

# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## Was steckt hinter FAUmac?

Gregor Longariva  
FAUmac Team RRZE

Drucken macOS iPad Softwareinstallation  
SLA Push Notifications Community Apple School Manager  
autopkg Kerberos Philosophie Apple Configurator  
FAUmac Self Service Lizenzverwaltung Cancom FAU API  
MDM JAMF Pro Schulungen AppleTV Betatests Updates  
Schoolwork App tvOS VPP python **FAUmac** configuration profiles  
NFS shares DEP idUP design Fehler machen VPN  
Rückmeldungen Seriennummer CI LDAP WIFI security  
Mac viel espresso plist Active Directory iPhone Classroom App  
Administrator OTRS Windows shares Development  
Helpdesk AppleID GitLab Automatisierung  
iOS Microsoft Office

A large, faint watermark of the FAUmac logo is centered in the background. It consists of a circle containing a stylized 'F' and 'A' with a leaf-like shape above the 'A'.

**FAUmac**  
=  
unsere  
**Philosophie**  
der Betreuung

# Philosophie

---



- Unsere Nutzer sind wichtiger als die Technik
- geschulte, motivierte Mitarbeiter
- automatisieren
- weiterentwickeln
- modern bleiben

# Philosophie: Nutzerzentriert

---



Viel wichtiger als die  
(austauschbare) Technik:

- Es ist Dein Mac
- Arbeite so wie Du es möchtest
- Wir schränken Dich nicht unnötig ein, wir unterstützen Dich nur

# jedem Nutzer „sein“ Gerät

---



- ermögliche jedem Nutzer mit dem Gerät zu arbeiten, mit dem er möchte oder welches er schon kennt
- ermögliche dem Nutzer sein Gerät so benutzen zu dürfen, als wäre es seins



# jeder Nutzer soll sich selbst helfen können

---



- minimiere die Aufgaben, für die sich der Nutzer an die IT wenden muss
- gib dem Nutzer die Möglichkeiten und Werkzeuge, sich selbst zu helfen
- höre auf die Bedürfnisse der Nutzer

# Philosophie: motivierte Mitarbeiter

---



- regelmäßige Schulungen
- motiviertes Theken-Personal
- Macs für Support-Personal auch als persönliche Geräte zur Verfügung stellen



# Philosophie: automatisieren

---



- So viel wie möglich automatisieren (autopkg, API Skripte)
- Macs werden nicht ge-imaged
- Nur die zum Betrieb notwendigen Aspekte werden vorkonfiguriert
- Aufgaben nicht auf User abwälzen

# Philosophie: weiterentwickeln

---



- weiterentwickeln
- der Stand von heute ist die obsoletere Vergangenheit von morgen
- proaktiv Neues testen und probieren
- An Beta-Tests teilnehmen

# Philosophie: moderne IT

---



- Nutzer steht im Fokus, das Gerät selbst rückt mehr und mehr in den Hintergrund
- Menschen wollen nicht mehr nur in Büros arbeiten
- die Rolle der IT ändert sich

# Der Lohn

---



1. zufriedene Nutzer
2. zufriedene Nutzer
3. wenig Arbeit für uns :-)
4. zufriedene Nutzer



**Fragen? Gerne!**

# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## Auspacken und loslegen - so die Theorie

ASM, DEP, MDM



1. open box
  2. power on MacBook
  3. there is no step 3
- ♡IT





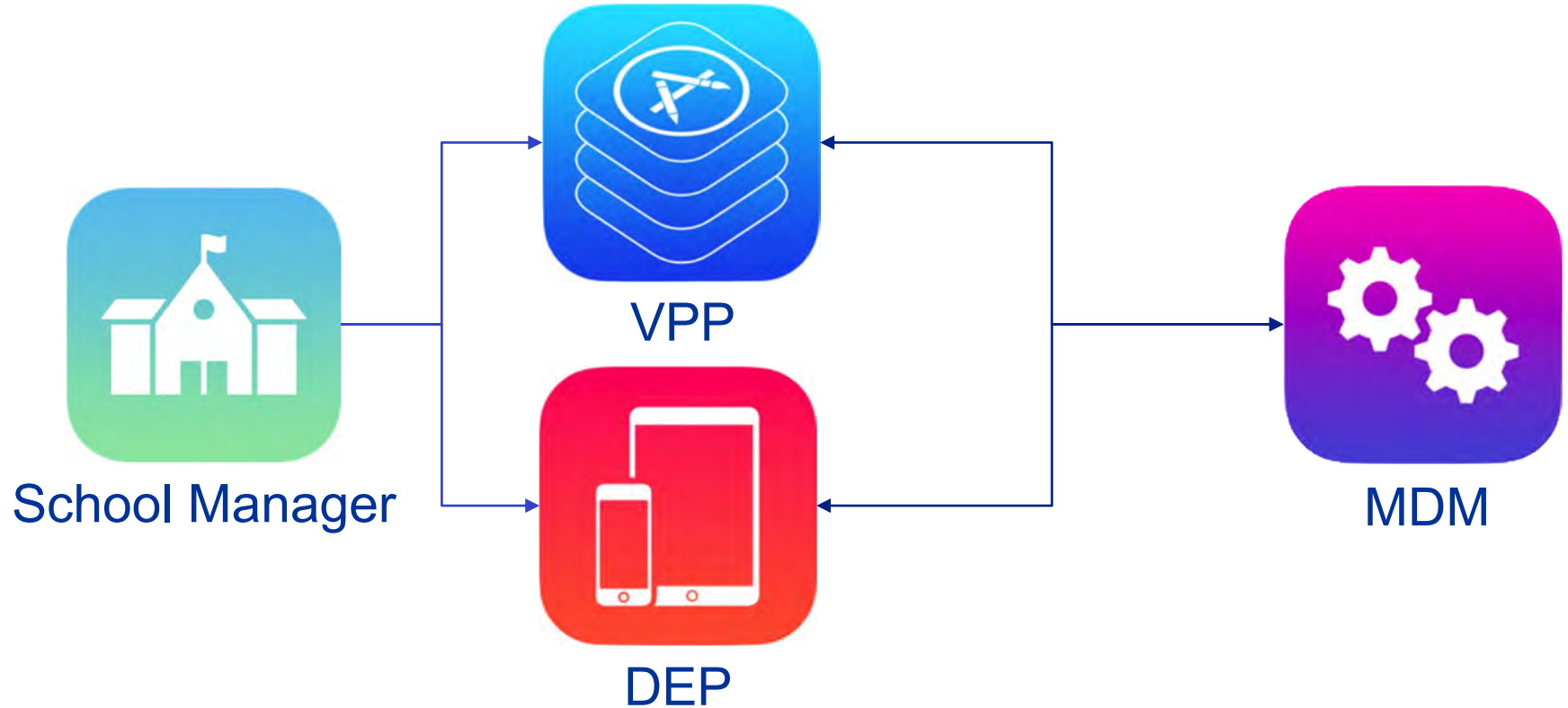
# Begriffserklärung



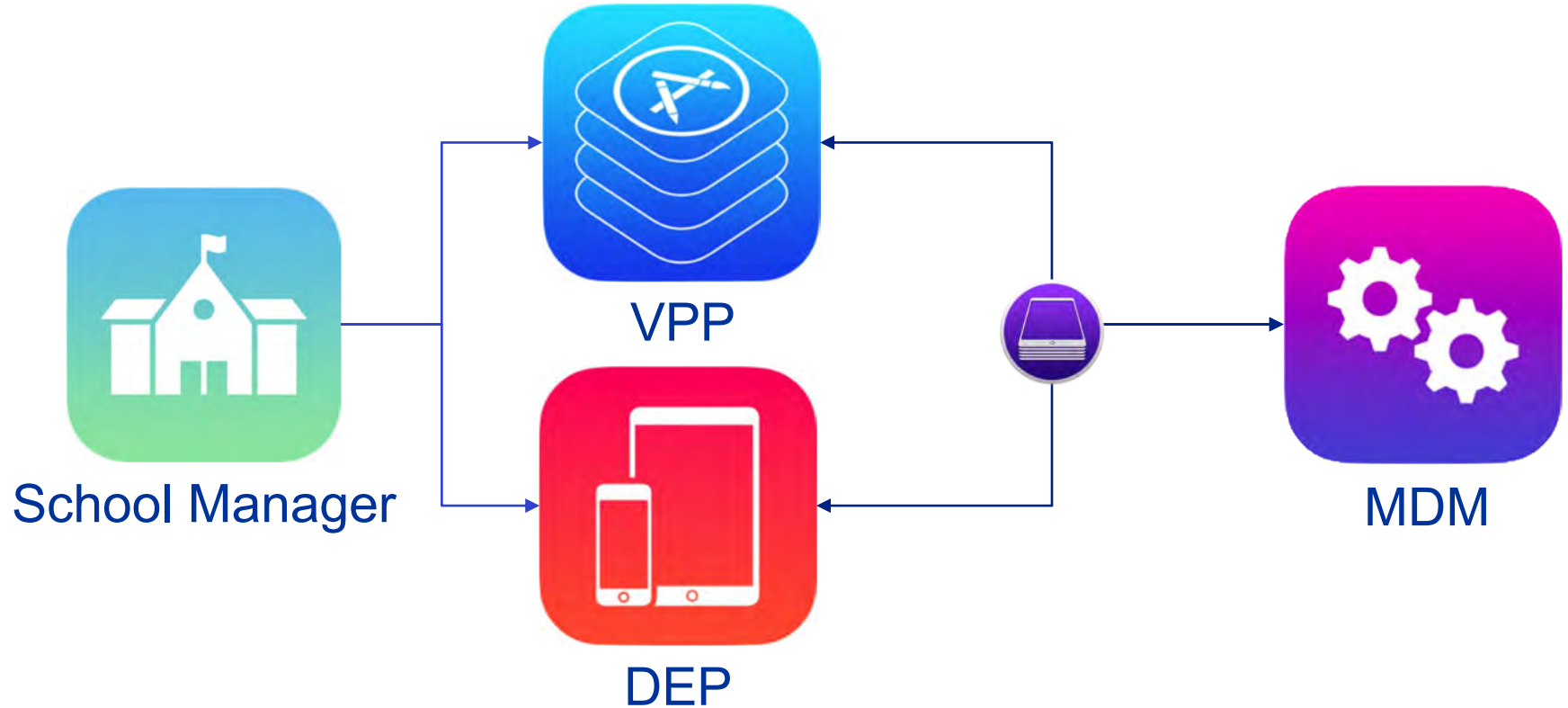
# Begriffserklärung



# Begriffserklärung



# Begriffserklärung





# AUSPACKEN UND LOSLEGEN - SO DIE THEORIE



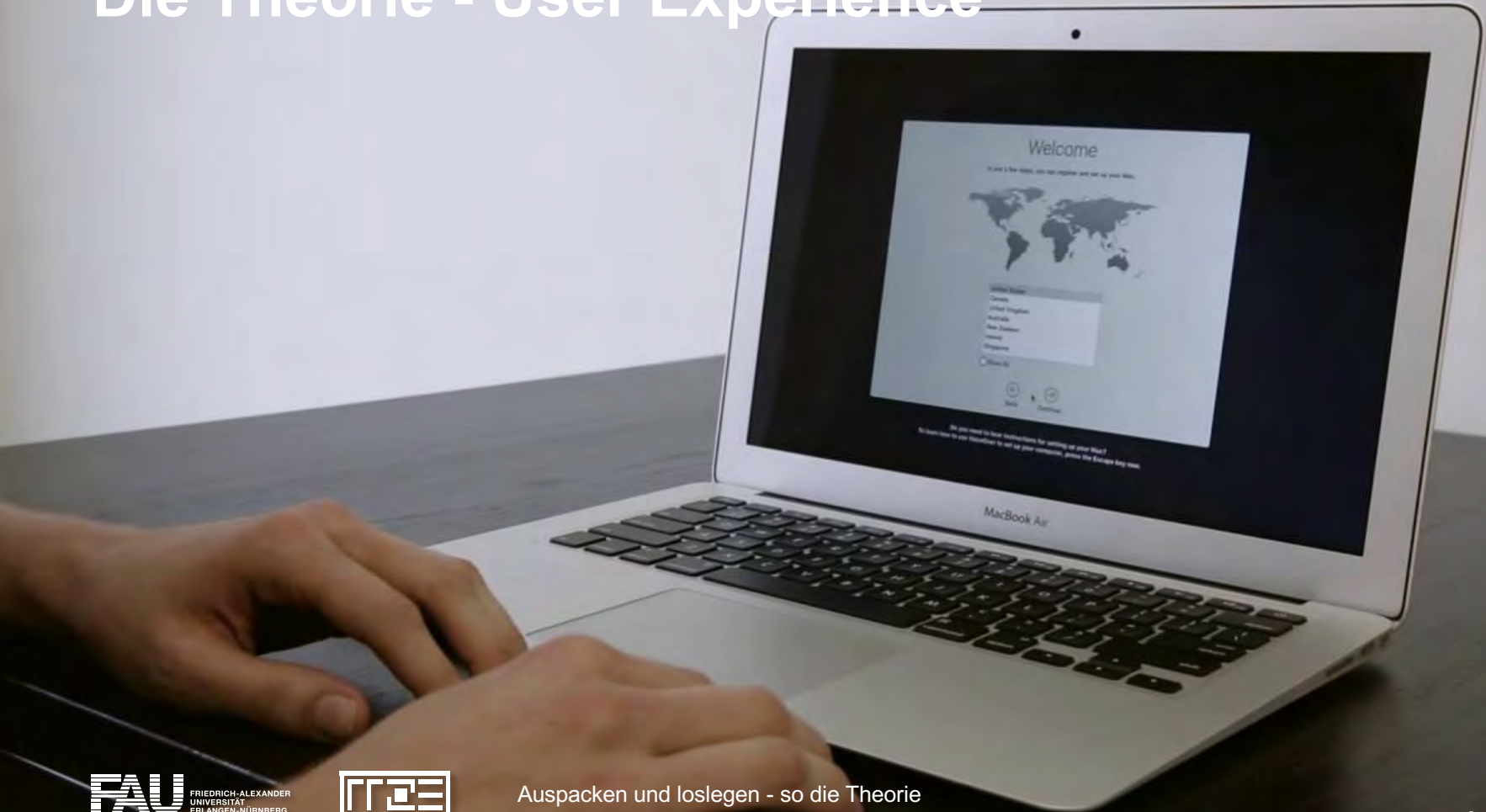
Die Theorie

# Die Theorie - User Experience





# Die Theorie - User Experience

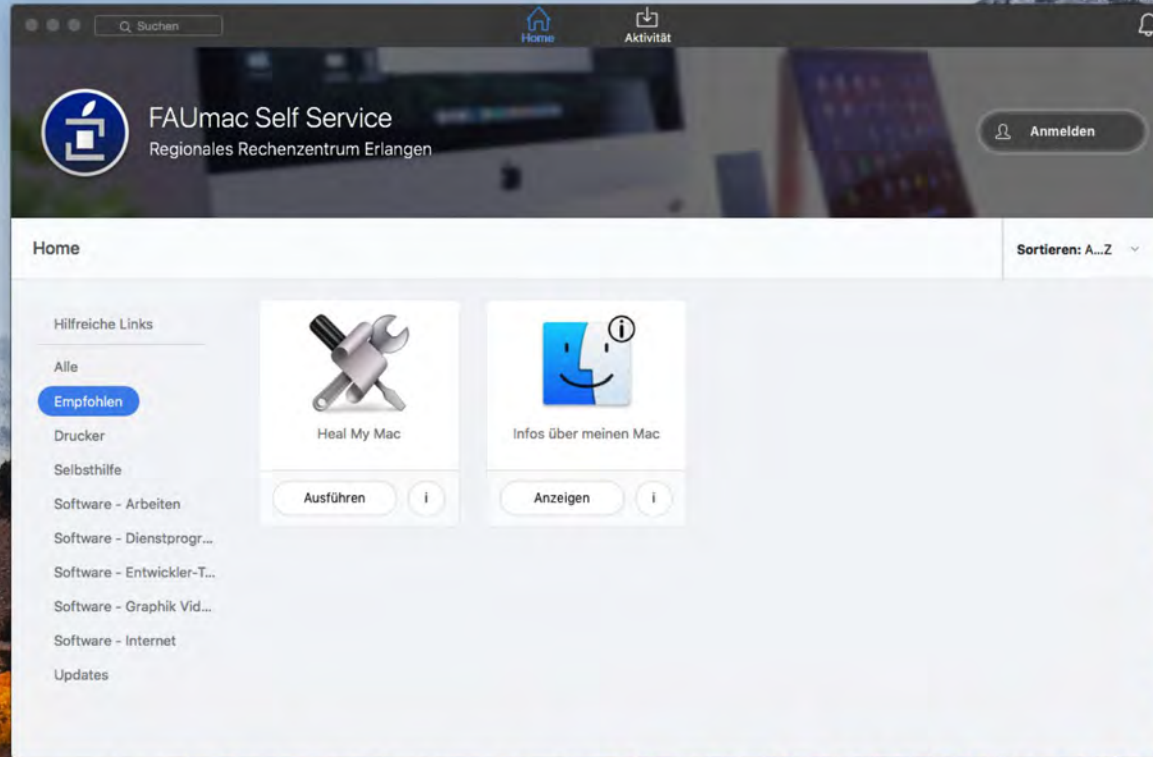




# Die Theorie - User Experience

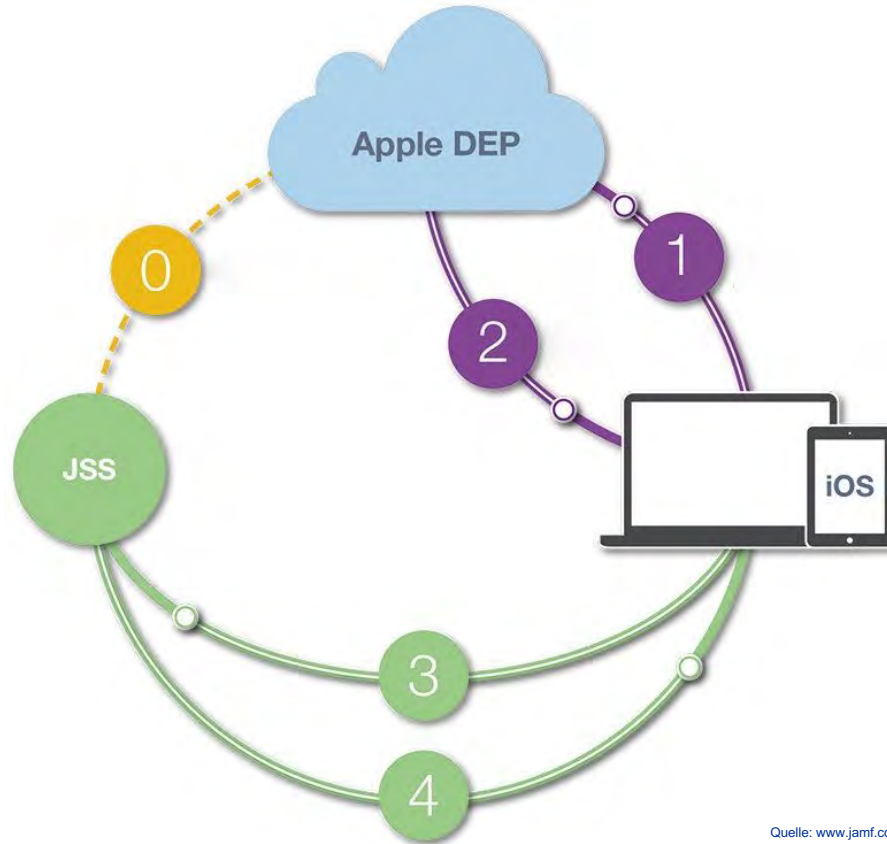


# Die Theorie - User Experience





# Die Theorie – Technik



Quelle: [www.jamf.com](http://www.jamf.com)

# Die Theorie – Admin





# AUSPACKEN UND LOSLEGEN - SO DIE THEORIE



So die Theorie... das ist die Praxis



# Die Praxis – Universität

---

- Fehlender Workflow für Bestellungen
- Kunde vergisst Seriennummer mitzuteilen
- „Viele kleine Fürsten“ aka Professoren





Quelle: pixabay.com

# Die Praxis – Apple, Händler & Jamf

---

- Fehlschlagende DEP-Übermittlungen
- Verlorene MDM-Zuordnungen („No name“)
- Fehlende Schnittstelle(n)

■ ...





# AUSPACKEN UND LOSLEGEN - SO DIE THEORIE



Unsere Lösung / geplante Zukunft

# Hoffen auf mehr Zuverlässigkeit und Schnittstellen

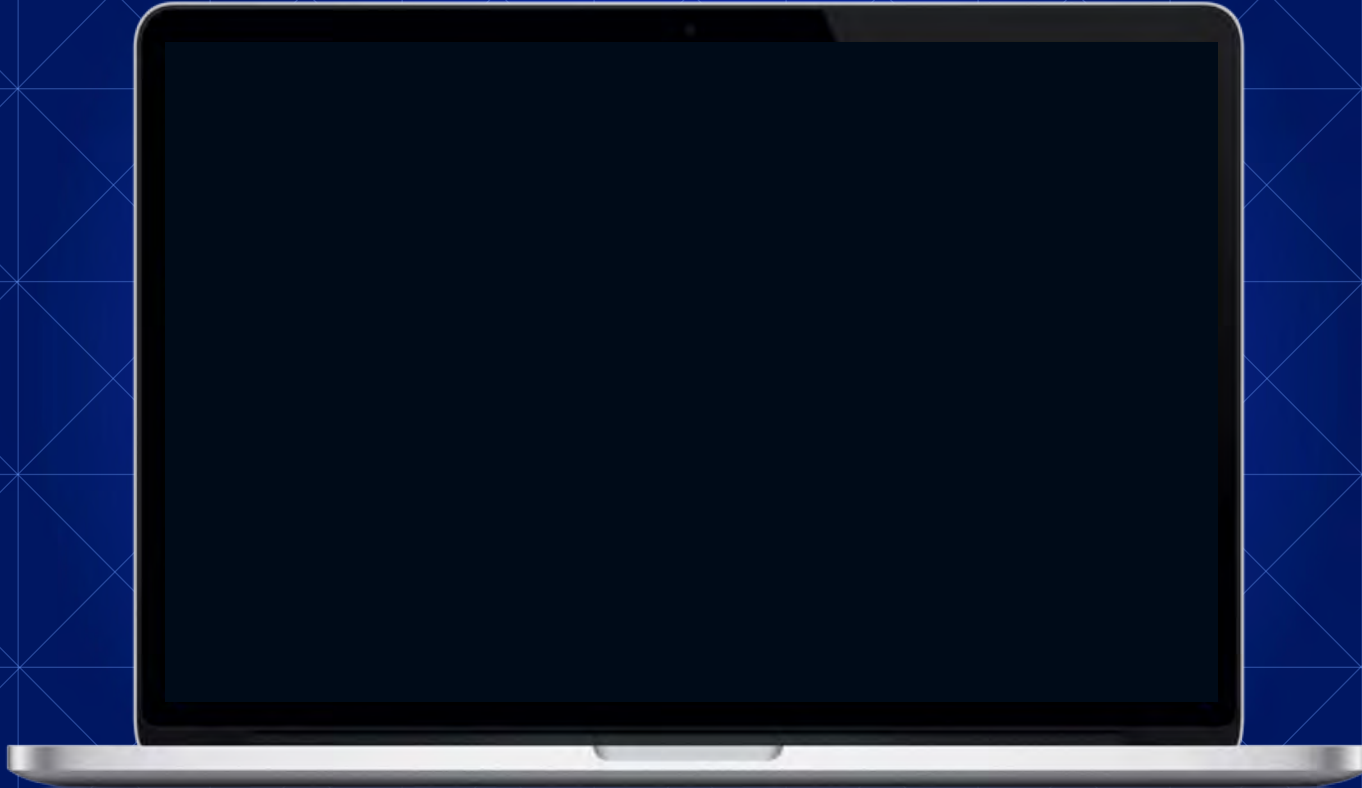
# DEP-Enrolment (App)

---

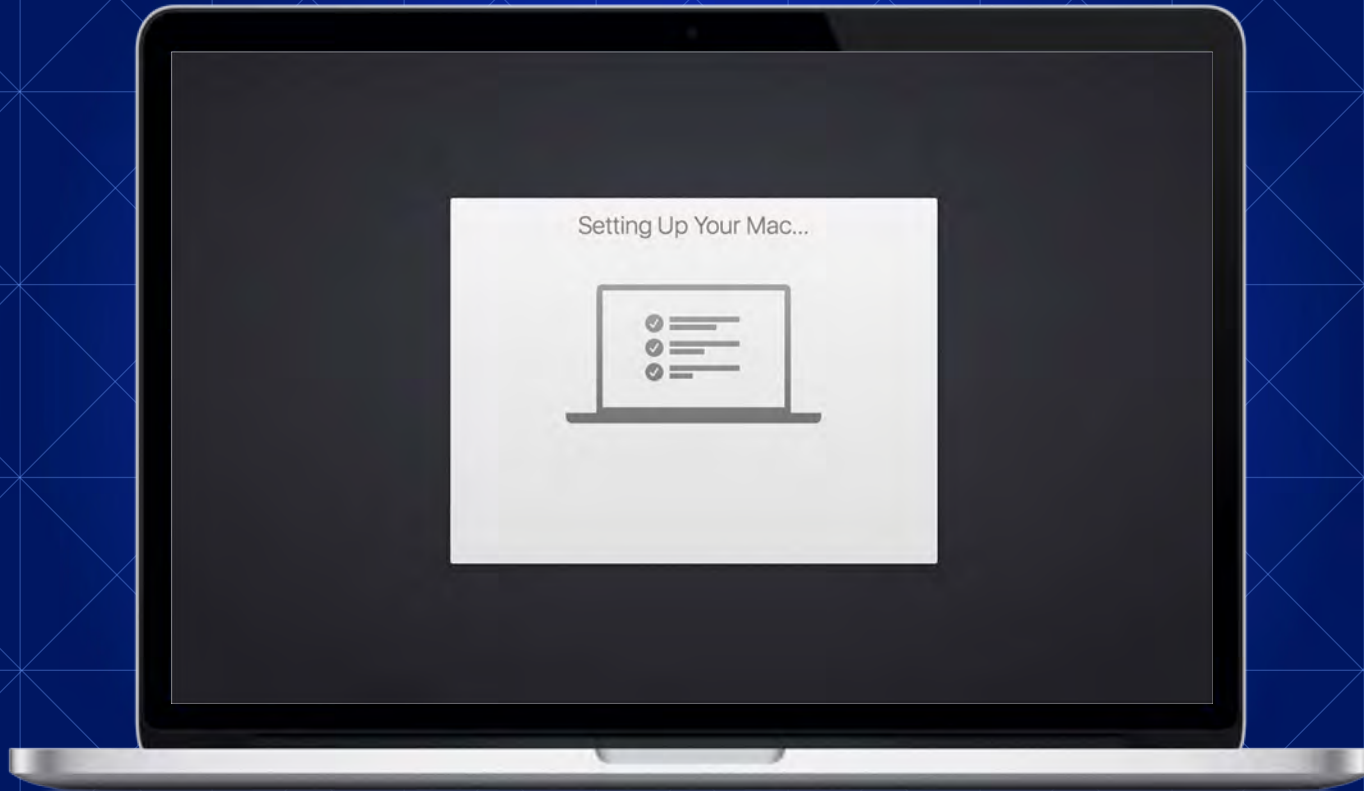


- Status über Ersteinrichtung
- Zuweisung des Departments
- Benutzerunterstützung bei Erstkonfiguration (*geplant*)
- Informationen über „FAUmac“

# DEP-Enrolment (App)



# DEP-Enrolment (App)





# DEP-Enrolment (App)



# Unser Ziel:

# Zero-touch enrollment

# Fragen?

# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## Macs und Active Directory an der FAU

Gregor Longariva  
FAUmac Team

# Wer von Ihnen bindet die Macs an Active Directory?



# Wer von Ihnen bindet die Macs an Apples OpenDirectory?

# Wer von Ihnen bindet die Macs an OpenLDAP?

**Wer von Ihnen verwendet  
(nur) lokale  
Authentifizierung?**

# kurz nach der macOS Schulung im April





**„wie bindet Ihr eure Macs  
an Active Directory?“**

„gar nicht\*“

(\*sort of...)



**„Wie macht ihr es dann?“**

**das wollen wir heute zeigen**





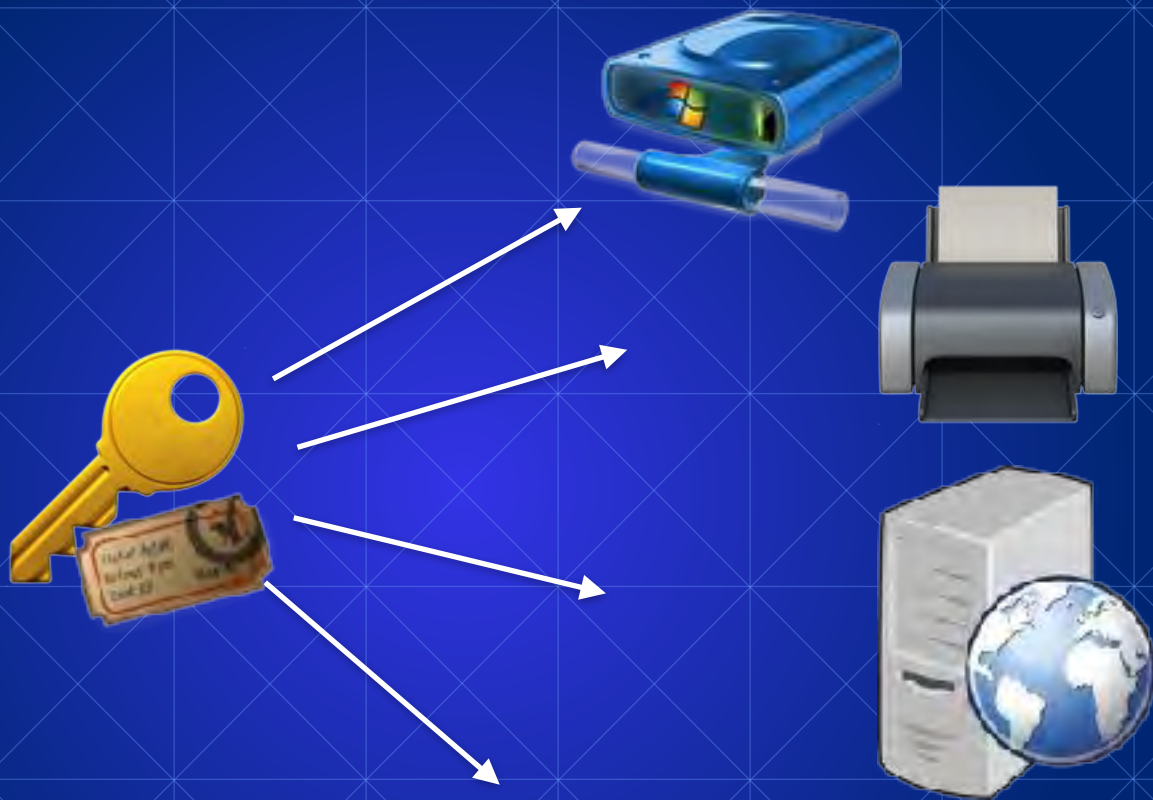












■ ■ ■



KEEP  
CALM  
AND  
USE  
ACTIVE DIRECTORY





# Erfahrungen mit Macs in der AD



# Macs in der AD

## Authentifizierung, Autorisierung

---



- Authentifizierung
  - Benutzername, Passwort
  
- Autorisierung
  - Rechteverwaltung am Rechner

# Macs in der AD

## Login-Prozess

---

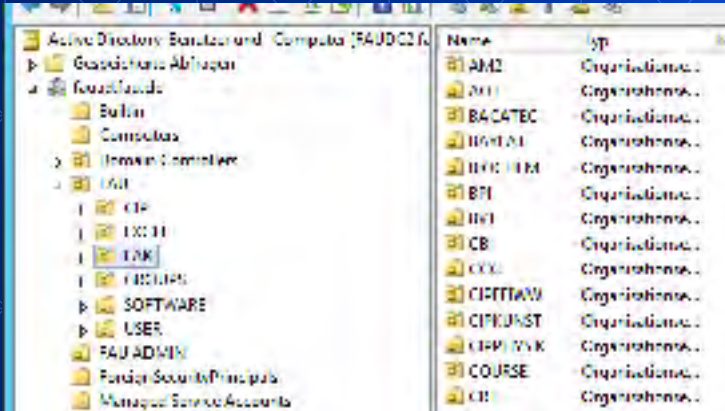
- Login aus nicht FAU-Netzen verzögert
- AD Zugangsdaten sind gecached



# Macs in der AD

Einbinden des Macs aufwändig

---



- Funktionsbenutzer mit entspr. Rechten in der AD für scripting
- Rechnername muss feststehen
- OU für Rechner muss bekannt sein
- Alternativ: Objekt in AD schon angelegt
- Rechner muss sich in einem Uni-Netz befinden

# Macs in der AD

## DEP

---



- User experience nicht so wie gedacht
- ggf. muss die IT den Mac vorkonfigurieren

**fassen wir zusammen:**



# Active Directory

---



- Authentisierung, Authentifizierung
- Autorisierung
- Konfiguration des Rechners
- Softwareverteilung per SCCM
- SSO gegenüber AD gebundener Systeme (Drucker, Freigaben, Webseiten, ...)

**gilt das auch für den Mac?**

# Active Directory

---



- Authentisierung, Authentifizierung
- Autorisierung
- Konfiguration des Rechners
- Softwareverteilung per SCCM
- SSO gegenüber AD gebundener Systeme (Drucker, Freigaben, Webseiten, ...)

# Active Directory

---



- Authentisierung, Authentifizierung
- **Autorisierung**
- Konfiguration des Rechners
- Softwareverteilung per SCCM
- SSO gegenüber AD gebundener Systeme (Drucker, Freigaben, Webseiten, ...)

# Active Directory

---



- Authentisierung, Authentifizierung
- **Autorisierung**
- **Konfiguration des Rechners**
- Softwareverteilung per SCCM
- SSO gegenüber AD gebundener Systeme (Drucker, Freigaben, Webseiten, ...)

# Active Directory

---



- Authentisierung, Authentifizierung
- Autorisierung
- Konfiguration des Rechners
- Softwareverteilung per SCCM
- SSO gegenüber AD gebundener Systeme (Drucker, Freigaben, Webseiten, ...)



# Active Directory

---



- Authentisierung, Authentifizierung
- **Autorisierung**
- **Konfiguration des Rechners**
- **Softwareverteilung per SCCM**
- SSO gegenüber AD gebundener Systeme (Drucker, Freigaben, Webseiten, ...)

**was bleibt übrig?**



# Kerberos



KEEP  
CALM  
AND  
USE  
ACTIVE DIRECTORY

rly?



**FAUmac**

**Philosophie**



*„Unsere Nutzer sind wichtiger  
als die Technik“*

*„Menschen wollen nicht mehr  
nur in Büros arbeiten“*







KEEP  
CALM

*Kerberos*

AND  
USE

~~ACTIVE DIRECTORY~~







<https://nomad.menu/products/>

Mac



AD



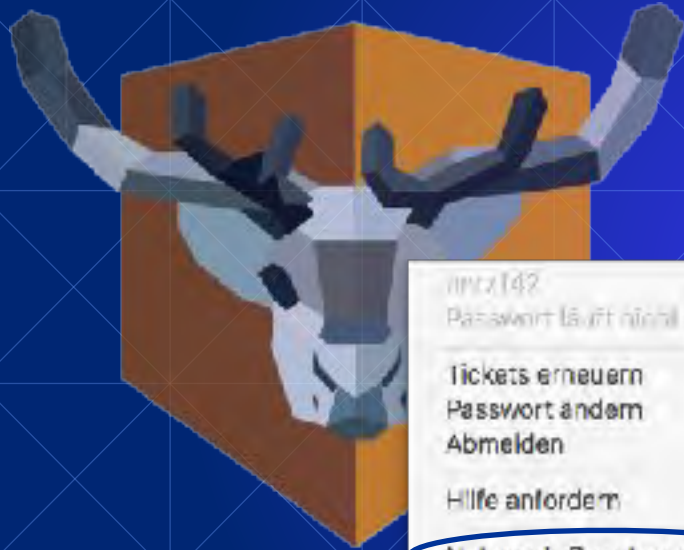






AD





- myz142
- Passwort läuft nicht ab
- Tickets erneuern
- Passwort ändern
- Abmelden
- Hilfe anfordern
- Netzwerk-Benutzerzeichnis**
- Einstellungen
- Beenden









**und dann gibt es noch**



NoMAD Login

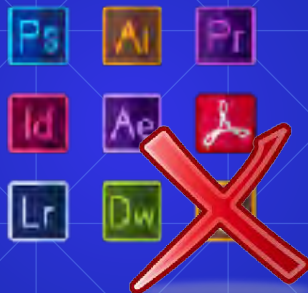
**sind damit alle Probleme  
gelöst?**

**Leider nein**

# Problem bleibt:











### Mobilen Account erstellen?

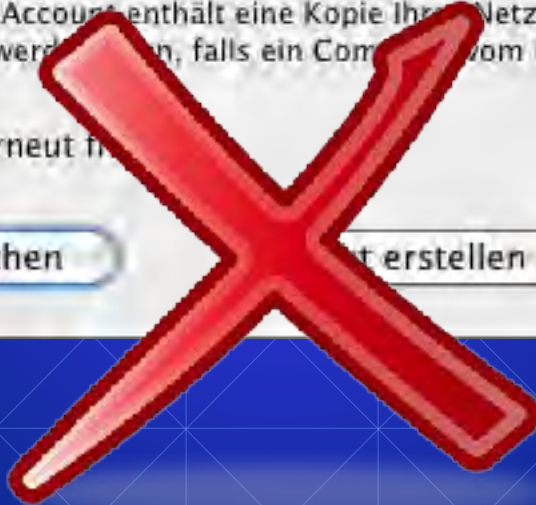
Der mobile Account enthält eine Kopie Ihrer Netzwerkaccounts, der verwendet werden können, falls ein Computer vom Netzwerk getrennt wird.

Nicht erneut fr...

Abbrechen

... erstellen

Jetzt erstellen



# wie sieht unsere derzeitige Lösung aus?











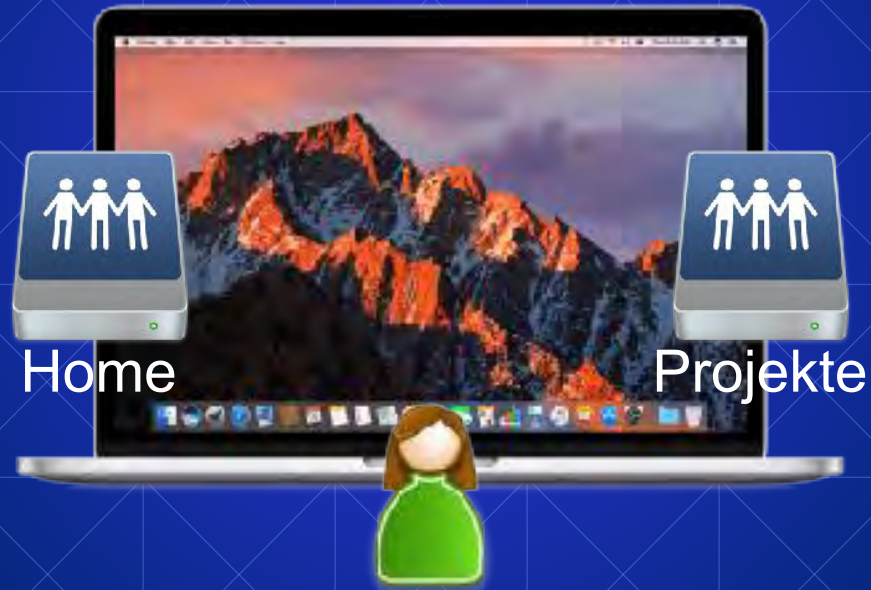


194GB / 200GB

67GB / 200GB

139GB / 200GB





# networkShareMounter

---



- von uns entwickelt
- automatisches mounten von Netzwerklaufwerken
- per MDM konfigurierbar
- bei Netzwechsel (WIFI,Ethernet,..) werden Laufwerke automatisch montiert
- <https://is.gd/Kvh87E>

# FAUAD.FAU.DE



# LINUX.FAU.DE



+



=



es gibt noch einiges zu tun







KEEP  
CALM  
AND  
USE  
~~ACTIVE DIRECTORY~~

*NoMAD +  
Kerberos*



**Fragen? Gerne!**

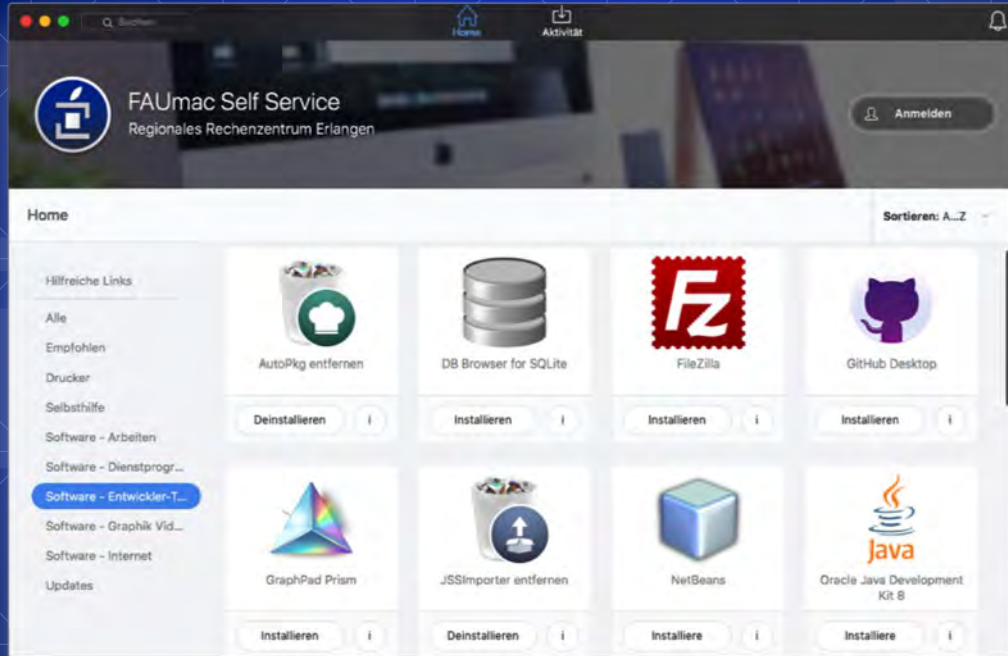
# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## Softwarepaketierung macht Spaß!

Vollautomatisierte Softwarepaketierung

AutoPkg, JSSImporter & GitLab CI vs. VPP



# 150 Softwaretitel



# 450 Policies

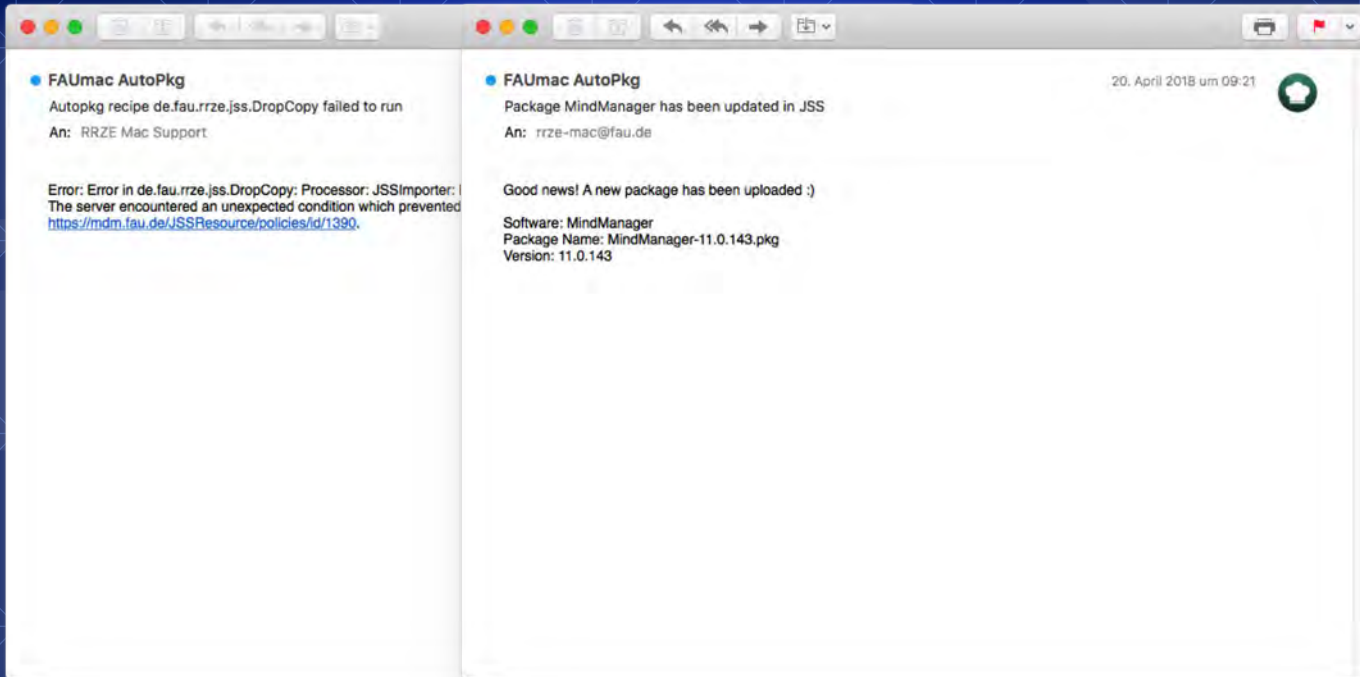


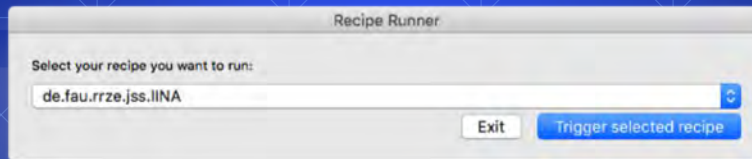






# Automatisierung













# SOFTWAREPAKETIERUNG MACHT SPASS!



Bestandteile

# Bausteine



# Bausteine



# Bausteine – AutoPkg & JSSImporter



- AutoPkg
  - Automatisierungsframework für macOS
  - Python geschrieben
  - Ursprünglich für Munki entwickelt
- JSSImporter
  - „Erweiterung“ für AutoPkg
  - Python-jss als Schnittstelle zum Jamf Pro

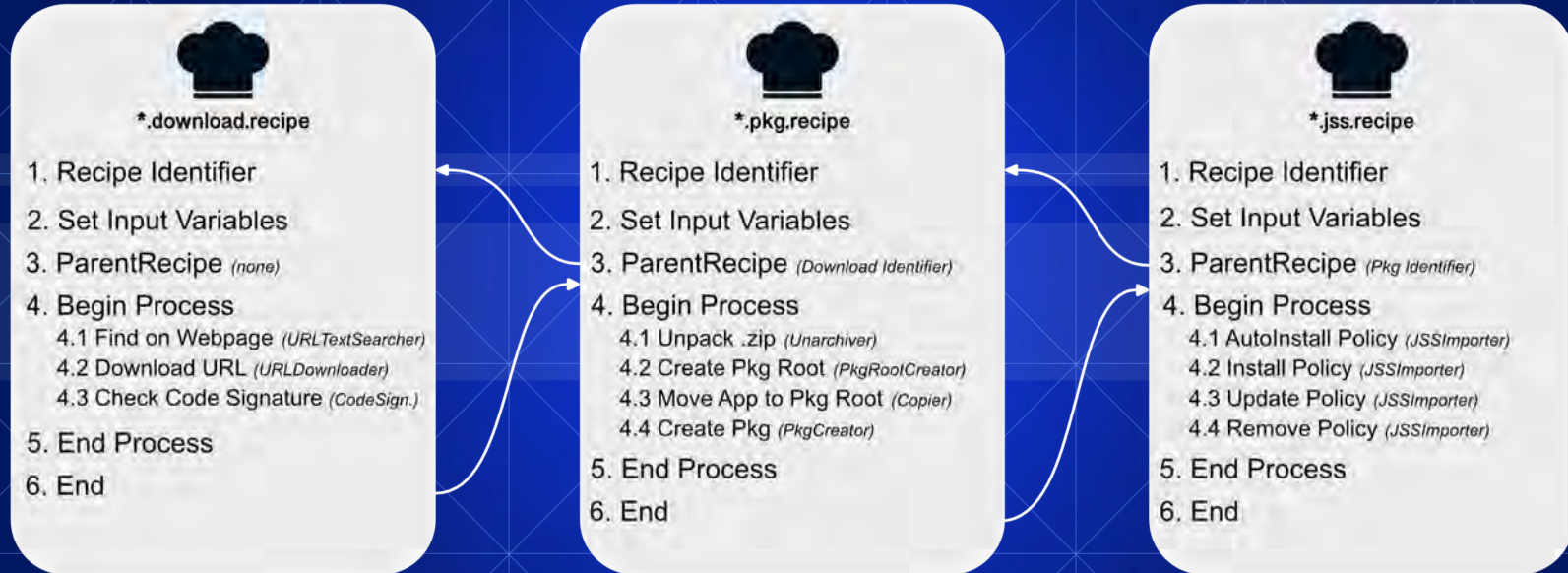


# Bausteine – AutoPkg & JSSImporter



- Paketierung erfolgt über Paketdefinitionen (Recipes)
- Recipes arbeiten hierarchisch Befehle ab
- Recipes können verknüpft werden

# Bausteine – AutoPkg & JSSImporter



# Bausteine – AutoPkg & JSSImporter



```
MaxQDA.download.recipe x
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4   <dict>
5     <key>Input</key>
6     <dict>
7       <key>IDENTIFIER</key>
8       <string>de.fau.rrze.download.MAXQDA2018</string>
9       <key>NAME</key>
10      <string>MaxQDA 2018</string>
11    </dict>
12    <key>MinimumVersion</key>
13    <string>0.2.0</string>
14    <key>Process</key>
15    <array>
16      <dict>
17        <key>Processor</key>
18        <string>URLDownloader</string>
19        <key>Arguments</key>
20        <dict>
21          <key>url</key>
22          <string>www.maxqda.de/updates/2018/MAXQDA2018.dmg</string>
23        </dict>
24      </dict>
25      <dict>
26        <key>Processor</key>
27        <string>EndOfCheckPhase</string>
28      </dict>
29      <dict>
30        <key>Processor</key>
31        <string>CodeSignatureVerifier</string>
32        <key>Arguments</key>
33        <dict>
34          <key>input_path</key>
35          <string>*pathname*/MAXQDA2018.app</string>
36          <key>requirement</key>
37          <string>identifier "de.verbi.MAXQDA2018" and anchor apple generic and certificate
38            1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13]
39            /* exists */ and certificate leaf[subject.OU] = "TME932KUT6"</string>
40        </dict>
41      </dict>
42    </array>
43  </dict>
44 </plist>
```

# Bausteine



# Bausteine



# Bausteine – GitLab (CI)



- CI = Continuous Integration
- Tool für Softwareentwicklung
  - Automatische Kompilierung des Quellcodes
  - Anschließende Distribution (daily builds)
- Aufgaben-Definition (gitlab-ci.yml)
- Aufgaben können von Runnern (parallel) abgefertigt werden

**→ Automatisierte (parallele) Durchführung von Jobs**



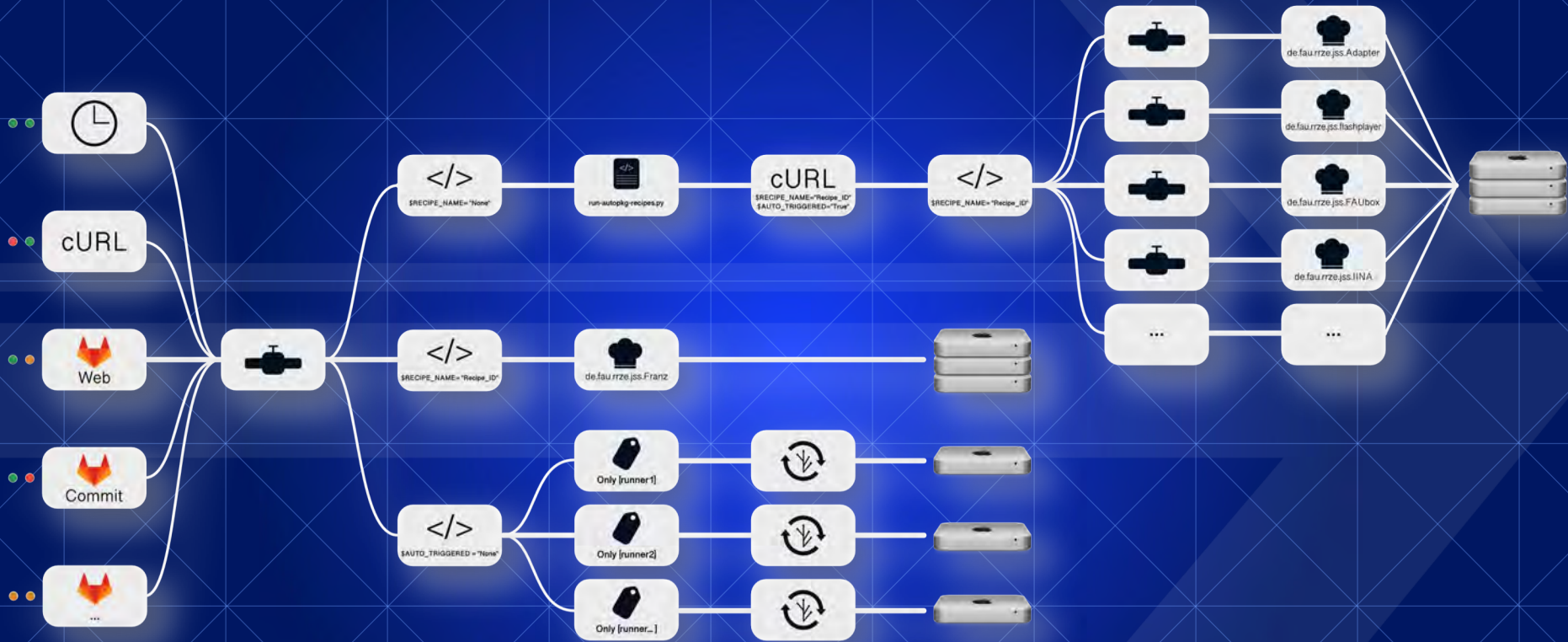


# SOFTWAREPAKETIERUNG MACHT SPASS!



Workflow

# Workflow



# DEMO



# SOFTWAREPAKETIERUNG MACHT SPASS!



Stolpersteine und Zukunft

# Stolpersteine

- Anpassung des *autopkg\_tools* von Facebook IT-CPE
- Fehlender Status zu hochgeladenen Paketen (Issue: 124)
- GitLab Runner unter macOS nur als Benutzer-Agent
- Diverse Kleinigkeiten

→ **Super einfach zu realisieren**



# Zukunft

- Paketier-Fehler über GitLab Issues abwickeln
- Kopplung mit einem Enterprise Collaboration Tool
  - Informierung über neue Pakete
  - Abfragen des Status
  - Triggern von Paketiervorgängen
  - ...



# Was ist mit VPP?

# Fragen?

# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## Apple Day am 12. Juli 2018

- **Neuigkeiten und Feedback zum Apple Rahmenvertrag**

# Rahmenvertrag Apple 2014 - 2018

## Vertrag mit Fa. Cancom 2014 - 2018

- Teilnehmer:
  - Insgesamt 33 Universitäten, Hochschulen, usw. in Bayern
- Laufzeit bis 31.10.2018
  - Wurde in KW 24 (15.6.2018) durch Würzburg bis 31.12.2018 verlängert
  - Weitere Verlängerung nicht möglich
- Deshalb ...

# Rahmenvertrag Apple 2019 - 2022

## Ausschreibung 2018 (Q3-Q4)

- EU-weite Ausschreibung (neutral)
  - **Umfrage zur Teilnahme inkl. Bedarfsmeldung (c/o: Würzburg)**
    - › **Deadline: Montag, 16.7.2018**
- Veröffentlichung: Ende September 2018
  - Angebotsabgabe: November 2018
- Zuschlag: Ende November 2018
- Vertragsstart: 1.1.2019
  - Laufzeit: 4 Jahre (2 + 1 + 1 Jahre)
- Apple-Vertragspartner 2019 - 2022: ???

# Rahmenvertrag Apple 2019 - 2022

## Ausschreibung-Portfolio

- Gesamtes Apple-Portfolio
  - inkl. iPhone, iPod, Apple Watch, HomePod, etc.
- Entsprechende Service-Leistungen, z.B.:
  - Reparatur durch Vertragspartner: PickUp & Return (max. 60 Monate)
  - Optional Apple Care (soweit möglich, iOS-Apple Care+ ist Versicherung)
  - Ggf. Apple Care for Enterprise-Service
    - › <https://www.apple.com/de/support/enterprise/onsite.html>
- Apple Care OS Support-Alliance
  - „Ähnlich Microsoft Enterprise Support“
    - › <https://www.apple.com/de/shop/product/D5691ZM/A/applecare-os-support-alliance>



# Rahmenverträge Apple 2014 - 2022

## Feedback Vertrag 2014 – 2018 (Fa. Cancom)

- Apple-Portfolio => Fehlte etwas?
- Abwicklung
  - Bestellungen, Servicefälle, etc.

## Neuer Vertrag 2019 -2022 (Fa. ???)

- Wünsche, Vorschläge, ...



**ZEIT FÜR FRAGEN**



**Fragen? Gerne!**

**Vielen Dank für Ihre Teilnahme!**

<http://blogs.fau.de/faumac>  
[rrze-mac@fau.de](mailto:rrze-mac@fau.de)



**CANCOM**