5.– 8. September 2011
in Nürnberg

Herbstcampus

Wissenstransfer
par excellence

Wer bin ich?

Von Active Directory zu einer Windows Azure Applikation

Robert Eichenseer

conplement AG

Wer bin ich?

WIF oder von AD zu einer CloupApp

Robert Eichenseer
conplement AG

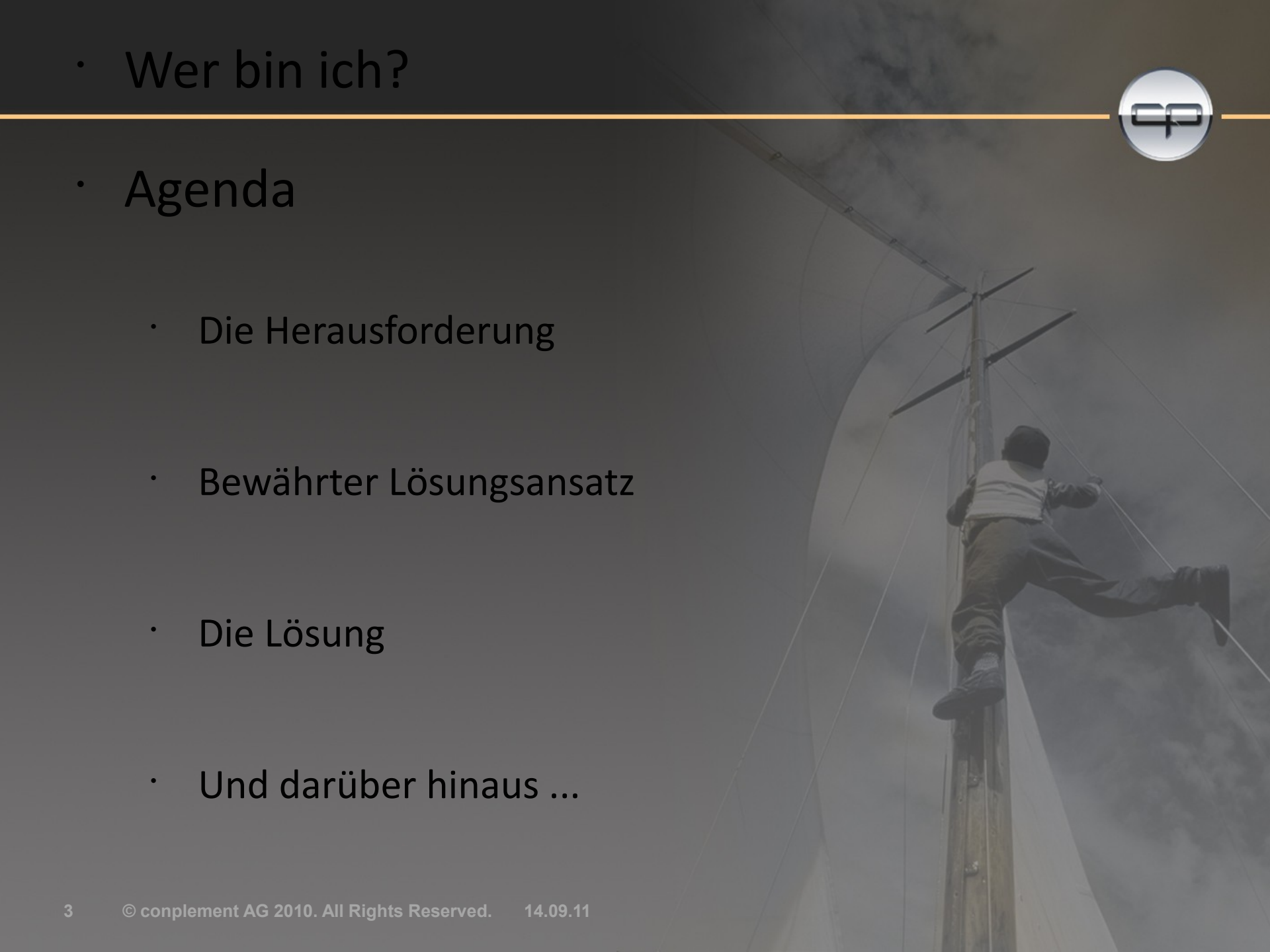
See# Party

- Wer bin ich?
- WIF oder von AD zu einer Cloud App

- 20. August 2011

- Robert Eichenseer
- robert.eichenseer@conplement.de

- Wer bin ich?
- Agenda
  - Die Herausforderung
  - Bewährter Lösungsansatz
  - Die Lösung
  - Und darüber hinaus ...



Die Herausforderung

Aktuelle Situation - User Authentication

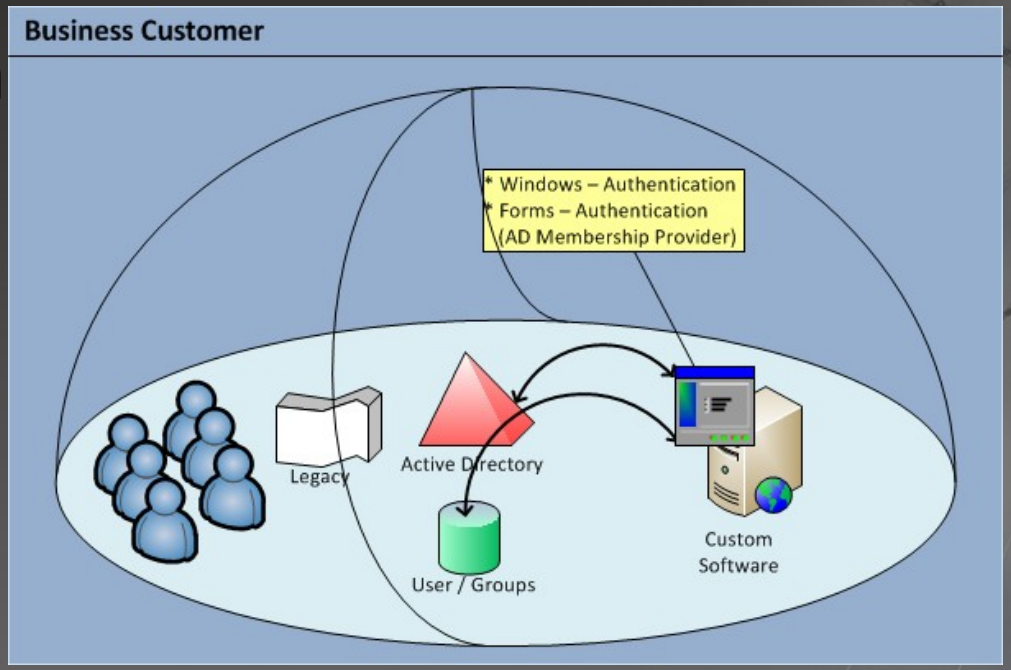
- **Private Situation**
  - Viele unterschiedliche User Credentials

- **Reise , Anmeldungen , Kommunikation , Shopping , Sparen , Social Network**

- **Unterschiedliche Logins (teilweise E-Mail, Username, ID …)**
- **Unterschiedliche Password-Policies (Lifetime / Complexity)**

Die Herausforderung

- Aktuelle Situation – Business Auth

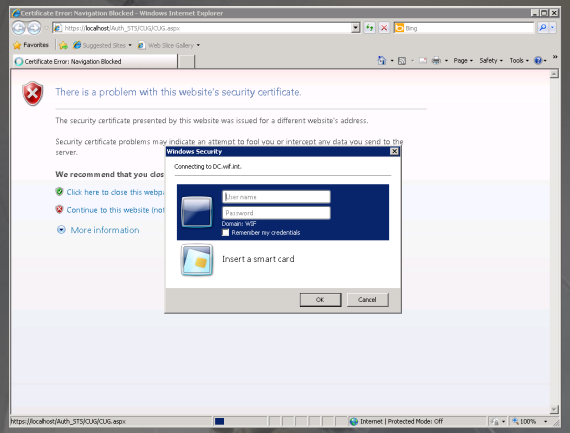


- **Legacy App + Authentication Infrastructure**
- **Single Sing-on muss erhalten bleiben**
- **AddOn on premise**
  - Benützt existierendes Active Directory
  - Neue proprietäre Infrastruktur

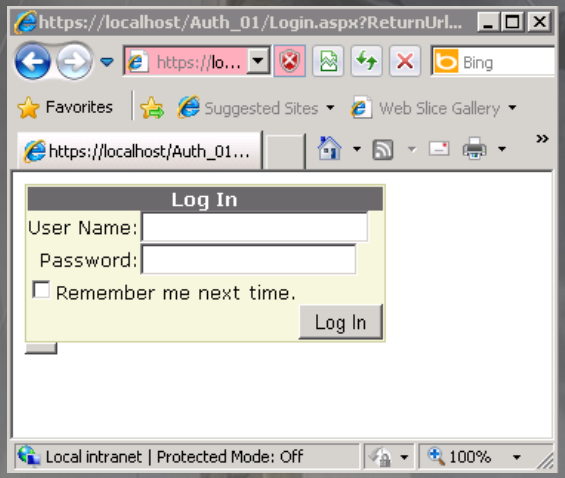
Bewährter Lösungsansatz

Authentication

- **Windows Authentication**
  - Anmeldedialog vom OS (vom Browser initiiert) wird angezeigt.
  - Benutzerdaten liegen in der AD vor

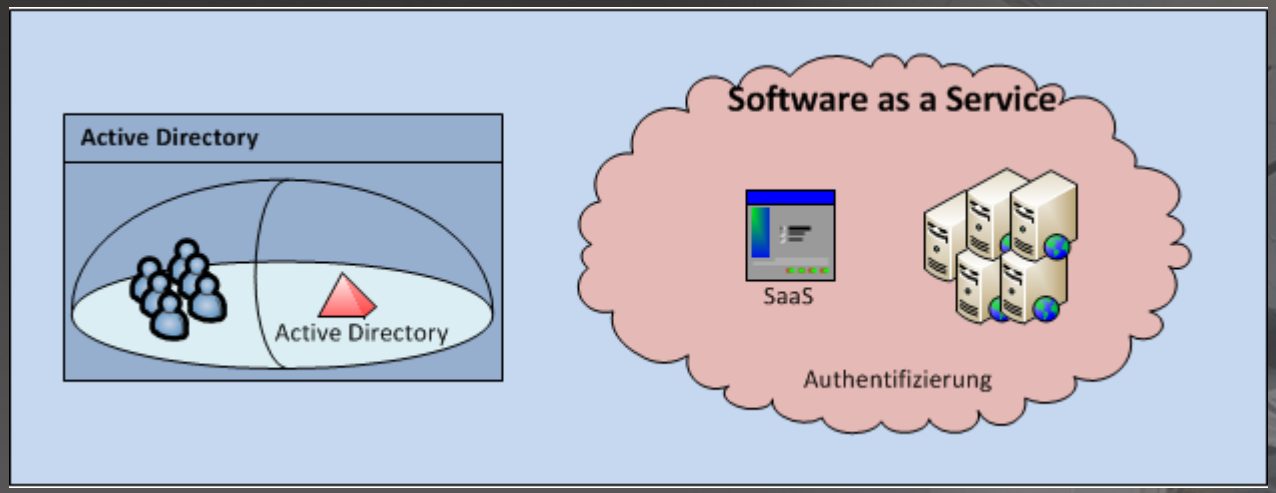


- **Forms Authentication**
  - Anmeldedialog kann frei designed werden.
  - User Control existiert
  - Benutzerdaten können in AD vorliegen (AD Membership Provider)
  - Benutzerdaten können in SQL Server DB gespeichert sein.



Die Herausforderung

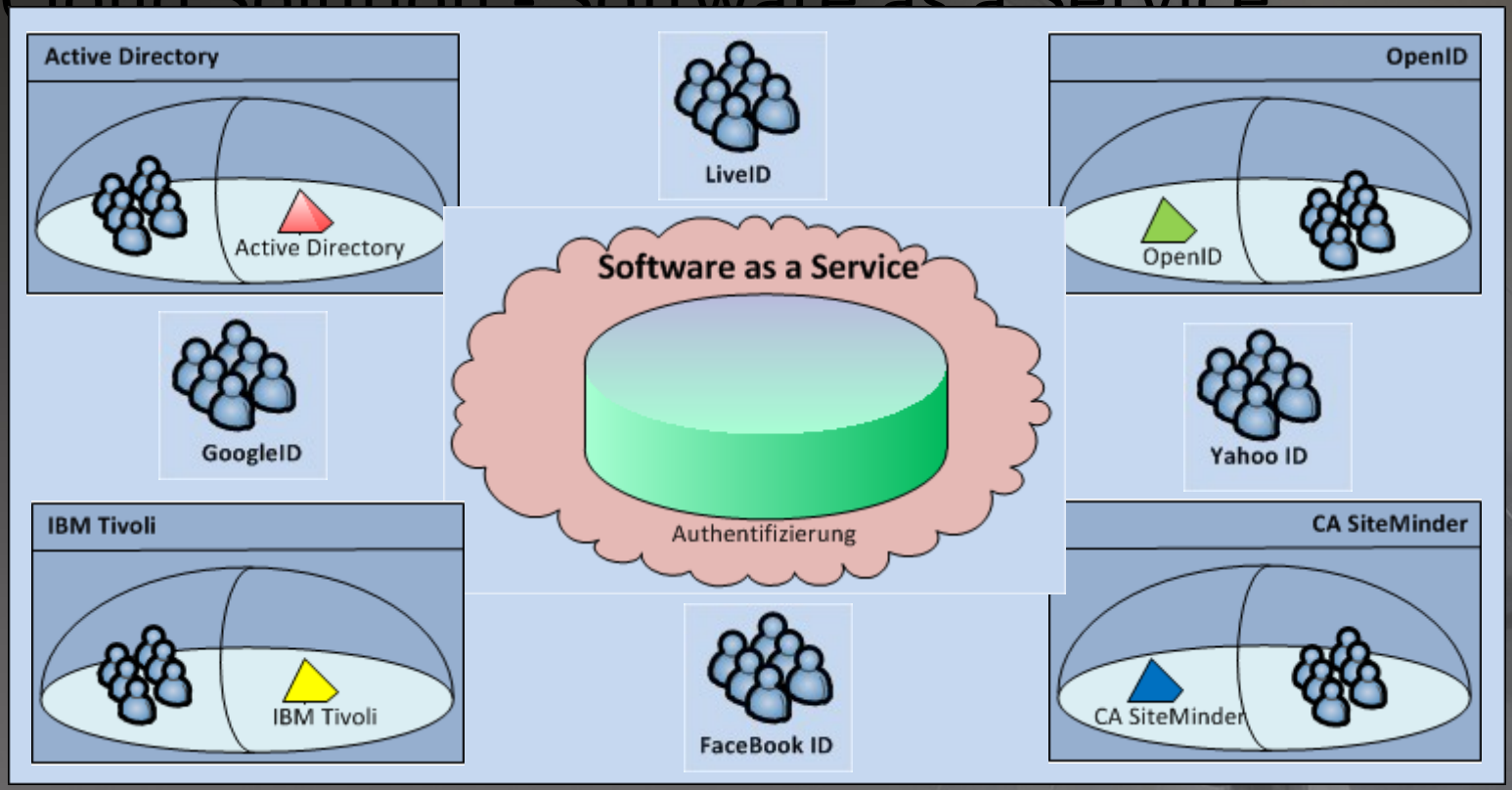
- Software as a Service
-



- **AddOn SaaS**
- **Single Sing-on muss erhalten bleiben**

Die Herausforderung

- Cloud Solution - Software as a Service



- **Key Feature Single Sign On muss erhalten bleiben**
  - Form Authentication mit lokaler DB
- **Code für nötige Authentifizierung bzw. Administration explodiert**
  - Software kann scheitern

Die Lösung

- IIdentity / IPrincipal

- 2002 * IPrincipal; IIdentity - .NET 1.0; ASP.NET
- 2006 * Security Token Claim – WCF
- 2009 * WIF (Windows Identity Foundation)

```
interface IClaimsPrincipal : IPrincipal
{
     ClaimsIdentityCollection Identities{get;}
}
interface IClaimsIdentity : IIdentity
{
     ClaimCollection Claims {get; }
     string NameClaimType {get; set;}
     string RoleClaimType {get; set;}
}
```

Einführung „Claims Based Authorization“

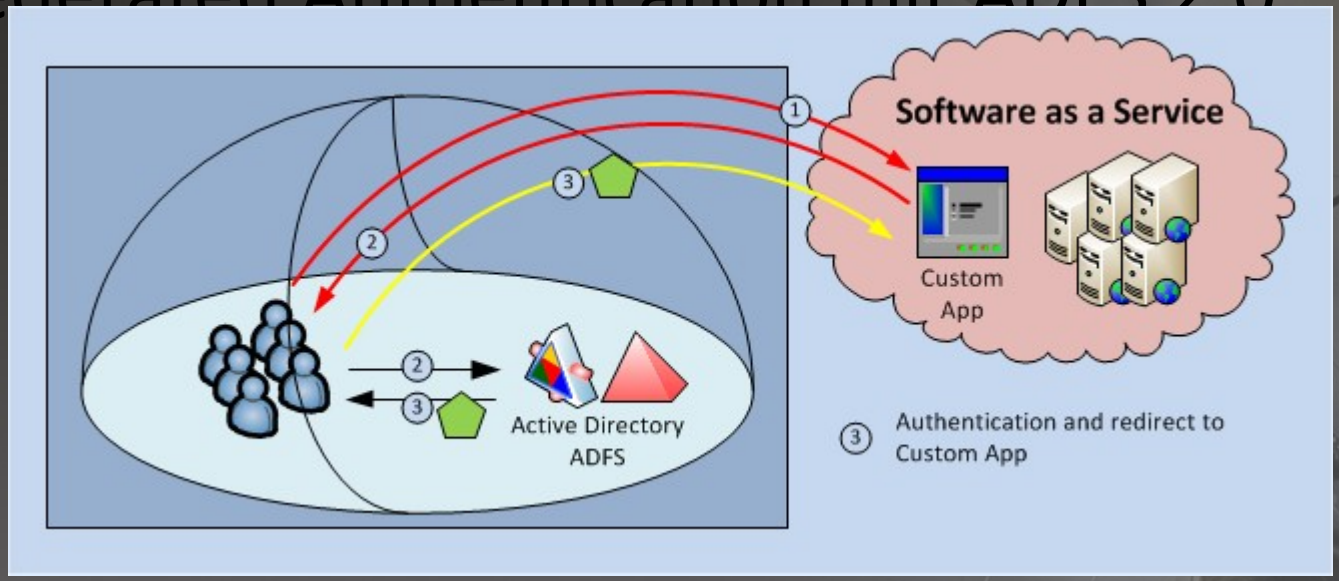
Die Lösung

Claims / ADFS

- **Rollen vs Claims**
  - AD vergibt Berechtigungen via Rollenzugehörigkeit
  - WIF definiert Claims
    - Bsp.:
      - „Bob ist ein Administrator“
      - „Die Email Adresse von bob ist robert.eichenseer@conplement.de“
      - „Bob darf neue Kunden hinzufügen“
      - „Sigi darf Dokumente nach ‚confidential‘ ablegen
    - Definition Claim
      - „Statement about an entity made by someone else“
    - Spezielle Claimtypen werden zu „Is-In-Role-Berechtigungen“ gemappt
  - Technisch: Collection von Name / Value Pairs
- **Erweiterung AD um „Token-Erzeugung“**
  - ADFS (Active Directory Federation Services)

Die Lösung

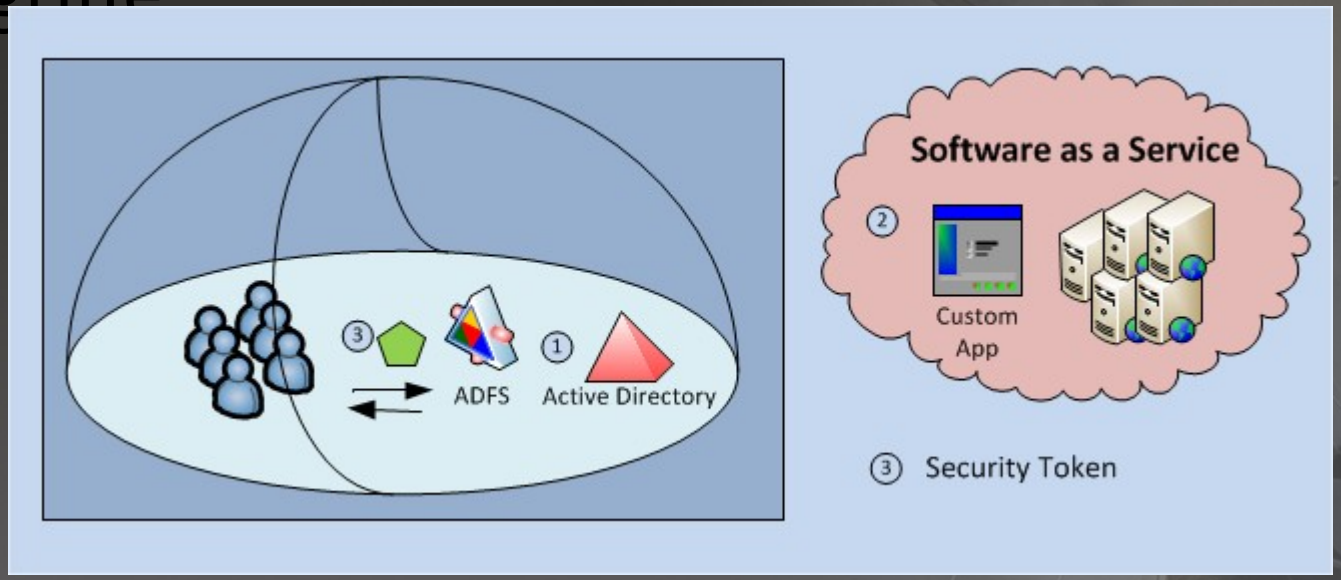
- Federated Authentication mit ADFS 2.0
-



- **Steps**
  - (1) Benutzer fordert Seite / Funktionalität an.
  - (2) Custom App „redirects“ zu lokalem ADFS
  - (3) Benutzer authentifiziert sich an loker AD viad ADFS und erhält Security Token; lokaler ADFS „redirects“ zu ursprünglicher Seite / Funktionalität incl. Security Token, welches zur Authentifizierung verwendet werden kann.

Die Lösung

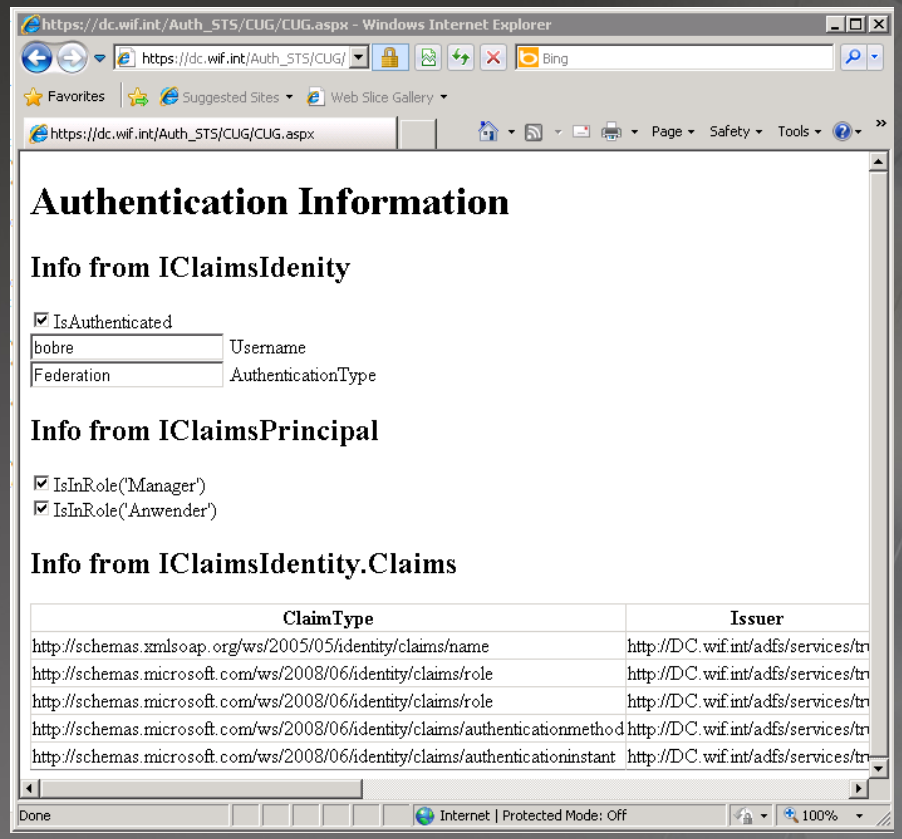
- Begriffe
-



- (1) Secure Token Service (STS) / Identity Provider / Issuer
- (2) Relying Party / Resource Provider
- (3) Security Token, SAML Token

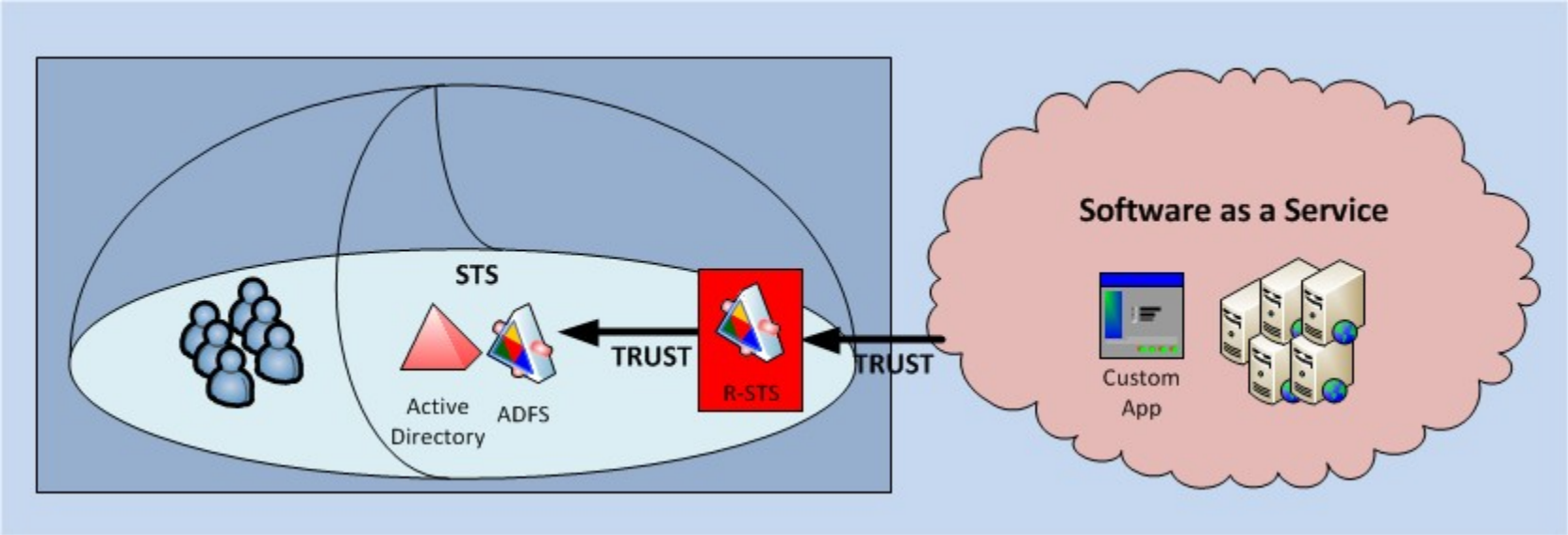
Die Lösung

- Demo Applikation STS Authentifizierung



Und darüber hinaus

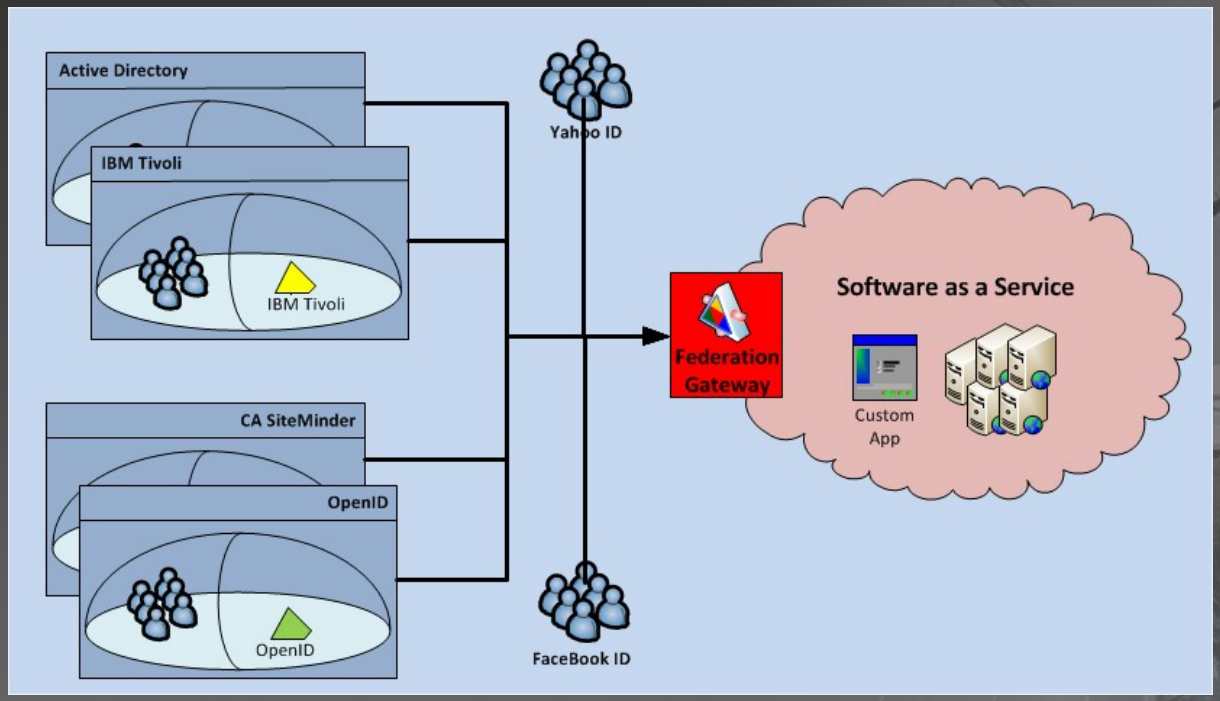
- Resource STS
-



- **Acitve Directory wird von technischen Admins gepflegt**
  - Meist sehr sichere statische Prozesse zur Pflege der AD
- **Trennung von Authentication / Authorization**
- **Kaskadierung von beliebig vielen STS**

Und darüber hinaus

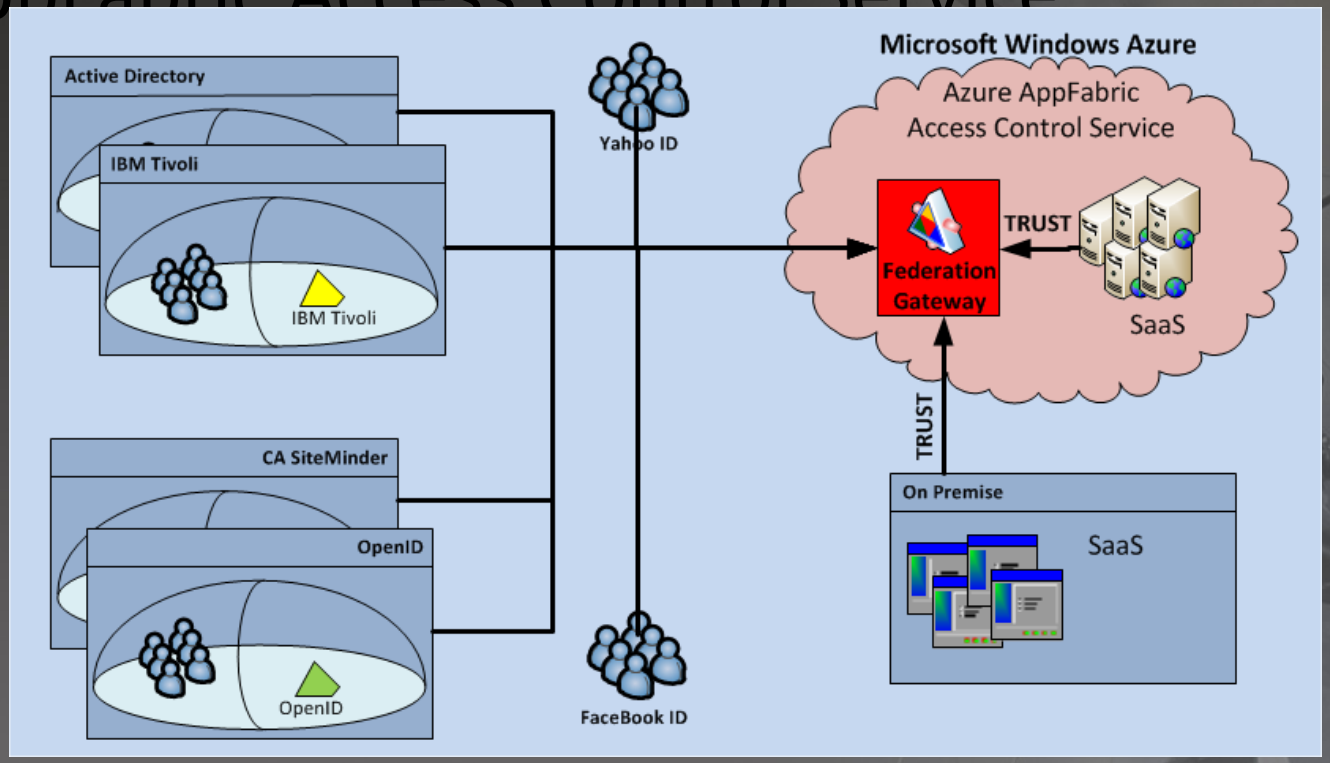
- Federation Gateway
-



- **Claims Converter**
  - Technisch (SAML 1.0 -> SAML 2.0; ...)
  - Logisch (Claims Transfer; ...)

Die Lösung

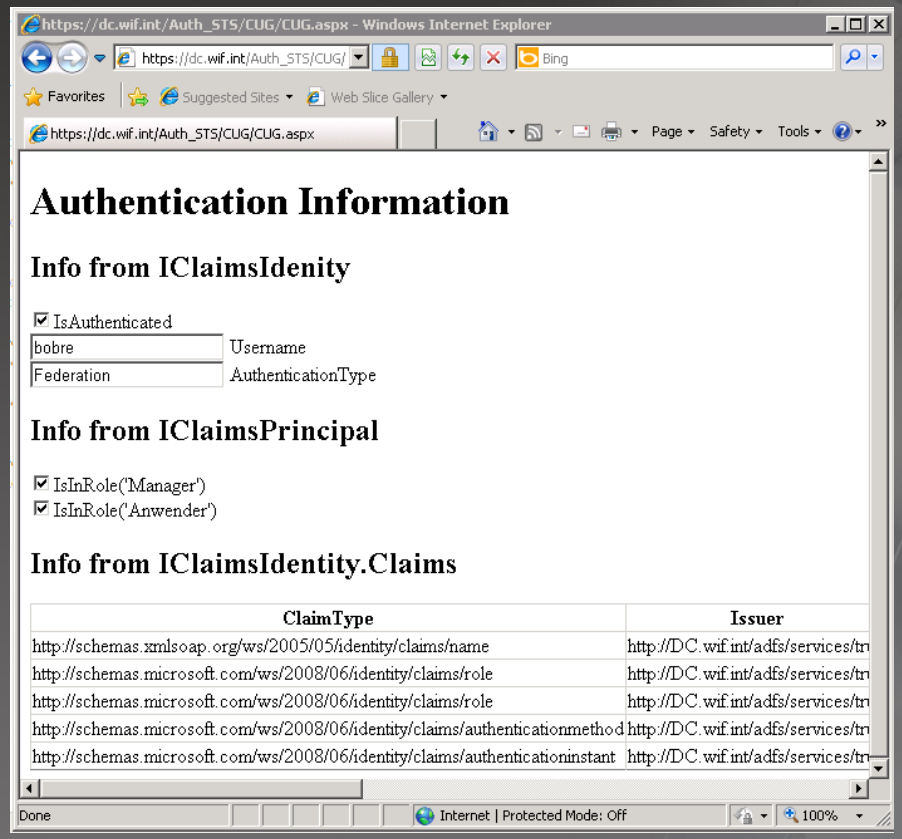
- AppFabric Access Control Service



- **Federation Gateway innerhalb der Azure Cloud**

Die Lösung

- Demo Applikation ACS – Social Identities



Zusammenfassung

WIF; Single sign-on

- **Single Sign On**
  - WIF stellt Abstraktion für Claims Based Authentication zur Verfügung
  - AD Authentifizierung kann transparent in Cloud übernommen werden
- **ADFS 2.0**
  - STS
  - R-STS
  - Federation Gateway
- **Windows Azure AppFabric Access Service**
  - Cloudbasiertes Federation Gateway
  - Unterstützung für Social Identities (Facebook, LiveID, GoogleID ...)

Ich freue mich auf Fragen

- Robert Eichenseer
- www.conplement.de