



Collaboration Days

Creating Hands-on Value



Microsoft®

SharePoint® Server 2010



Joël Hasler

Authentifizierungs- und Publishing- methoden von SharePoint 2010



SharePointCommunity.ch

... born to be shared!



In eigener Sache

Joël Hasler

Leiter Rechenzentrum



Bachelor of Science in Informatik

joel.hasler@ioz.ch

<http://www.ioz.ch>

In eigener Sache

Gesamtanbieter von SharePoint Lösungen

Zuständig für Organisation, Beratung und Projektrealisierung:



Zuständig für Hosting und massgeschneiderte Programmierungen:



Zertifizierungen:



Agenda

Einleitung

Authentifizierungsmethoden

Publishing Szenarien

Entscheidungshilfe

Fragen

Einleitung

Ausgangslage

- Mobilität steigt (Arbeiten von unterwegs, Home Office usw.)
- Extranet (Zusammenarbeit)

- Sicherheit
- Benutzerverwaltung
- Antivirus
- URL Thematik
- Lizenzen
- ...

Authentifizierung

Übersicht

Classic Mode

- NTLM
- Kerberos

Claim Based

- Form Based Authentication
- Trusted Identity Provider

Authentifizierung

Unterscheid Classic / Claim

- Classic Mode
 - Standard
 - Windows Authentication (eigenes AD)
 - Closed Domains
- Claim Based
 - über Domaingrenze hinweg (Cloud Trend)
- Wird auf WebApp Ebene definiert
- Konvertieren auf Claim möglich (Irreversibel Operation)

Authentication

Select the authentication for this web application.

- Claims Based Authentication
- Classic Mode Authentication

Classic Mode

Übersicht

Classic Mode

- NTLM
- Kerberos

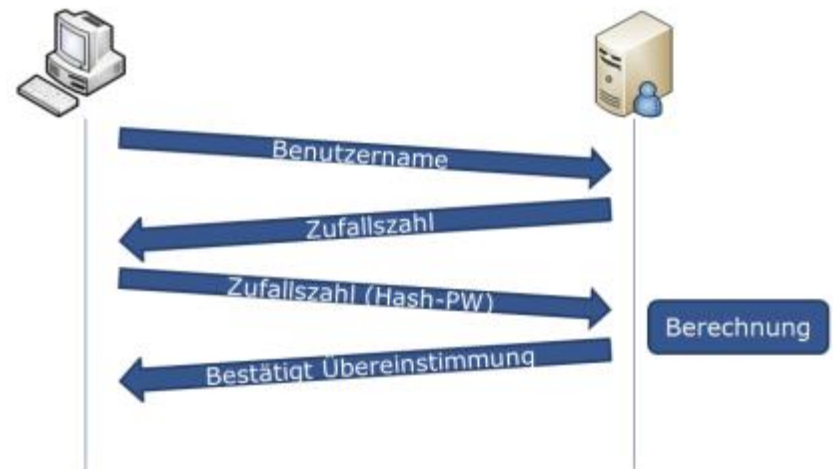
Claim Based

- Form Based Authentication
- Trusted Identity Provider

Classic Mode

NTLM → NT LAN MANAGER

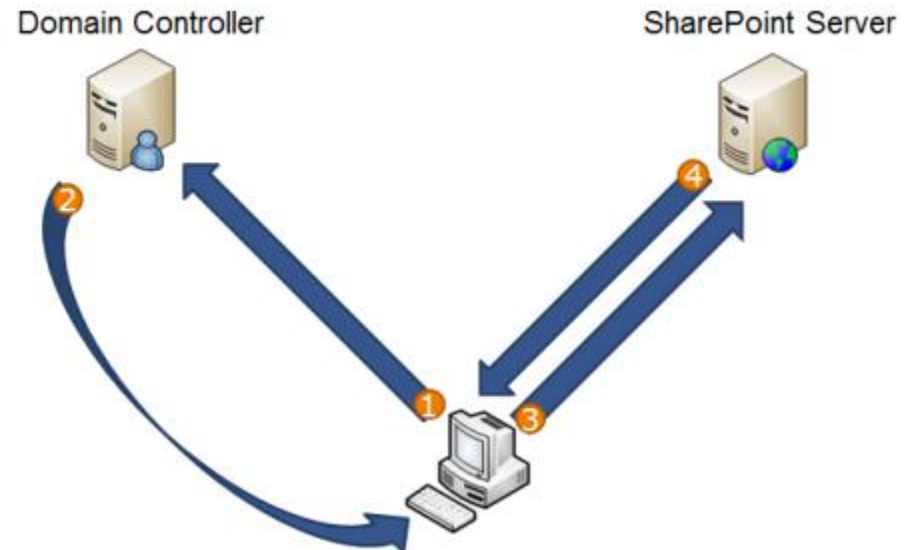
- SharePoint Standard Authentifizierung
- Windows Protokoll (NTLMv2)
- Challenge Response Authentifizierungsverfahren
- Bekannte Sicherheitsprobleme (nicht sicher)
- Kein richtiges SingleSignOn



Classic Mode

Kerberos

- Sichere Authentifizierung
- Industriestandard
- Tickets für Authentifizierung
- Ermöglicht SingelSignOn
- Intranet und MySite



Classic Mode

Vor- und Nachteile

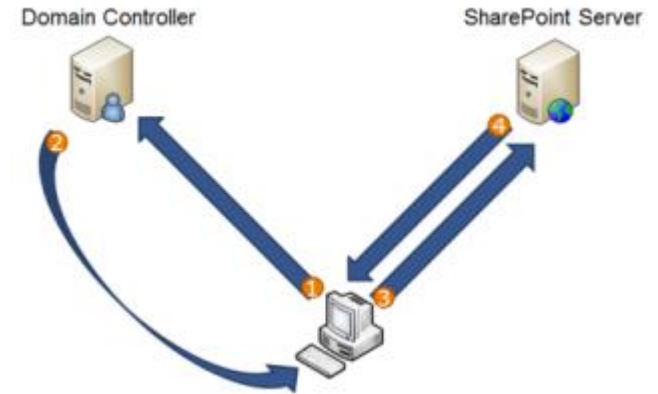
- + NTLM benötigt keine Konfiguration
- NTLM benötigt immer die Anmeldung auf den jeweiligen Dienst
- NTLM führt zu einer höheren Last auf dem DC

- + Kerberos ist sicherer und hat eine geringere Last auf dem DC
- + Kerberos benötigt nur einmalige Anmeldung
- + Delegation (Multi Hop möglich Bsp. BCS auf SQL DB)
- + Verbesserte Kompatibilität
- Höherer Konfigurationsaufwand (für jeden Dienst)

Kerberos

Konfiguration

- Ablauf
 - Service Principal Name (SPN) :
 - Definiert welches Konto zu welchem Dienst passt
 - SQL Server + SharePoint für Kerberos konfigurieren
- Tools
 - GUI:
 - ADSI Edit
 - AD User and Computers (View mit Advanced Features)
 - CLI: setspn.exe



Kerberos

Konfiguration SQL

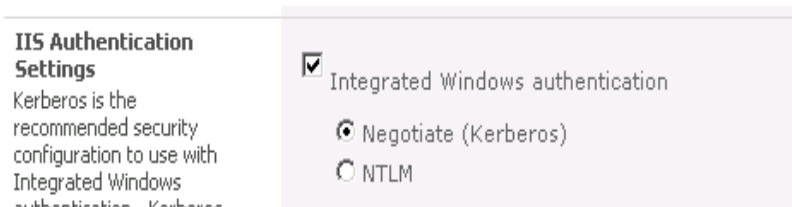
- SPN Syntax
 - MSSQLSvc/name:instancename → Named Instanz
 - MSSQLSvc/name:port → Default Instanz
 - Name → NetBIOS und FQDN
- SQL Alias berücksichtigen
- SQL seitig sonst nichts anpassen

```
Values:
MSSQLSvc/IOZSRV113.ioz.local
MSSQLSvc/iozsrv113.ioz.local:1433
MSSQLSvc/iozsrv113:1433
MSSQLSvc/IOZSRV118
MSSQLSvc/IOZSRV118.ioz.local
MSSQLSvc/IOZSRV118.ioz.local:1433
MSSQLSvc/IOZSRV118:1433
MSSQLSvc/SharePointDB01.ioz.local:1433
MSSQLSvc/SharePointDB01:1433
```

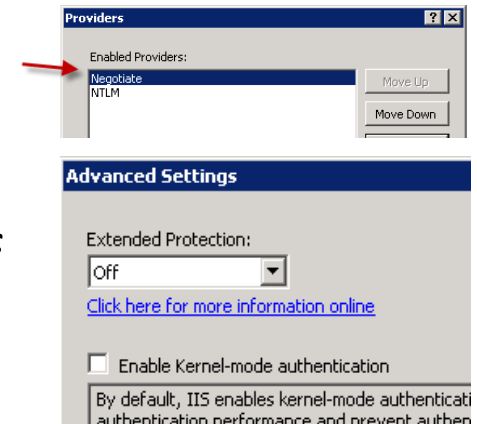
Kerberos

Konfiguration SharePoint

- Central Admin
 - WebApp → Authentication auf Negotiate (Kerberos) stellen



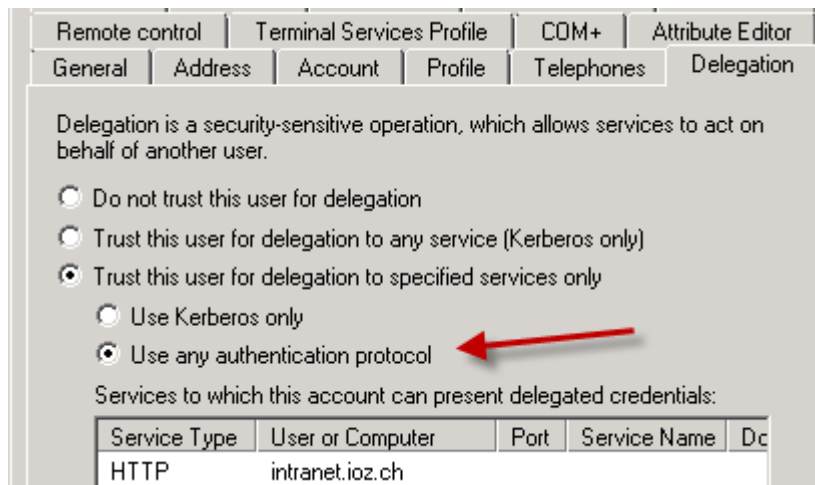
- IIS Website Einstellungen prüfen
 - Windows Authentication → Providers
 - Enable Kernel-mode authentication off



Kerberos

Konfiguration SharePoint

- SPN Syntax
 - `HTTP/intranet.kunde.ch` → Alternate Access Mapping
 - Egal ob HTTP oder HTTPS
- Delegation anpassen nicht nur «Kerberos Only»



Kerberos

Troubleshooting

- Tools zum Testen
 - IE für SharePoint und UDL File für SQL
 - Event Logs Security (ID 4624)
 - klist Tool ob Ticket erstellt (nicht auf dem gleichen Server)
- SPN immer eindeutig
- Replikation abwarten oder forcieren bei mehreren DCs

Classic

Live Demo

Claim Based

Übersicht

Classic Mode

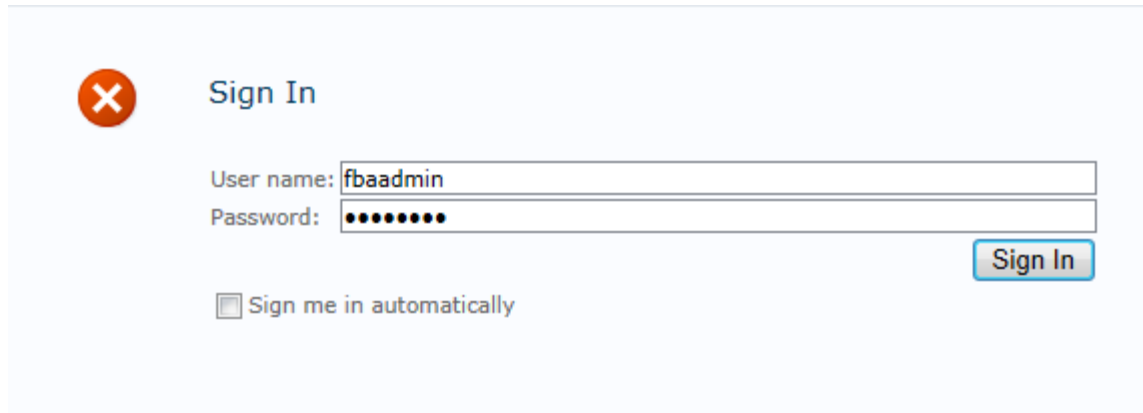
- NTLM
- Kerberos

Claim Based

- Form Based Authentication
- Trusted Identity Provider (ADFS / LiveID)

Claim Based

Form Based Einsatzgebiet



The screenshot shows a 'Sign In' form with a light blue background. In the top left corner, there is a red circular icon with a white 'X' inside. To the right of this icon, the text 'Sign In' is displayed in a blue font. Below this, there are two input fields: 'User name:' followed by a text box containing 'fbaadmin', and 'Password:' followed by a text box containing ten black dots. To the right of the password field is a blue button with the text 'Sign In'. Below the input fields, there is a checkbox followed by the text 'Sign me in automatically'.

- Formular zum Anmelden
- Externer Zugriff für Partner oder anderer externe Personen
- Benutzerverwaltung vom AD entkoppelt

Form Based

Anforderungen

- OOTB möglich
- SP nutzt dabei ASP.NET Framework
- Folgende Speicher für Benutzerdaten werden unterstützt:
 - SQL DB, LDAP Verzeichnisse, eigene Membership Provider
- WebApp in SharePoint muss Claim Based sein
- CodePlex Erweiterung (Benutzerverwaltung vereinfachen)
 - <http://sharepoint2010fba.codeplex.com/>

Form Based

Konfiguration mit SQL DB

- Ablauf
 - SQL DB erstellen lassen
 - SQL Login erfassen → SQL Instanz im mixed Mode
 - IIS Anpassungen (.Net User und Role)
 - SharePoint Anpassungen (.Net Providers + Client Integration)
 - Codeplex Erweiterung installieren (Optional)
- <http://blogs.technet.com/b/mahesm/archive/2010/04/07/configure-forms-based-authentication-fba-with-sharepoint-2010.aspx>

Form Based

Live Demo

Form Based

Vor- und Nachteile

- + Man kann damit «arbeiten» aber...
- SharePoint Gruppen, keine AD Gruppen
- Problematik bei mixed Mode (Windows und FBA) mit Auswahl
- FBA Authentication Cookie in Memory
- Suche nur mit Windows Authentication (Security trimmed)
- Min. Office 2007 CU April 2009 + Vista SP2
 - PopUp zum anmelden im Office
- Div. Registry Keys für Unterstützung
- <http://msdn.microsoft.com/en-us/library/bb977430.aspx>

Claim Based

Was ist ein Claim?

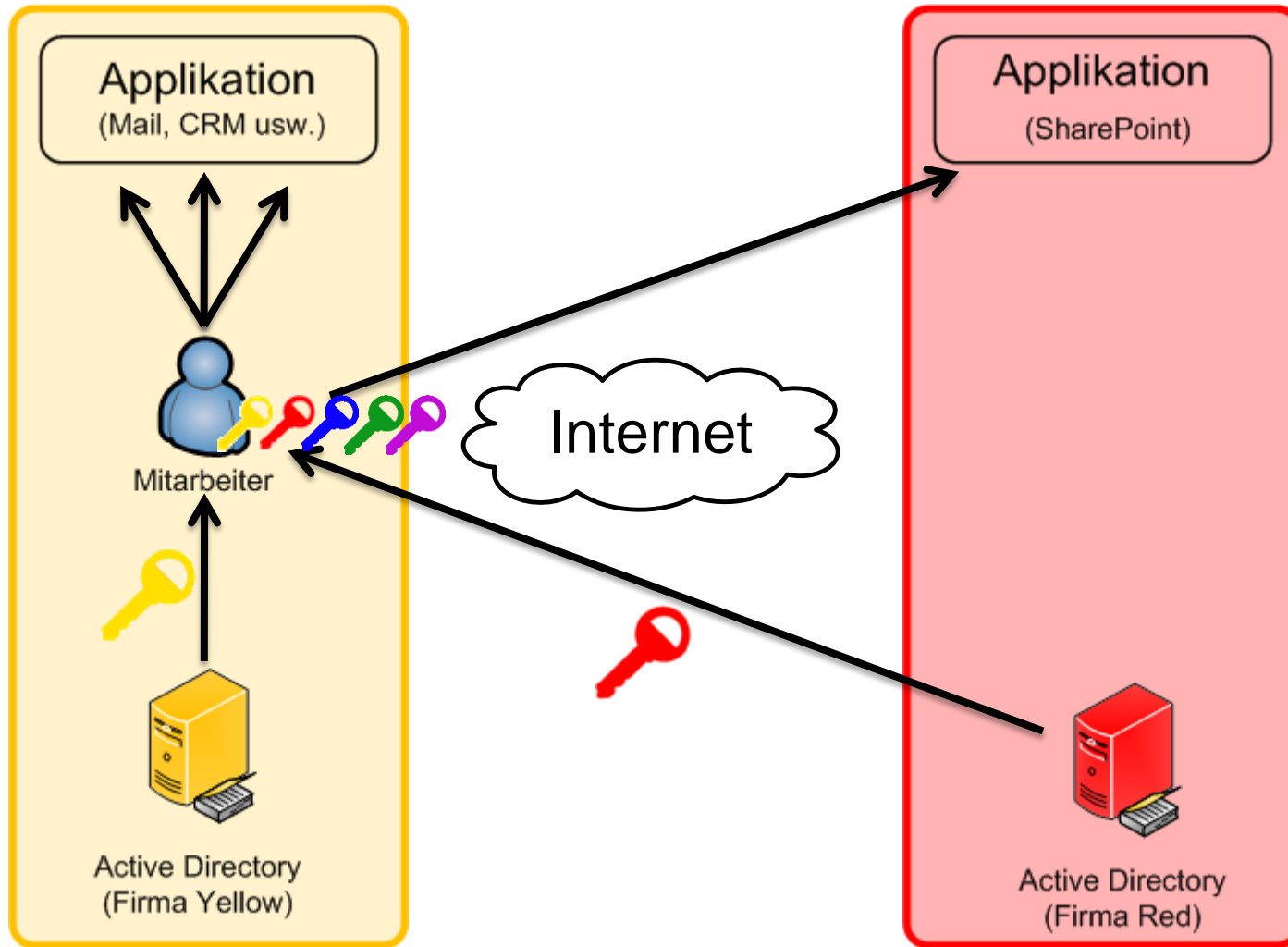
- Auch «Behauptung» genannt
- Beispiel: Online Alkoholshop (USA)
 - Applikation muss nur prüfen ob Käufer min. 21 Jahre alt ist
 - Claim: Ich bin 27 Jahre alt
 - Privacy
 - nur Infos welche wirklich nötig sind
 - Applikation muss nicht wissen wie ich heisse usw.
 - Compliance
 - anderen Stellen vertrauen

ADFS

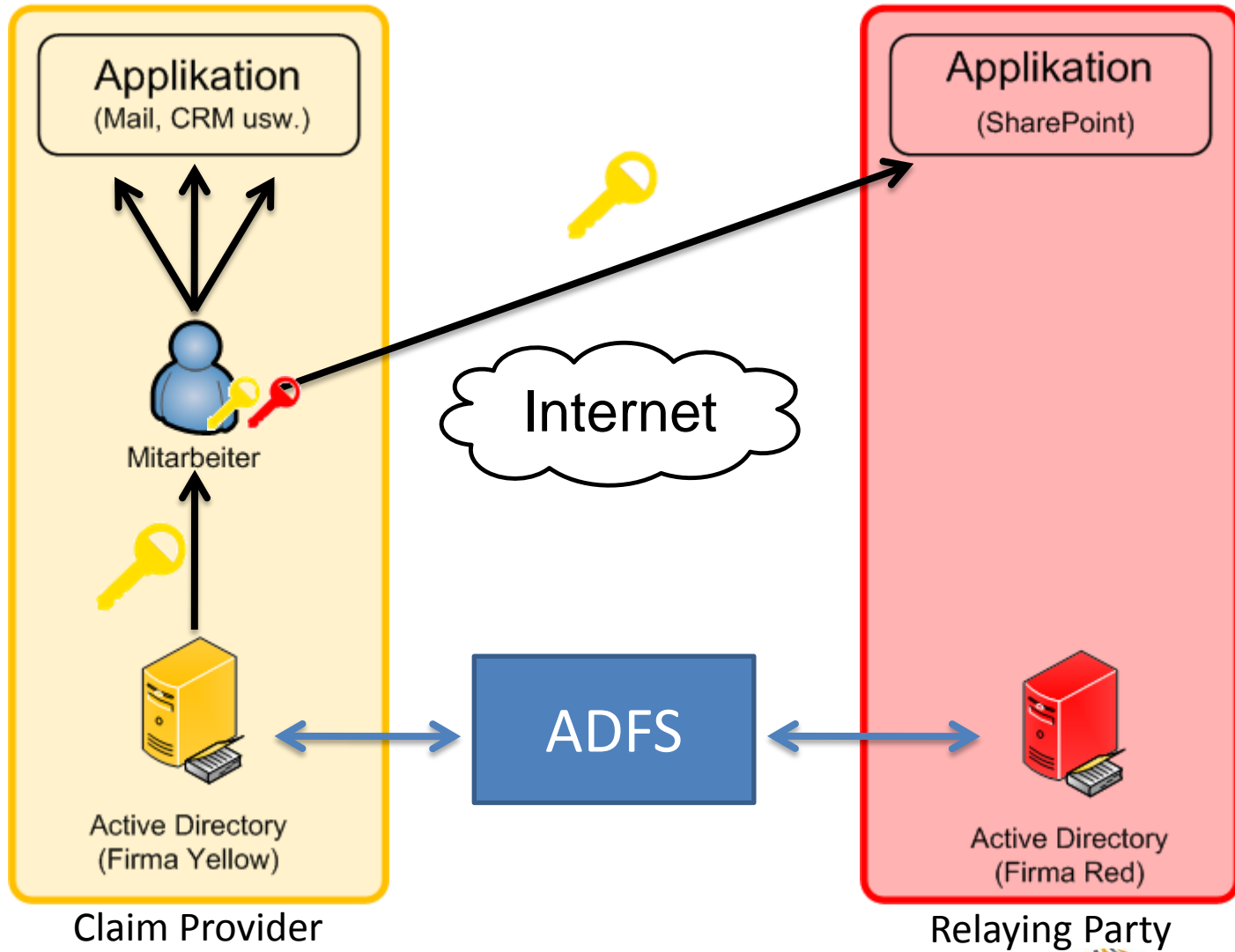
Beispiel Trusted Identity Provider

- Zwei Organisationen (Active Directory) verbinden
- Federation über das Internet
- Claim
 - Privacy → Es wird definiert was es für die Authentifizierung benötigt (Bsp.: Email oder Benutzername)
 - Compliance → Vertrauen der anderen Organisation

Was ist ADFS?



Was ist ADFS?



ADFS

Anforderungen (Claim Provider – gelb)

- ADFS 2.0 Infrastruktur (Version 2.0 ist mit SP 2010 supported)
 - 1 oder mehrere ADFS FE Server
 - 1 oder mehrere ADFS Proxy Server (optional)
 - SQL Server oder Cluster
 - Windows Integrated Database nicht empfohlen
 - Ab Windows Server 2003 SP1 und SQL Server 2005
- Zertifikate (externes oder von interner CA)
- Externe URL
- Konfiguration vom ADFS Relaying Party Trust
- [http://technet.microsoft.com/en-us/library/adfs2-design-guide\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/adfs2-design-guide(WS.10).aspx)

ADFS

Anforderungen (Relaying Party – rot)

- Nichts 😊
- SharePoint bietet dies OOTB an
- Konfiguration des TrustedIdentityTokenIssuer

ADFS

Konfiguration Relaying Party

- WebApp muss auf Claim sein

```
$App = get-spwebapplication "URL"
```

```
$app.useclaimsauthentication = "True"
```

```
$app.Update()
```

- Definieren des SPTrustedIdentityTokenIssuer benötigt:

- Zertifikat von Claim Provider
- STS URL (Secure Token Service)
- Claim (Username, Email oder andere)
- Realm (um Service zu identifizieren)

- <http://blogs.technet.com/b/speschka/archive/2010/07/30/configuring-sharepoint-2010-and-adfs-v2-end-to-end.aspx>

ADFS

Live Demo

Windows Live ID

Beispiel Trusted Identity Provider

- Nicht das AD als Claim Provider sondern Windows Live ID
- Konfigurationsschritte
 1. Windows Live ID Security Token Service konfigurieren
 - Auf [Microsoft Service Manager Service](#) registrieren
 - Zertifikat herunterladen
 2. SharePoint mit Windows Live ID konfigurieren
 - SPTrustedIdentityTokenIssuer erstellen via PowerShell
 - WebApp Claim Based erstellen und TokenIssuer auswählen
 - Berechtigungen in SiteCollection setzen
 3. Von Live ID INT Umgebung auf Prod konvertieren
- <http://technet.microsoft.com/en-us/library/ff973117.aspx>

Windows Live ID

Live Demo

Publishing

Verschiedene Varianten

- SharePoint extern zur Verfügung stellen
- Authentifizierungsmethoden richtig einsetzen
- Verschiedene Szenarien
- Kundenbeispielen

Szenario 1

URL Thematik

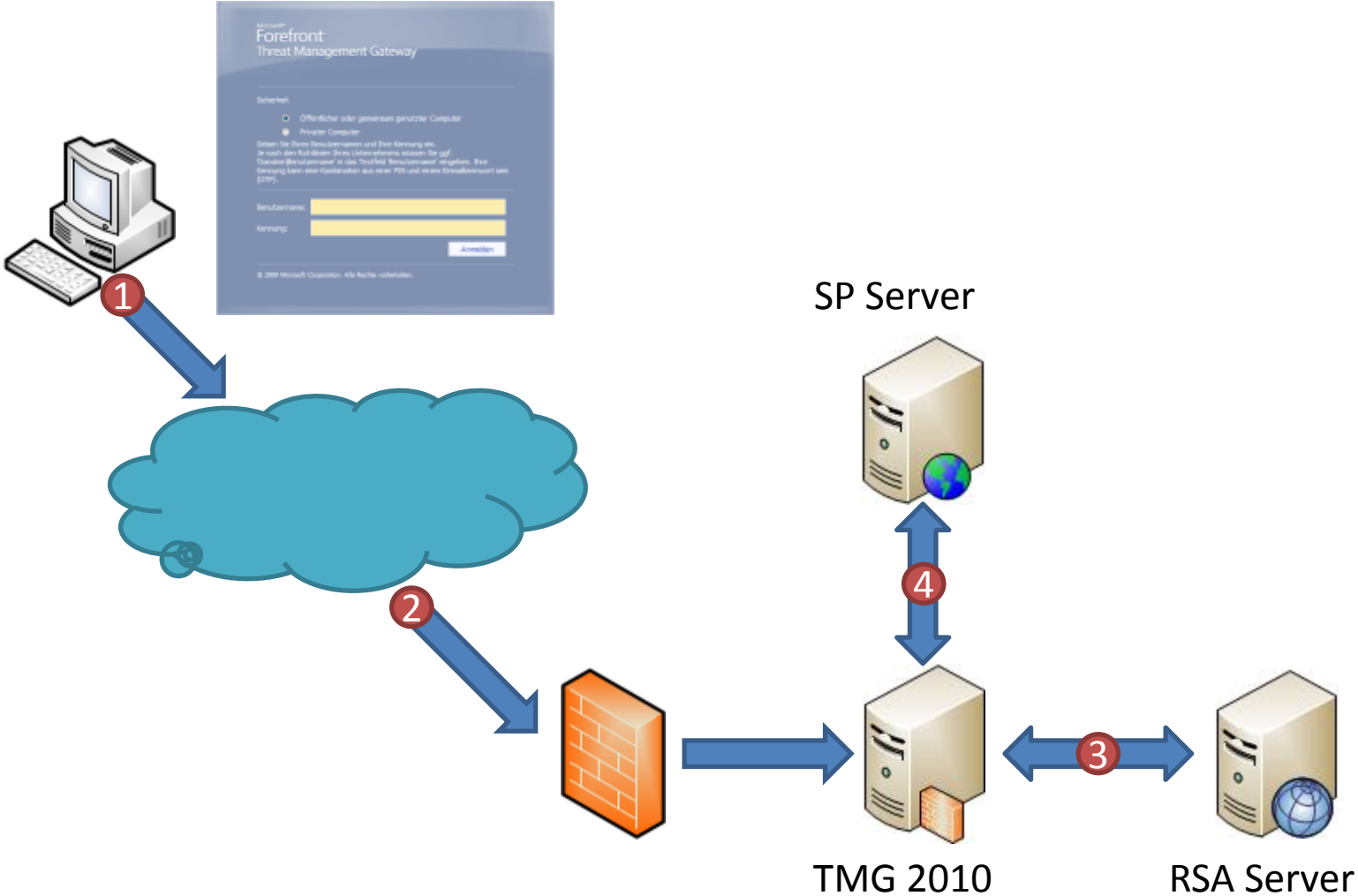
- Ausgangslage
 - Intranet extern verfügbar halten
- Eingesetzte Technologie
 - NAT Publishing bei NTLM
 - Reverse Proxy (Bsp. TMG 2010) bei Kerberos
- Grundsatz (Best Practice)
 - URL intern und extern immer gleich und alles auf HTTPS
 - Wenigste Probleme (Support, Links intern extern usw.)

Szenario 2

2-stufige Authentifizierung

- Ausgangslage
 - Erhöhte Sicherheitsbedürfnisse bei der Anmeldung an SharePoint
- Eingesetzte Technologie
 - RSA Infrastruktur mit RSA Tokens als zweiter Faktor
 - Publishing via TMG 2010
 - Kerberos

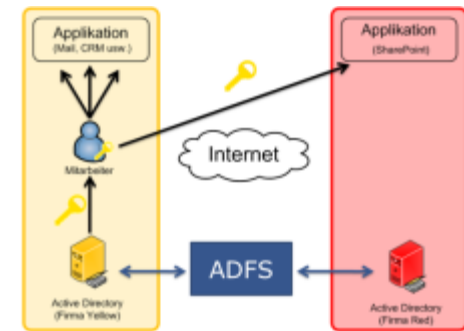
Szenario 2



Szenario 3

ADFS

- Ausgangslage
 - Domain Problematik bei uns im RZ
 - Ein Login für alles
- Eingesetzte Technologie
 - ADFS 2.0
- Vor- und Nachteile erfassen
 - + Ganze Berechtigung und Gruppenverwaltung beim Kunden
 - + Einfacher für den User
 - Grosse Konfiguration nötig



Szenario 4

Dedizierte Farm

- Ausgangslage
 - Geschützte SharePoint Farm
- Eingesetzte Technologie
 - Eigenständige SharePoint Farm in DMZ mit eigenem AD
- Vor und Nachteil erfassen
 - + Sichere Variante, da komplett entkoppelt
 - Erhöhter Wartungsaufwand
 - Benutzerverwaltung doppelt

Szenario 5

Form Based Authentication

- Ausgangslage
 - Externe Partner Zugriff
 - Benutzerverwaltung nicht im AD
- Eingesetzte Technologie
 - FBA mit SQL DB
- Vor- und Nachteil erfassen
 - + Benutzerverwaltung nicht im AD
 - + Flexible Benutzeradministration
 - Abhängigkeiten vom Client Computer

Entscheidungshilfe

	NTLM	Kerberos	NAT Publishing	Reverse Proxy	2ter Faktor	Form Based	Trusted Identity Provider
Intranet	x	x					
Intranet (extern verfügbar)	x	x	x	x			
Extranet (viele verschieden)	x	x	x	x		x	x
Extranet (eine Unternehmung)	x	x	x	x			x

Fragen





Collaboration Days

Creating Hands-on Value



Microsoft®

SharePoint® Server 2010



Joël Hasler

Herzlichen Dank für Ihre Aufmerksamkeit



SharePointCommunity.ch

... born to be shared! 