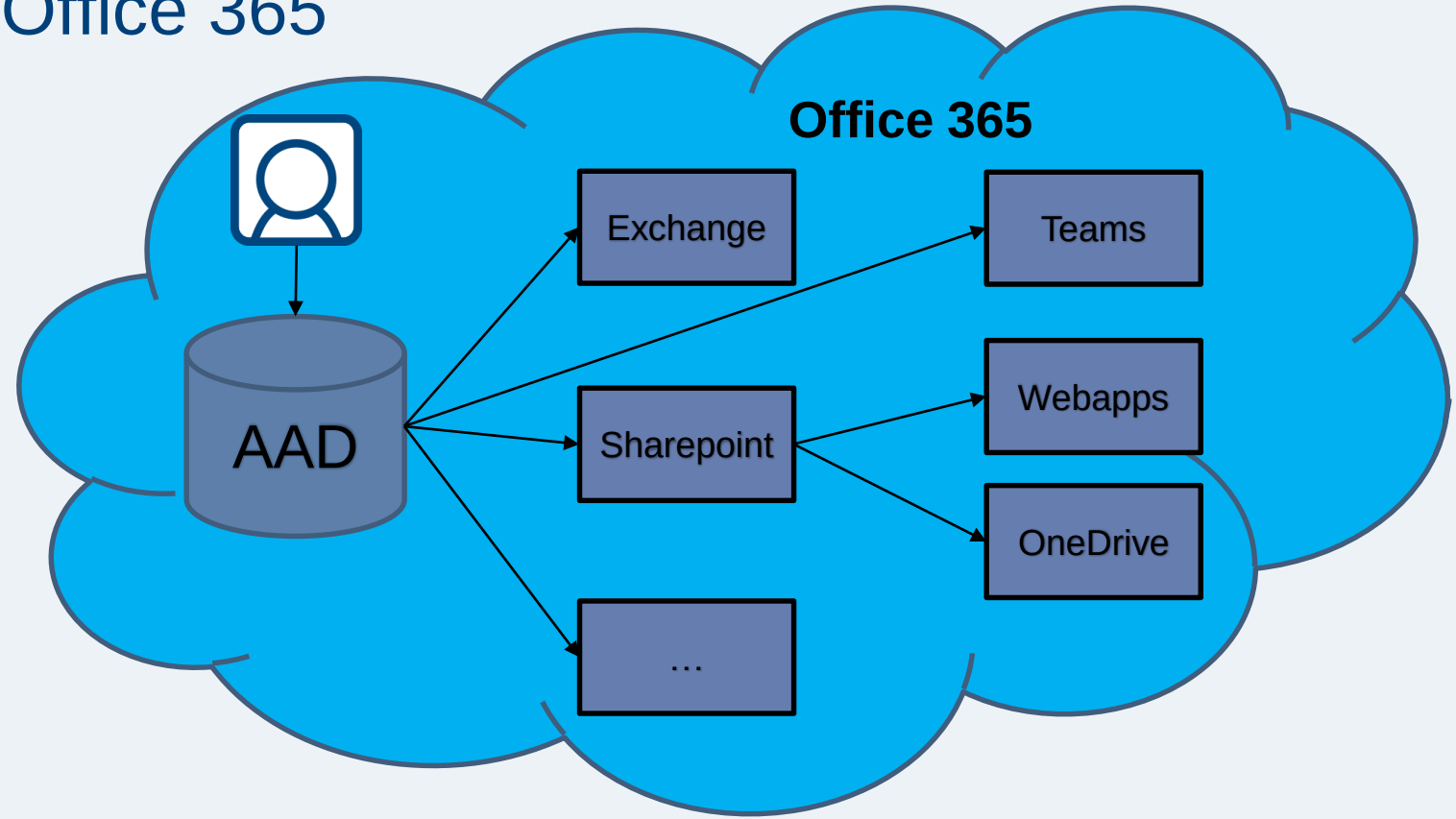
# Office 365 - ADFS - Shibboleth

71. DFN-Betriebstagung 24./25.09.2019

# Office 365


Office 365
Exchange
Teams
AAD
Sharepoint
Webapps
OneDrive
…

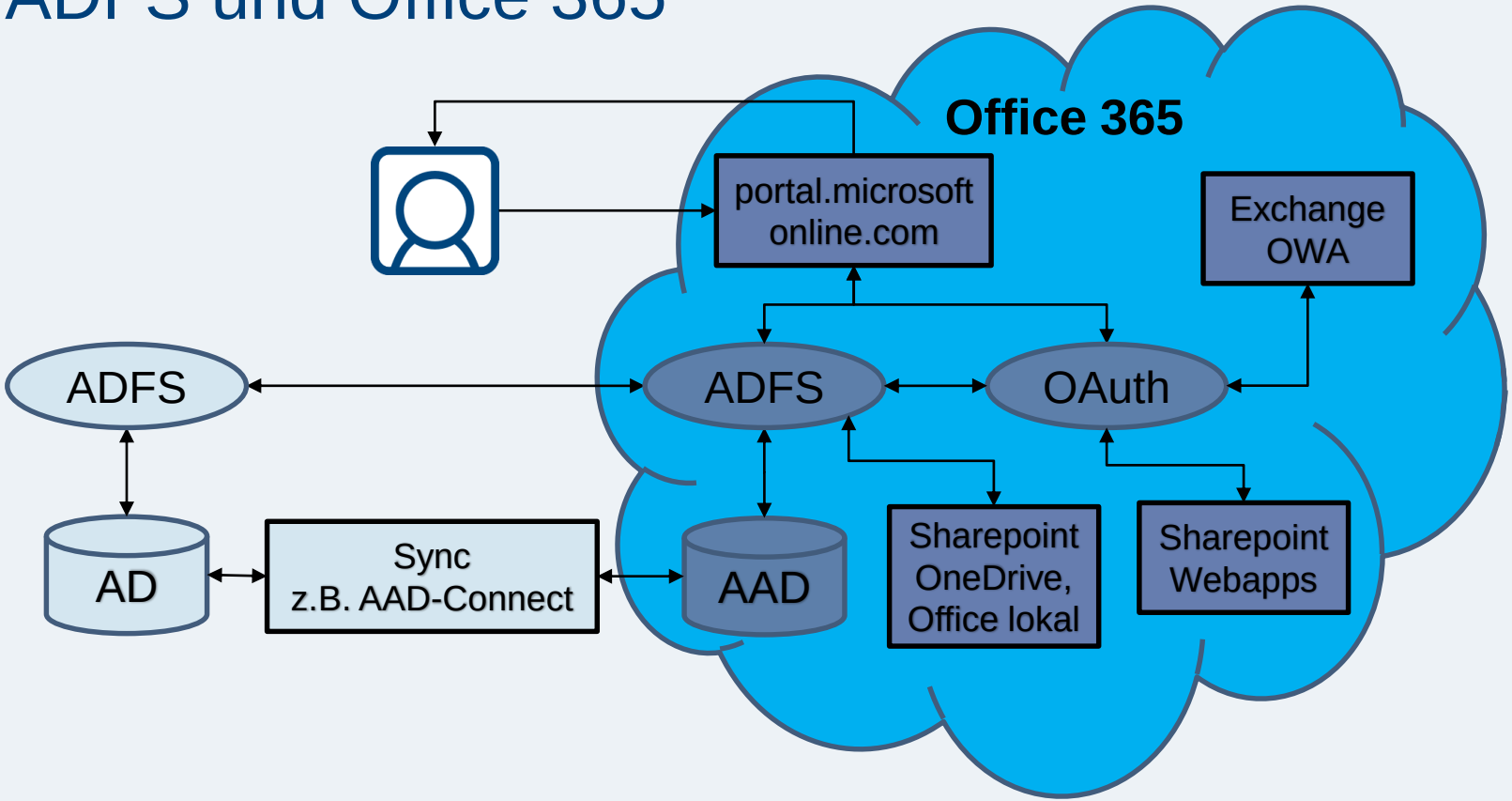
# Sync AAD (Azure Active Directory)

- Idealer Weise föderiert per Shibboleth
- Praxis (soweit mir bekannt):
  - stets Sync mit lokalem IAM und AAD
  - teilweise eigenes Passwort in Cloud ➔ keine Nutzung der AAI
  - Shibboleth prinzipiell unterstützt, aber nicht alle Funktionen von Office 365 vollständig nutzbar, für reine Exchange-Nutzung wohl ausreichend
  - Vollständige Funktionen nur mit ADFS (Active Directory Federation Services) gewährleistet

# ADFS (Active Directory Federation Services)

- Funktionsweise ähnlich Shibboleth - spricht „Microsoft-SAML“
- Bestandteil von Windows-Server – Achtung: Versionsupdate = Serverupdate
- Authentifizierungs- und Attributverzeichnis Active Directory (Standard)
- Attributquellen: AD, LDAP, Datenbanken oder
- SAML-Anbieter als Anspruchsanbieter (Authentifizierung und Attribute)
  ➔ ADSF als Proxy einsetzbar

# ADFS und Office 365



# ADFS und Shibboleth

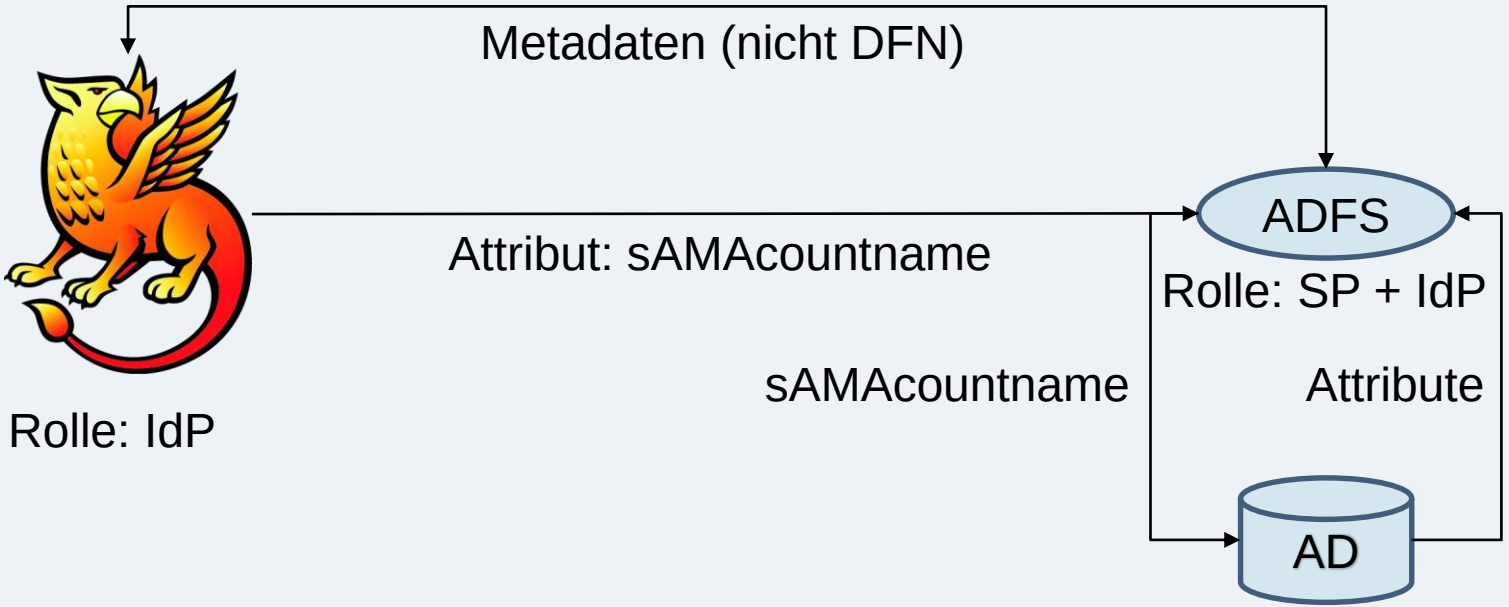


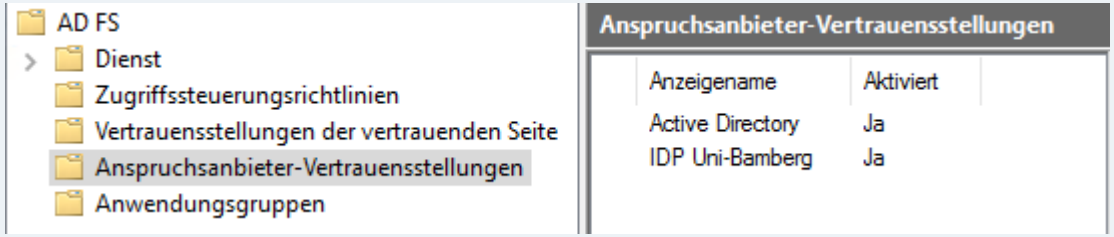

Bild: https://shibboleth.net

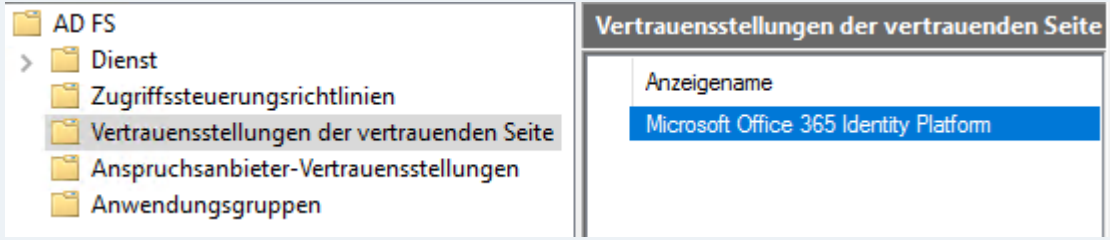
# ADFS und Shibboleth

- attribute-resolver.xml

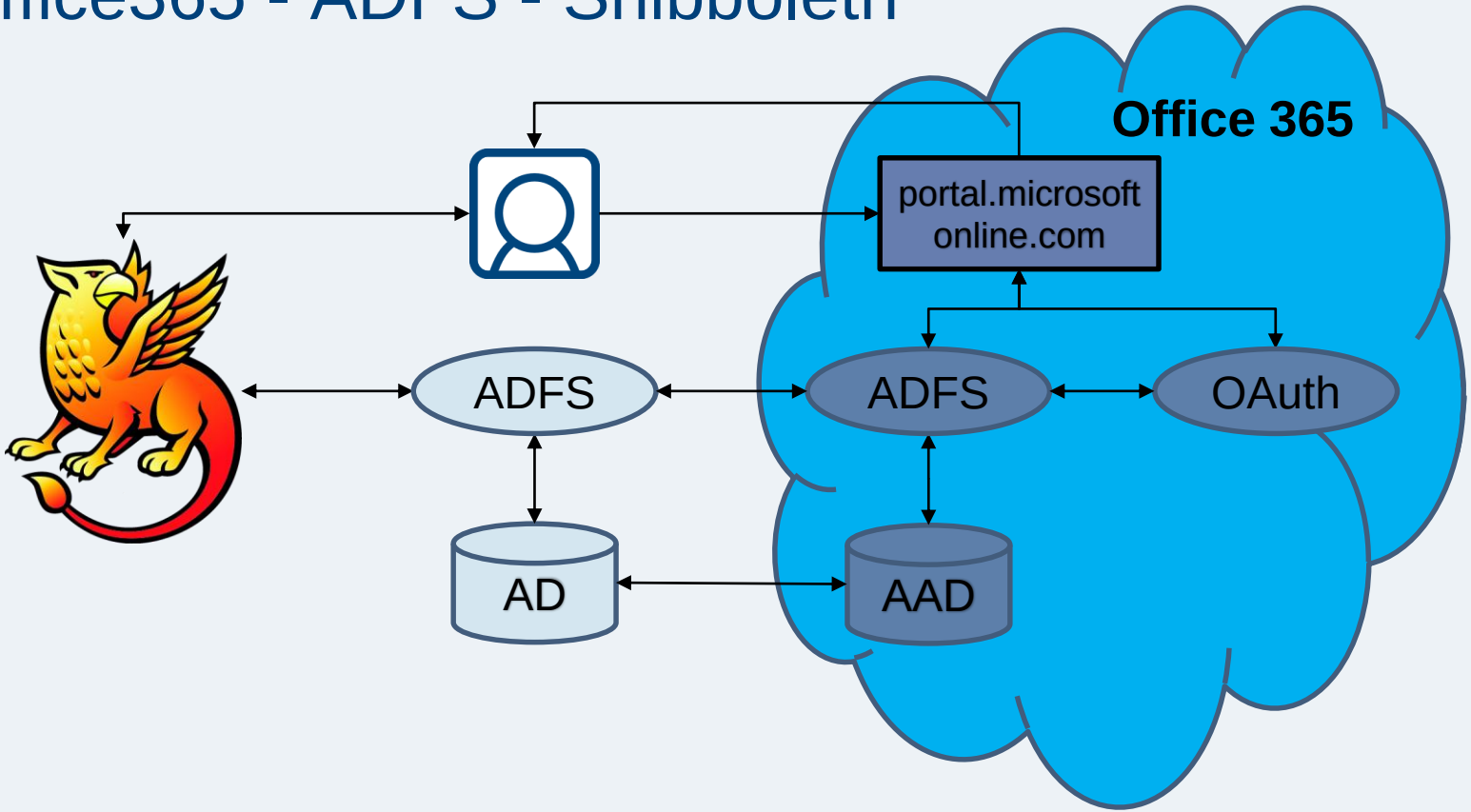
```
<AttributeDefinition xsi:type="Simple" id="sAMAccountName">
        <InputDataConnector ref="myLDAP" attributeNames="uid" />
        <AttributeEncoder xsi:type="SAML2String"
        name="urn:oid:1.2.840.113556.1.4.221" friendlyName="sAMAccountName"
        encodeType="false" />
</AttributeDefinition>
```

# ADFS und Shibboleth



# Office365 - ADFS - Shibboleth



# Demo

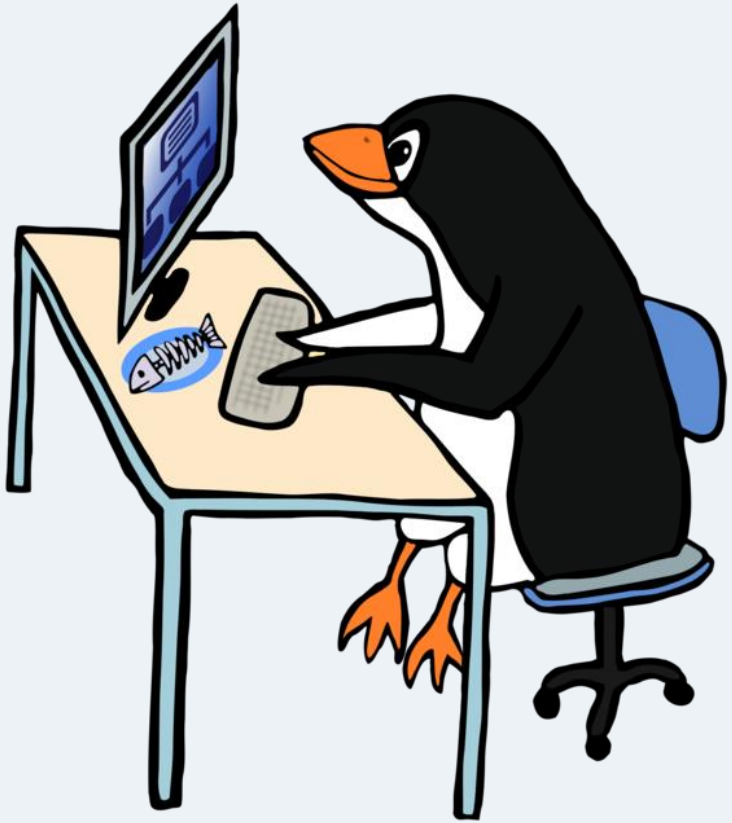


Bild: https://flyclipart.com

# Wirklich so einfach?

- Natürlich nicht!
- Aber: Alles ist lösbar!

# Probleme und Lösungen ADFS

- sAMAccountname allein reicht nicht zum Auslesen AD
  - ✓ Claimrule für Office 365 Identy Plattform anpassen:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/UPN",
"http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"), query =
"samAccountName={0};userPrincipalName,objectGUID;{1}", param = regexreplace(c.Value,
"(?<domain>[^\\]+)\\(?<user>.+)", "${user}"), param = c.Value);
NACH
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname" =>
issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/UPN",
"http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"), query =
"samAccountName={0};**userPrincipalName,objectGUID;<<NetBios-Domain>>\{0}**", param =
regexreplace(c.Value, "(?<domain>[^\\]+)\\(?<user>.+)", "${user}"), param = c.Value);
Beispiel: **userPrincipalName,objectGUID;uni-bamberg\{0}**"

# Probleme und Lösungen ADFS

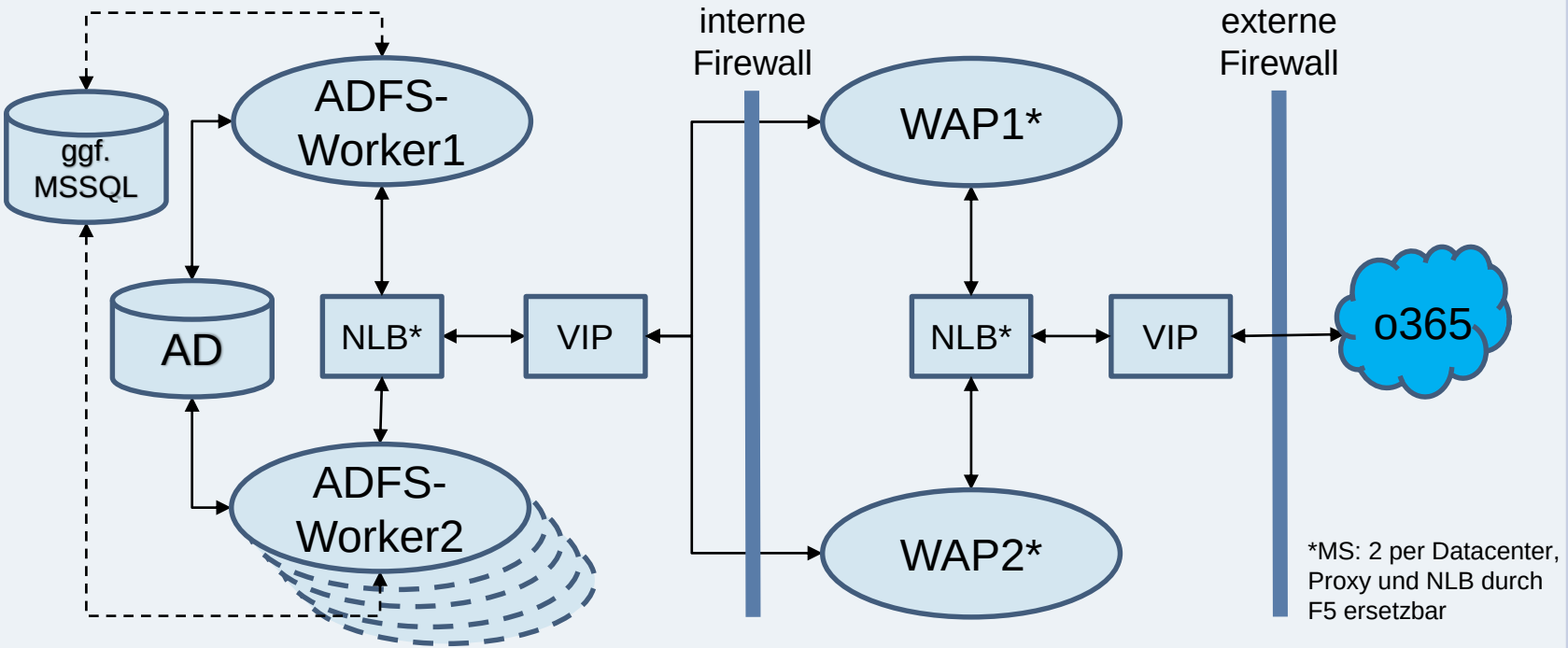
- Datenschutz ggf. problematisch
  - ✓ sorgfältige! Konfiguration AAD Connect synchronization services (per default sync all to cloud!) oder
  - ✓ Eigenständiges AD aus IAM provisionieren
- portal.microsoftonline.com und Shibboleth: zweimalige Eingabe des Nutzernamens erforderlich (erst WAYF, dann login)
  - ✓ Einrichtung eines Webservers, DNS-Eintrag o365.uni-bamberg.de, der Redirect auf das lokale ADFS mit WAYFless-Url erledigt (Prinzip ähnlich profile/SAML2/Unsolicited)

# Probleme und Lösungen ADFS

- Standard-IdP ist das AD und nicht Shibboleth ➔ Authentifizierungsquelle muss ausgewählt werden
  - ✓ über custom theme kann der Shibboleth-IdP per JS ausgewählt werden ➔ Umleitung zum Shibboleth-IdP

# Probleme und Lösungen ADFS

- Komplexe Technik (nicht nur bei HA)



# Probleme und Lösungen ADFS

- „Intelligenz“ des MS-Netzwerklastenausgleichsmanagers (NLB)
  - ✓ ADFS ab Version 3 (Server 2012R2) Überwachungs-URL
    ➔ per Skript Funktionsüberwachung und ggf. defekte Node aus dem Verbund entfernen
    oder
  - ✓ Web Application Proxy (WAP) vollständig und NLB bei Workern durch F5 ersetzen

# Nützliche Links – Shibboleth und ADFS

- http://download.microsoft.com/documents/France/Interop/2010/Federated_Collaboration_With_Shibboleth_2_0_and_SharePoint_2010_technologies-1_0.docx
- https://wiki.shibboleth.net/confluence/display/SHIB2/MicrosoftInterop?preview=%2F4358293%2F4751396%2FADFS_and_Shib.pdf&searchId=VV3GU92OB

# Nützliche Links - ADFS

- Einstieg: https://docs.microsoft.com/de-de/windows-server/identity/active-directory-federation-services
- Sizing: https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/design/planning-for-federation-server-capacity
- Drittanbieter-Proxy-Lösungen (ms-adfspip): https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/overview/ad-fs-faq

# Nützliche Links – ADFS und O365

- Einstieg: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity
- Verbund: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-whatis

# Fragen

- Umsetzung an der RTWH Aachen: Gerhard Lemoine Lemoine@itc.rwth-aachen.de