

**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

# Einführung Microsoft Exchange an der Universität Stuttgart

Dr. Sebastian Kiesel  
René Heidenreich  
68. DFN-Betriebstagung

# Universität Stuttgart

## Eckdaten

- Technisch orientierte Universität mit weltweiter Ausstrahlung und interdisziplinärer Integration von Ingenieur-, Natur-, Geistes- und Gesellschaftswissenschaften
- 28.000 Studierende
- 5.300 Beschäftigte, davon 265 Prof.
- 140 Gebäude an 2 Standorten, 350.000m<sup>2</sup> HNF
- 10 Fakultäten
- Hohes Drittmittelaufkommen
- Dezentrale Organisationsstrukturen, auch bei der IT-Betreuung
- Starke Kooperation mit außeruniversitären Forschungseinrichtungen, Forschungscampus ARENA2036, Startup Incubator, ...



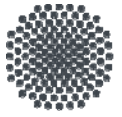
# Universität Stuttgart

## Technische Informations- und Kommunikationsdienste (ehemals Rechenzentrum)

- Abteilung „Netze und Kommunikationssysteme“
  - LAN, WAN, WLAN, Firewalls, DNS, PKI, ...
  - E-Mail, VoIP
  - Identity Management (OpenIDM)
- Abteilung „Server und Arbeitsplatzsysteme“
  - 2 Data Center: UCS, NetApp (Metrocluster), VMware
  - Windows-Server-Betrieb, Active Directory, Backup
  - PC-Pools für Studierende
- Abteilung „Zentrale Verwaltungsdienste“
  - Fachanwendungen: Campus Online, HIS SVA, SAP, ...
  - Desktop-Support für Beschäftigte der Zentralen Verwaltung
- Abteilung „Neue Medien in Forschung und Lehre“
  - Webauftritt, E-Learning, Vorlesungsaufzeichnungen, ...

Betreuung der Arbeitsplatzrechner für Wissenschaftler (und Instituts-Sekretariate) erfolgt dezentral





**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

# Ausgangssituation, Projekt-Übersicht, Zeitstrahl

Einführung Microsoft Exchange an der  
Universität Stuttgart



# E-Mail an der Universität Stuttgart

## Ausgangssituation in 2011

- Vom damaligen Rechenzentrum (RUS, heute TIK) betrieben
  - Mail-Relays (Postfix, Spamassassin, ClamAV, ...)
  - POP3/IMAP-Server für Studierende (30.000 Accounts in 1 DNS-Domain)
  - CommuniGate Pro für Beschäftigte (knapp 7.000 Accounts in 150 DNS-Domains)
- Dezentral betrieben
  - Ca. 50 Mailserver auf 9 Plattformen (soweit uns bekannt) für ca. 1/3 der Beschäftigten
- Defizite der beiden zentralen Systeme
  - Hardware am Ende der wirtschaftlich sinnvollen Nutzungsdauer
  - Fremdkörper im DataCenter (CGP auf Solaris/UltraSPARC vs. x86-Virtualisierung)
  - Defizite in der Groupware (Kalender-Freigaben, Web-Frontend, mobile Geräte, ...)

# E-Mail an der Universität Stuttgart

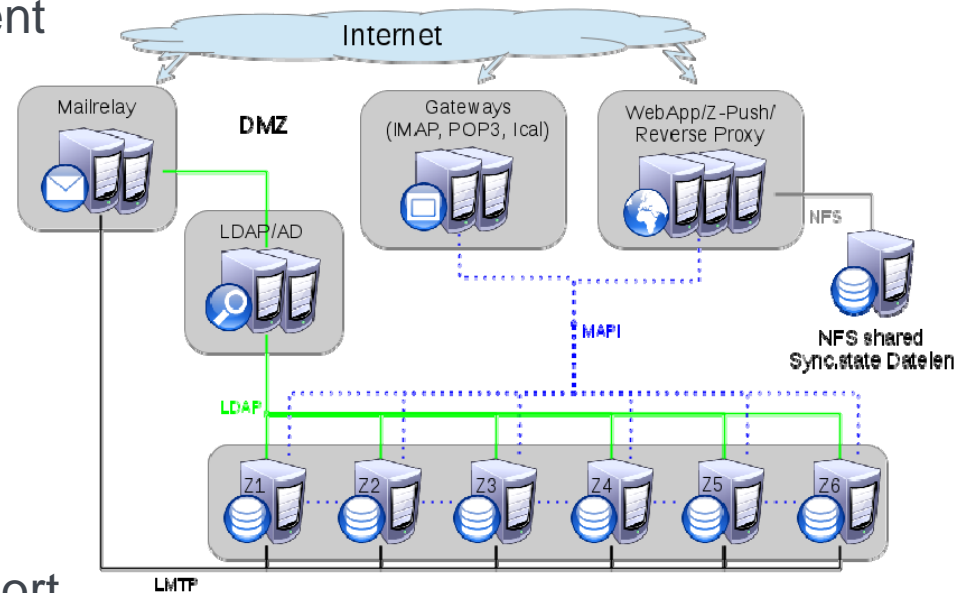
## Erste Schritte zur Veränderung

- 2010/2011
  - Diskussionen zu "Exchange aus der Cloud" (hie damals noch nicht Office365...)
  - Datenschutz-Fragen zum damaligen Zeitpunkt nicht lösbar
  - Beschluss: On-premises Lösung für (mindestens) einen weiteren HW-Lebenszyklus
- 2012
  - Evaluation verschiedener Groupware-Lösungen
  - Ziel: Ermitteln der insgesamt wirtschaftlichsten Lösung
    - Leistungsmerkmale
    - Universelle Verwendbarkeit: Client des „Marktführers“ und offene Standards
    - Integrierbarkeit in unsere IT-Landschaft, Administrierbarkeit
    - Verfügbarkeit von ext. Dienstleistern / Beratern
    - Kosten (Lizenz, Hardware, Personal, Schulungen, ...)
  - Gewinner: Zarafa

# E-Mail an der Universität Stuttgart

## Zarafa

- 2013
  - Beschaffung und Aufbau der Zarafa-Server
  - Integration in das Identity Management
  - Umstellung aller Studierenden
- 2014
  - Weitere Arbeiten an IDM-Integration
  - Schrittweise Umstellung von 3000 Beschäftigten- und Funktionskonten
- 2015
  - Januar: Zarafa kündigt Outlook-Support zu 04/2016 ab, später zu 04/2017
  - Mai: Beschluss: Abbruch des Zarafa-Projekts, Wechsel zu on-prem. Exchange

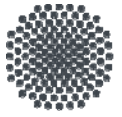


# E-Mail an der Universität Stuttgart

## Projektverlauf – Wechsel zu Exchange

- 2015
  - Auswahl- und Vergabeverfahren für einen Dienstleister
  - Leistungsumfang
    - Design und Aufbau der Exchange-Umgebung in unserer Virtualisierungsumgebung
    - Remoteüberwachung und -betrieb der Server (→ ADV-Vertrag)
    - Auswahl bzw. Erstellung von Werkzeugen zur Migration der Nutzerkonten
- 2016
  - Juni: Design-Workshops
  - November: Exchange-Server laufen, Arbeiten am Identity Management
- 2017
  - Migration der Zarefa-Konten (bis Mai) und der CGP-Konten (bis Dez.)
- 2018
  - Restarbeiten, weiterer Ausbau der Groupware





**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

# Exchange Infrastruktur

Einführung Microsoft Exchange an der  
Universität Stuttgart



# Exchange 2016 Infrastruktur

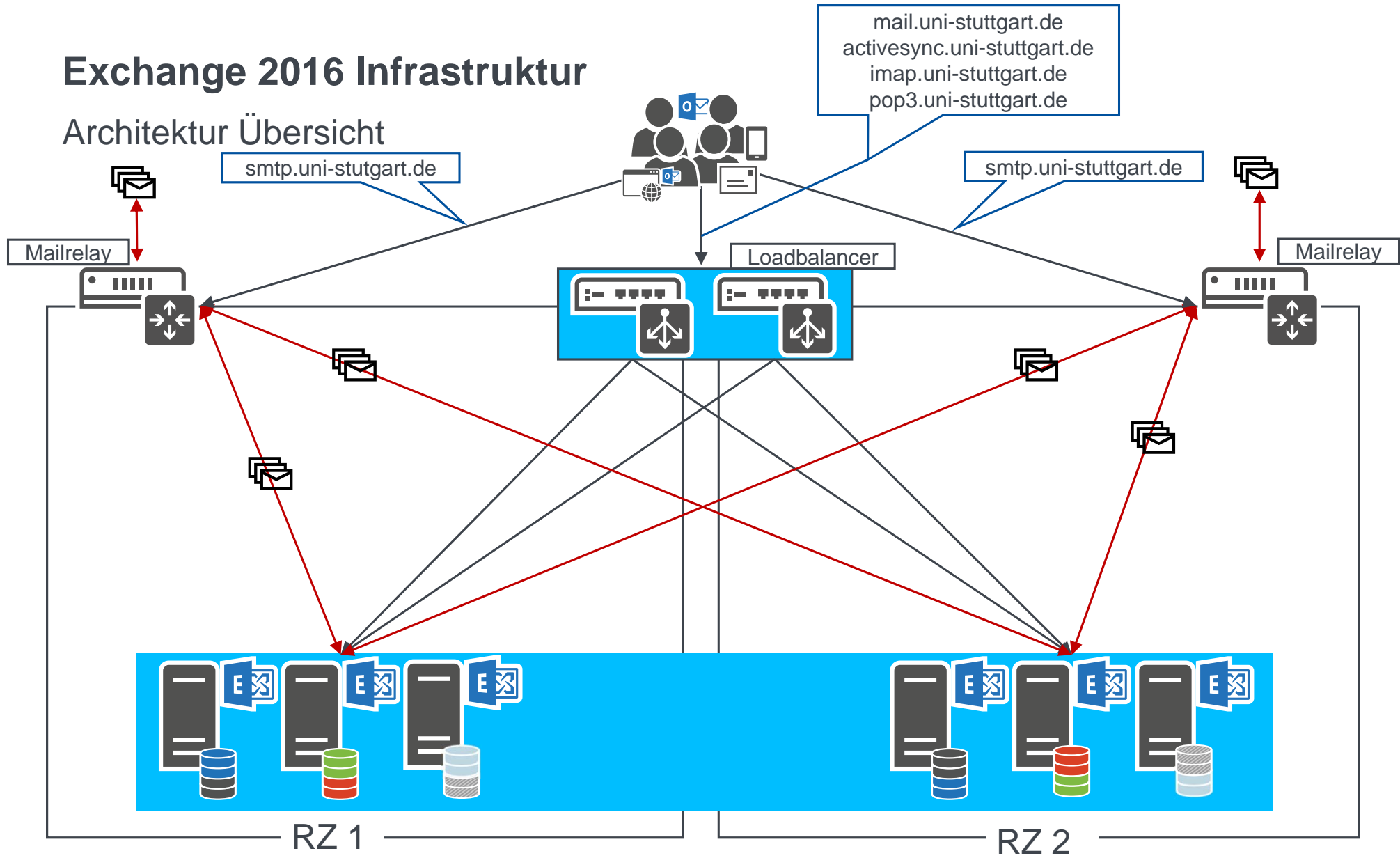
## Grundsatzentscheidung & Planung

- Exchange 2016 auf Windows Server 2012R2
  - Multi-Role-Server, d.h. keine Unterscheidung zwischen Frontend und Datenbank
  - Nur eine Art von Server, Load Balancer / Reverse Proxy davor
- Abwägen zwischen einer virtualisierten Infrastruktur und einer hyperkonvergenten Lösung
  - Snapshots nur bei einer virtualisierten Lösung möglich
  - Virtualisierung bereits im Einsatz für eine hyperkonvergente Lösung keine Management-Prozesse
  - Hohe Konvergenzzeiten bei DAG?

→ Entscheidung für virtualisierte Server

# Exchange 2016 Infrastruktur

## Architektur Übersicht



# Exchange 2016 Infrastruktur

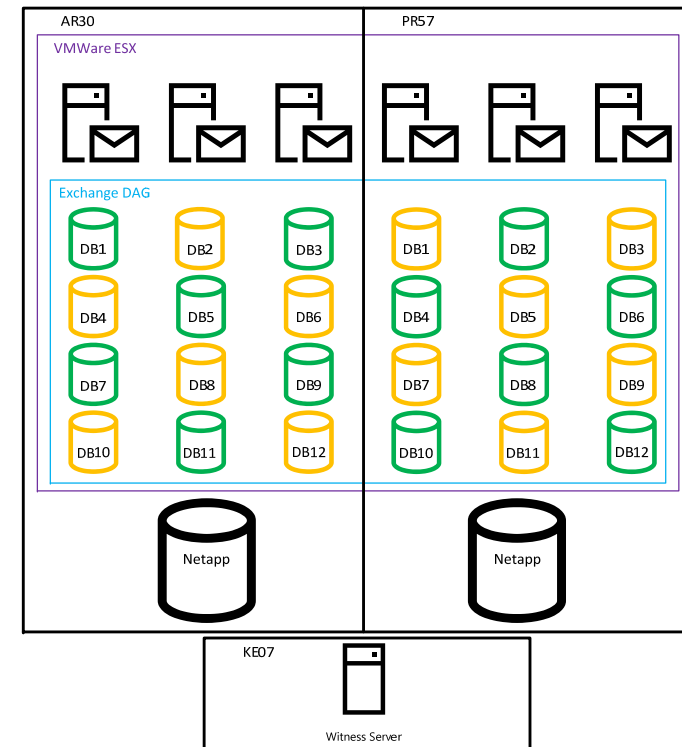
## Exchange Server

- Komplette virtualisierte Infrastruktur, je 2 ESX-Hosts an 2 Standorten
  - Virtuelle Festplatten werden von einem redundanten NetApp System in die virtuellen Maschinen gemappt
  - Snapshot Sicherung per NetApp SnapManager
  
  - Berechnung der Server-Dimensionierung durch "Exchange Server Role Requirements Calculator"
    - 6 Exchange-Server mit je 12 vCPU's und 96GB RAM
    - Gesamtprojekt: 1TB RAM und 150 CPU Cores
- Sehr gute Performance im Live-Betrieb

# Exchange 2016 Infrastruktur

## Exchange Server

- Database Availability Group (DAG)
  - 2 aktive und 2 passive Datenbanken pro Exchange-Server



- Identitätsmanagement-System (IdM) für automatisierte Prozesse wie z.B. Mailboxaktivierung, Aliase hinzufügen, Account-Deaktivierung
- Konfiguration als mehrmandantenfähige Lösung (Multi Tenancy)
  - Strikte Trennung zwischen Studierenden, Beschäftigten und Gästen



# Exchange 2016 Infrastruktur

## Loadbalancer

- 2 Kemp Loadbalancer VLM-10G mit Edge Security Pack (ESP)
- Virtuelle Appliances
- ESP - Reverse-Proxy mit Pre Authentication Service
- Healthcheck der virtuellen Verzeichnisse der Microsoft Exchange Server Infrastruktur
- Lastverteilung auf die einzelnen Exchange-Server
- Während der Koexistenz von Zarafa & Exchange Weiterleitung der Client-Requests zum entsprechenden Mailserver (Realisierung durch Steering Groups auf den Loadbalancern)

# Exchange 2016 Infrastruktur

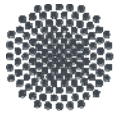
## Mailrelays

- Einsatz von 2 Postfix Servern als Mailrelays exklusiv für Exchange
- Für Relaydienste existieren 4 separate Postfix Server
- Spam- und Virenprüfung mit Amavis, Spamassasin, ClamAV und Sophos
- Postausgangserver für IMAP/POP3 smtp.uni-stuttgart.de:587, ESMTPS+STARTTLS
- LDAP-Authentifizierung über Dovecot

# Exchange 2016 Infrastruktur

## Autoconfig, Management, Monitoring

- 1 VM mit installiertem Webserver
  - Stellt die automatische Konfiguration für Thunderbird zur Verfügung
- 1 VM für das Mailmanagement
  - Verwaltung virtueller Gruppen
  - Verwaltung der Maildomänen
  - Import/Exportskripte
  - Abfragen Mailrouting für Benutzer und E-Mail-Adressen
- Einbindung in die Icinga/Grafana Infrastruktur des TIK



**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

# Migration der Postfächer von Zarafa und CommuniGate Pro nach Microsoft Exchange

Einführung Microsoft Exchange an der  
Universität Stuttgart



# Migration

## Planung und Organisation

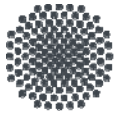
- Festlegung, dass erst Zarafa und danach CommuniGate Pro migriert wird
- Unterteilung der Migrationen in einzelne Wellen
  - Bis zu 500 Benutzer pro Welle
  - Migration einer Welle innerhalb einer Nacht abgeschlossen
  - 2 Wellen pro Woche (Nacht Mo/Di und Nacht Mi/Do)
- Technischer Support:
  - Im wissenschaftlichen Bereich:
    - Dezentrale IT-Admins übernehmen viele Aufgaben nach Schulung durch TIK
    - Zwei First-Level-Mitarbeiter und zwei Second-Level-Mitarbeiter des TIK unterstützen bei Neukonfiguration der Clients
  - Separater Prozess und Support für die Zentrale Verwaltung



# Migration

## Technischer Ablauf

- Koordination der einzelnen Migrationsschritte über Zustandsautomat im IDM
- Neues Attribut „Mail Routing Key“ im Active Directory
  - Mailrelays fragen über LDAP das Ziel einer Mail (CommuniGate, Zarafa, Exchange, temporäres Queueing während Migration) ab
- Zarafa → Exchange
  - Script-gesteuerter Export und Import einer PST-Datei  
→ alle Objekte werden automatisch migriert
  - Rollback im Fehlerfall
- CommuniGate → Exchange
  - Script-gesteuertes Kopieren der E-Mails mit imapsync
  - Kalendereinträge müssen vom Nutzer händisch kopiert werden
  - Kein Rollback notwendig, ggf. manuelle Nach-Synchronisierung



**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

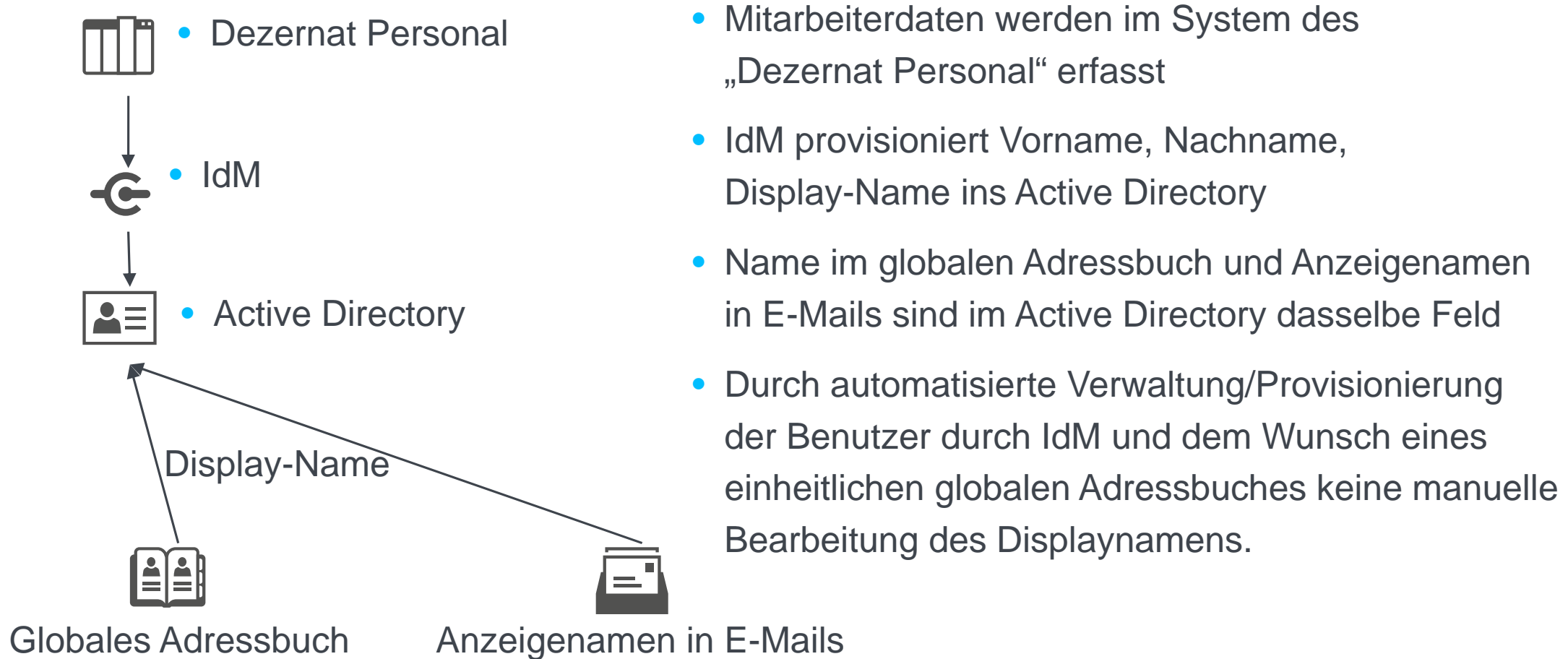
# Herausforderungen und Erfahrungen

Einführung Microsoft Exchange an der  
Universität Stuttgart



# Herausforderungen und Erfahrungen

## Display-Name



# Herausforderungen und Erfahrungen

## Display-Name

- Um das Adressbuch sinnvoll nutzen zu können, wird eine einheitliche Struktur des Displaynamens benötigt. Sinnvolle Suche im Adressbuch nur möglich, wenn die „relevante“ Komponente des Nachnamens vorne steht
- Display-Name wird aber auch als Absender in verschickten E-Mails verwendet

→ Konfliktpotential

- Beispiele
  - von Mustermann, Michael vs. Mustermann, Michael von
  - Mustermann, Michael, Prof. Dr.-Ing. Dr. h.c. mult. Dr. eh.

# Herausforderungen und Erfahrungen

## Sichtbarkeit im Exchange Adressbuch

- Muss datenschutzkonform sein
- Getrennte globale Adressbücher für Studierende, Beschäftigte und Gäste
- Einführung „Multi Tenancy“ für die strikte Trennung

Sichtbarkeit im Adressbuch	Beschäftigte	Studierende	Gäste
Beschäftigte (Wissenschaftlich)	X		
Beschäftigte (Verwaltung)	X		
Studierende			
Gäste			

Getrennte Globale Adresslisten

- ABER: Freigaben wie Kalender benötigen eine Adressbuchsichtbarkeit
- Keine Möglichkeit der Freigabe von z.B. Kalender zwischen Beschäftigten und Studierenden!



# Herausforderungen und Erfahrung

## Adminportal

- CommuniGate Pro bietet Admin-Portal zur Verwaltung der Mail-Domänen durch Instituts-Admins
- Exchange bietet im ECP nur teilweise Möglichkeiten der Verwaltung, weiterführende Einstellungen werden über PowerShell gemacht
- In Zusammenarbeit mit IDM erweitern des Admin-Portals für Exchange
- Erweitern des Selfservice-Portal der Benutzer für Exchange

Passwort ändern E-Mail einrichten

## E-Mail einrichten

Hier können Einstellungen für Exchange-Mailboxen des zentralen TIK-Mailservice angepasst werden. Wählen Konto mit einer Mailbox aus, passen Sie dann bei Bedarf die Einstellungen an und klicken Sie dann unten auf

Angemeldet als: [Redacted]@uni-stuttgart.de

Konto: [Redacted]@uni-stuttgart.de

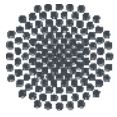
### Primäre E-Mailadresse

Hier können Sie festlegen, welche der E-Mailadressen der Mailbox als primäre Adresse von Exchange verwendet wird von Exchange immer als Ihre Absenderadresse eingesetzt (außer wenn Sie über IMAP/SMTP auf Ihre Exchange zugreifen), sowie im Exchange-Adressbuch als Hauptadresse eingetragen. Beim Speichern wird die Änderung allerdings kann es bis zu 8 Stunden dauern bis auch die Adresse im globalen Exchange-Adressbuch aktualisiert wird z.B. in Outlook verwendet wird, ggf. noch länger. Allerdings kann die Aktualisierung in Outlook ausbleiben werden.

E-Mailadresse:	Alias	Primär
	[Redacted]@rus4.uni-stuttgart.de	<input type="checkbox"/>
	[Redacted]@rus4.uni-stuttgart.de	<input type="checkbox"/>
	[Redacted]@rus4.uni-stuttgart.de	<input type="checkbox"/>
	[Redacted]@tik.uni-stuttgart.de	<input checked="" type="checkbox"/>

# Fazit

- Erfolgreiche Einführung von Microsoft Exchange
  - Störungsfreier technischer Betrieb
  - Auch Linux und Mac-User zufrieden
  - Neue Groupware-Funktionalitäten werden von Benutzern gerne angenommen
  - Institute mit dezentralen Mailservern wollen zu uns wechseln
  - Stufenweise Migration mit ca. 500 Benutzern pro Nacht hat gut funktioniert
- Um das Adressbuch sinnvoll nutzen zu können, wird eine einheitliche Struktur des Displaynamens benötigt. Dieser wird aber auch als Absender in verschickten E-Mails verwendet → Erhebliche Diskussionen
- An dezentrale Administratoren delegierte Administration erfordert teilweise Nachbau der Web-Admin-Oberfläche von CommuniGate Pro



**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

**Vielen Dank!**



**René Heidenreich**

E-Mail [rene.heidenreich@tik.uni-stuttgart.de](mailto:rene.heidenreich@tik.uni-stuttgart.de)

Telefon +49 (0) 711 685-65952

[www.tik.uni-stuttgart.de](http://www.tik.uni-stuttgart.de)

Universität Stuttgart

Technische Informations- und Kommunikationsdienste (TIK)

Allmandring 30a

70550 Stuttgart



**Universität Stuttgart**

Technische Informations- und  
Kommunikationsdienste (TIK)

**Vielen Dank!**



**Dr. Sebastian Kiesel**

E-Mail [sebastian.kiesel@tik.uni-stuttgart.de](mailto:sebastian.kiesel@tik.uni-stuttgart.de)

Telefon +49 (0) 711 685-62503

[www.tik.uni-stuttgart.de](http://www.tik.uni-stuttgart.de)

Universität Stuttgart

Technische Informations- und Kommunikationsdienste (TIK)

Allmandring 30A

70550 Stuttgart