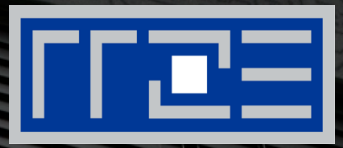
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Web Single Sign-On (WebSSO)

RRZE-Campustreffen, 28.04.2016

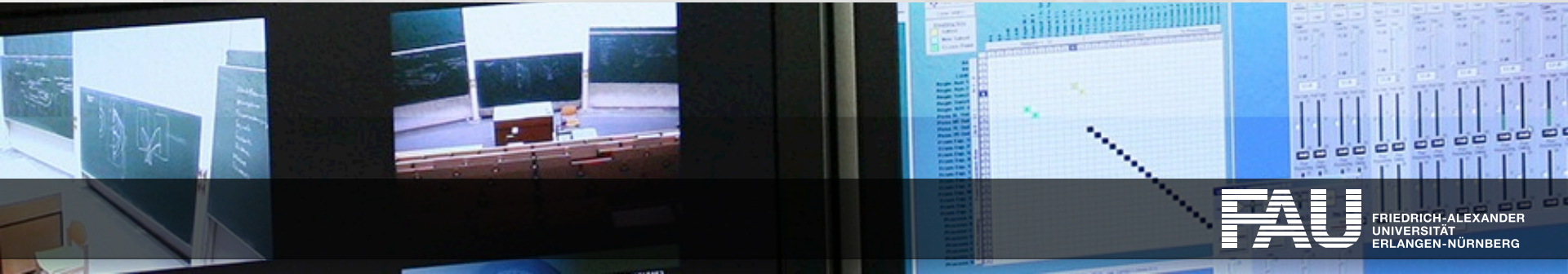
Frank Tröger, RRZE

Agenda

1. Einführung
   - „Was ist WebSSO?“
2. Historie
   - „Wie hat sich das WebSSO an der FAU entwickelt?“
3. Technik
   - „Welche Technik steht hinter dem WebSSO?“
4. Eigene Anwendung
   - „Wie kann ich eine eigene Anwendung an das WebSSO anbinden?“
5. Fazit

EINFÜHRUNG

Wieso? Weshalb? Warum? …



Web-Dienste eines (externen) Anbieters

Früher

- Anforderung
  - Benutzer einer Einrichtung will Web-Dienste eines Anbieters nutzen
- Umsetzung
  - Lokaler Account (dann aber nicht als Benutzer einer Einrichtung!)
  - Zugriff auf LDAP-Verzeichnis der Einrichtung
  - Austausch von Benutzerdaten (Login und Passwort-Hash)
  - …
- Problem: Benutzer meldet sich mit seinem Passwort an!

Web-Dienste eines (externen) Anbieters

Heute

- Anforderung
  - Benutzer einer Einrichtung will Web-Dienste eines Anbieters nutzen
- Umsetzung
  - Vertrauensstellung zwischen der Einrichtung und dem Anbieter
  - Zusicherung von „Attributen“ ohne die direkte Bereitstellung von Benutzername und Passwort-Hash
  - Keine Lieferung aller Benutzer
- Authentifikations- und Autorisierungs-Infrastruktur

Beteiligte Komponenten

Identity-Provider
Webserver
Einrichtung

Benutzer
Browser

Service-Provider
Webserver
Anbieter

Identity-Provider (IdP)

- Authentifiziert einen Benutzer
  - Normalerweise mittels Benutzername und Passwort
- Sichert Service-Providern „Attribute“ des Benutzers zu
  - Entscheidet pro SP über die weiterzugebenden „Attribute“

Service-Provider (SP)

- Bietet Benutzern einen Dienst an
  - Authentifizierung wird an den IdP ausgelagert
- Vertraut auf die von Identity-Providern übergebenen „Attribute“
  - Verwendet die „Attribute“
- Erhält nie das Passwort des Benutzers!

„Attribute“

- Beliebige Attribute übertragbar
- Vordefinierte Schemata erleichtern die Kooperation
- Beispiele:
  - eduPersonScopedAffiliation: employee@uni-erlangen.de
  - sn: Tröger
  - …

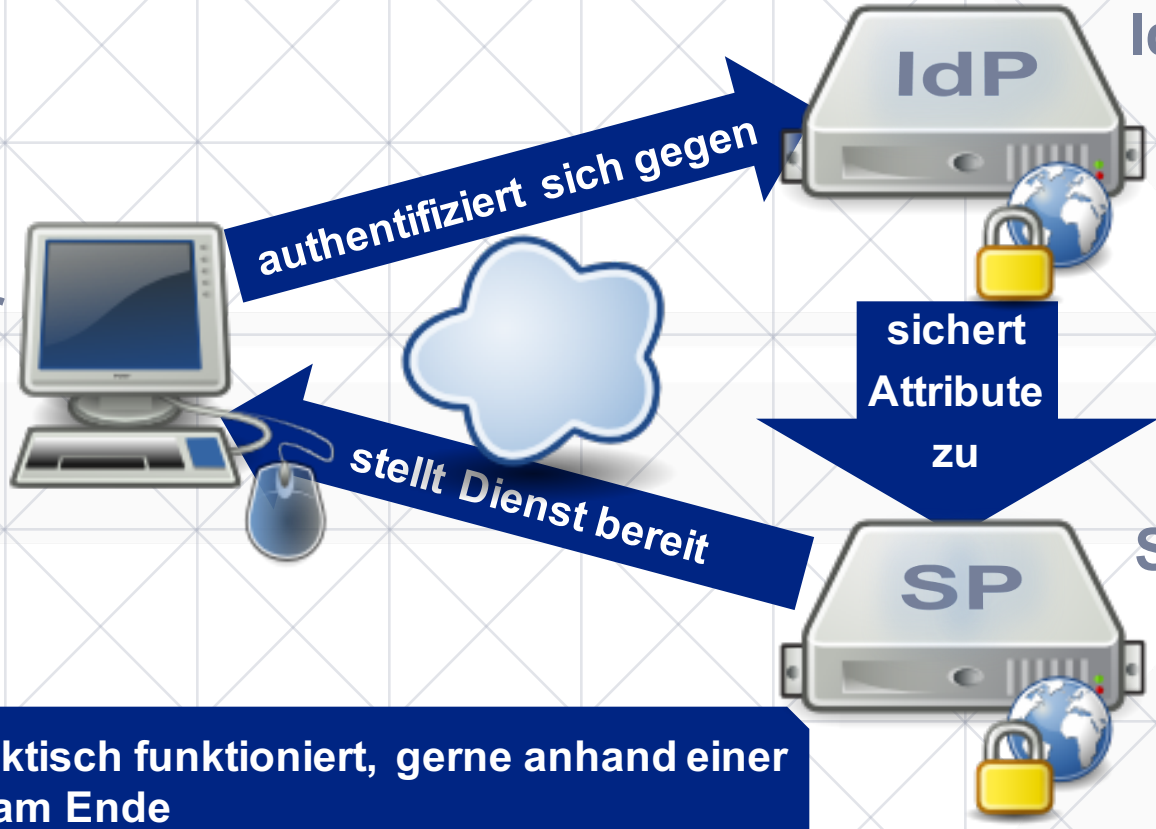
Föderation

- Mittler zwischen (meist vielen) IdPs und SPs

„Sie schafft das notwendige Vertrauensverhältnis sowie einen organisatorischen und technischen Rahmen für den Austausch von Benutzerinformationen zwischen Einrichtungen und Anbietern.“

Quelle: https://www.aai.dfn.de/ (Stand: 28.04.2016)
DFN-AAI – Authentifikations- und Autorisierungs-Infrastruktur

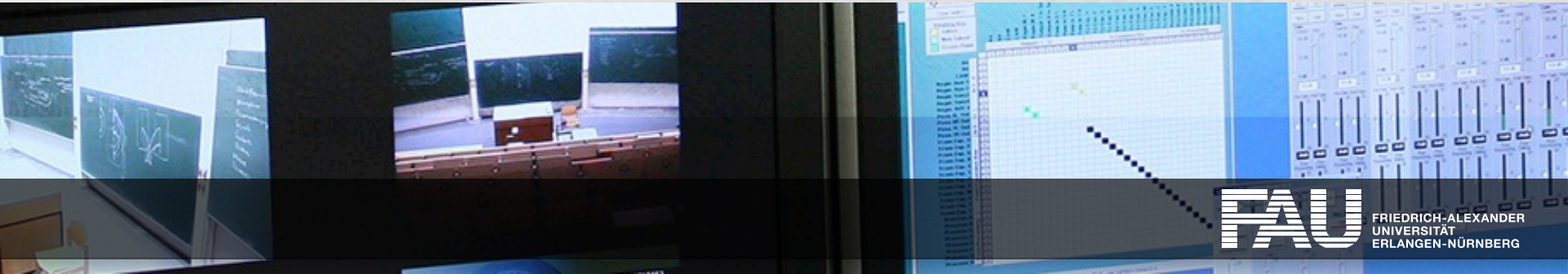
Überblick



Wie das praktisch funktioniert, gerne anhand einer Live-Demo am Ende

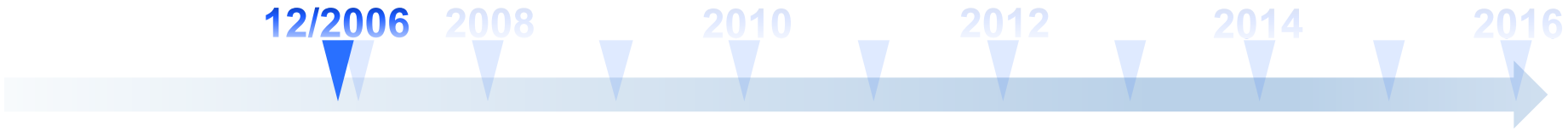
HISTORIE

„Vor dem Gewinnen steht stets das Beginnen.“



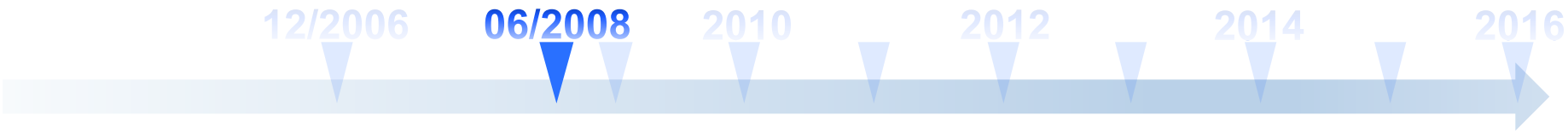
Historie – … wie alles begann

- Beschäftigung mit dem Thema WebSSO / Shibboleth



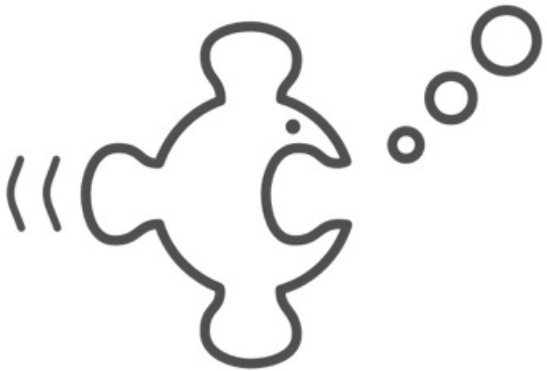
SimpleSAMLphp IdP

- Beschäftigung mit dem Thema WebSSO / Shibboleth
- Erster Kontakt mit SimpleSAMLphp



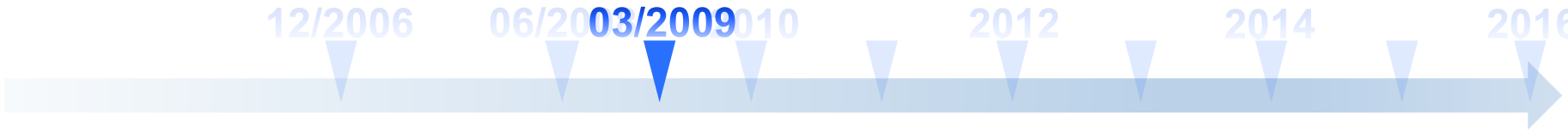
Produkte – damals wie heute

- Sowohl IdP als auch SP
  - Shibboleth
    - IdP: Java-Anwendung
    - SP: Apache2-Modul + Daemon
    - https://shibboleth.net/
  - SimpleSAMLphp
    - PHP-Anwendung
    - https://simplesamlphp.org/



SimpleSAMLphp IdP

- Beschäftigung mit dem Thema WebSSO / Shibboleth
- Erster Kontakt mit SimpleSAMLphp
- Erste Testinstallation



SimpleSAMLphp IdP

- Beschäftigung mit dem Thema WebSSO / Shibboleth
- Erster Kontakt mit SimpleSAMLphp
- Erste Testinstallation
- Produktiver Betrieb

SimpleSAMLphp IdP

- Beschäftigung mit dem Thema WebSSO / Shibboleth
- Erster Kontakt mit SimpleSAMLphp
- Erste Testinstallation
- Produktiver Betrieb
- Beitritt DFN-AAI-Föderation

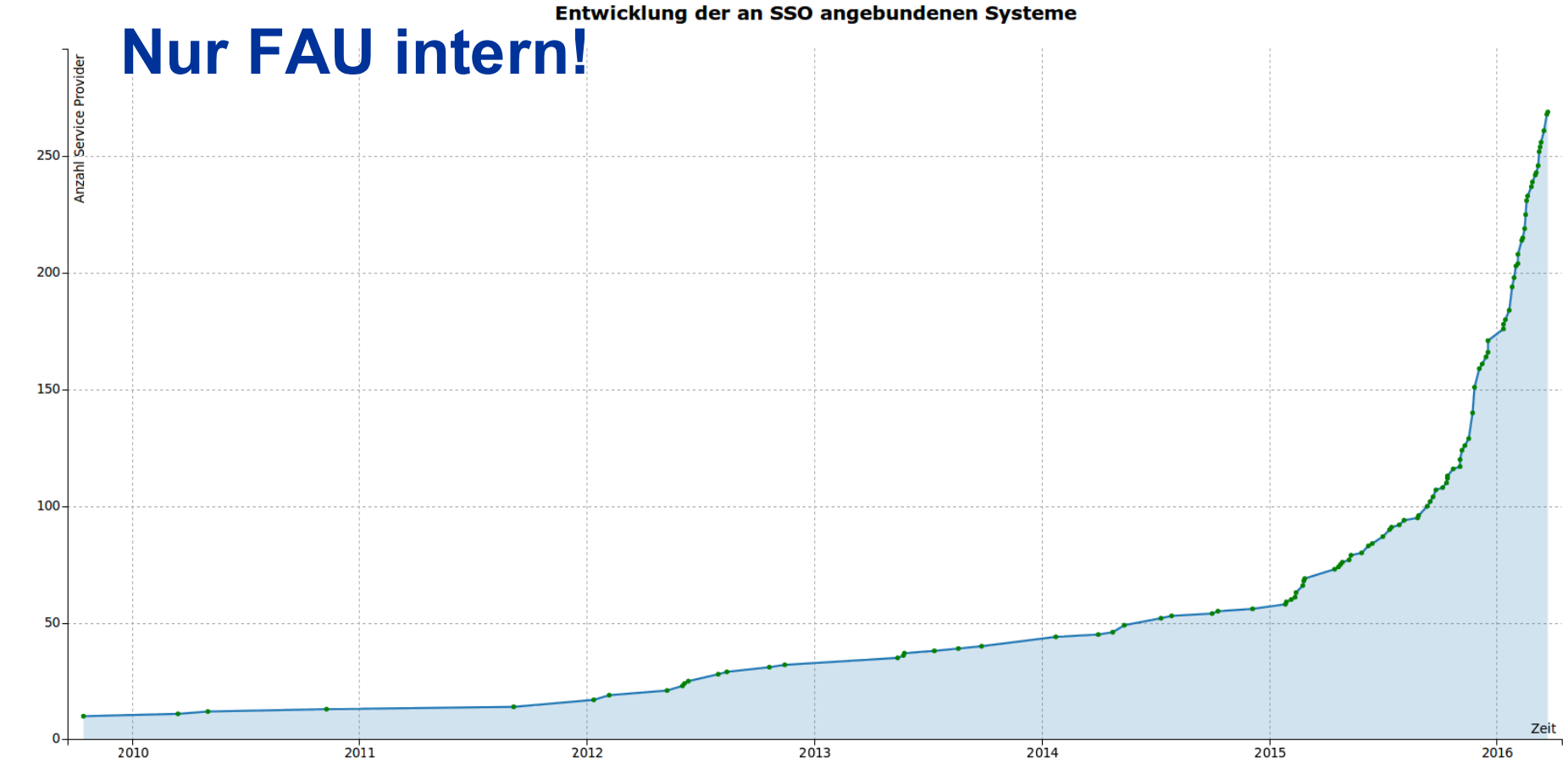
SimpleSAMLphp IdP

- Beschäftigung mit dem Thema WebSSO / Shibboleth
- Erster Kontakt mit SimpleSAMLphp
- Erste Testinstallation
- Produktiver Betrieb
- Beitritt DFN-AAI-Föderation
  - Registrierung VHB mittels WebSSO

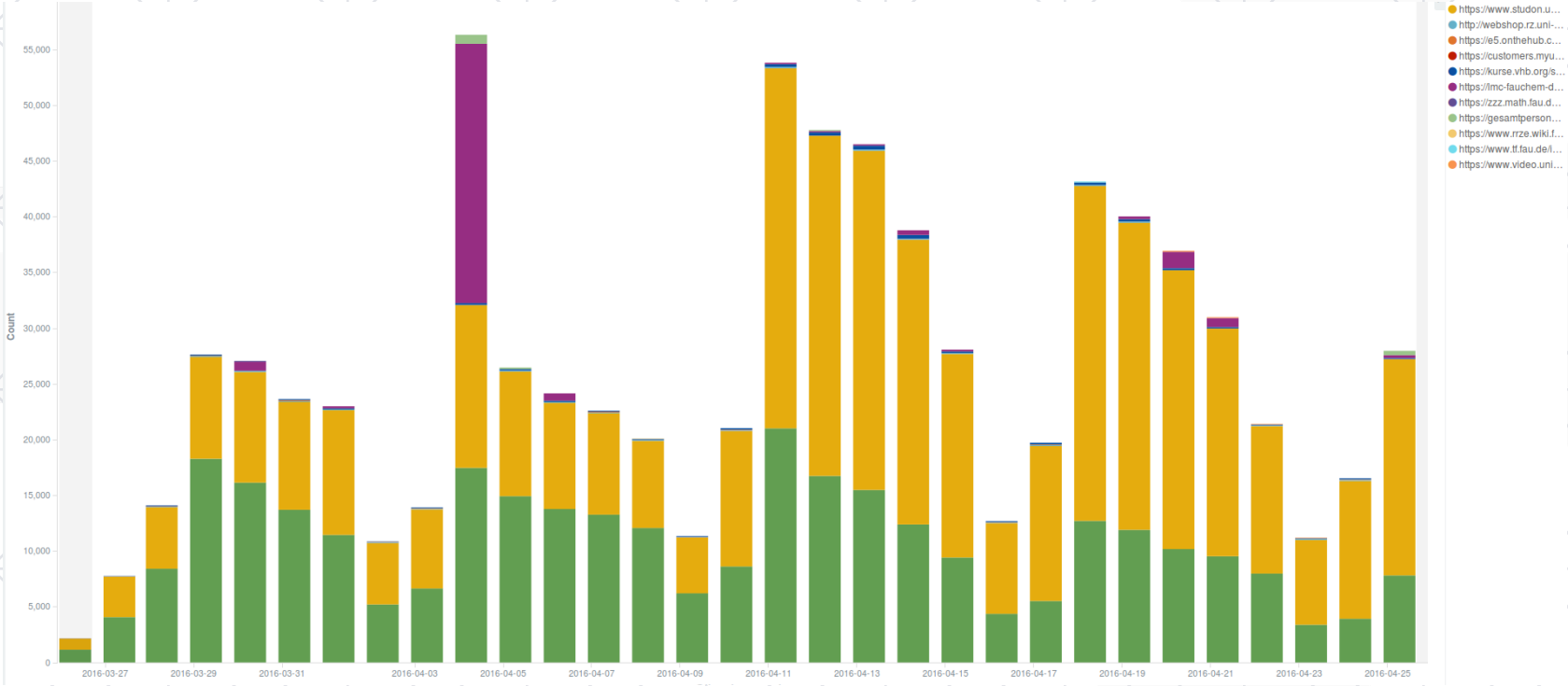
SimpleSAMLphp IdP

- Beschäftigung mit dem Thema WebSSO / Shibboleth
- Erster Kontakt mit SimpleSAMLphp
- Erste Testinstallation
- Produktiver Betrieb
- Beitritt DFN-AAI-Föderation
  - Registrierung VHB mittels WebSSO
- Beitritt eduGAIN-Interföderation

Nur FAU intern!



Anmeldungen pro Tag
Auszug 27.03.16 bis 25.04.16



Randbedingungen

- Stiefmütterliche Behandlung, da „kleiner Bruder“ des Identity-Management-Projekts
  - Keine explizite Personalressourcen!
- Seit 02/2012:
  Aufbau einer neuen Infrastruktur als Abschlussprojekt eines Auszubildenden
- http://blogs.fau.de/pp/category/idm/web-sso/

TECHNIK

„Software is like Sex: it‘s best if it‘s free.“

Linus Torvalds

IdP der FAU

Benutzer
Browser

„Infrastruktur“ bis 18.02.2016

Neue Infrastruktur seit 02/2012 im „Aufbau“!!!

Ein virtueller Server:

- **SimpleSAMLphp**
- **Apache2**
- **OpenLDAP**
- **PostgreSQL**

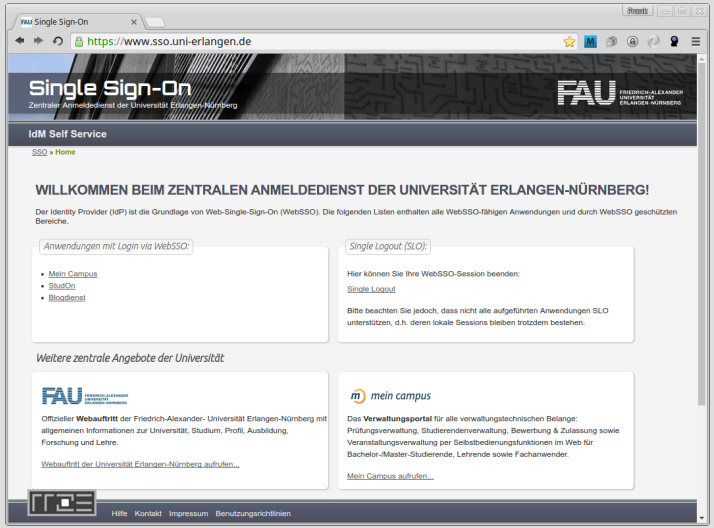
Und heute …

Vorne … (Mitnutzung der IdM-Infrastruktur)

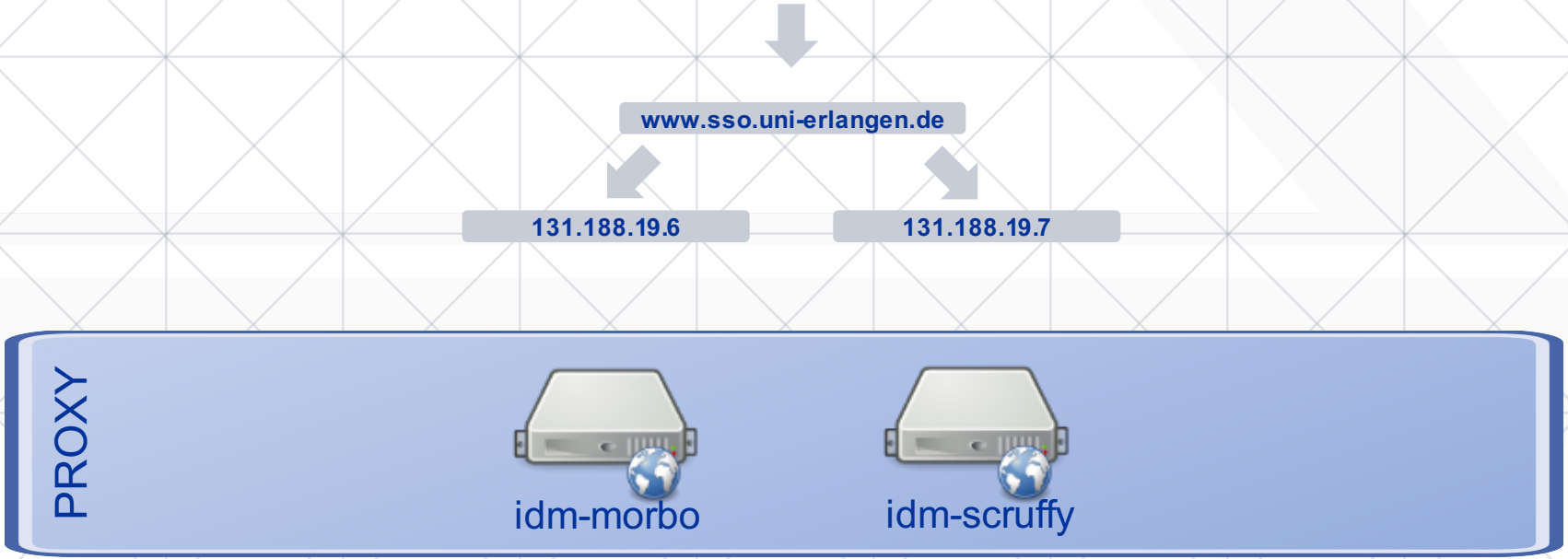
Stichwort: Apache HTTP Server

www.sso.uni-erlangen.de

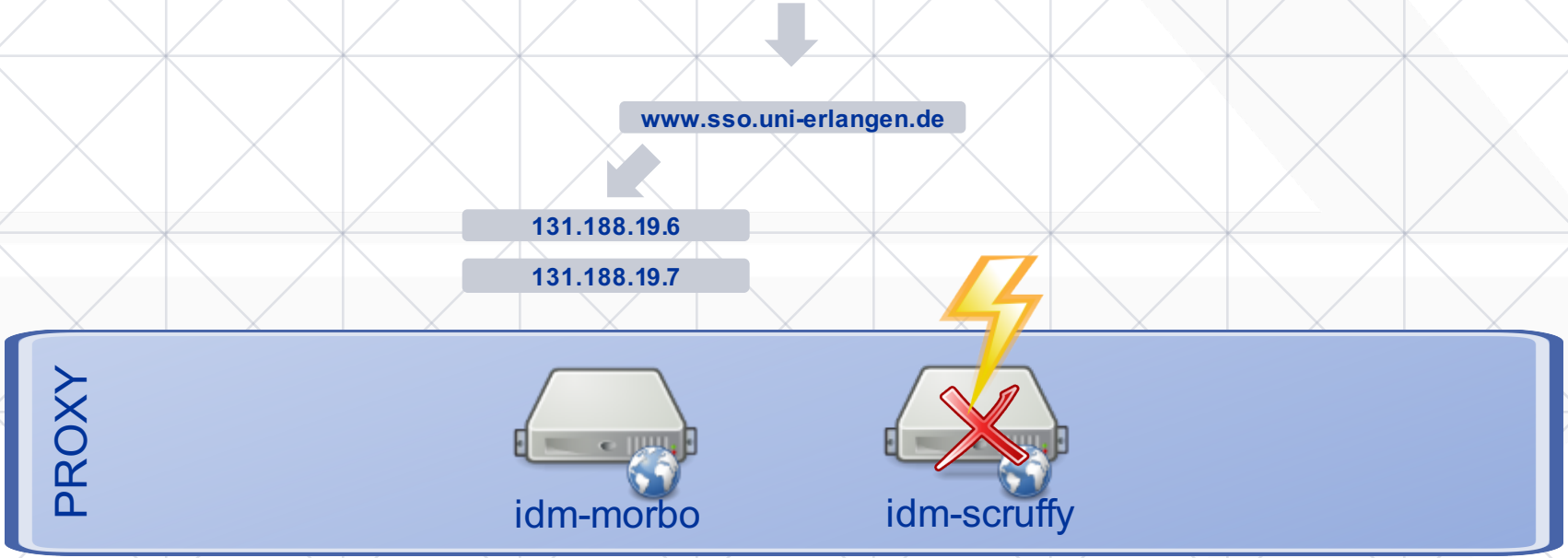
```
foo@bar:~$ dig www.sso.uni-erlangen.de +short
131.188.19.7
131.188.19.6
```



Web-/Proxy-Server – DNS „Load-Balancing“



Web- / Proxy-Server – Ausfall / Wartung



Stichworte: Corosync und Pacemaker

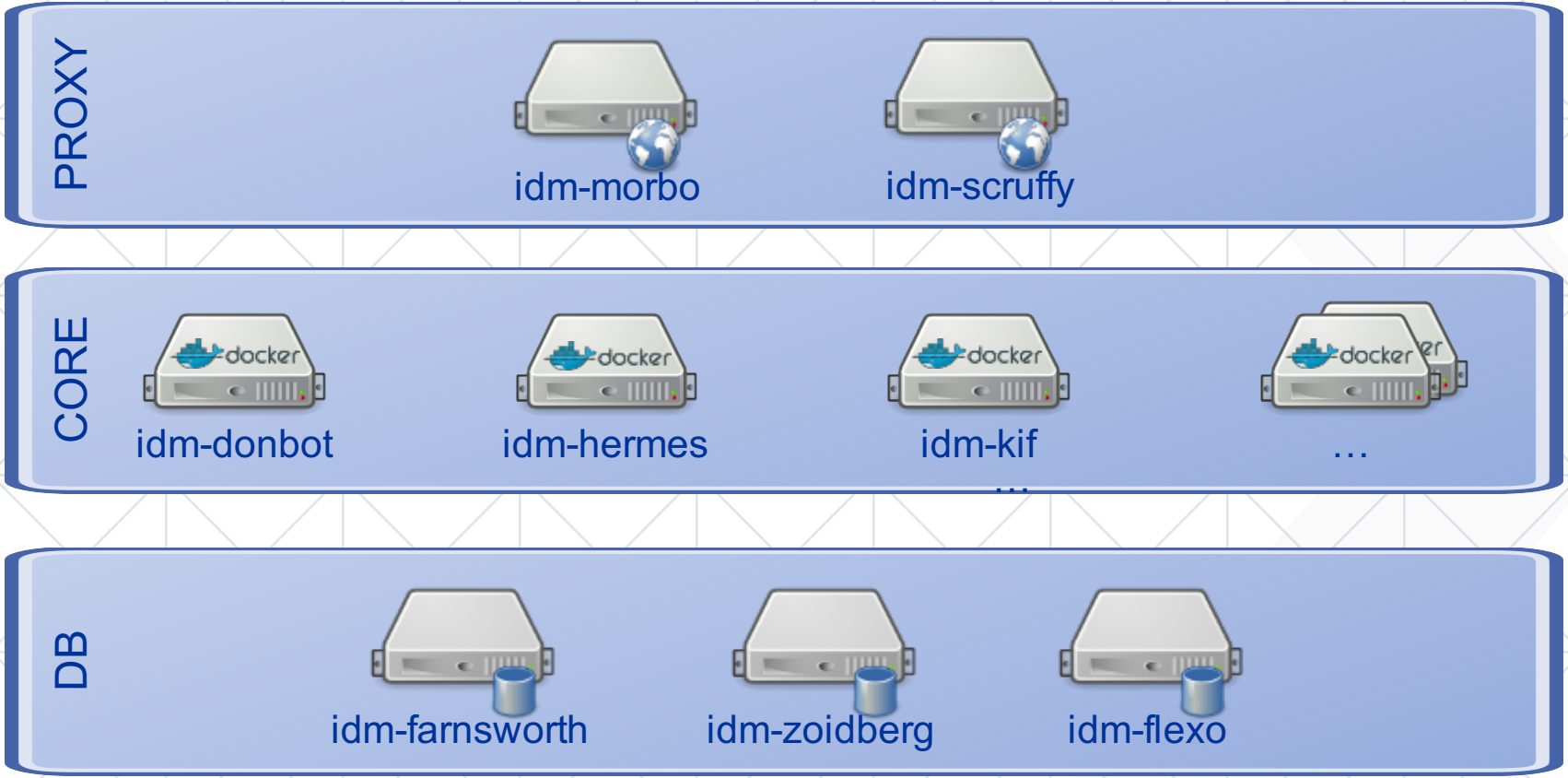
Hinten … (Mitnutzung der IdM-Infrastruktur)

Stichworte: Memcache, MongoDB, PostgreSQL, OpenLDAP

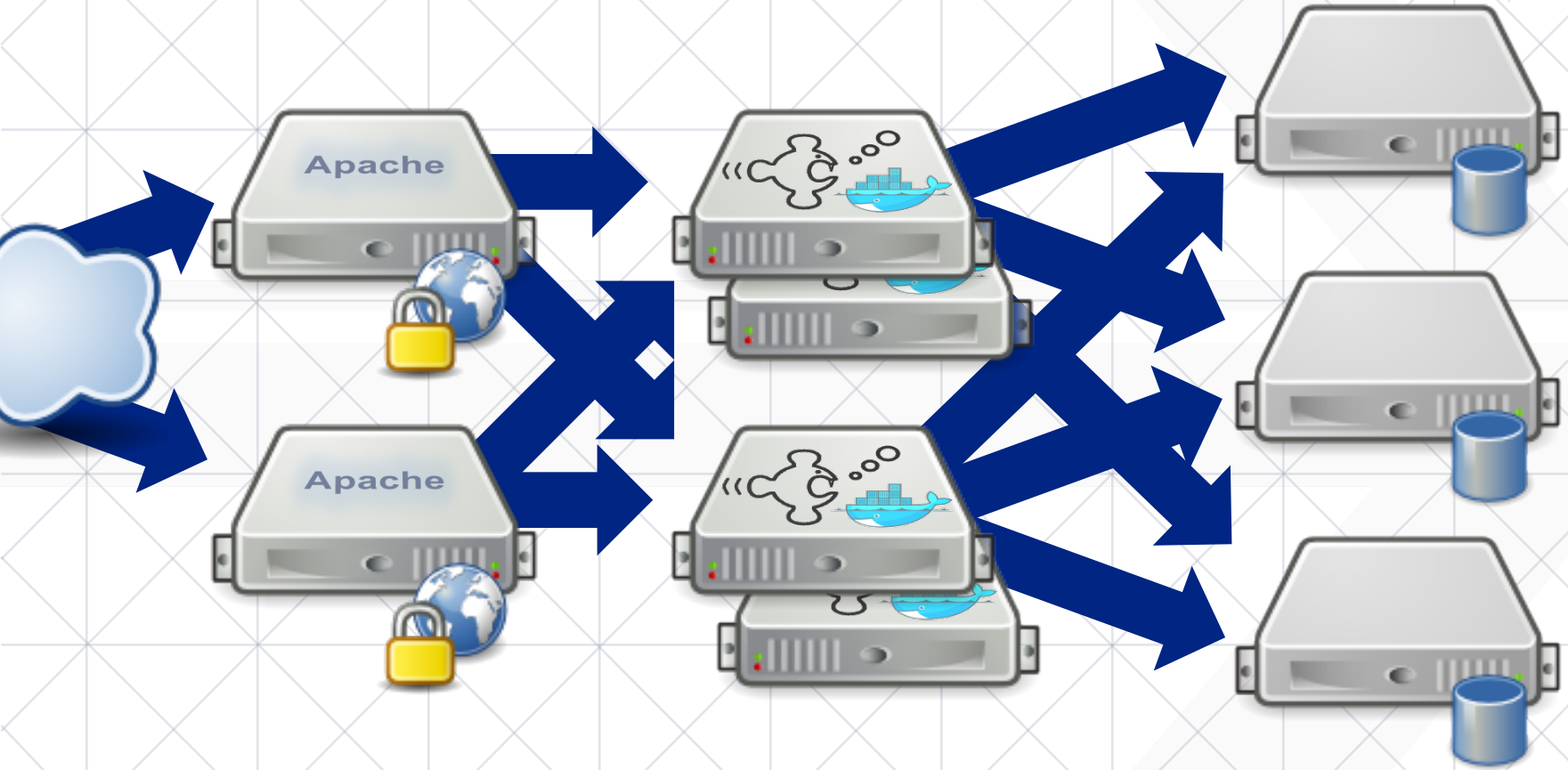
Mitte … (Mitnutzung der IdM-Infrastruktur)

Stichwort: Docker

Überblick (Mitnutzung der IdM-Infrastruktur)



Infrastruktur seit 18.02.2016



EIGENE ANBINDUNGEN

Selbst ist die Frau / der Mann

Was muss ich als Betreiber einer Anwendung tun?

- Mit uns (sso-support@fau.de) in Kontakt setzen
- Service-Provider-Software aufsetzen und betreiben
- Rechtliche Voraussetzungen schaffen
- Aufstellung der benötigten Attribute

WebSSO-Admins der FAU

- https://www.helpdesk.rrze.uni-erlangen.de – FAQ – SSO
- E-Mail an sso-support@fau.de
- Telefon: 09131 / 85-28727
- Infos:
  - Name, Telefon, E-Mail-Adresse des Ansprechpartners
  - Name des Systems
  - Technische Attribute (Metadaten)
  - Benötigte Attribute

Service-Provider-Software

- **Shibboleth SP**
  - Daemon
  - Apache2-Modul
  - Beliebige Web-Anwendungen

- **SimpleSAMLphp**
  - PHP-Anwendung
  - Sehr einfache Integration bei PHP-Anwendungen

Rechtliche Voraussetzungen

- Freigabe des Verfahrens durch den Datenschutzbeauftragten (DSB)
- Frühzeitig informieren
- https://www.fau.de/universitaet/leitung-und-struktur/gremien-und-beauftragte/beauftragte/datenschutzbeauftragter/

Warum sollte ich mein System anbinden?

1. Gesteigerte Datenqualität und -aktualität
   - Achtung: „Datenübertragung“ nur bei der Anmeldung!
2. Verbesserte Benutzerfreundlichkeit
   - Single Sign-On
3. Weniger bis kein Aufwand mit der „Benutzerverwaltung“
   - Passwort vergessen
   - …

FAZIT

Da war doch was mit Single Sign-On …

Single Sign-On

- Eigentlich nur ein netter Nebeneffekt

Mehr dazu in der Live-Demo … jetzt

Live-Demo

KONTAKT

E-Mail: frank.troeger@fau.de
Tel: 09131 / 85-28727
IRL: Raum 1.020, RRZE, Martensstr. 1, 91058 Erlangen

ORGANISATORISCHES

- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Weitere Vorträge im Rahmen des „Campustreffens“

21.04.2016 − Adobe InDesign und Photoshop

28.04.2016 − Web Single Sign-On (WebSSO)

12.05.2016 − NVIDIA

02.06.2016 − Videokonferenzen

09.06.2016 − Webmaster-Campustreffen

23.06.2016 − Apple-Day

30.06.2016 − HPC-Campustreffen

07.07.2016 − Windows 10 – Windows 10 Umfeld

14.07.2016 − FAUbox-Campustreffen

- immer donnerstags (ab 15 c.t.)
- Raum 2.049 im RRZE

Andere Vortragsreihen des RRZE

Systemausbildung „Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten”

- immer mittwochs ab 14 Uhr c.t. (in den Sommersemestern)
- Ergänzung zur Netzwerkausbildung “Praxis der Datenkommunikation”
- führt in den grundsätzlichen Aufbau eines Systems sowie eingesetzte Techniken und Komponenten ein
- richtet sich primär an alle Interessierten (Studierende & Beschäftigte)

Netzwerkausbildung „Praxis der Datenkommunikation“

- immer mittwochs ab 14 Uhr c.t. (in den Wintersemestern)
- führt in die Grundlagen der Netztechnik ein
- richtet sich primär an Studierende & Netzwerkadmins

Vortragsfolien & Vortragsaufzeichnung

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

http://www.rrze.fau.de/news/campustreffen.shtml

Die meisten Vorträge des RRZE werden aufgezeichnet und können nach der Veranstaltung vom Videoportal der FAU herunter geladen werden:

www.fau.tv

RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter: http://www.rrze.fau.de/news/kalender.shtml

- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet.
  - Auch diese Liste kann man abonnieren: https://lists.fau.de/mailman/listinfo/rrze-aktuelles

Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Campustreffen)

Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
http://www.rrze.fau.de