ADFS

Oliver Ryf

Partner: Microsoft Computerworld

DIGICOMP

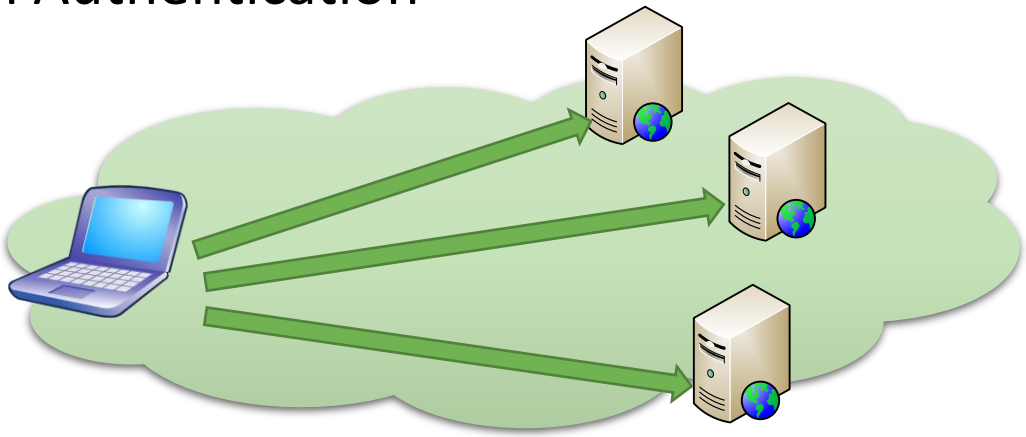
Agenda

- Begrüssung
- Vorstellung Referent
- Active Directory Federation Services (ADFS)
- F&A
- Weiterführende Kurse

Vorstellung Referent

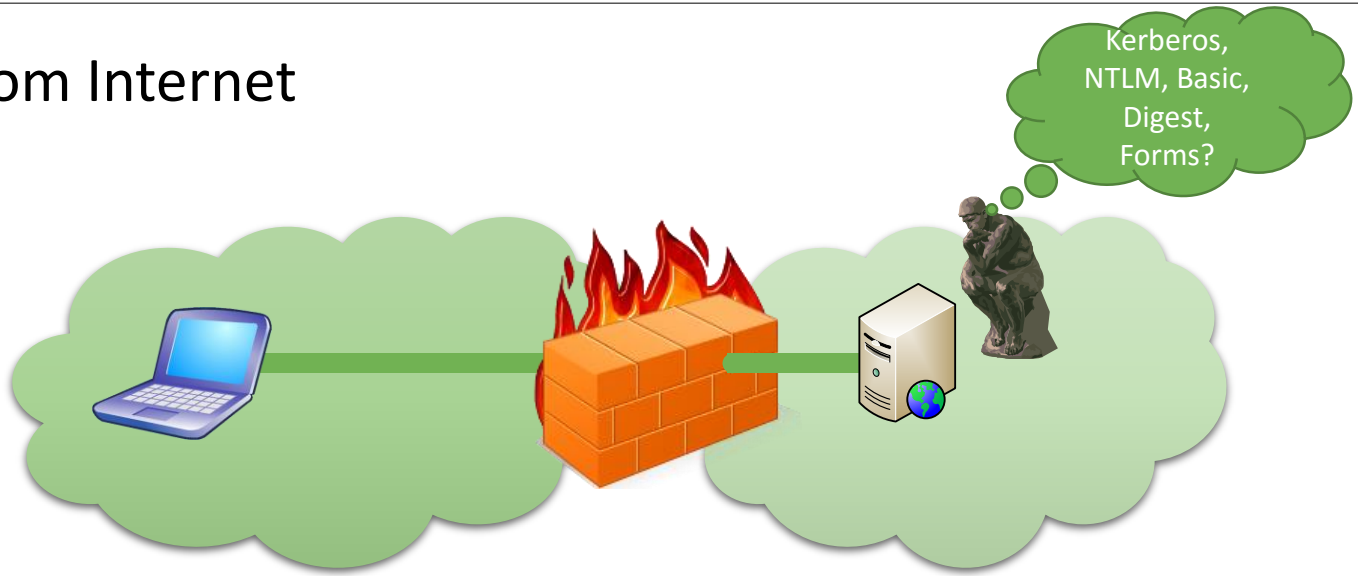
- Seit 1991 IT-Trainer
- 1995 MCSE und MCT
- Seit 2000 diverse Projekte im Bereich Windows/Office Migrationen, Active Directory, Infratruktur, Hyper-V und Azure Cloud
- Seit 2006 Trainer bei Digicomp
- Seit 2014 Principal Consultant und Cloud Archiect bei UP-Great AG Fehraltorf

Application Authentication



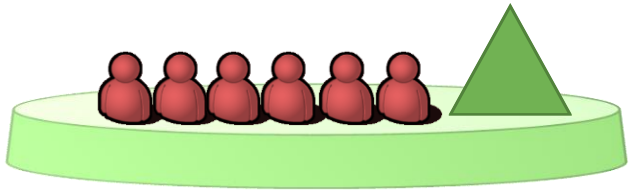
- Innerhalb Ihrer Umgebung bietet Ihnen die Windows Authentication ein Single Sign-On für alle Applikationen
  - Windows Authentication liefert die erforderlichen Informationen über den Benutzer und seine Gruppenzugehörigkeiten

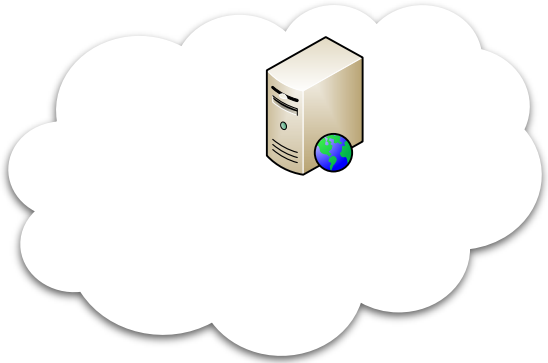
Zugriff vom Internet



- Ohne VPN, DirectAccess oder eine Authentication Proxy Lösung
  - Kerberos funktioniert nicht mehr
  - Entwickler brauchen ein anderes Authentisierungs-Modell

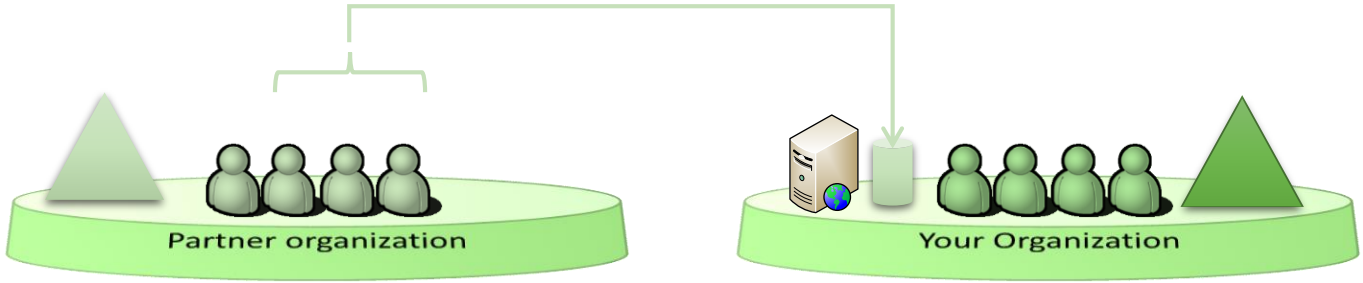
Application in der Cloud





- Wie gehen wir mir Authentisierung um, ab dem Zeitpunkt ab dem wir unsere Applikationen in die Cloud transferieren?
- Ganz Neu - Azure AD Domain Services!

Zugang für Geschäftspartner



- SIE verwalten für jeden Benutzer Ihres Partners, der auf Ihre Geschäftsapplikation zugreifen will, einen Account inkl. Profil
- SIE müssen den Account pflegen
  - Werden Sie bei Änderungen von Ihrem Partner informiert?
- Noch ein Login und noch ein Passwort für die Benutzer

Die Antwort

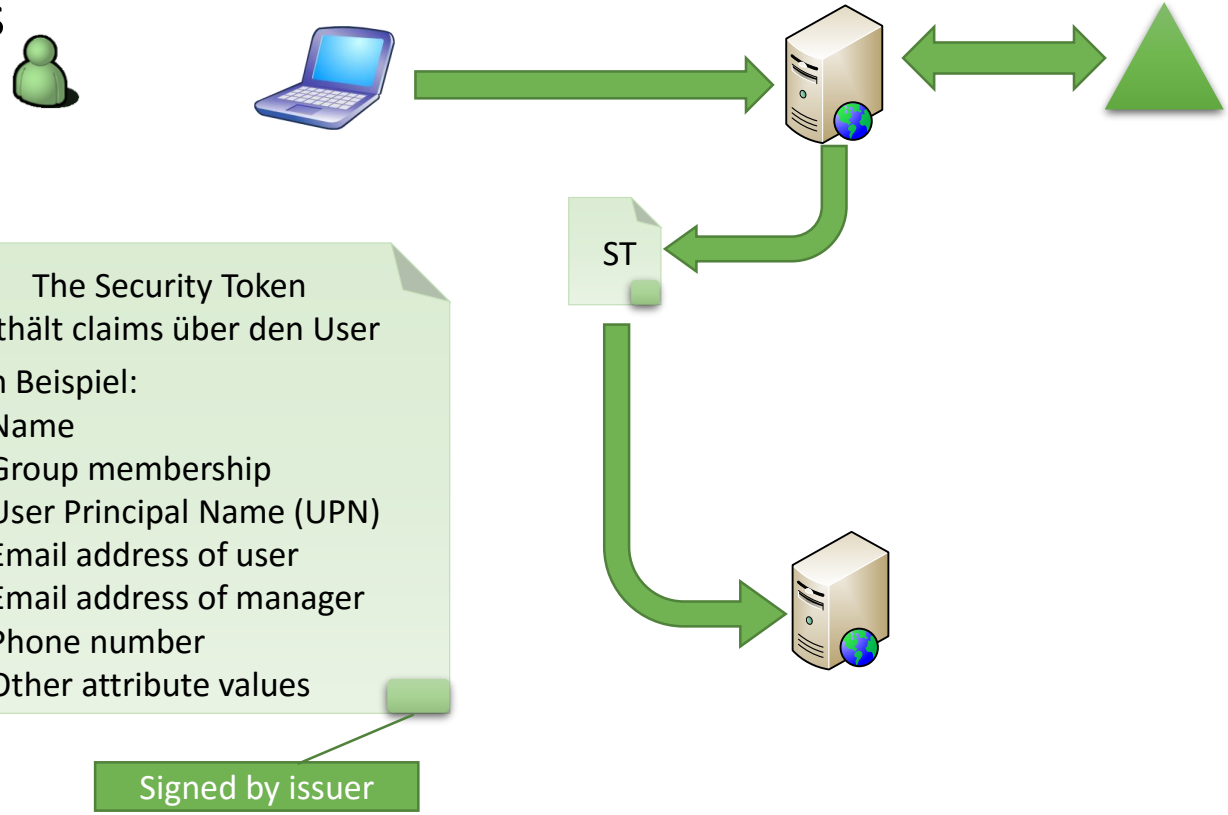
- Erstellen Sie ein Identity (inklusive Authentication) Framework, das von allen Ihren Applikation verwendet warden kann, unabhängig davon, wo sich diese befinden
- Erlauben Sie den sogenannten Identity Token mehr Informationen zu übermitteln als lediglich der Benutzer und seine Gruppenzugehörigkeiten
- Vertrauen Sie Ihren Partnern, dass sie deren Benutzer authentisieren
- Verwenden Sie eine Lösung, die auf Industrie Standards setzt
- Stellen Sie diese für Browser und Web Services bereit

Die Lösung

- Verschieden Anbieter auf dem Markt…
- Microsoft Active Directory Federation Services
  - The latest release AD FS v 2.0

Federation of Identity

Key Concepts



Claims-Aware Application

- Die Applikation autorisiert basierend auf den Claims, welche im Security Token enhalten sind
  - Keine Notwendigkeit mehr eine Authentisierung zu Machen
- Der gleiche Authentisierungs-Mechanismus für Applikationen
  - Unabhängig ob On-Premise im Intranet oder in der Cloud
  - Claims können von der eigenen Organization genauso akzeptiert werden, wie solchen von Bernutzern von vertrauten Partnern

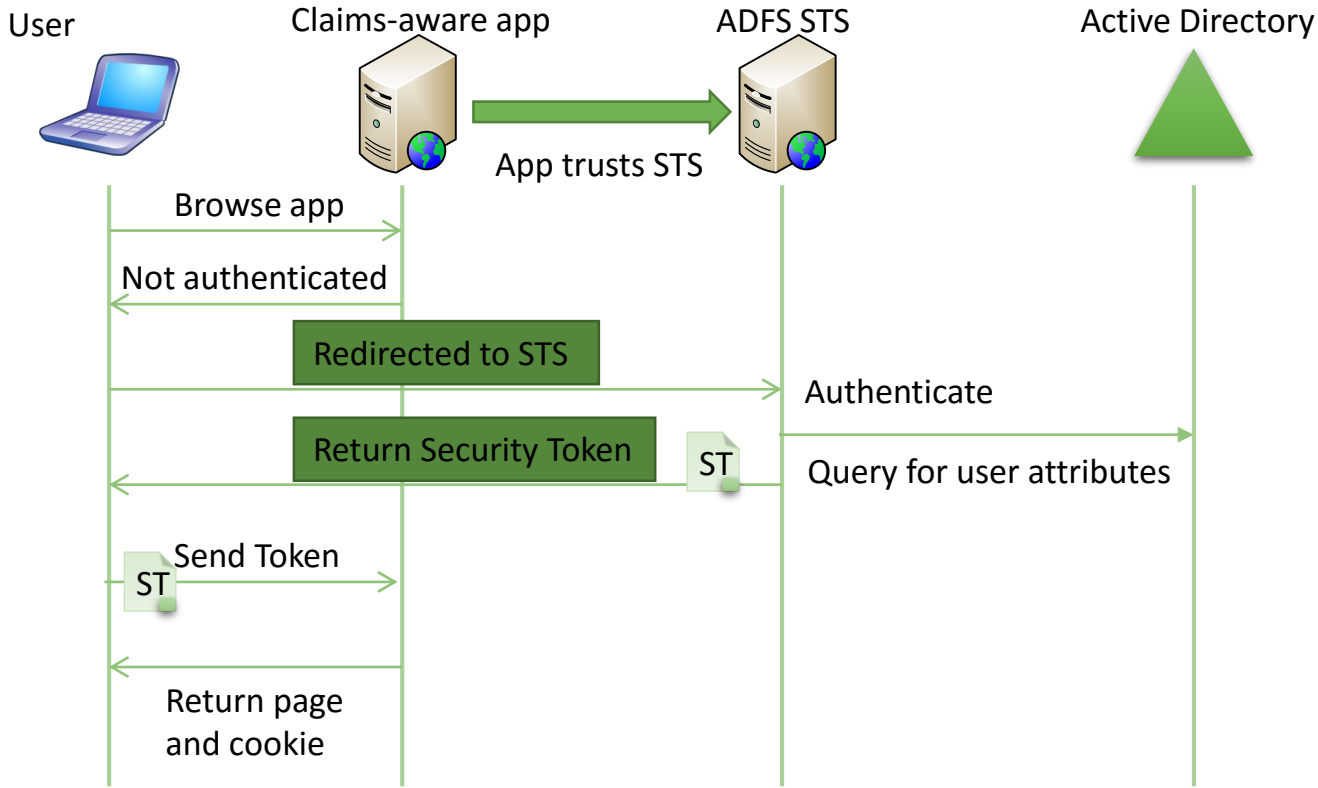
Building Claims-Aware Applications

- Window Identity Foundation (WIF) bietet das gemeinsame Programming Modell für Claims
- SharePoint Services unterstützt seit der Version 2007 claims-based Identities

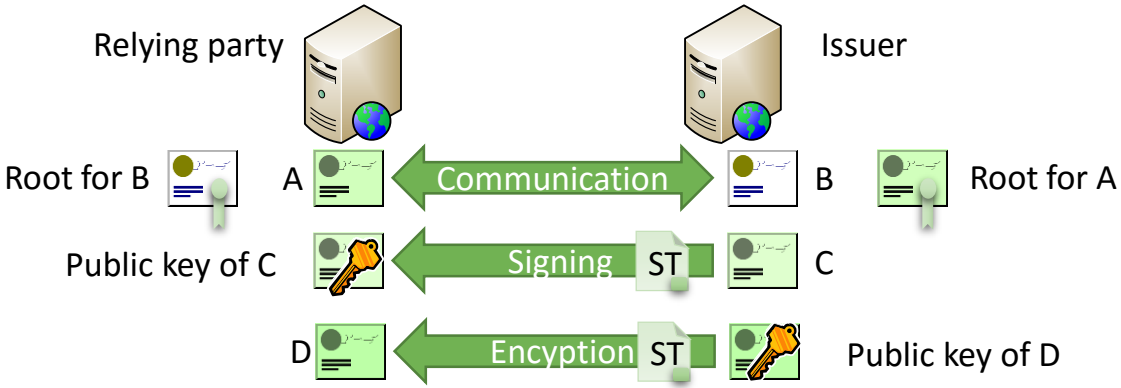
Standards and Protocols

- ADFS v 2.0 unterstützt sowohl aktive wie passive Clients
  - Active Klients interagieren mit Web Services
  - Passive Klients interagieren mit Browser Requests
- Support für Industry Standard Protokolle erlauben das Zusammenspiel mit Third-party Lösungen
  - WS-Federation
    - SharePoint braucht WS-Federation v 2
  - SAML 2.0

Was ist ein Passive Client



X.509 Certificates



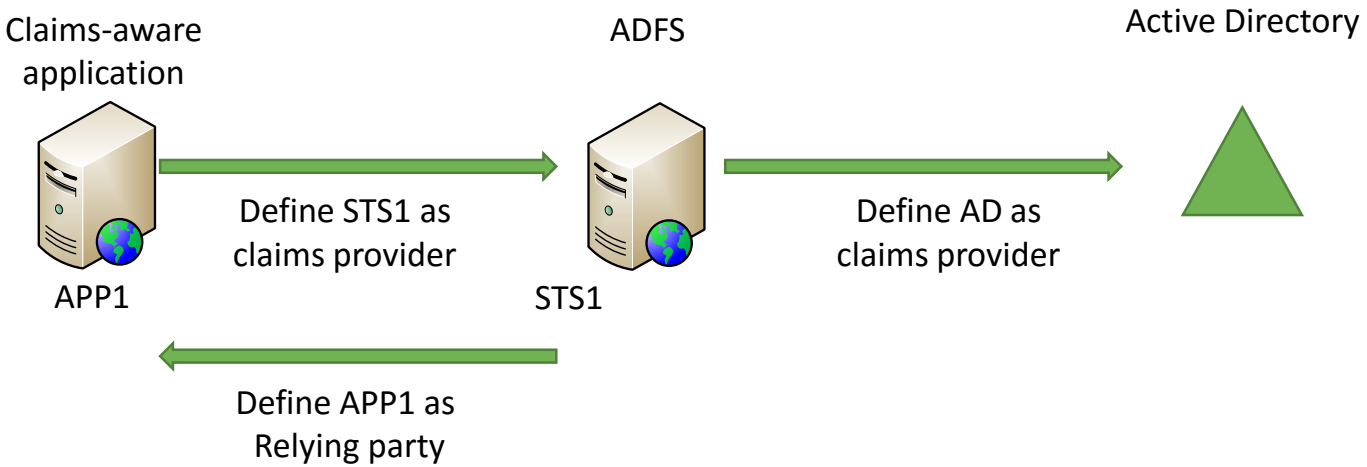
- Trust is managed through certificates
- Certificates for
  - HTTPS Communications
  - Security token signing and encryption
- Require PKI for A & B certificates, C & D can be self-signed by ADFS server

Federation Metadata

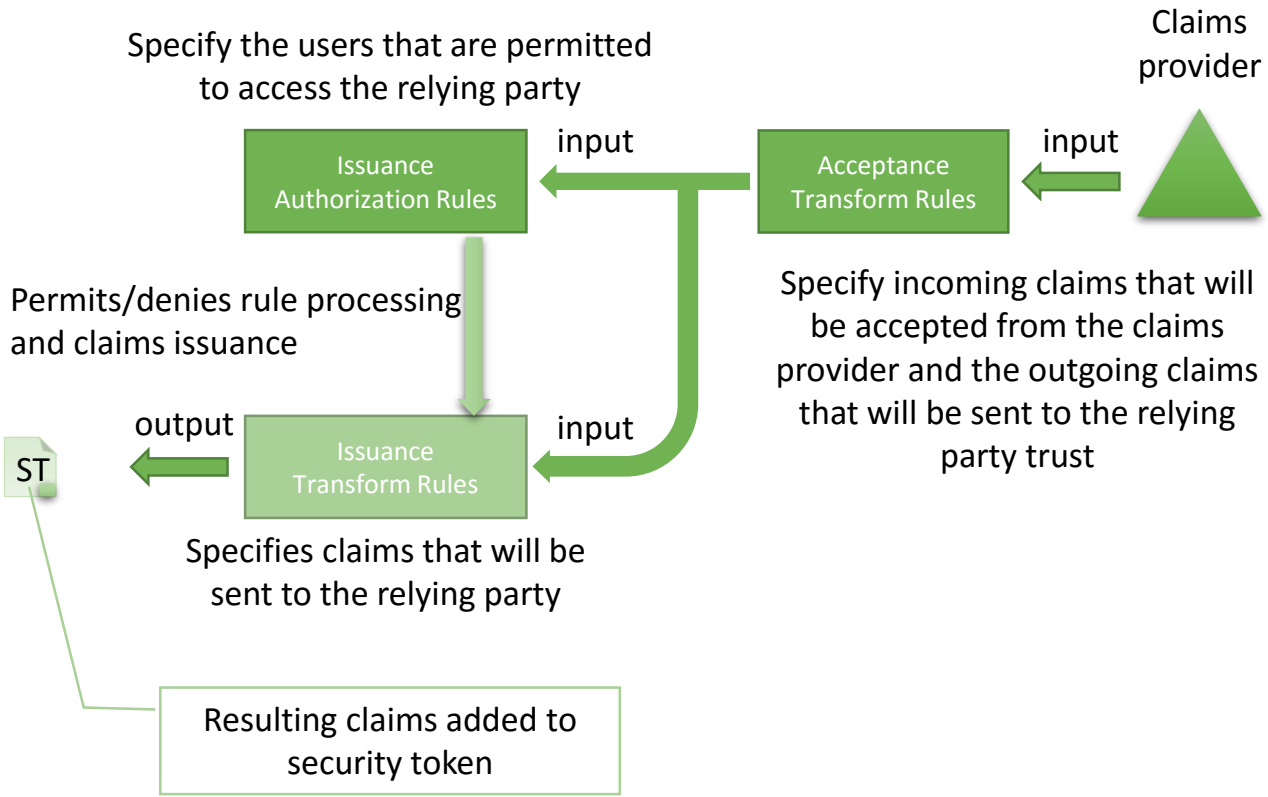
- Beim Aufbau des Issuer / Relying Party Trust, müssen beide Beteiligten in ihrer Konfiguration die folgenden Punkte berücksichtigen
  - End-points für die Kommunikation
  - Claims offered by Issuer (dort wo die Accounts liegen)
  - Claims accepted by replying party (dort wo die Ressource ist)
  - Public keys for signing and encryption
- Diese Informationen können entweder Manuell oder automatisch via Austausch der Federation Metadaten konfiguriert werden
  - Federation Metadaten können automatisch aktualisiert werden

DEMO

Configuration



Claims Pipeline



Frage - Wo wird ADFS überall eingesetzt?

- Federation Trusts
- Workplace Join
- Workfolders
- Webapplication Proxy
- …

Was kommt als Nächstes

- Azure AD B2B
- Azure AD B2C

F&A

Weiterführende Kurse

- Configuring Advanced Windows Server 2012 R2 Services («L32»)
- Implementing an Advanced Server Infrastructure («L34»)