



# 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
  - Simple and Protected GSSAPI **N**egotiation Mechanism
  - SPNEGO wird 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

New Application

Specify New Application Name and Location

Server: domino1/Admincamp

Title: Directory Assistance

File name: da.nsf

Create full text index for searching

Specify Template for New Application

Server: domino1/Admincamp

Template:

- Directory Assistance (8.5.2)
- Directory Catalog (8.5)
- Discussion - Notes & Web (8.5.3)
- Doc Library - Notes & Web (8.5)
- DOLS Administration Template
- DOLS Resource Template

File name: da.nsf

Show advanced templates

Inherit future design changes

Server: domino1/Admincamp domino1

Basics | Security | Ports... | Server Tasks... | Internet Protocols...

Basics

Server name:	domino1/Admincamp
Server title:	Admincamp Server Windows
Domain name:	Admincamp
Fully qualified Internet host name:	domino1.admincamp.local
Cluster name:	
Load Internet configurations from Server/Internet Sites documents:	Disabled
Maximum formula execution time:	120 seconds

Directory Information

Directory assistance database name:	da.nsf
-------------------------------------	--------



# Directory Assistance



## 2. Directory Assistance konfigurieren

**DIRECTORY ASSISTANCE**

Basics | Naming Contexts (Rules) | LDAP

**Basics**

Domain type: LDAP

Domain name: Admincamp AD

Company name: Admincamp

Search order: 1

Make this domain available to:  
 Notes Clients & Internet Authentication/ Authorization  
 LDAP Clients

Group authorization: No

Use exclusively for group authorization or credential authentication: Yes

Enabled: Yes

**SSO Configuration**

Attribute to be used as name in an SSO token (map to Notes LTPA\_UsrNm):

Windows single sign-on for Web clients  Enabled

Comments:

▶ Administration

**DIRECTORY ASSISTANCE**

Basics | Naming Contexts (Rules) | LDAP

- Use the first rule to configure the Base for this LDAP server

	OrgUnit4	OrgUnit3	OrgUnit2	OrgUnit1	Organization	Country	Enabled	Trusted for Credentials
N.C. 1:	*	*	*	*	*	*	Yes	Yes
N.C. 2:							No	No
N.C. 3:							No	No
N.C. 4:							No	No
N.C. 5:							No	No

Comments:

▶ Administration



# Directory Assistance



## 2. Directory Aissance konfigurieren .....

**DIRECTORY ASSISTANCE**

Basics | Naming Contexts (Rules) | LDAP

Configure Directory Assistance access to a remote LDAP server.

**LDAP Configuration**

Hostname:

LDAP vendor:

Optional authentication credential for search: Username:  Password:

Base DN for search:

**Connection Configuration**

Channel encryption:

Port:

**Advanced Options**

Timeout:  seconds

Maximum number of entries returned:

Dereference alias on search:

Preferred mail format:

Enable name mapping

Attribute to be used as Notes distinguished name:

Attribute is to be used for all lookups:

Type of search filter to use:

Comments:

Administration

```
show xdir
DomainName      DirectoryType  ClientProtocol Replica/LDAP Server
-----
1 ADMINCAMP     Primary-Notes Notes & LDAP  names.nsf
2 ADMINCAMP AD  Secondary-LDAP Notes        DC.ADMINCAMPLOCAL: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

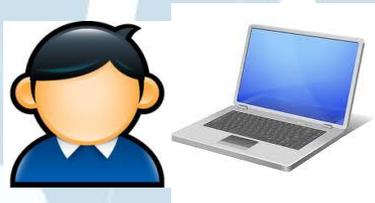


# Session based Authentication

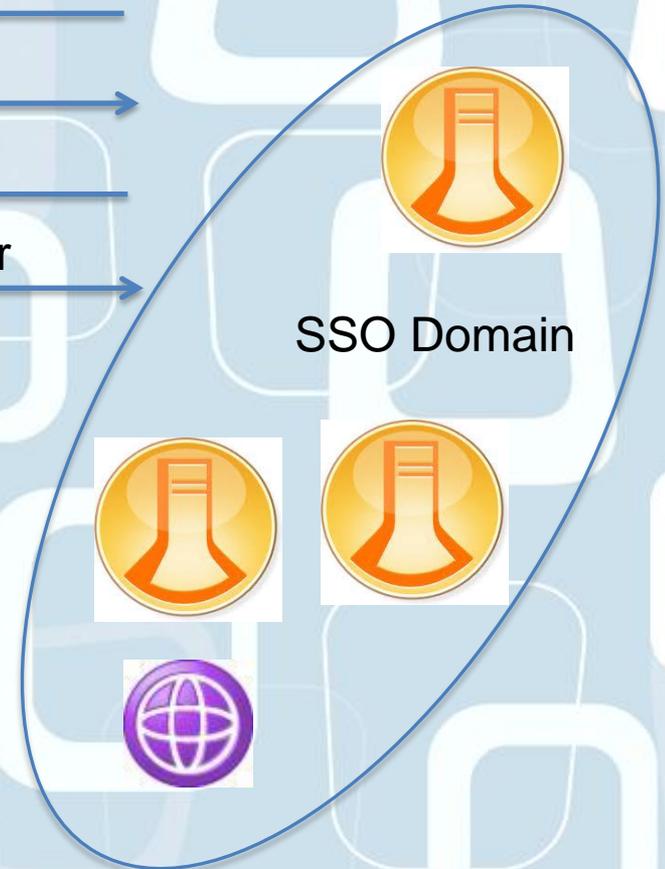
- Einmalige Anmeldung in einer Web-Sitzung
- Browser muss Cookies zulassen (LTPA-Token)
- Zwischen mehreren Domino Servern
- Zwischen Domino und Websphere
- Vorteile:
  - Abmeldung möglich ohne den Browser zu schliessen über „?logout“
  - Anzeige der aktiven Sessions über „tell http show users“
  - Anmeldeseite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

Domino Directory

Add Internet Site... Create Global We

Site name

- admindcamp
  - Web SSO Configuration: LtpaToken
  - Web SSO Configuration: LtpaToken

Domino Directory

Edit Document View Servers

Type

- \* - Web SSO Configurations -
  - Web SSO Configuration for LtpaToken
  - Web SSO Configuration for LtpaToken
    - domino1/Admincamp
    - domino2/Admincamp



# LTPA einrichten

- Neue Domino Keys generieren oder vorhandene WebSphere Keys importieren

**Web SSO Configuration for : LtpaToken**

Basics | Comments | Administration

Token Configuration	
Configuration Name:	LtpaToken
Organization:	admincamp
DNS Domain:	.admincamp.local
Map names in LTPA tokens:	Disabled
Require SSL protected communication (HTTPS):	Disabled
Restrict use of the SSO token to HTTP/HTTPS:	Disabled

Token Expiration	
Expiration (minutes):	600
Idle Session Timeout:	<input type="checkbox"/> Enabled

Participating Servers	
Domino Server Names:	domino1/Admincamp, domino2/Admincamp
Windows single sign-on integration (if available):	Disabled

**Document**

Field	Value
\$Seal	
\$SignatureStatus	
\$UpdatedBy	
Comments	
DocumentAccess	
Form	
ISiteOrg	
LastMod	
LocalAdmin	
LTPA_DominoSecret	"b13PHPaLX+MmskFUMqtXAbuOf7o="



# LTPA einrichten

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

Administration	
<u>Owners:</u>	Admincamp Administrator/Admincamp
<u>Administrators:</u>	Admincamp Administrator/Admincamp
<u>Last updated:</u>	12.06.2012 12:31:26 Admincamp Administrator/Admincamp

- 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

Save & Close   Keys...   Cancel

## Web SSO Configuration for : LtpaToken

Basics | Comments | Administration

Token Configuration	Token Expiration
Configuration Name: LtpaToken	Expiration (minutes): 600
Organization:	Idle Session Timeout: <input type="checkbox"/> Enabled
DNS Domain: admincamp.local	
Map names in LTPA tokens: Disabled	
Require SSL protected communication (HTTPS): Disabled	
Restrict use of the SSO token to HTTP/HTTPS: Disabled	

Participating Servers
Domino Server Names: domino1/Admincamp, domino2/Admincamp
Windows single sign-on integration (if available): Disabled



# 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:

The screenshot shows the Cookies Manager+ v1.5.1 interface. The search bar contains 'admindcamp'. A table lists cookies, with 'admindcamp.local' selected. The details for the 'LtpaToken' cookie are shown below the table.

Website	Name
<input checked="" type="checkbox"/> admincamp.local	LtpaToken
<input type="checkbox"/> sametime.admindcamp.local	SessionID
<input type="checkbox"/> sametime.admindcamp.local	STAdminRedirect

**Name:** LtpaToken  
**Inhalt:** AAECAzRGREQ5MTdCNEZERTFFMUJDTj1BZG1pbmlzdHJhdG9yL09VPUFkbWlucy9EQz1hZG1pbmNhbXAvmEM9bG9jYWzKzVLuuW/+ZMoAZzUKMAGXLABU0A==  
**Domain:** .admindcamp.local  
**Pfad (H):** /  
**Senden für:** Jeden Verbindungstyp  
**Gültig bis (X):** Am Ende der Sitzung

Buttons: Add, Edit, Delete, Schließen



# 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.

Basics | Naming Contexts (Rules) | LDAP

Configure Directory Assistance access to a remote LDAP server.

LDAP Configuration	
Hostname:	192.168.2.51 <input type="button" value="Verify"/>
LDAP vendor:	Active Directory
Optional authentication credential for search:	Username: admincamp\ldapbind Password: <input type="button" value="Verify"/>
Base DN for search:	DC=admincamp,DC=local <input type="button" value="Verify"/>
Connection Configuration	
Channel encryption:	None
Port:	389
Advanced Options	
Timeout:	60 seconds
Maximum number of entries returned:	100
Dereference alias on search:	Always
Preferred mail format:	Internet Mail Address
<input checked="" type="checkbox"/> Enable name mapping	
Attribute to be used as Notes distinguished name:	Info <input type="button" value="Verify"/>



# Name Mapping

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

Basics	Comments	Administration	
<b>Token Configuration</b>		<b>Token Expiration</b>	
Configuration Name:	LtpaToken	Expiration (minutes):	600
Organization:	admincamp	Idle Session Timeout:	<input type="checkbox"/> Enabled
DNS Domain:	.admincamp.local		
<b>Map names in LTPA tokens:</b>	<b>Enabled</b>		
Require SSL protected communication (HTTPS):	Disabled		
Restrict use of the SSO token to HTTP/HTTPS:	Disabled		



# Name Mapping

- LTPA Username wird im Domino Directory hinterlegt.
  - o Im Feld LTPA\_UserName

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

- o Und als zusätzlicher Fullname

Basics	Work/Home	Other	Miscellaneous	Certificates	Roaming	Administration
<b>Basics</b>						
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



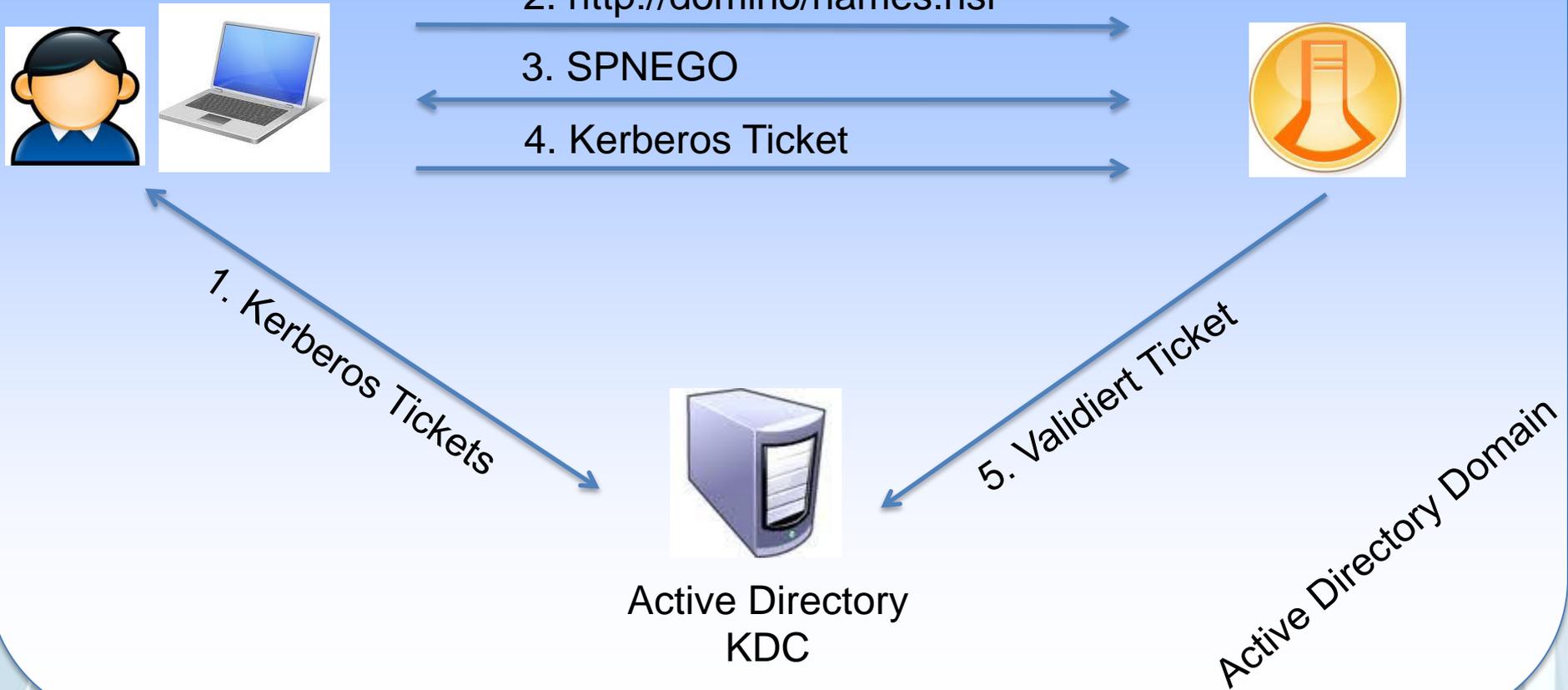
# SPNEGO



- 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

Suchen: network.negotiate

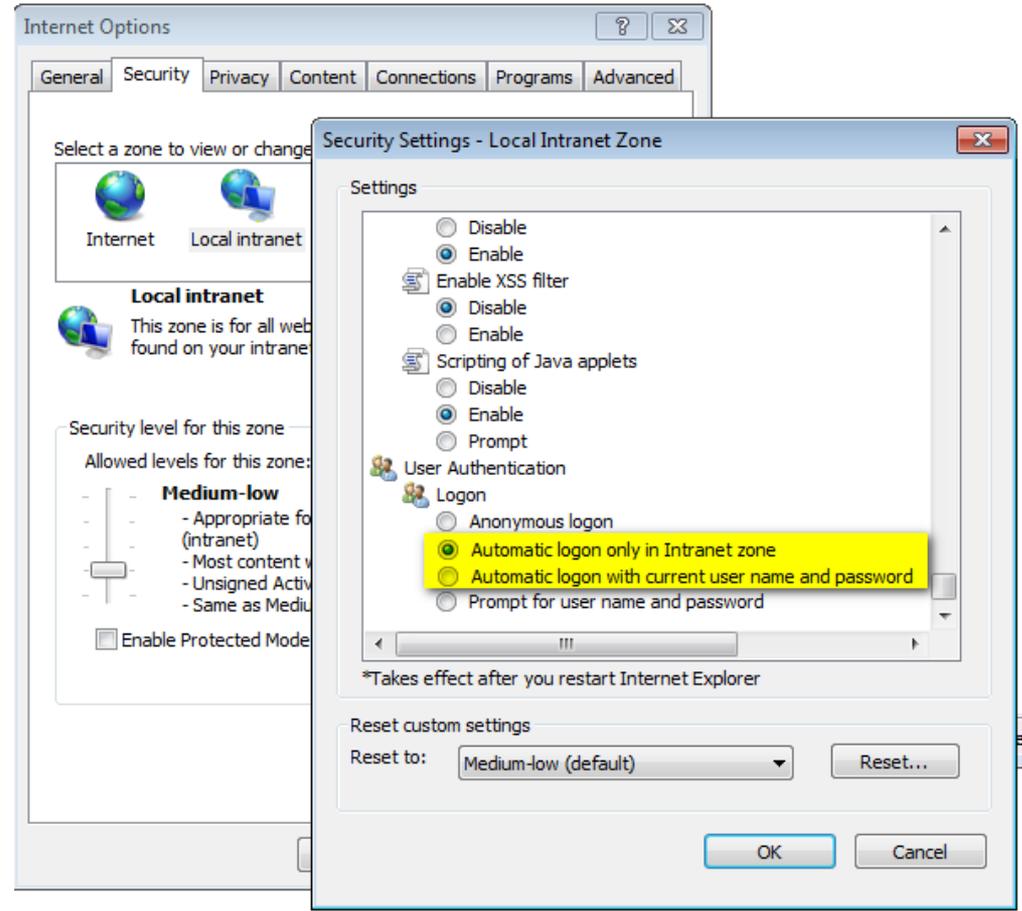
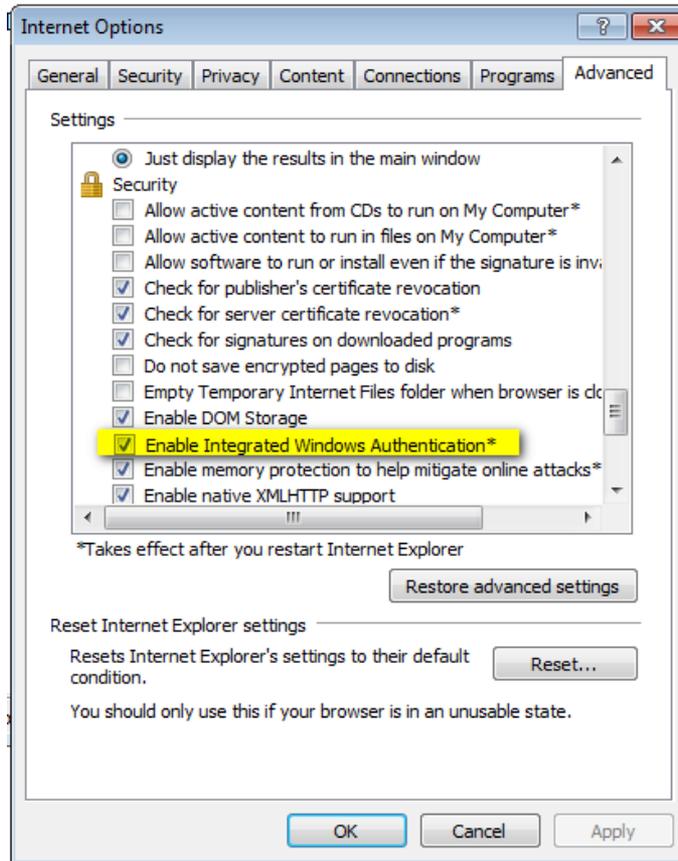
Einstellungsname	Status	Typ	Wert
network.negotiate-auth.allow-non-fqdn	Standard	boolean	false
network.negotiate-auth.allow-proxies	Standard	boolean	true
network.negotiate-auth.delegation-uris	Standard	string	
network.negotiate-auth.gsslib	Standard	string	
<b>network.negotiate-auth.trusted-uris</b>	<b>vom Ben...</b>	<b>string</b>	<b>admincamp.local</b>
network.negotiate-auth.using-native-gsslib	Standard	boolean	true



# SPNEGO Browser Konfiguration



- Internet Explorer
  - Internet Optionen:





# SPNEGO einrichten



- Web SSO Configuration erstellen und SPNEGO aktivieren

## Web SSO Configuration for : LtpaTokenSSO

Basics | Comments | Administration

### Token Configuration

Configuration Name:	LtpaTokenSSO
Organization:	admincamp
DNS Domain:	.admincamp.local
Map names in LTPA tokens:	Enabled
Require SSL protected communication (HTTPS):	Disabled
Restrict use of the SSO token to HTTP/HTTPS:	Disabled

### Token Expiration

Expiration (minutes):	600
-----------------------	-----

### Participating Servers

Domino Server Names:	domino1/Admincamp
Windows single sign-on integration (if available):	Enabled



# SPNEGO einrichten



- Internet Site für SSO einrichten

Server: **domino1/Admincamp** domino1.admincamp.local

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Misc

### Basics

Server name: domino1/Admincamp  
Server title: Admincamp Server Windows  
Domain name: Admincamp  
Fully qualified Internet host name: domino1.admincamp.local  
Cluster name:

Load Internet configurations from Server/Internet Sites documents: **Enabled**

### Web Site

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

#### Site Information

Descriptive name for this site:

Organization:

Use this web site to handle requests which cannot be mapped to any other web sites:  Yes  No  
Note: only one web site should have this option set to Yes

Host names or addresses mapped to this site:

Domino servers that host this site:



# SPNEGO einrichten



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

**Web Site**

Basics | Configuration | Domino Web Engine | Security | Comments | A

**HTTP Sessions**

Session authentication:

Web SSO Configuration:

Force login on SSL:

When overriding session authentication, generate session cookie:



# SPNEGO einrichten



- Weitere Web Sites entsprechend konfigurieren

## Web Site

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

### Site Information

<u>Descriptive name for this site:</u>	<input type="text" value="Domino1 kein SSO"/>
Organization:	<input type="text" value="admincamp"/>
Use this web site to handle requests which cannot be mapped to any other web sites:	<input type="radio"/> Yes <input checked="" type="radio"/> No Note: only one web site should have this option set to Yes
Host names or addresses mapped to this site:	<input type="text" value="domino1.admincamp.local"/>
Domino servers that host this site:	<input type="text" value="domino1/Admincamp"/>

## Web Site

Basics | Configuration | Domino Web Engine | Security | Commer

### HTTP Sessions

<u>Session authentication:</u>	<input type="text" value="Multiple Servers (SSO)"/>
Web SSO Configuration:	<input type="text" value="LtpaToken"/>
Force login on SSL:	<input type="text" value="No"/>
When overriding session authentication, generate session cookie:	<input type="text" value="Yes"/>



# SPNEGO einrichten



- Service Account für Domino in Active Directory erstellen

**New Object - User** [X]

Create in: admincamp.local/ServiceAccounts

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Ca

**New Object - User** [X]

Create in: admincamp.local/ServiceAccounts

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel



# SPNEGO einrichten



- Service Account für Domino

The screenshot shows the 'Service Domino1 Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'domino1' and the domain is '@admincamp.local'. The 'User logon name (pre-Windows 2000)' is 'ADMINCAMP\domino1'. The 'Account options' section is circled in red and contains the following options:

- Use Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication

Below the 'Account options' section, the 'Account expires' section is visible with the 'Never' radio button selected.



# SPNEGO einrichten



- Service Account beim Domino Service hinterlegen und Server neu starten

The screenshot shows the 'Lotus Domino Server (CIBMLotusDominodata) Properties (Local C...)' dialog box with the 'Log On' tab selected. The 'Log on as:' section has two radio buttons: 'Local System account' (unselected) and 'This account:' (selected). Under 'Local System account', there is an unchecked checkbox for 'Allow service to interact with desktop'. The 'This account:' section includes a text box containing 'admicamp\domino1' with a 'Browse...' button to its right. Below this are two password fields labeled 'Password:' and 'Confirm password:', both containing masked characters (dots). A blue hyperlink '[Help me configure user account log on options.](#)' is located below the password fields. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.



## 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](http://sso.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 SPM accountname
-S = add arbitrary SPN after verifying no duplicates exist
Usage: setspn -S SPM accountname
-D = delete arbitrary SPN
Usage: setspn -D SPM 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

Directory Search - [dc.admincamp.local:389]

Search DN: dc=admincamp,dc=local

Filter: (servicePrincipalName=HTTP/sso.admincamp.local)

Attributes: servicePrincipalName

Scope:  One level  Sub-tree level

Handle referrals  Enable Paging

Page size: 1000

Example: uid, mail

Favorite Parameters

Save As... Delete

View History...

Name	Value	Parent DN	servicePrincipalName
CN	Service Domino 1	OU=ServiceAcco...	HTTP/dc.admincamp.local, HTTP/domino1.admincamp.local, HTTP/sso.admincamp.local



# 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
      - o Notes.ini WIDE\_SEARCH\_FOR\_KERBEROS\_NAMES=1 aktivieren
      - o UserPrincipalNames im Domino Personen Dokument hinterlegen (TDI)

Person: **Admincamp Administrator/Admincamp** Admincamp Administrator/Admincamp@Admincamp

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

---

**Administration**

Owners: Admincamp Administrator/Admincamp

Administrators:

Allow foreign directory synchronization: Yes

Last updated: 11.06.2012 15:34:11 domino1/Admincamp

---

Password Management	Policy Management
Check password: Don't check password	Assigned policy:
Required change interval: 0	Setup profile(s):
Grace period: 0	
Last change date:	
Password digest:	
Last change date: (Internet Password) 11.06.2012 12:10:14 CEDT	
Force user to change Internet Password on next login: <input type="checkbox"/> Yes	

---

**Client Information**

Name change request: None

Network account name:

LTPA user name:

DB2 account name:

Active Directory (Kerberos) logon name: Administrator@ADMINCAMP.LOCAL



# Name Mapping

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

**DIRECTORY ASSISTANCE**

Basics | Naming Contexts (Rules) | LDAP

**Basics**

Domain type:	LDAP
Domain name:	Admincamp AD
Company name:	Admincamp
Search order:	1
Make this domain available to:	<input checked="" type="checkbox"/> Notes Clients & Internet Authentication/ Authorization <input type="checkbox"/> LDAP Clients
Group authorization:	No
Use exclusively for group authorization or credential authentication:	No
Enabled:	No

**SSO Configuration**

Attribute to be used as name in an SSO token (map to Notes LTPA_UsrNm):	Info
Windows single sign-on for Web clients:	<input checked="" type="checkbox"/> Enabled
Kerberos realm:	ADMINCAMP.LOCAL



## 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](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



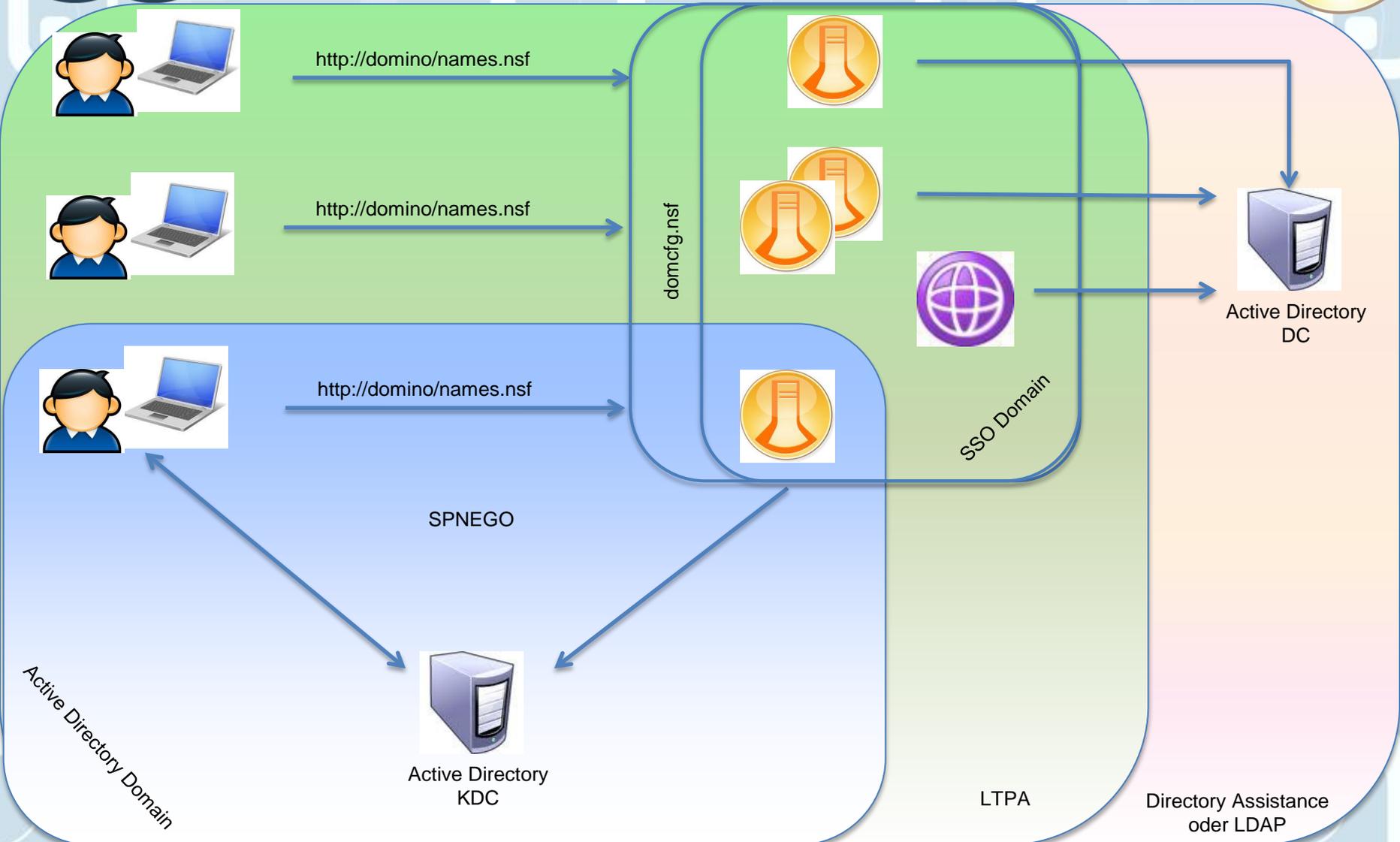
## Alles zusammen....

### 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

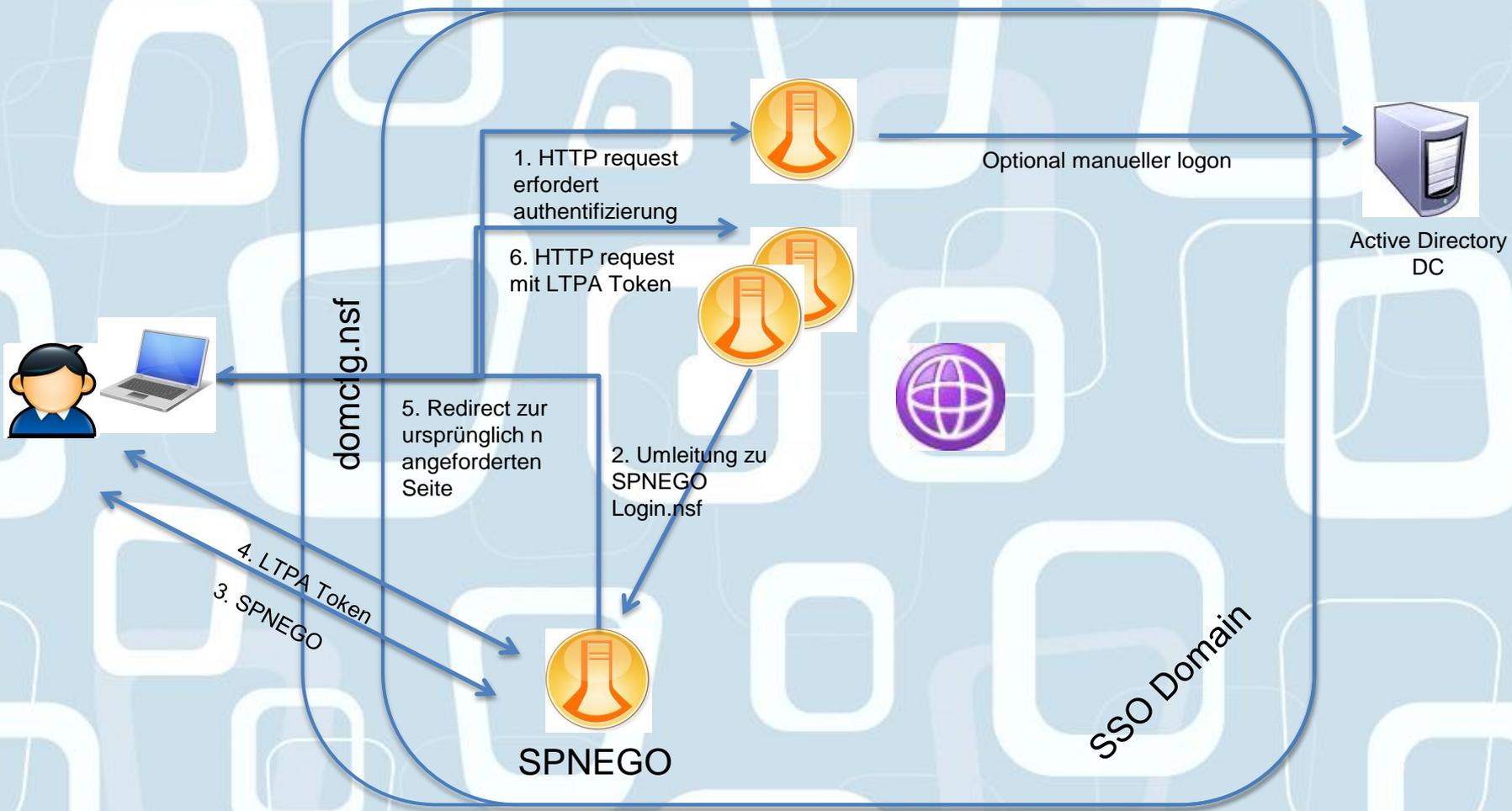


# Alles zusammen....





# 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

The screenshot displays the Domino Web Server Configuration interface. On the left, a navigation pane shows 'Web Server Configuration' with sub-items: 'All Documents', 'Sign In Form Mappings', 'Change Password Form Mappings', and 'Error & Response Form Mappings'. The main area shows a table with a 'Type' column containing 'ErrorMap', 'LoginMap', and 'SetupLoginPage'. Below this, the 'Sign In' Form Mapping configuration is shown with the following details:

'Sign In' Form Mapping	
<b>Site Information</b>	
Applies To:	All Web Sites/Entire Server
Comment:	
<b>Form Mapping</b>	
Target Database:	domcfg.nsf
Target Form:	F_AutoLogon



# 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		End
192.168.2.139	<->	192.168.2.140

HostName Authentication 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

Default Domain 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: ac.gif

Resource must be available

Defined Variables

Variable Names	To be replaced with this fields
<SPNEGOUser>	SPNEGOUser
<SessionUser>	SessionUserNameAbbr
<ErrorMsg>	errmsg
<scheme>	scheme
<FullPath>	Fullpath

- both fields must contain the same number of entries  
- Variable Names are case sensitive

**Language I**

enable additional language support  True  False

Language: German

**LogonPage**

Logon Page Title: (manual logon): <h2>Manuelle Anmeldung</h2>

Information text: (manual logon): <p>Zur Anmeldung verwenden Sie bitte Ihre:</p><p><b>eMail Adresse</b><br></p>und Ihr <b>Lotus Notes Passwort</b></p><p>Sollte eine Anmeldung nicht möglich sein, setzen Sie sich bitte mit dem Helpdesk unter der Telefonnummer +49 190 / 999 99 in Verbindung</p>

Logon Page Title: (SSO): <h2>Automatische Anmeldung</h2>

Information text: (SSO): <input type="button" class="loginButton" value="Manuelle Anmeldung" onclick="javascript:manuallogon();">

Label Login Domain: AD Domäne

Label Login User: Benutzename

Label Login Password: Passwort

Label Login Button: Anmelden



# Login.nsf

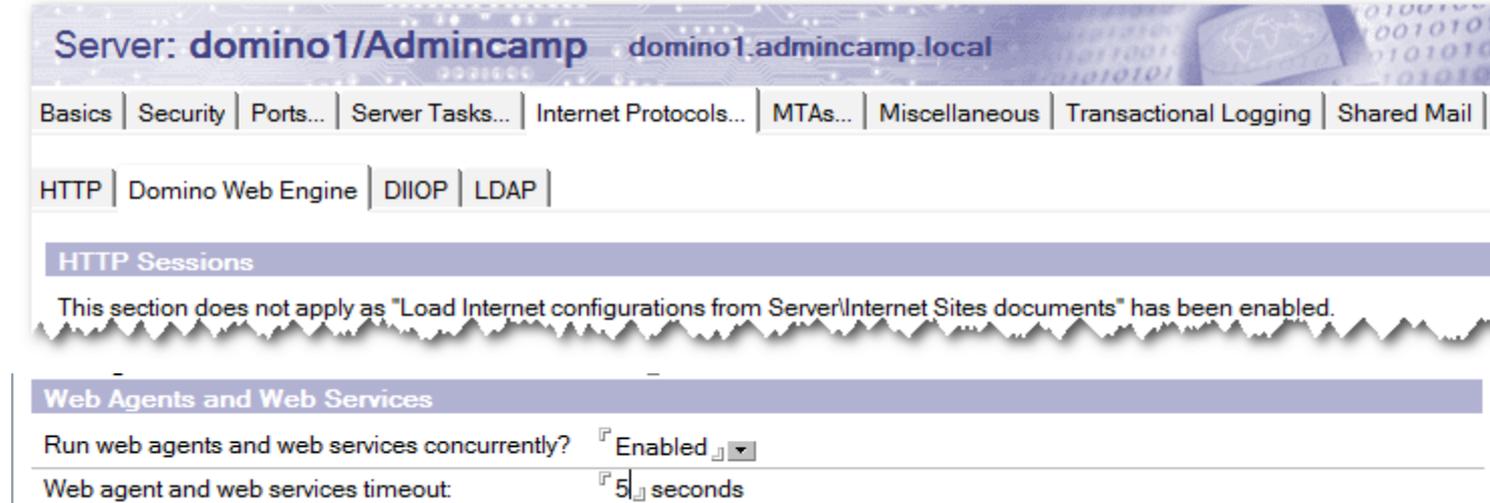
- Datenbank enthält nur einen einfachen Agenten
  - ag\_loginhandler
- Wird automatisch über die domcfg.nsf aufgerufen
- Parameter wie „&redirectto“ in einer Domino URL werden berücksichtigt
  - <http://domino1.admncamp.local/names.nsf?login&redirectto=http://domino1.admncamp.local/whoami.nsf>
- Der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



# Login.nsf



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



Server: **domino1/Admincamp** domino1.admincamp.local

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail |

HTTP | Domino Web Engine | DIIOP | LDAP |

### HTTP Sessions

This section does not apply as "Load Internet configurations from Server\Internet Sites documents" has been enabled.

### Web Agents and Web Services

Run web agents and web services concurrently?  Enabled ▾

Web agent and web services timeout:  seconds



# 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)

The screenshot shows the configuration page for 'sametime.admincamp.local'. It displays server community details and login options. The 'Log In' tab is active, showing fields for 'User name' (hans sametime) and 'Password'. There are checkboxes for 'Remember password' and 'Automatically log in'. A section for 'Token based single sign on' is visible, with the checkbox 'Use token based single sign on' checked. Below this, the 'Authentication server' field is empty, and the 'Authentication Type' dropdown is set to 'Domino Single Sign On'. A description at the bottom explains that Domino single sign on allows automatic login after authenticating with a Domino server.

Server community type: Sametime  
Server community status: Available  
Server community name: sametime.admincamp.local:hans sam

This is your default server community. The default server community can be reset using the server communities preference page or the main login dialog.

Log In | Server | Connection | Icon | Options

User name: hans sametime  
Password:   
 Remember password  
 Automatically log in

Token based single sign on allows you to log into Sametime without a password.  
 Use token based single sign on  
Authentication server:   
Authentication Type: Domino Single Sign On

Description: Domino single sign on allows you to automatically log into Sametime after authenticating with a Domino server. If an authentication server is not specified, the Sametime server is used for authentication.



# Embedded Clients

- SPNEGO (auch mit dem Domino SPNEGO Server)

sametime.admincamp.local

Server community type: Sametime  
Server community status: Available  
Server community name: sametime.admincamp.local:hans same

This is your default server community. The default server community can be reset using the server communities preference page or the main login dialog.

Log In **Server** Connection Icon Options

User name: hans sametime  
Password:   
 Remember password  
 Automatically log in

Token based single sign on allows you to log into Sametime without a password.  
 Use token based single sign on

Authentication server: http://sso.admincamp.local/names.nsf  
Authentication Type: SPNEGO

Description: SPNEGO single sign on allows you to automatically log into Sametime after authenticating with a remote server using your operating system login. Your administrator must provide you with a single sign on authentication server URL in order to use this feature.

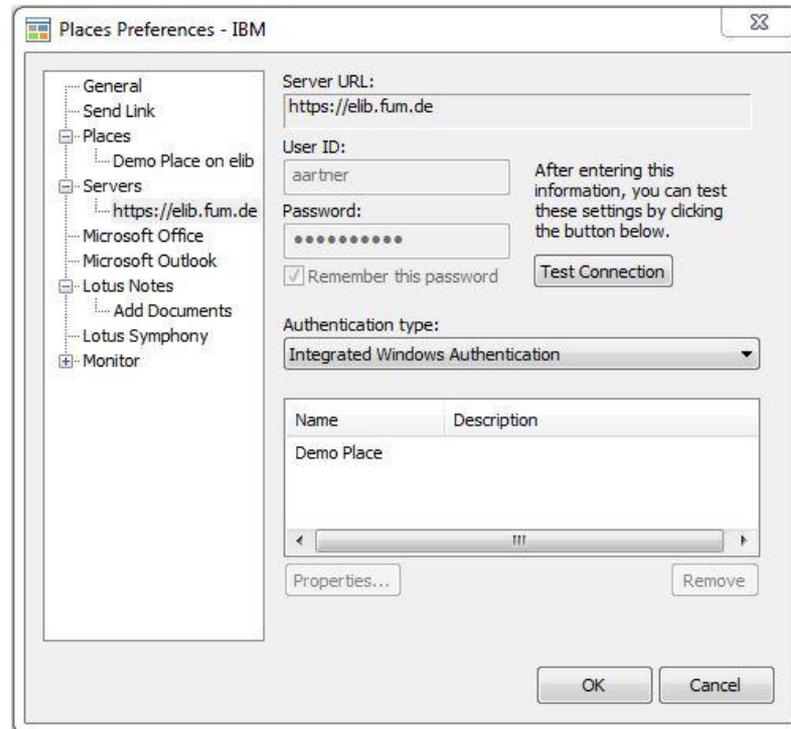


# Embedded Clients

- 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](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 !

Directory Search - [domino1.admincamp.local:2389]

Search DN: RootDSE

Filter: (dominoAccessGroups=CN=LocalDomainAdmins)

Attributes:

Scope:  One level  Sub-tree level

Handle referrals  Enable Paging Page size: 1000

Example: uid, mail

Favorite Parameters

Save As... Delete

Name	Value	Parent DN

Search Stop Save Results...

Entries found: 0 Elapsed time : 00:00:00



# 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**

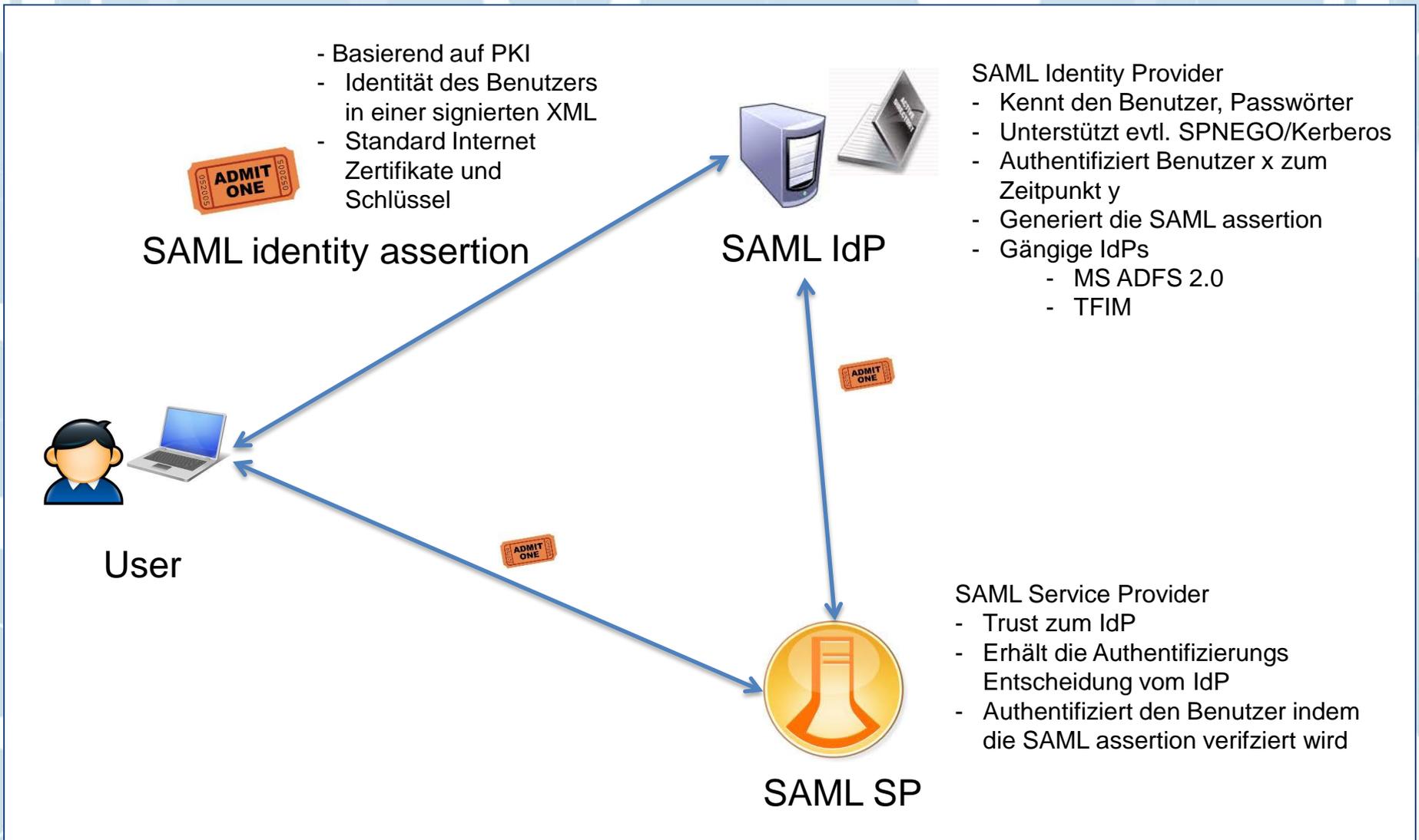


## Die Zukunft - SAML

- **SAML - Security Assertion Markup Language**
  - 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





# 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