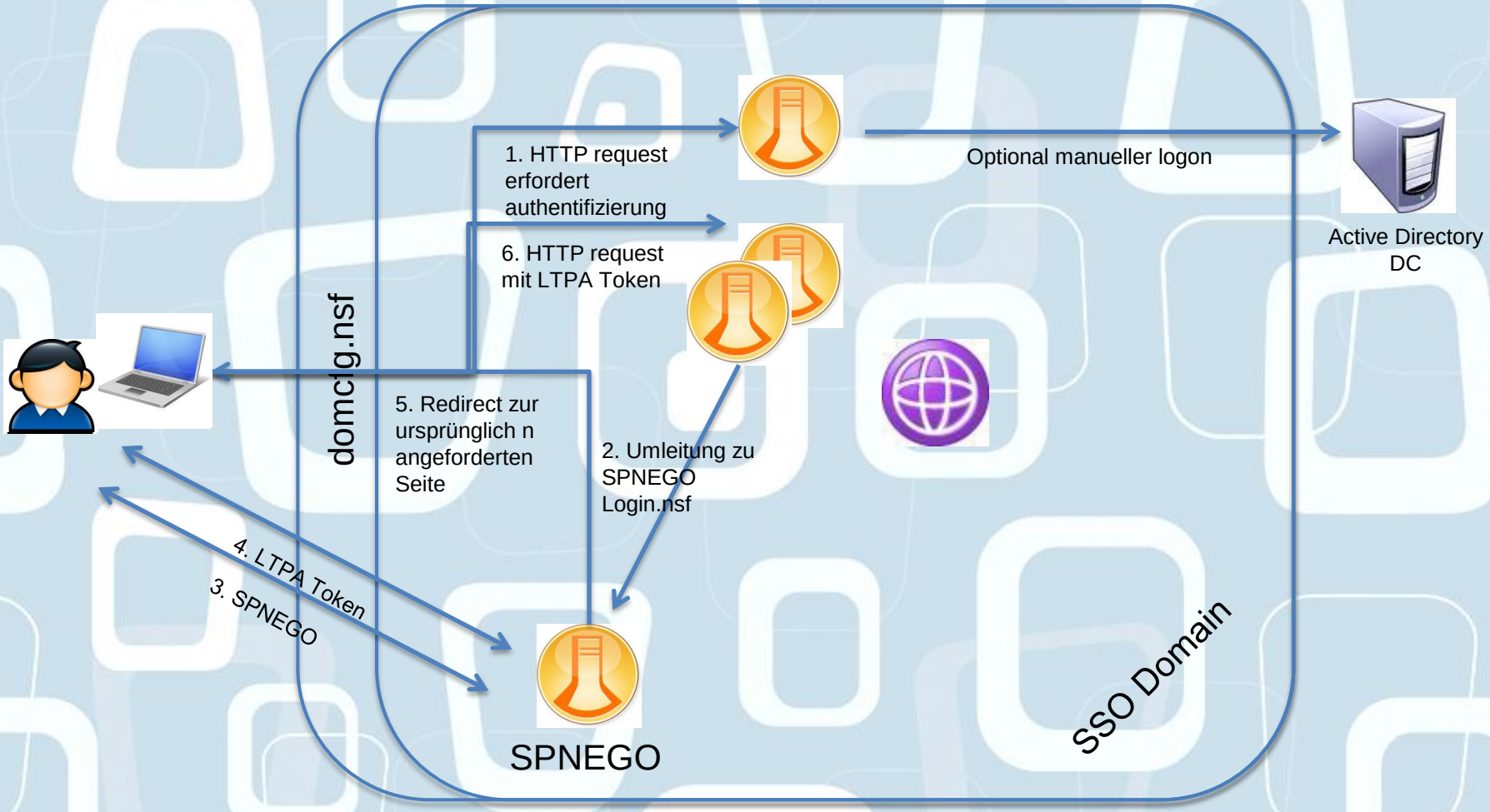
Die Idee:

- Ein zentraler SPNEGO-Server
- Verwenden des LTPA-Token um z.b Linux oder WebSphere basierte System mit abzudecken
- Manueller Login möglich:
  - wenn Voraussetzungen für SPNEGO nicht erfüllt sind
  - Oder z.b für Tests
  - Directory Assistance um Passwörter gegen Active Directory zu validieren
- Support für embedded Clients
- Benutzerfreundliches Error Handling
- Alles frei konfigurierbar

Alles zusammen….

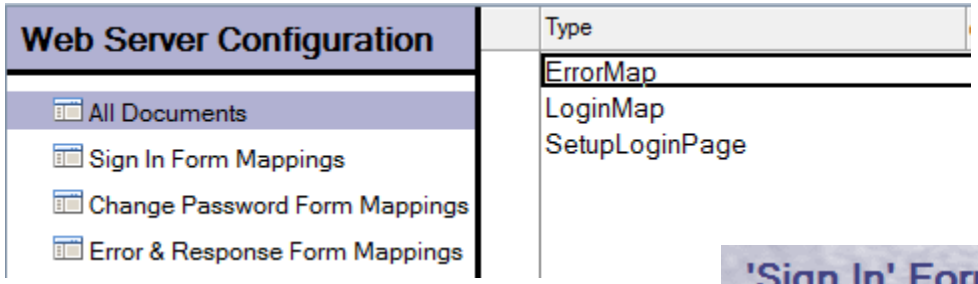


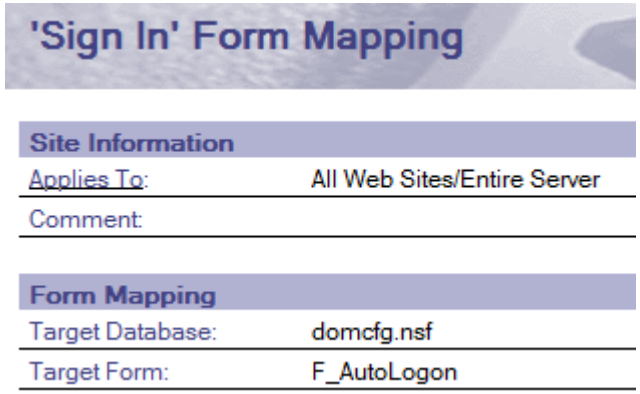
Alles zusammen.....



Domino Web Server Configuration

- domcfg.nsf
- Erlaubt die Gestaltung einer angepassten Login Seite
- Definition von Error und Login Seiten Mappings
  - Per Internet Site oder global





Setup Login Page

General Setup | Text, Help and Images

SSO Setup

Enable Single Sign On	(•) True ( ) False
for	( ) All ( ) IP Range(s) (•) Exclude IP Range(s)
IP Range(s)	Start: 192.168.2.139 <-> End: 192.168.2.140
HostName Authetication Server	sso.admincamp.local
Authentication Server Port	80 ( ) https:// (•) http://
SSO Login Page	sso/login.nsf/ag_loginhandler?openAgent
SSO Domain (DNS-Domain in LTPA Token)	admincamp.local
Delay for Redirect in sec.	3
List of AD Domains participating in SSO (";" seperated)	ADMINCAMP
List of AD Domains for manual Logon (";" seperated)	<none>; ADMINCAMP
DefaultDomain for manual Logon (if set SF_ManualLogonAD will be used)	
Supported Browser (";" seperated)	Firefox; Shiretoko; MSIE

ErrorHandler Setup

URL ErrorHandler Page	/domcfg.nsf/F_CustomErrorHandler?OpenForm
Delay for Redirect in sec.	0

Debug Browser Frontend

Enable Debug	( ) True (•) False

General Setup | Text, Help and Images

LogonPage and ErrorHandler

LogoTop Resource must be available	ac.gif	
Defined Variables	Variable Names	To be replaced with this fields
	<SPNEGOUsr>	SPNEGOUsr
	<SessionUser>	SessionUserNameAbbr
	<ErrorMsg>	errormsg
	<scheme>	scheme
	<FullPath>	Fullpath
	- both fields must contain the same number of entries - Varaible Names are case sensitive	

Language I

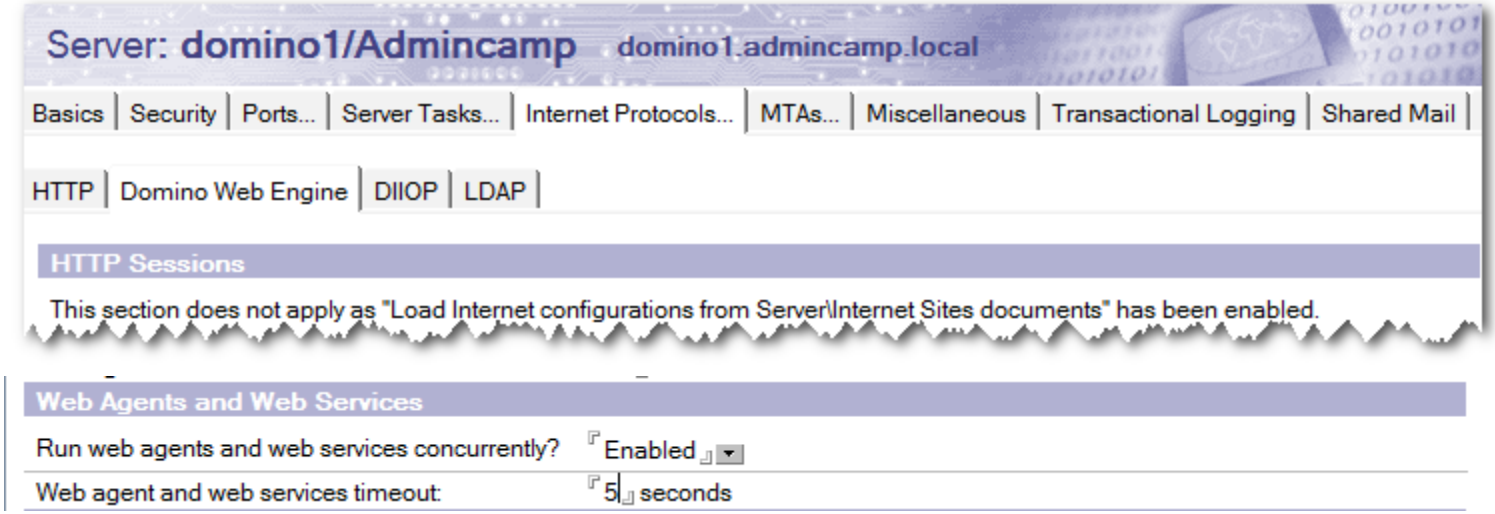
enable additional language support	( ) True (•) False
Language:	German
	LogonPage
Logon Page Title: (manual logon)	Manuelle Anmeldung
Information text: (manual logon)	Zur Anmeldung verwenden Sie bitte Ihre: eMail Adresse und Ihr Lotus Notes Passwort Sollte eine Anmeldung nicht möglich sein, setzen Sie sich bitte mit dem Helpdesk unter der Telefonnummer +49 190 / 999 99 in Verbindung
Logon Page Title: (SSO)	Automatische Anmeldung
Information text: (SSO)	<input type="button" class="loginButton" value="Manuelle Anmeldung" onclick="javascript:manuallogon();">
Label Login Domain:	AD Domäne
Label Login User:	Benutzername
Label Login Password:	Passwort
Label Login Button:	Anmelden

Login.nsf

- Datenbank enthält nur einen einfachen Agenten
  - ag_loginhandler
- Wird automatisch über die domcfg.nsf aufgerufen
- Parameter wie „&redirectto“ in einer Domino URL werden berücksichtigt
  - http://domino1.admincamp.local/names.nsf?login&redirectto=http://domino1.admincamp.local/whoami.nsf
- Der Agent erwartet einen Parameter „&sso_back_to“ der die ursprünglich aufgerufene URL enthält
  - http://sso.admincamp.local/sso/login.nsf/ag_loginhandler?openAgent&sso_back_to=http%3A%2F%2Fdomino1.admincamp.local%3A80%2Fwhoami.nsf

Login.nsf

- Am zentralen SPNEGO Server „Concurrent Web Agents“ aktivieren und eine vernünftige timeout definieren



Single Sign On

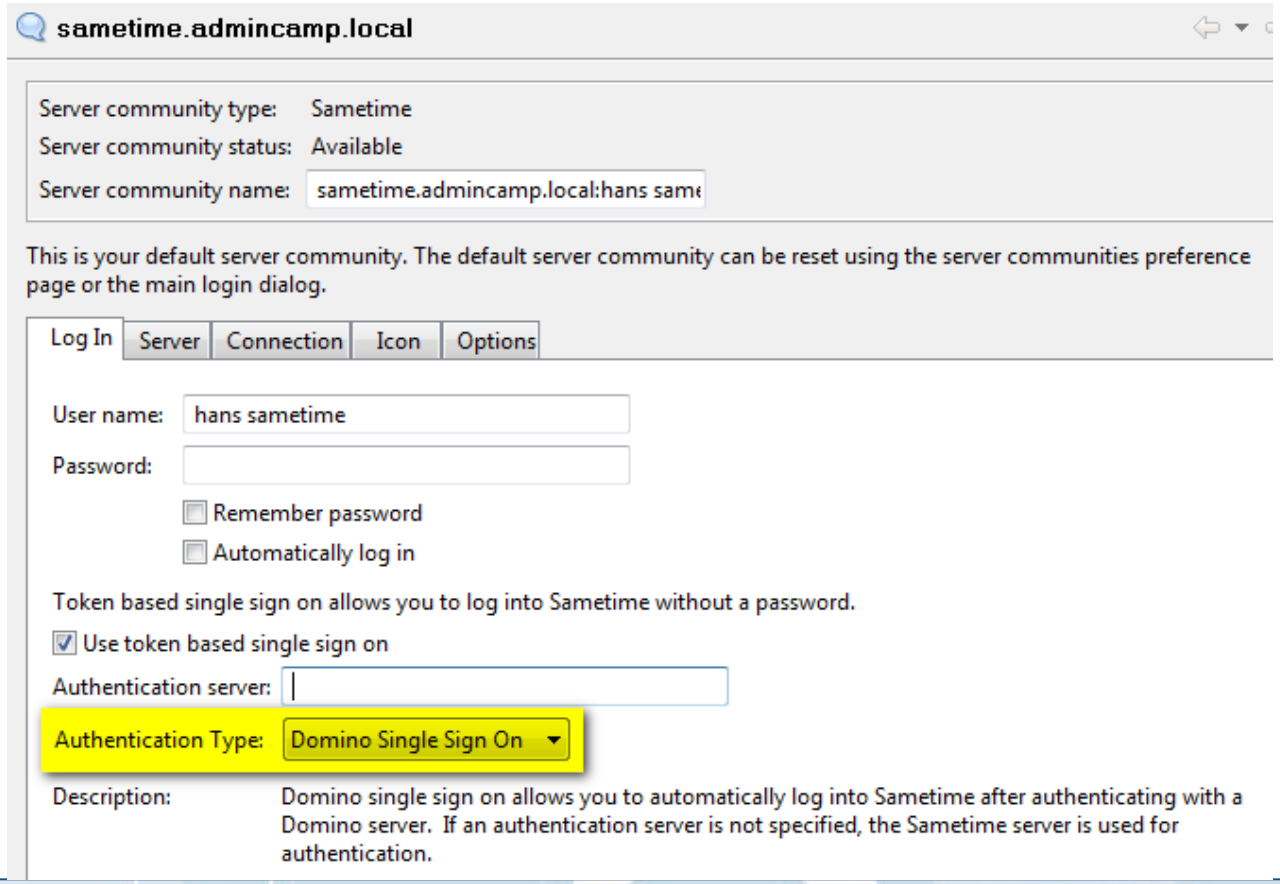
DEMO

Agenda

- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

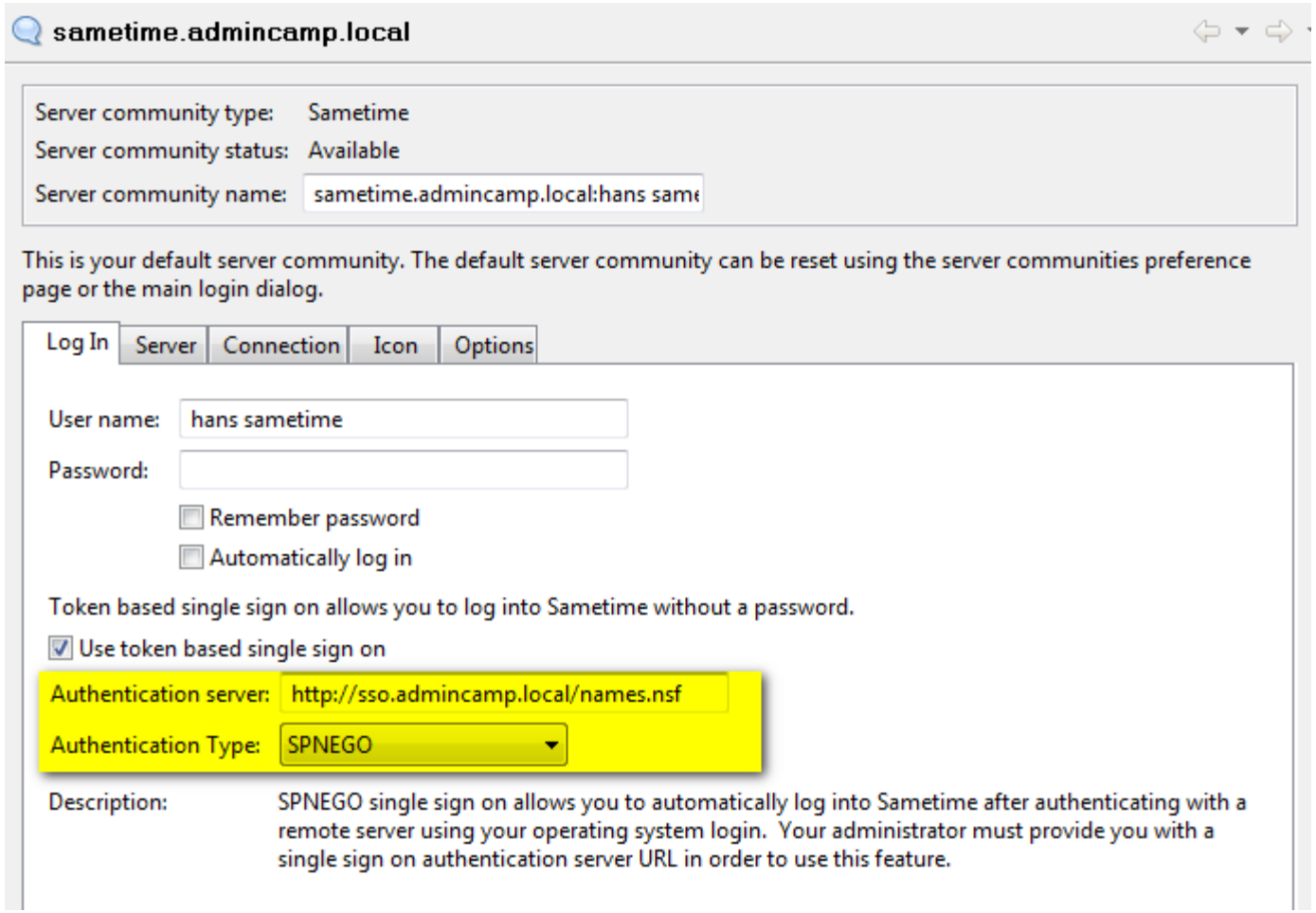
Embedded Clients

- Sametime - stellt zwei SSO Optionen zur Verfügung:
  - Domino Single Sign On (LTPA Token basierend auf der Notes-ID)



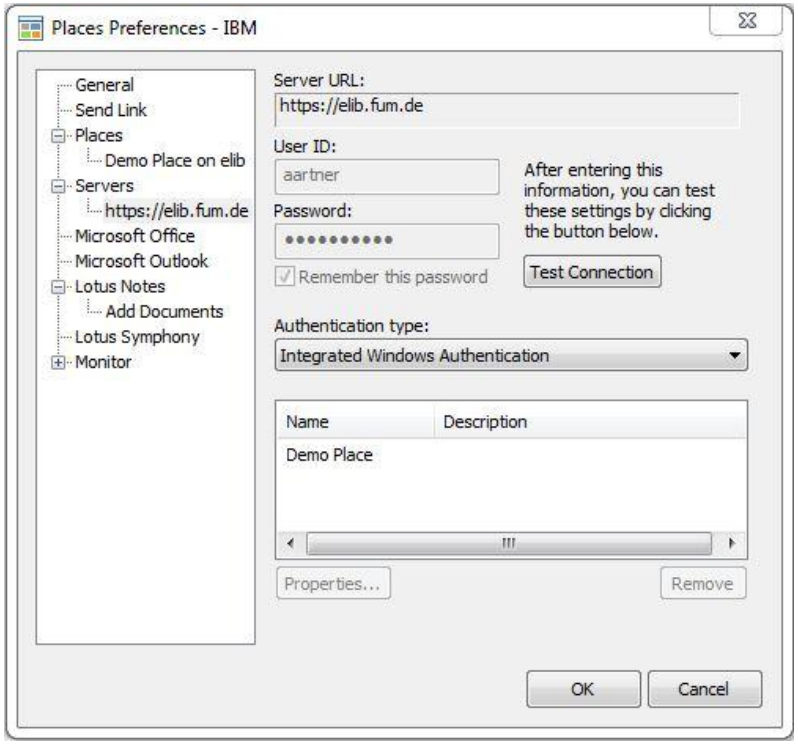
Embedded Clients

- SPNEGO (auch mit dem Domino SPNEGO Server)



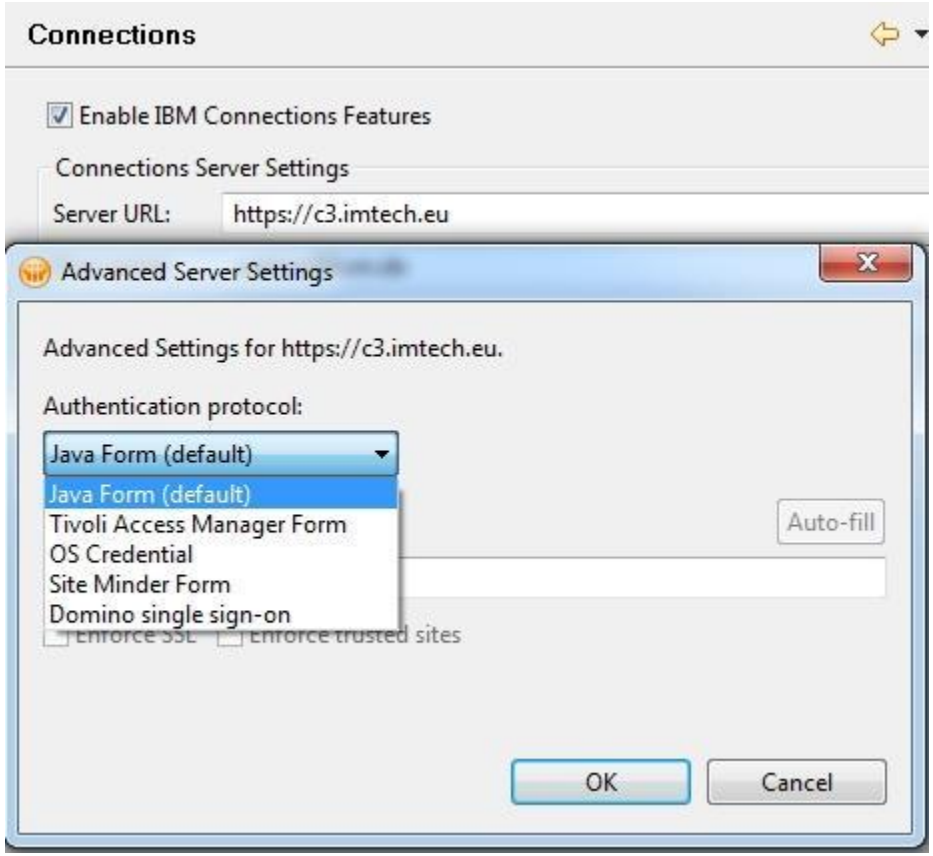
Embedded Clients

- Quickr
  - Quickr Connector unterstützt SPNEGO
    - http://www-10.lotus.com/ldd/lqwiki.nsf/dx/SPNEGO_SSO_Deployment_in_Lotus_Quickr_8.5_Services_for_Lotus_Domino



Embedded Clients

- IBM Connections
  - Unterstützt SPNEGO und Domino Single Sign On



Was geht ?

Produkt	Directory Assistance	LTPA	SPNEGO	Besonderheit
iNotes	✓	✓	✓ Nur Windows	
Domino Web	✓	✓	✓ Nur Windows	
Quickr J2EE	LDAP	✓	✓	
Quickr Domino	LDAP	✓	✓ Nur Windows	
Sametime	LDAP	✓	✓	Domino Single Sign On
Connections	LDAP	✓	✓	
Traveler	✓			
Lotus Notes				Notes Shared Login
Embedded Sametime		✓	✓	Domino Single Sign On
Embedded Quickr			✓	

Agenda

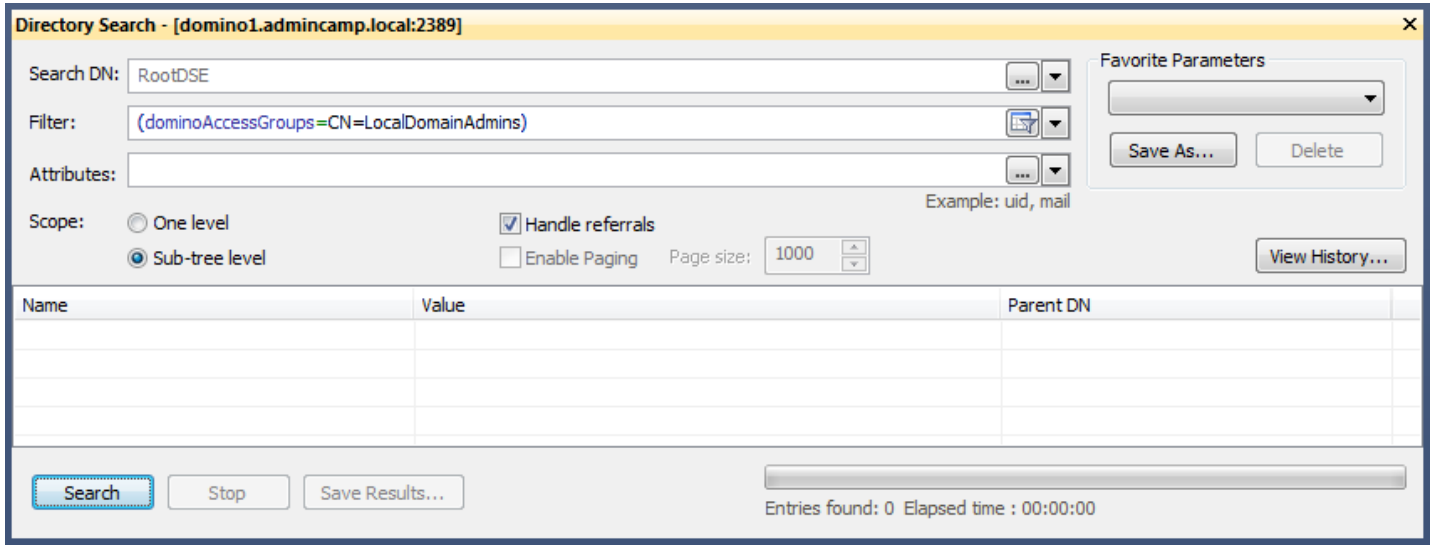
- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

Domino oder Active Directory

- Viele IBM Lösungen wie Quickr, Sametime oder Connections erfordern die Anbindung an einen LDAP-Server
- Welcher LDAP-Server ist der richtige ?
  - Letztlich Abhängig von Ihrer Umgebung
  - Einige Punkte die Sie berücksichtigen sollten:
    - Welches Directory enthält alle relevanten Benutzer
    - In welchen Directory werden die Passwörter geändert
    - Performance

Domino oder Active Directory…

- Domino verlangt als einziger LDAP Server keine Base-DN
  - sehr verbreitet - speziell bei Gruppen
  - WebSphere fix führt dann zu folgenden Namen in LTPA-Token
    - CN=Admincamp Administrator/O=Admincamp/O=Admincamp !
- LDAP-Filter die die Mitgliedschaft in einer Gruppe abfragen funktionieren nicht in Domino ☹
  - AD: (memberof=CN=Domain Admins,CN=Users,DC=admincamp,DC=local) – ok
  - Domino: (dominoAccessGroups=CN=LocalDomainAdmins) – nicht ok !



Agenda

- Single Sign On Definition
- Directory Assistance
- Session based Authentication
- Name Mapping
- SPNEGO
- Alles zusammen…
- Embedded Clients
- Domino oder Active Directory als LDAP-Server
- Die Zukunft - SAML

Die Zukunft - SAML

- SAML - **S**ecurity **A**ssertion **M**arkup **L**anguage
  - Standard für Internet SSO
  - IBM arbeitet an der Implementierung von SAML für Lotus Notes und Domino
  - SAML basiert auf einer PKI Infrastruktur und einer Vertrauensstellung der teilnehmenden Systeme

SAML

- Basierend auf PKI
- Identität des Benutzers in einer signierten XML
- Standard Internet Zertifikate und Schlüssel

SAML identity assertion

SAML IdP

SAML Identity Provider
- Kennt den Benutzer, Passwörter
- Unterstützt evtl. SPNEGO/Kerberos
- Authentifiziert Benutzer x zum Zeitpunkt y
- Generiert die SAML assertion
- Gängige IdPs
  - MS ADFS 2.0
  - TFIM

User

SAML SP

SAML Service Provider
- Trust zum IdP
- Erhält die Authentifizierungs Entscheidung vom IdP
- Authentifiziert den Benutzer indem die SAML assertion verifziert wird

SAML

- Herausforderungen die mit der Technologie gelöst werden sollen:
  - Authentifizierung von Benutzern aus anderen Organisationen
  - SSO für Lotus Notes unter Citrix
  - iNotes – Zugriff auf die ID-Datei für verschlüsselte emails
  - SSO für Notes Plug-Ins zum Zugriff auf Sametime, Feeds …..
  - …..

Single Sign On

- Vielen Dank für die Aufmerksamkeit !

- Fragen ?
  - jederzeit gerne
  - auch per email

Andreas Artner
aartner@fum.de