



Microsoft Active Directory Federation Service

SharePoint Community

24.11.2010

Joël Hasler IOZ DataCare AG





Inhalt

Situation heute

Was ist ADFS

Architektur

Demo

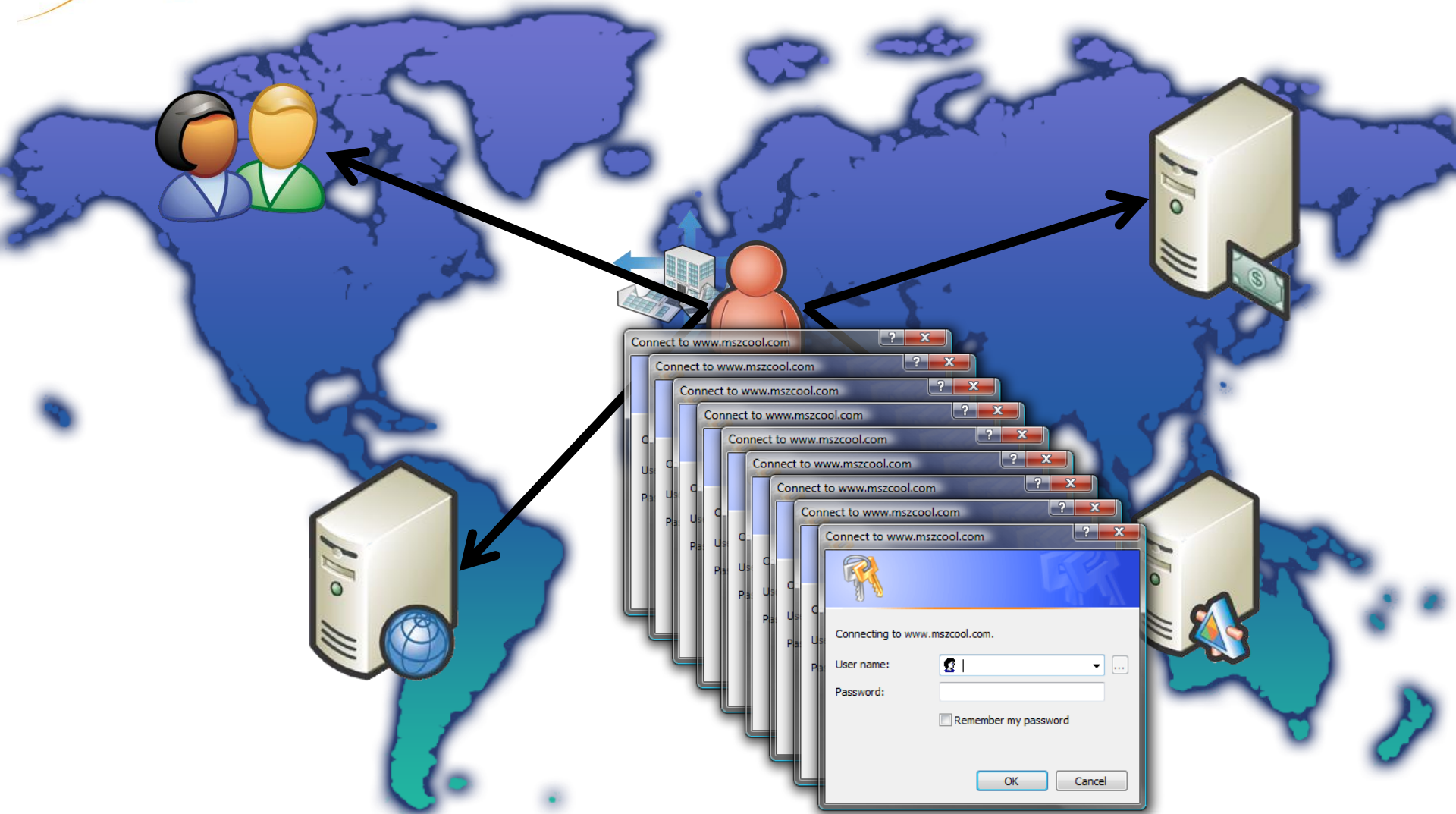
Fragen



- Trend
 - Unternehmen hinter Firewall
 - Cloud Computing
- Problematik
 - Feste Kopplung Applikation und Anmeldeinformation
- Ziel
 - Kein Unterschied lokal oder Cloud
 - Ein Login für alles



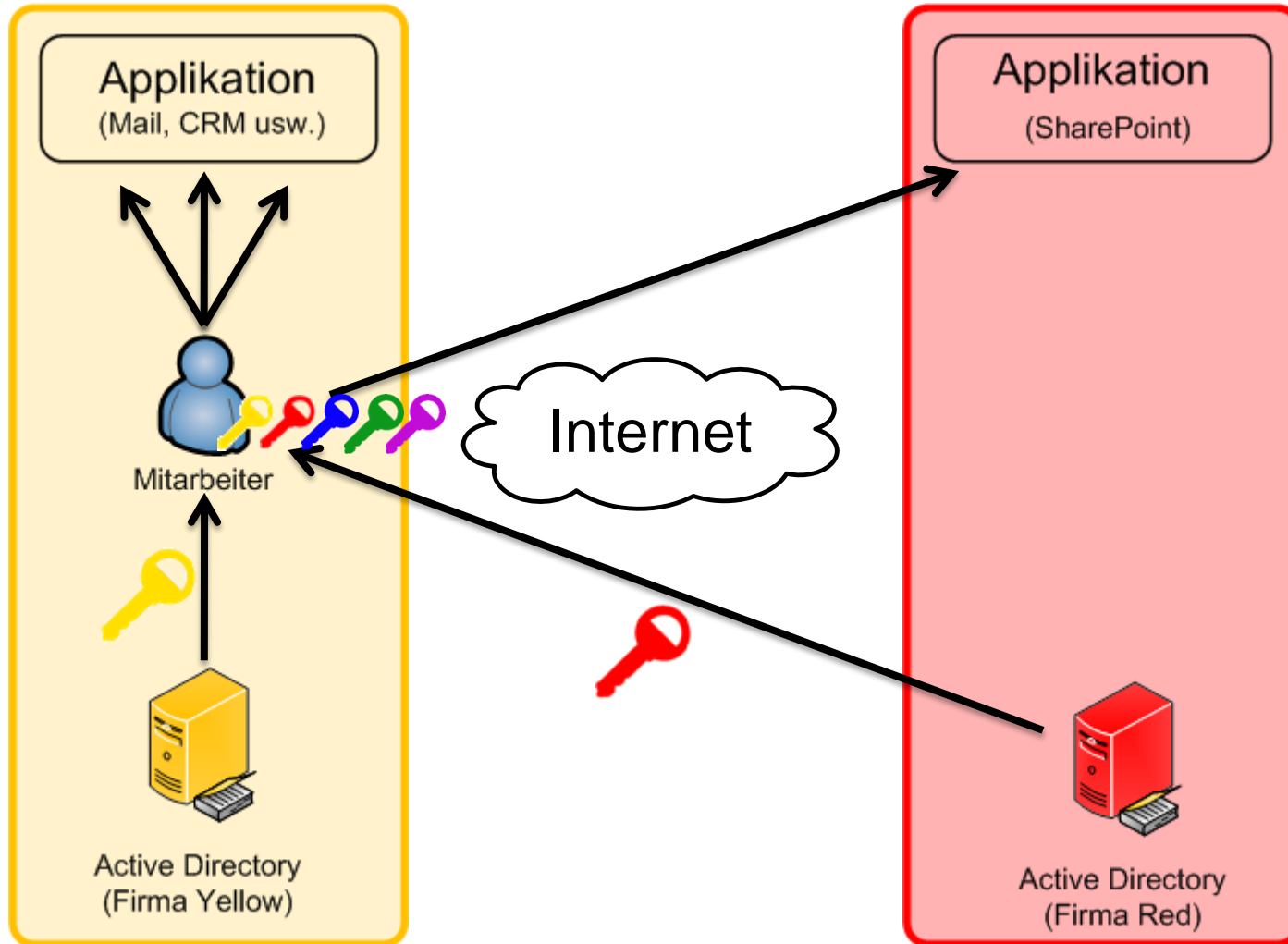
SITUATION HEUTE

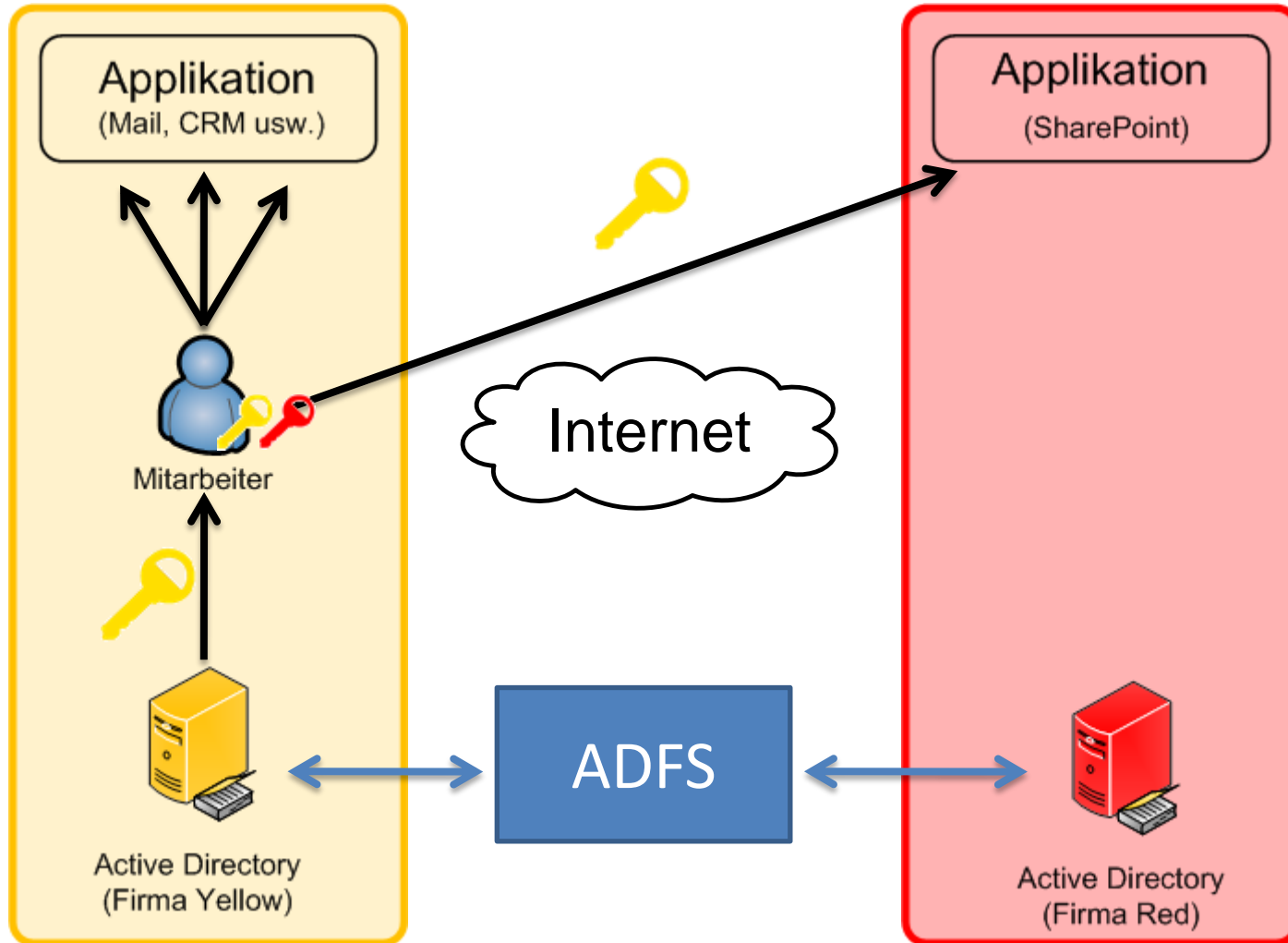


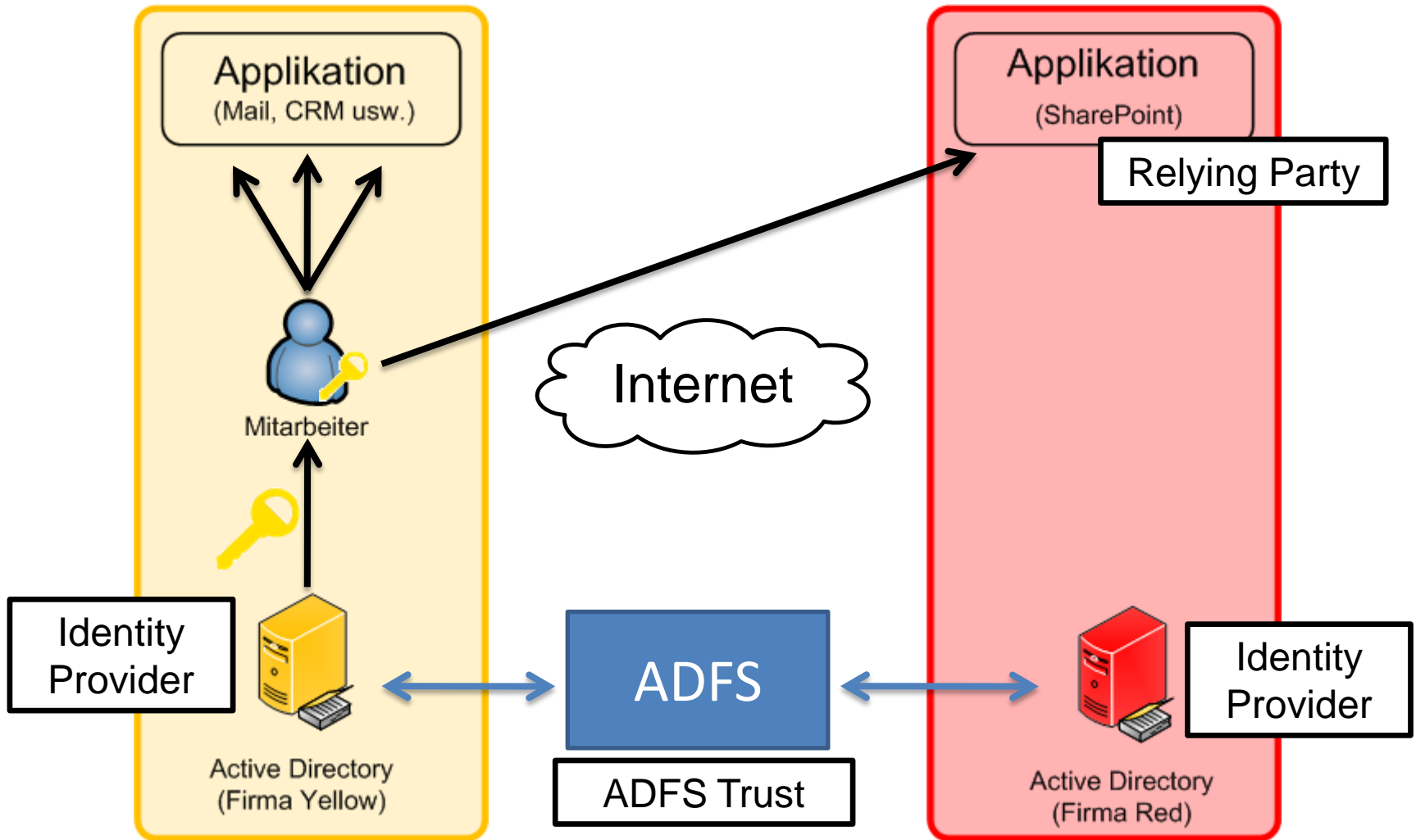


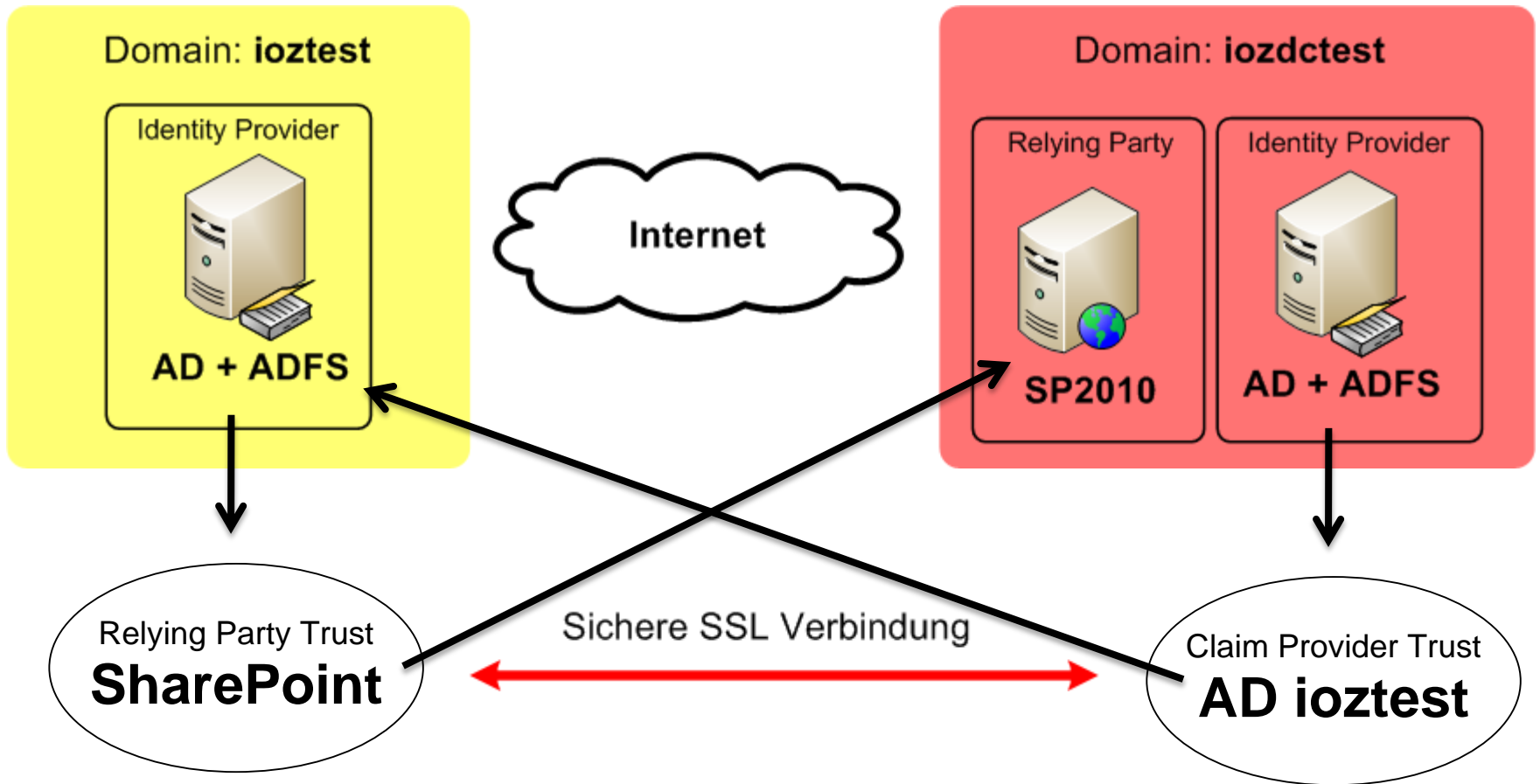
WAS IST ADFS

- Active Directory Federation Services
- Geneva-Projekts
- Zusammenarbeit über Unternehmensgrenzen hinweg
- End-to-end Vertrauensbeziehung über Internet
- Ohne Firewallanpassungen (alles via Webservice)
- Infrastrukturerweiterung (Serverrolle)





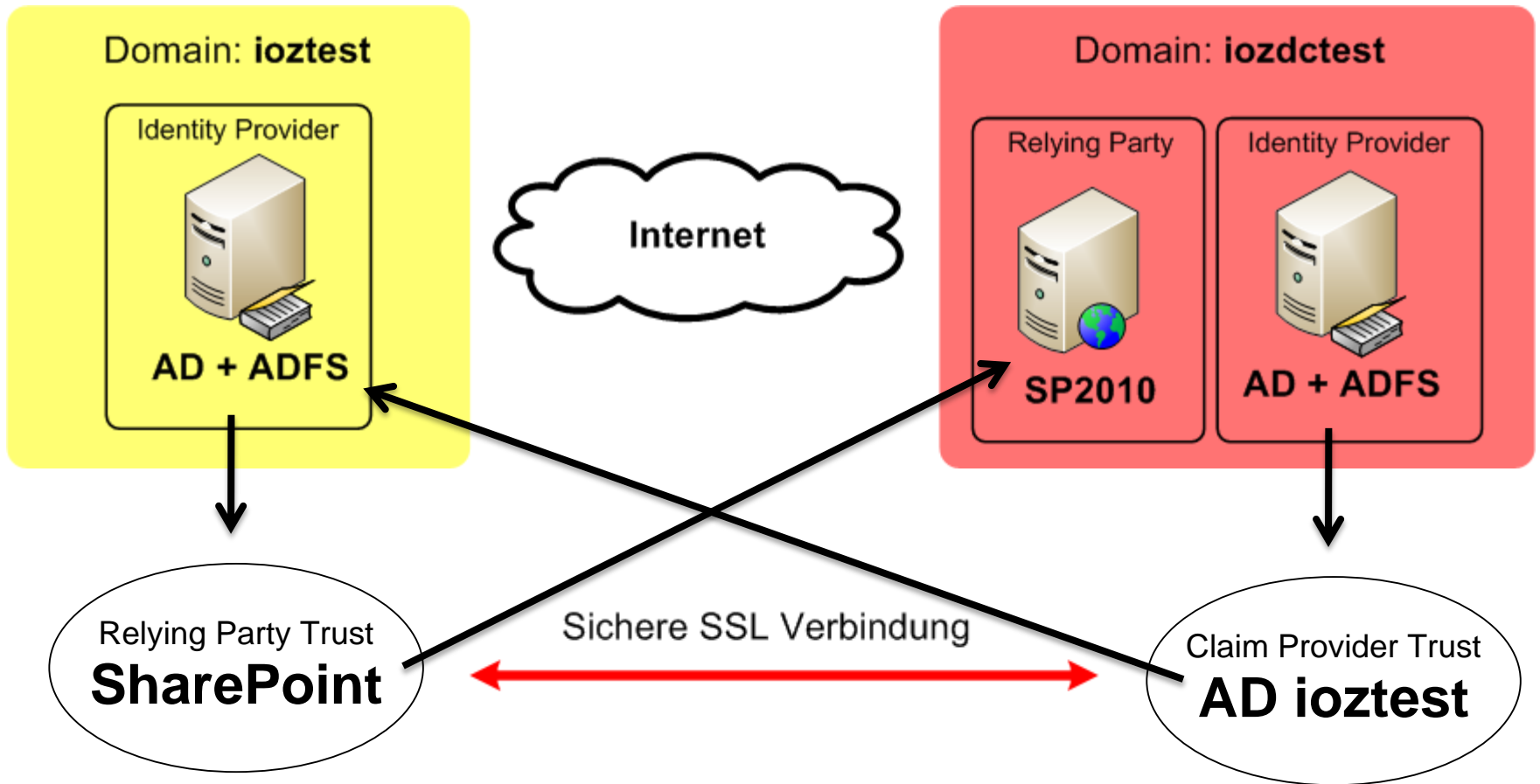




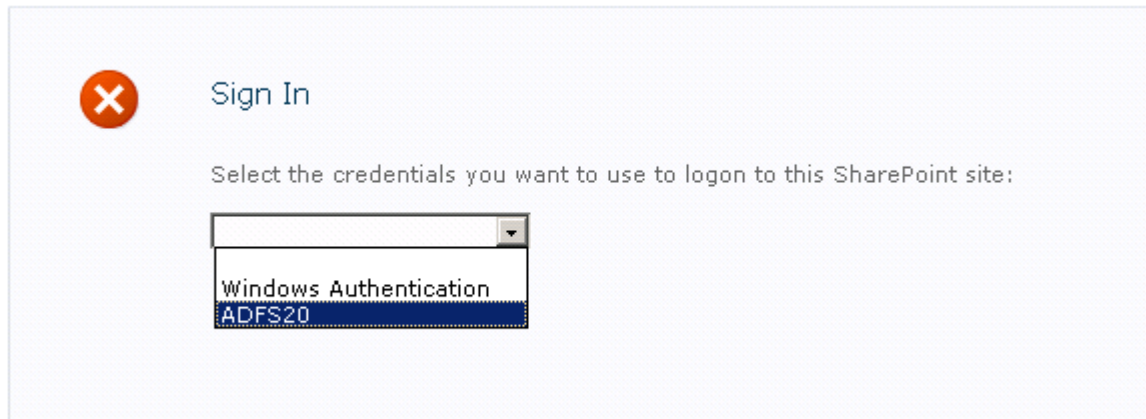


Live Demo





- SharePoint integrierter Identity Provider → Active Directory
- Erweitern mit zweitem Identity Provider → ADFS 2.0





ZUSAMMENSPIEL ADFS/SP2010

- Claims-basierten WebApp
- TrustedIdentity Provider erstellen via PowerShell
 - New-SPTtrustedIdentityTokenIssuer
 - Beinhaltet
 - Zertifikat: *ioztest*
 - Claim Set Mapping: *windowsaccountname*
 - Realm: *urn:sharepoint:intranet*
 - Anmelde URL: *https://sts.ioztest.ch/adfs/ls/*



Live Demo



- Gruppenauflösung funktioniert über Domaingrenze hinweg
- Office Integration, MySite, Suche funktioniert
- ADFS akzeptiert alles → Bsp.: Zuweisen eines Tasks an Mister X
- Auflösung unschön



- Good News für Hosting SharePoint Server im RZ

- ADFS 2.0 manuell herunterladen (Standardrolle ist ADFS 1.0!)
- Self Signed Zertifikate nicht empfehlenswert
- Service Account für ADFS muss zugriff haben auf Private Key von Token signing Zertifikat
- Nur via SSL!
- Für Produktiveinsatz
 - Federation Server Farm (redundant mit min. 2 ADFS Server)
 - Federation Proxy in DMZ (Security)

Fragen





Vielen Dank für Ihre
Aufmerksamkeit

24.11.2010

Joël Hasler IOZ DataCare AG

