Karlsruher Institut für Technologie

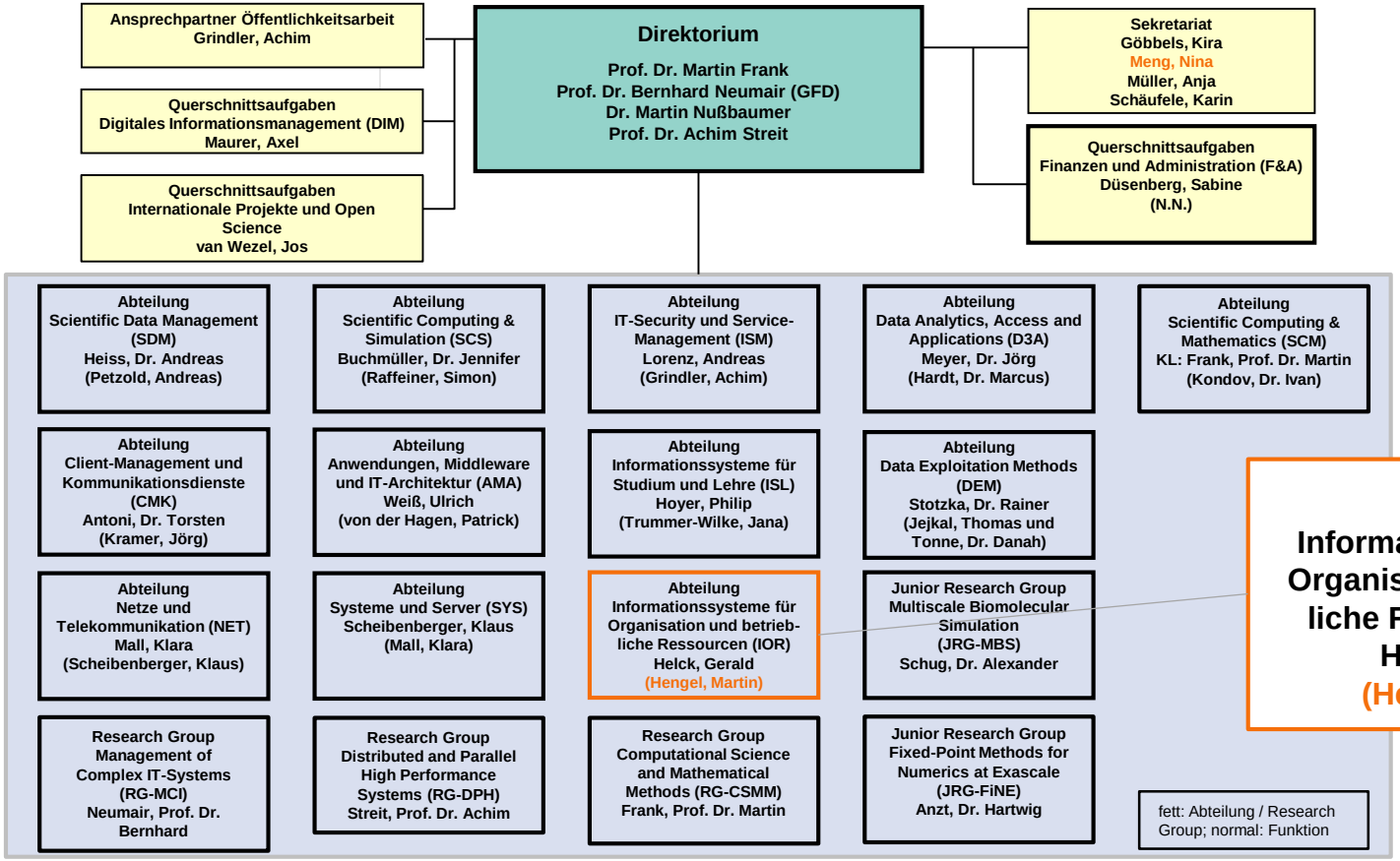
21. IT-Beauftragten Versammlung am 12. Mai 2021

Partnerschaftliche Zusammenarbeit zwischen SCC und ITB

Agenda

- Begrüßung & Neues aus dem SCC
- Behandlung von Sicherheitslücken in Embedded Systems
- Single Sign-On für dezentrale Anwendungen – Authentifizierung mit Shibboleth/SAML und OpenID Connect
- Backuplösung mobiler Geräte – Update
- Änderungen an IT-Infrastruktur und IT-Diensten
  - NHR@KIT - Inbetriebnahme HoreKa
  - SAP Portal - Umstellung Neues Framework
  - Netzwerk-Infrastruktur - KITnet, VPN
  - Filesharing und Datenbanken
  - Umstellung der KIT-Webserver auf https-only
- Sonstiges / Diskussion
  - Ausblick:
    - Zentrale Empfehlung für Stockwerksdrucker
    - Zentrale E-Mail-Archivierung
  - Virtueller Rundgang

Begrüßung & Neues aus dem SCC



Abteilung

Informationssysteme für Organisation und betrieb-liche Ressourcen (IOR)
Helck, Gerald
(Hengel, Martin)

Behandlung von Sicherheitslücken in Embedded Systems

Was sind Embedded Systems?

- Computer, die in einem technischen Gerät eingebaut sind
  - Drucker
  - Messgeräte
  - Appliances
  - …
- Die meisten davon haben heutzutage eine Internetanbindung
  - „Intelligent“
  - „Smart Home“
  - „Connected Drive“
  - „Internet of Things“ (IoT)
  - …

Embedded Systems als Angriffsziel

- Durch Netzwerkverbindung aus der Ferne angreifbar
- Am Sicherheitsmanagement des Herstellers wird gespart
- Beim Sicherheitsmanagement im Betrieb schnell vergessen
- Dadurch leichter angreifbar als Desktops oder Server:
  - Definierter Security-Lifecycle vs. Sell-and-Forget
  - Schlimm: Keine automatischen Updates
  - Schlimmer: Der Hersteller veröffentlicht keine Sicherheitsupdates
  - Worst Case: Es gibt gar keine Möglichkeit, ein Update einzuspielen

Beispiele

- September 2020: RIPPLE 20 (vorgestellt im September-IT-EK)
- Dezember 2020: Amnesia-33
- Mitte April 2021: NAME:WRECK
- Ende April 2021: BadAlloc
- Was bringt die Zukunft…?

Problematik

- Angreifbare Systeme können übernommen werden
- Auch auf einem Embedded-Gerät können vertrauliche oder personenbezogene Daten verarbeitet werden
  - Credentials
  - Ausdrucken von Gehaltsabrechnungen / Verträgen / …
  - …
- Auch von einem Embedded-Gerät kann ein Angreifer andere Systeme angreifen

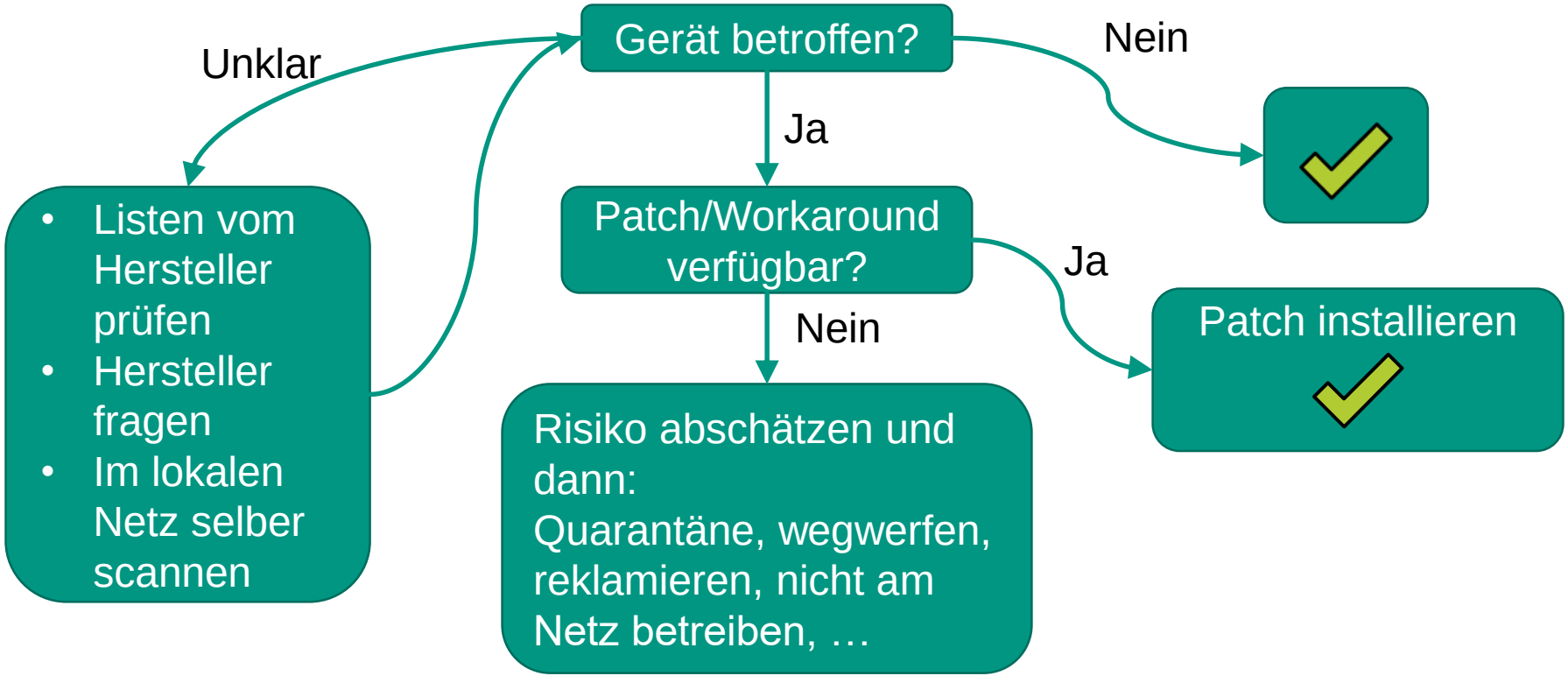
Was tun?

- Beim Hersteller von solchen Systemen nachschauen/nachfragen, ob ein System angreifbar ist
- Es gibt einen Scanner[1], um potentiell anfällige Geräte zu erkennen
  - Erkennt nicht direkt die Sicherheitslücken, sondern nur ob potentiell angreifbare Software auf dem Gerät läuft
  - Die Erkennung ist ungenau
  - Liefert nur im lokalen Netz (BCD) nutzbare Ergebnisse

→ Ihr müsst das selbst machen, wir können das nicht zentral

[1] Install-Skript für Debian hier

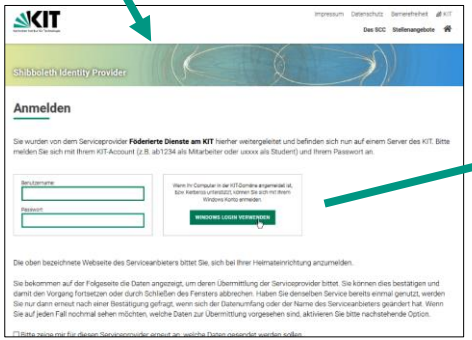
Flowchart

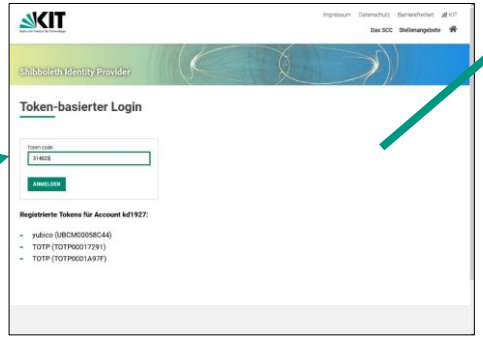

Gerät betroffen?
Nein
Unklar
Ja
Patch/Workaround verfügbar?
Ja
Nein
Patch installieren
• Listen vom Hersteller prüfen
• Hersteller fragen
• Im lokalen Netz selber scannen
Risiko abschätzen und dann:
Quarantäne, wegwerfen, reklamieren, nicht am Netz betreiben, …

Single Sign-On für dezentrale Anwendungen
Authentifizierung mit Shibboleth/SAML und OpenID Connect

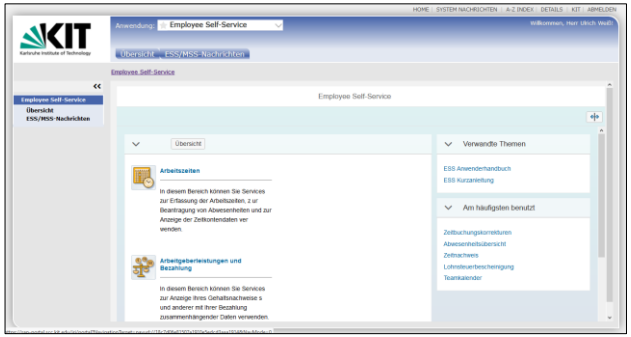
Single Sign-On

Anwendung





Heimat Identitätsprovider (IdP)

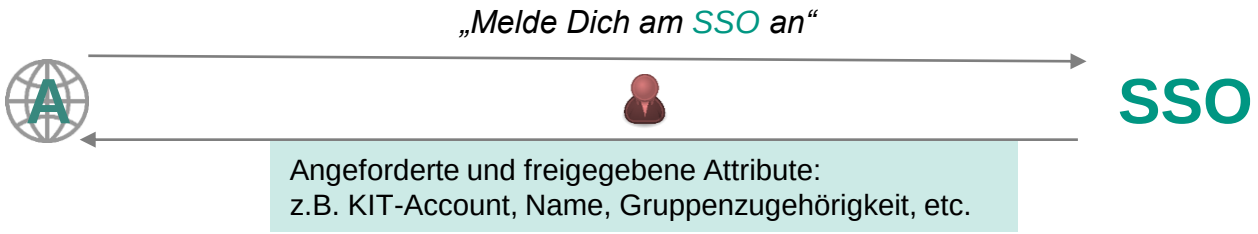


Anwendung/Service/
Service Provider (SP)

Steinbuch Centre for Computing

Single Sign-On

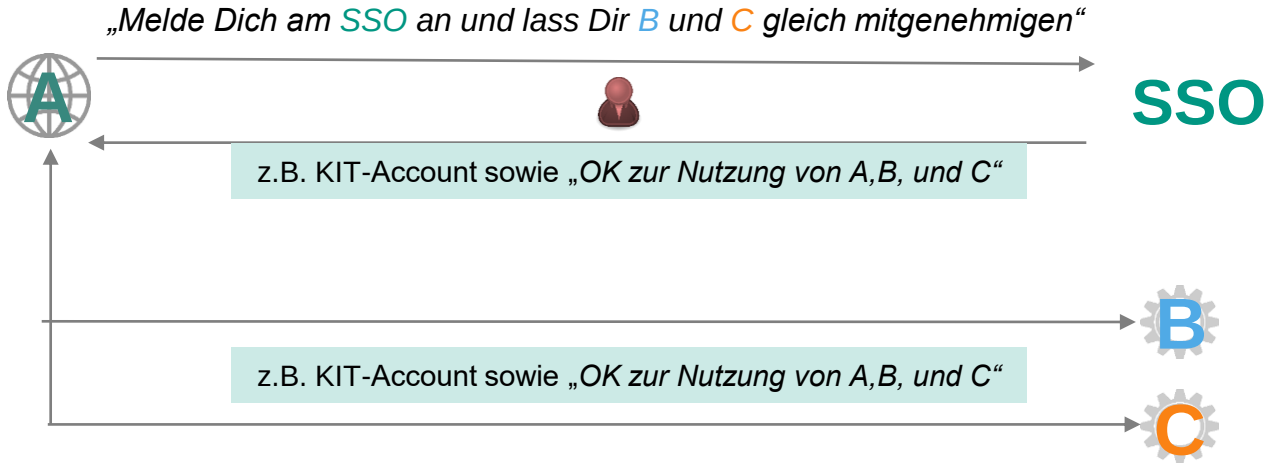
- **Person** möchte **Dienst A** nutzen
- **Dienst A** authentifiziert **Person** am zentralen **Single Sign-On**



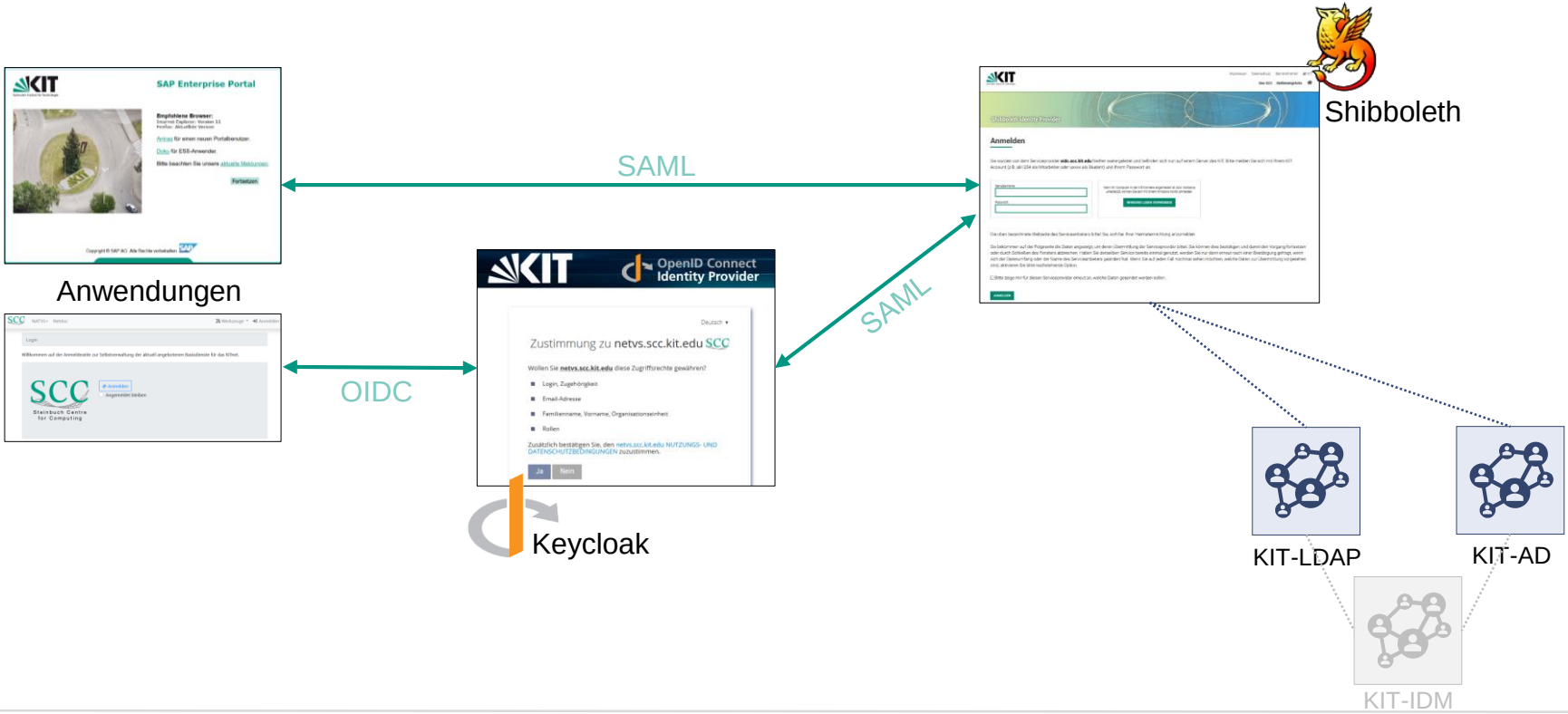
- **Dienst A** kann sicher sein, dass sich *ab1234@kit.edu* angemeldet hat

Erweitertes Anwendungsszenario

- **Person** möchte **Dienst A** nutzen
- **Dienst A** authentifiziert **Person** am zentralen **Single Sign-On**
- **Dienst A** will dabei zusätzlich **Dienst B** und **Dienst C** nutzen

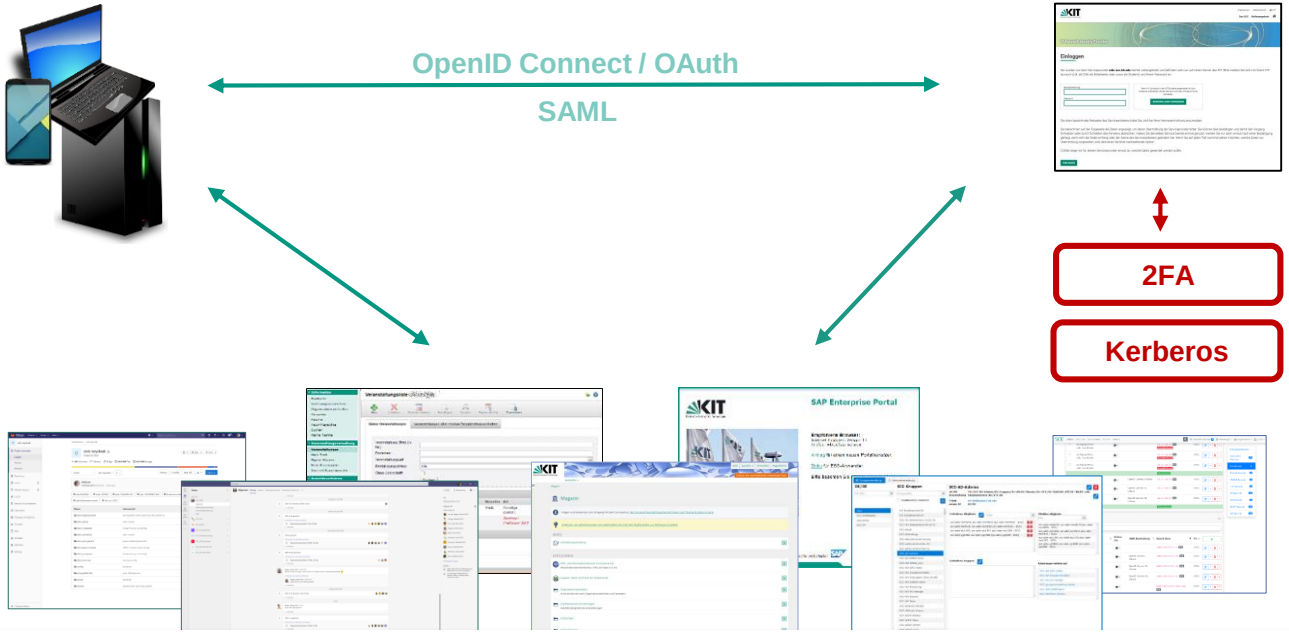


SAML oder OpenID Connect am KIT?



Steinbuch Centre for Computing

SSO-Landschaft am KIT mit 2FA & Kerberos



Technik / Attribute

- Attribute (nach Dienstanforderung und nach Freigabe durch Nutzende)
  - KIT-Account
  - Zugehörigkeiten (member, employee, student, affiliate)
  - Berechtigungen (entitlements)
  - Vor- und Nachname
  - Organisationseinheit
  - Gruppenmitgliedschaften
  - Studiengang
  - …weitere möglich, meist aber nicht notwendig
- Identitätsinformationen werden als signiertes XML (SAML) oder als signiertes JSON (OIDC) geliefert

Technik / Attribute

- Filterung von Attributen und Zugangsbeschränkungen auf Basis von Kontoeigenschaften/Zugehörigkeiten möglich
- 2FA auch auf Nutzergruppen/Zugehörigkeiten einschränkbar
- Admin- und Servicekonten werden unterstützt, sofern Dienst diese benötigt

Voraussetzungen

- Alle Anwendungen mit nativer SAML/OIDC-Funktion werden unterstützt
  - Web, Single-Page-Apps, Standalone, Mobile, Kommandozeile
  - Autologin für (Hintergrund-) Dienste und Skripte
  - Integration von modernen API-Diensten: Dienst integriert andere Dienste im Namen der angemeldeten Person
- Webanwendungen auch mit vorgeschaltetem Proxy möglich
- Web- und Single-Page-Apps nur mit https
- Anwendung sollte Konten durch KIT-Kürzel identifizieren (nicht: Email!)
- Email-Zertifikat wegen verschlüsselter Kommunikation mit SCC

Eigene Daten und weitere Infos

- OpenID Connect
  - https://oidc.scc.kit.edu
  - Kontoinformationen, Sitzungen, Anwendungen inkl. freigegebener Daten: https://oidc.scc.kit.edu/auth/realms/kit/account
  - SCC-Infos: https://www.scc.kit.edu/dienste/openid-connect

- Shibboleth / SAML
  - https://bwidm.scc.kit.edu
  - SCC-Infos: https://www.scc.kit.edu/dienste/6921

Am KIT: SAML oder OpenID Connect?

SAML

Für föderierte Dienste oder
falls Anwendung kein OIDC kann

Anwendungen

OIDC

Einfach bevorzugt

In den letzten sieben Tagen

ILIAS

MS-Teams

CAMPUS

intranet.kit.edu

SAP

30.000 verschiedene Benutzende

bwIDM

450.000 Logins an **190** Diensten

my.kit.edu

portal.wiwi

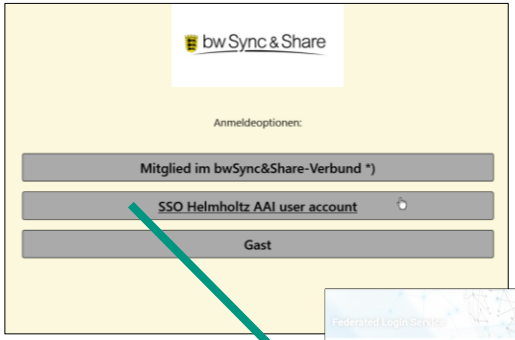
bwservices.uni-fr

Zoom

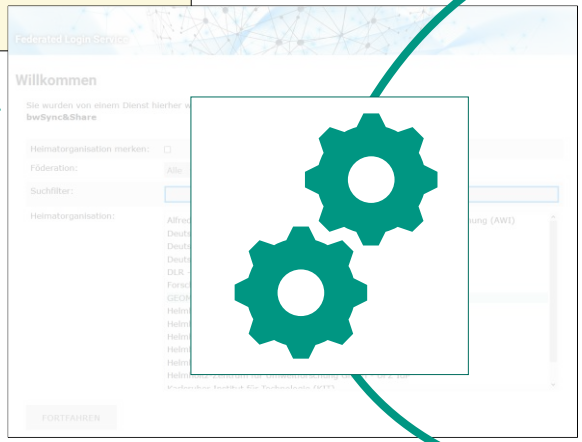
sciencedirect.com

bwservices.uni-hd

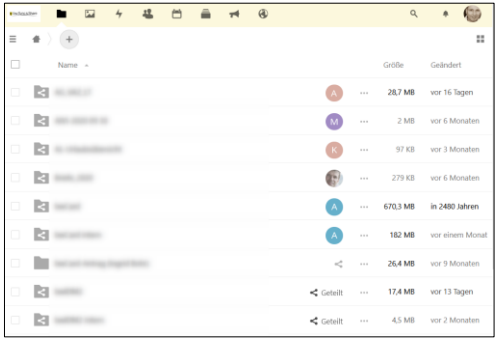
Föderierte Dienste



Service



RegApp

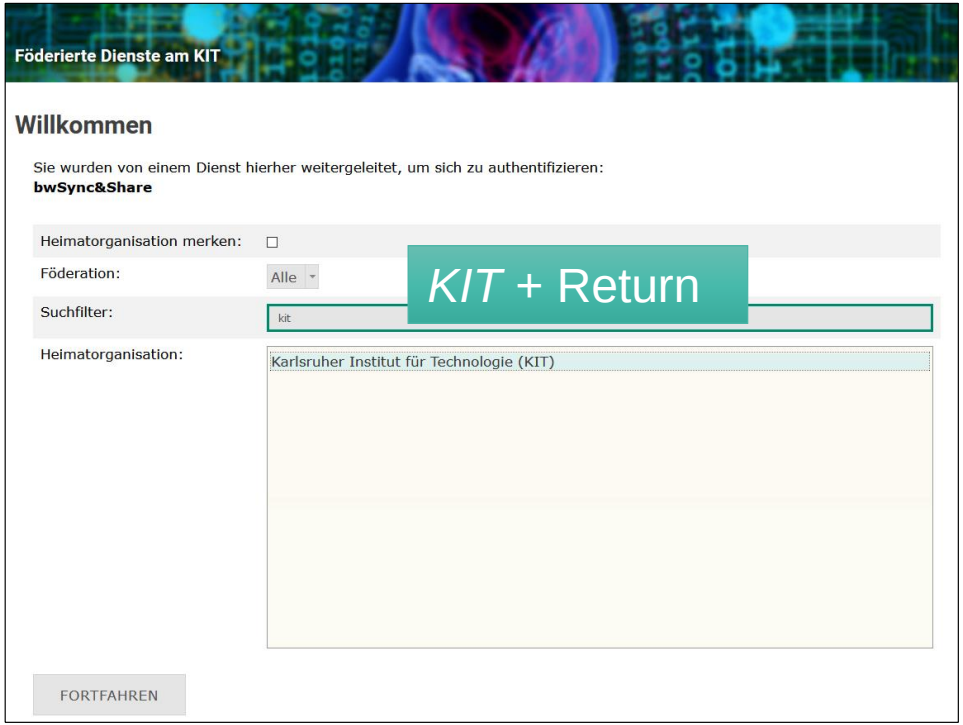


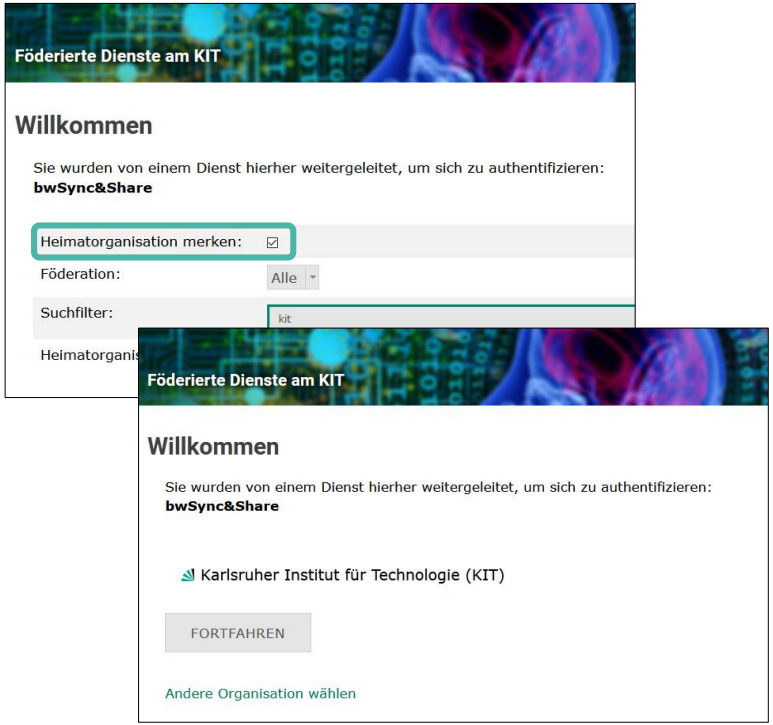
Service

Heimat IdP

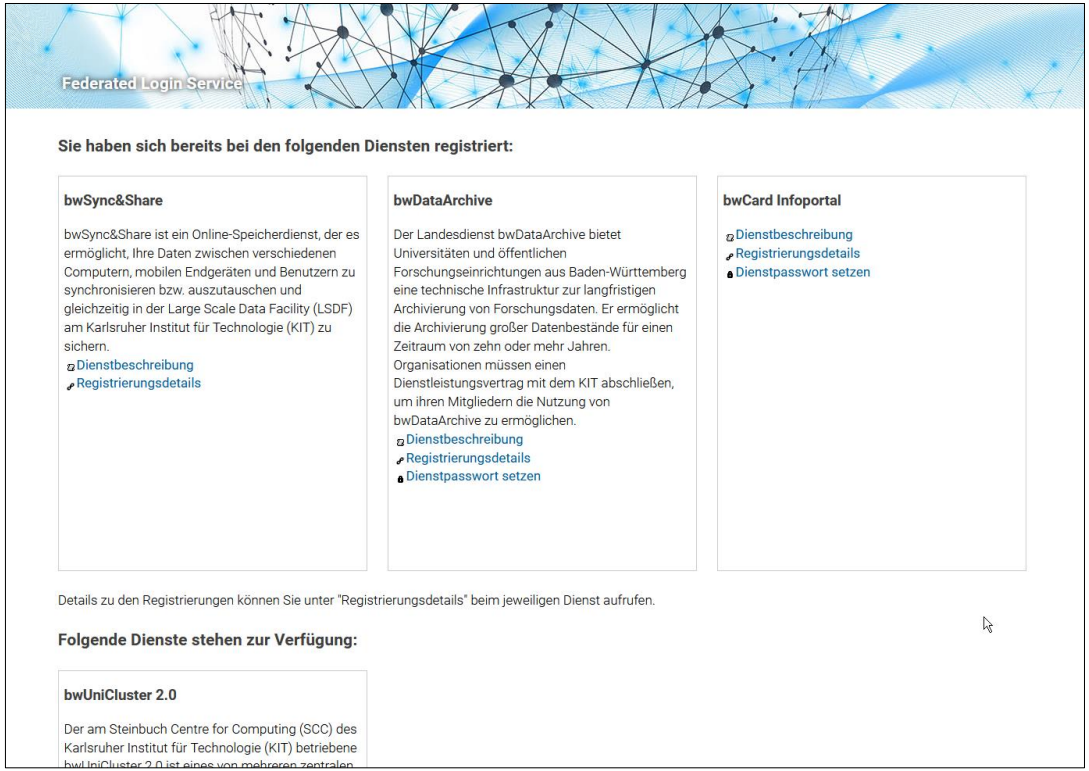
Steinbuch Centre for Computing

Shortcuts


Föderierte Dienste am KIT
Willkommen
Sie wurden von einem Dienst hierher weitergeleitet, um sich zu authentifizieren:
bwSync&Share
Heimatorganisation merken:
Föderation:
Alle
Suchfilter:
kit
Heimatorganisation:
Karlsruher Institut für Technologie (KIT)
FORTFAHREN
KIT + Return

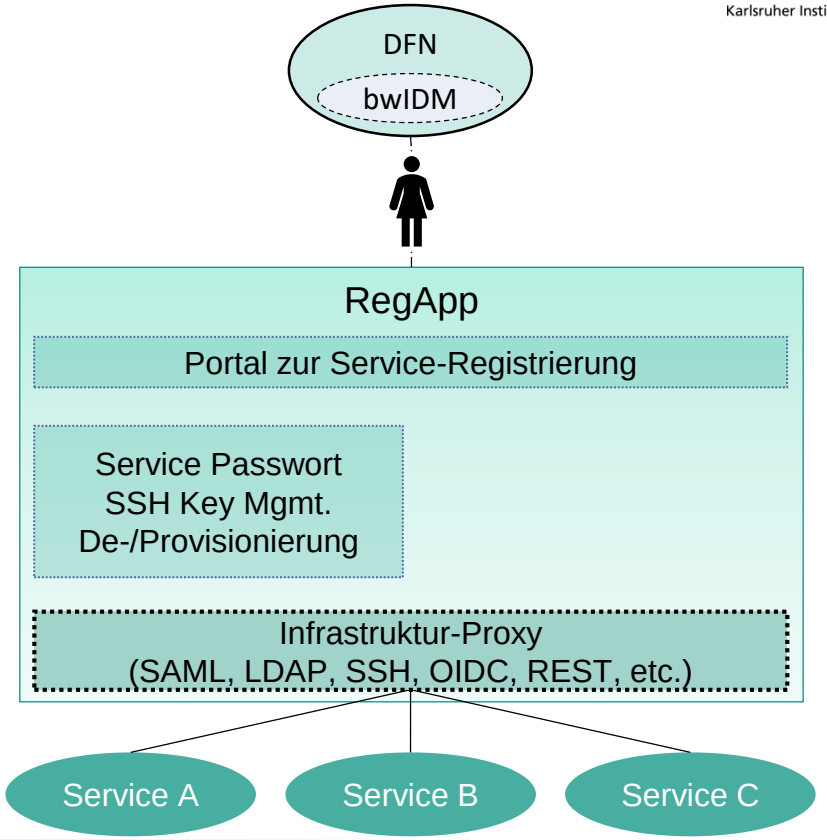

Föderierte Dienste am KIT
Willkommen
Sie wurden von einem Dienst hierher weitergeleitet, um sich zu authentifizieren:
bwSync&Share
Heimatorganisation merken:
Föderation:
Alle
Suchfilter:
kit
Föderierte Dienste am KIT
Willkommen
Sie wurden von einem Dienst hierher weitergeleitet, um sich zu authentifizieren:
bwSync&Share
Karlsruher Institut für Technologie (KIT)
FORTFAHREN
Andere Organisation wählen

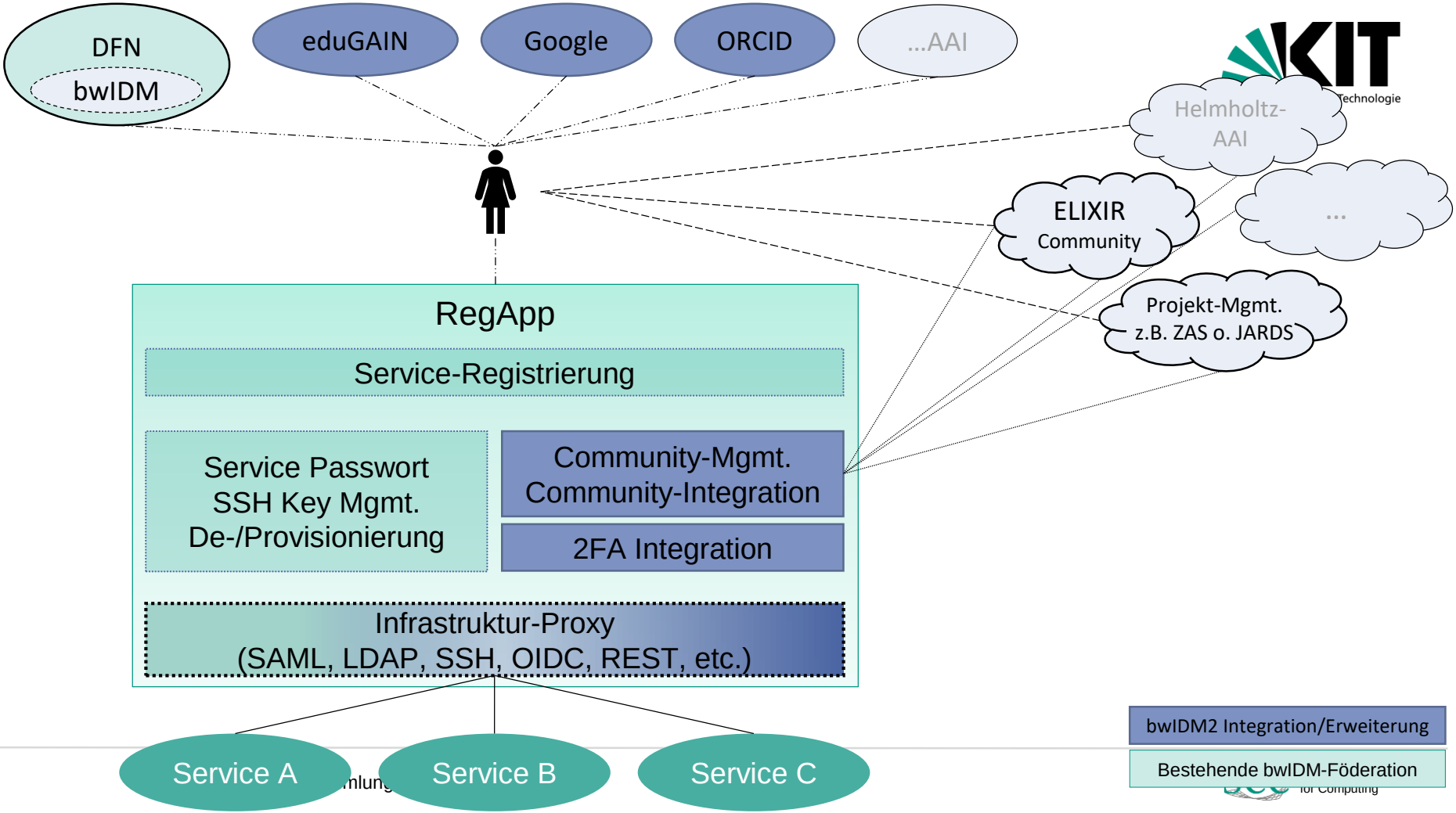
Registrierungsportal



RegApp – AAI-Software

- Einsatz in u.a. in bwIDM, bwHPC, HIFIS
- bwIDM
  - Derzeit >38.000 Benutzer
  - KIT-Services sind daran angeschlossen
- Funktionsumfang sehr groß
- Entwicklung am KIT




DFN
bwIDM
eduGAIN
Google
ORCID
...AAI
Helmholtz-AAI
ELIXIR Community
...
Projekt-Mgmt.
z.B. ZAS o. JARDS
RegApp
Service-Registrierung
Service Passwort
SSH Key Mgmt.
De-/Provisionierung
Community-Mgmt.
Community-Integration
2FA Integration
Infrastruktur-Proxy
(SAML, LDAP, SSH, OIDC, REST, etc.)
Service A
Service B
Service C
bwIDM2 Integration/Erweiterung
Bestehende bwIDM-Föderation

Fragen und Antworten

- Shibboleth / SAML → Michael Simon
- OpenID Connect / OAUTH → Matthias Bonn
- Allgemeines → Uli Weiß

Backuplösung mobiler Geräte
Update zur neuen Lösung

Unterschiede der Backup Lösungen

Druva inSync

- NutzerInnen basiert
- Speicherung auf Platte
- NutzerIn definiert was wird gesichert
- NutzerIn definiert wann wird gesichert
- Pausieren des Backups
- VPN
- E-Mail wenn eine Woche kein Backup

IBM Spectrum Protect (TSM)

- Rechner basiert
- Speicherung auf Magnetband
- Installation nur mit Admin Rechten
- Konfigurationsdatei auf dem Client
  - Was wird gesichert!
- VPN
- Scheduler wenn zwischen 0 und 6 Uhr das Backup gestartet wird
  - E-Mail bei Misserfolg
- Cron Job oder Aufgabenplanung
  - E-Mail wenn 15 Tage kein Backup

Backup Versionierung

Druva inSync

- Retain all backups for 7 Days
- Retain weekly backups for 3 Weeks
- Retain monthly backups for 3 Months

IBM Spectrum Protect (TSM)

- 3 Version Exist (wenn verändert)
- 1 Version Deleted
- 62 Tage Retain

Installation des IBM Spectrum Protect Client

- Formular ausfüllen
- https://www.scc.kit.edu/scc/sw/backup/tsm/anmeldung/backup.php
- Rechner wird auf dem Server definiert
- Installationsanleitung für das Betriebssystem wird erstellt.
- Incl. Konfigurationsdatei die nur noch an die richtige Stelle kopiert werden muss.
- Bei Fragen wenden Sie sich bitte direkt an das Backup-Team des SCC mailto:dataprotection@lists.kit.edu.

Wesentliche Installationsschritte

- Installation nur mit **Administrator/root** Rechten
- Herunterladen des neuesten Client für das Betriebssystem:
  - https://www.scc.kit.edu/backupbw/
- Auch die Windows EXE erzeugt nur ein neues Verzeichnis (wie zip/tar)
- Wechsel in das neue Verzeichnis „TSMClient“ und ausführen von
  - spinstall.exe
- Kopieren der Konfigurationsdatei an die richtige Stelle
- Wichtig ein erstes Backup muss manuell erfolgen
- Grafisches Tool (dsm)
- Befehlszeilen Tool (dsmc incr -ve) *incr = incremental –ve = verbose*

Vom Client gesteuertes Backup

- Linux: cronjob
- Windows Aufgabenplanung
  - Als BenutzerIn angelegt, aber auszuführen als Admin erlaubt manuelles Backup als BenutzerIn
  - Script als BAT speichern und von Aufgabenplanung ausführen

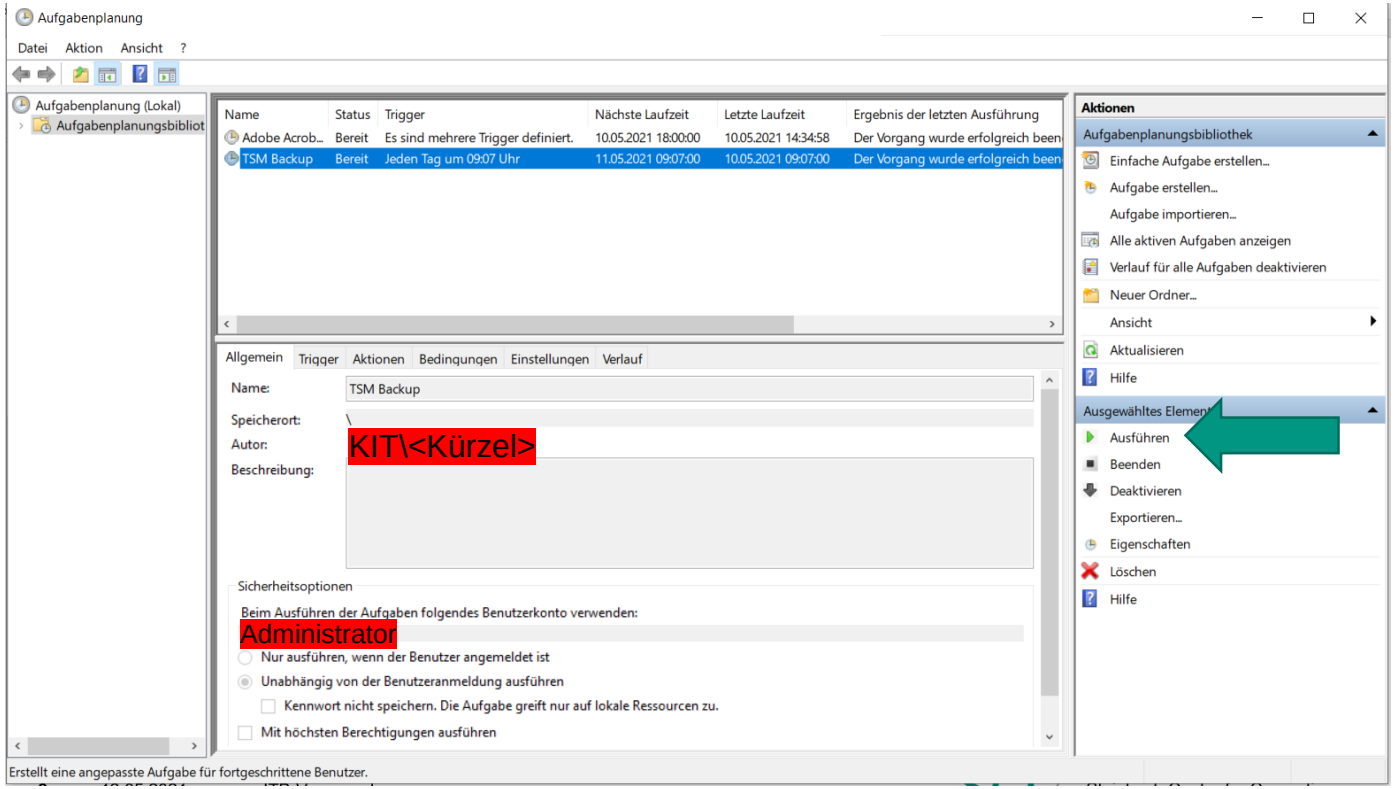
```
set dsmerror_log=c:\tmp\dsmerror.log
set dsmcincr_log=c:\tmp\dsmcincr.log


cd c:\Program Files\tivoli\tsm\baclient

dsmc incr -errorlogname=%dsmerror_log% >> %dsmcincr_log%
```

  - Achtung Log-Dateien sollten von Zeit zu Zeit geleert werden.

Vom Client gesteuertes Backup



Abfrage der letzten Sicherung

- Befehlszeile als Administrator
  - dsmc q fi
- In der entsprechenden log Datei (Leseberechtigung für BenutzerIn setzen)

Sicherheitslücken im IBM Spectrum Protect Client

- Update auf Version 8.1.12.0
- Beschreibung der Sicherheitslücken:
  - IBM Security Bulletin 6445483
    https://www.ibm.com/support/pages/node/6445483
  - IBM Security Bulletin 6445489
    https://www.ibm.com/support/pages/node/6445489
  - IBM Security Bulletin 6445497
    https://www.ibm.com/support/pages/node/6445497
  - IBM Security Bulletin 6445503
    https://www.ibm.com/support/pages/node/6445503

Änderungen an IT-Infrastruktur und IT-Diensten

KIT wird Zentrum für Nationales Hochleistungsrechnen (NHR)

- Das KIT wird mit GWK-Beschluss vom 13.11.2020 in der NHR-Allianz (Jahresbudget i.H.v. 62,5 Mio. €) mit hohem **einstelligen Millionenbetrag** jährlich gefördert.
- Mit „HoreKa“ wird am KIT ab 01.06.2021 einer der **leistungsstärksten Supercomputer Europas** stehen.
- Die Rechenleistung ist ca. 17x höher als des Vorgängersystems ForHLR II.
- Informationen zur Antragsstellung unter: **https://www.nhr.kit.edu/userdocs/horeka/**

SAP Portal - Umstellung Neues Framework

- Einführung des neuen Portal-Framework zum Jahreswechsel
  - Erleichterte Bedienbarkeit
  - Zusätzliche Funktionalitäten (z.B. Favoritenvoreinstellung der Anwendung)
- Betriebsprobleme mit chromium-basierten Browsern im ESS-Umfeld mittlerweile behoben
- Für die Nutzung des SRM wird Firefox empfohlen, da es im Chrome-Umfeld öfters zu Nutzersperren kommt

Netzwerk-Infrastruktur

KITnet

- Drei von vier alten Core-Routern außer Dienst gestellt
- Neue Border-Router in Betrieb
- Neue Firewall im Testbetrieb
- IPv6 fast vollständig im KIT ausgerollt

VPN-Zugang

- Aktualisierung der OpenVPN-Server auf aktuelle Version 2.5
- Neue Client-Konfigurationsdateien
- Erhöhung der Sicherheit
- Skalierung der VPN-Zugänge in die Breite

File Sharing und Datenbanken

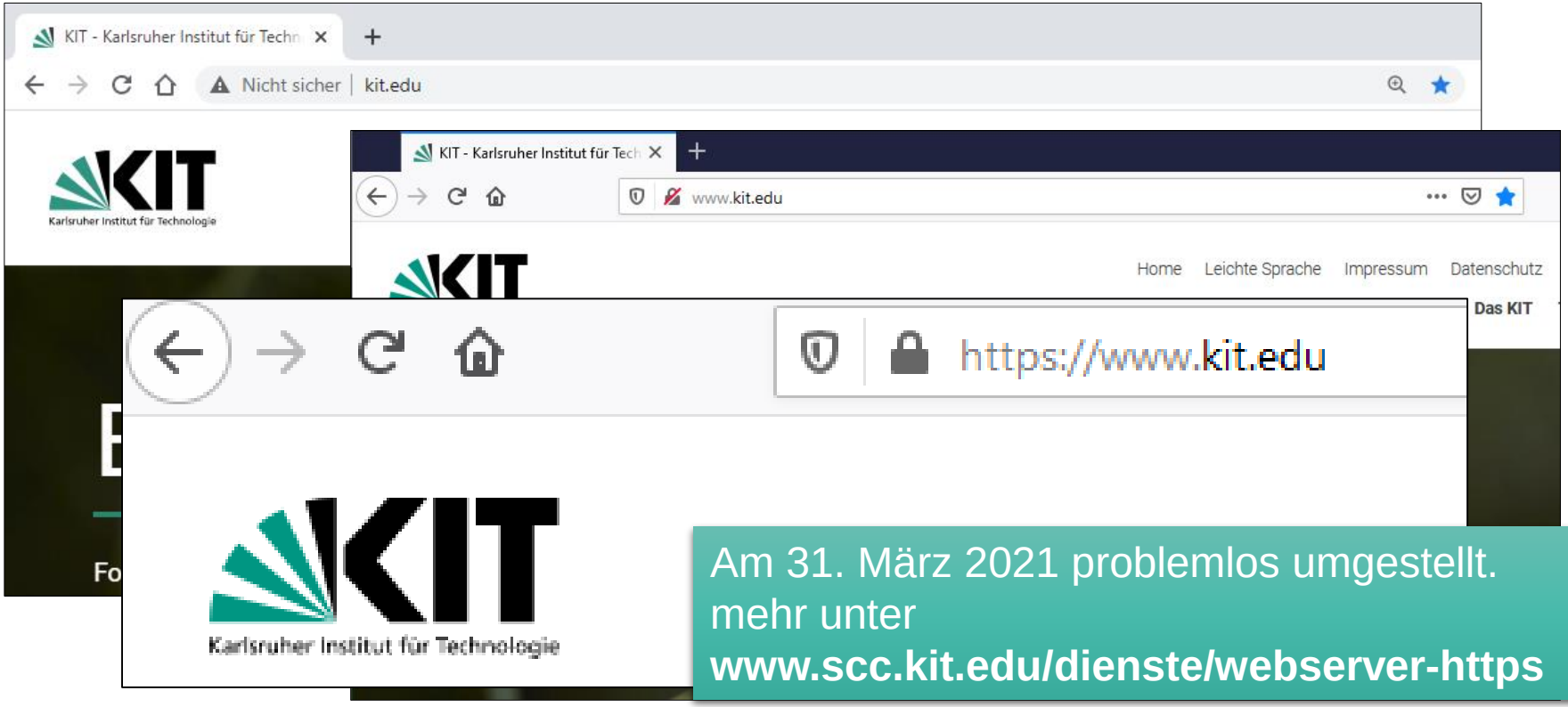
bwSync&Share

- Hardware erweitert
- Update auf Nextcloud Version 20
- Derzeit:
  - Optimierung der Datenbank-Installation
  - Ziel: weitere Stabilisierung des Dienstes

PostgreSQL

- Neuer zentraler Dienst am KIT
- PostgreSQL Version 13
- Derzeit kein Cluster

Umstellung der KIT-Webserver auf https-only



Am 31. März 2021 problemlos umgestellt.
mehr unter
www.scc.kit.edu/dienste/webserver-https

Ausblick:
Zentrale Empfehlung für Stockwerksdrucker

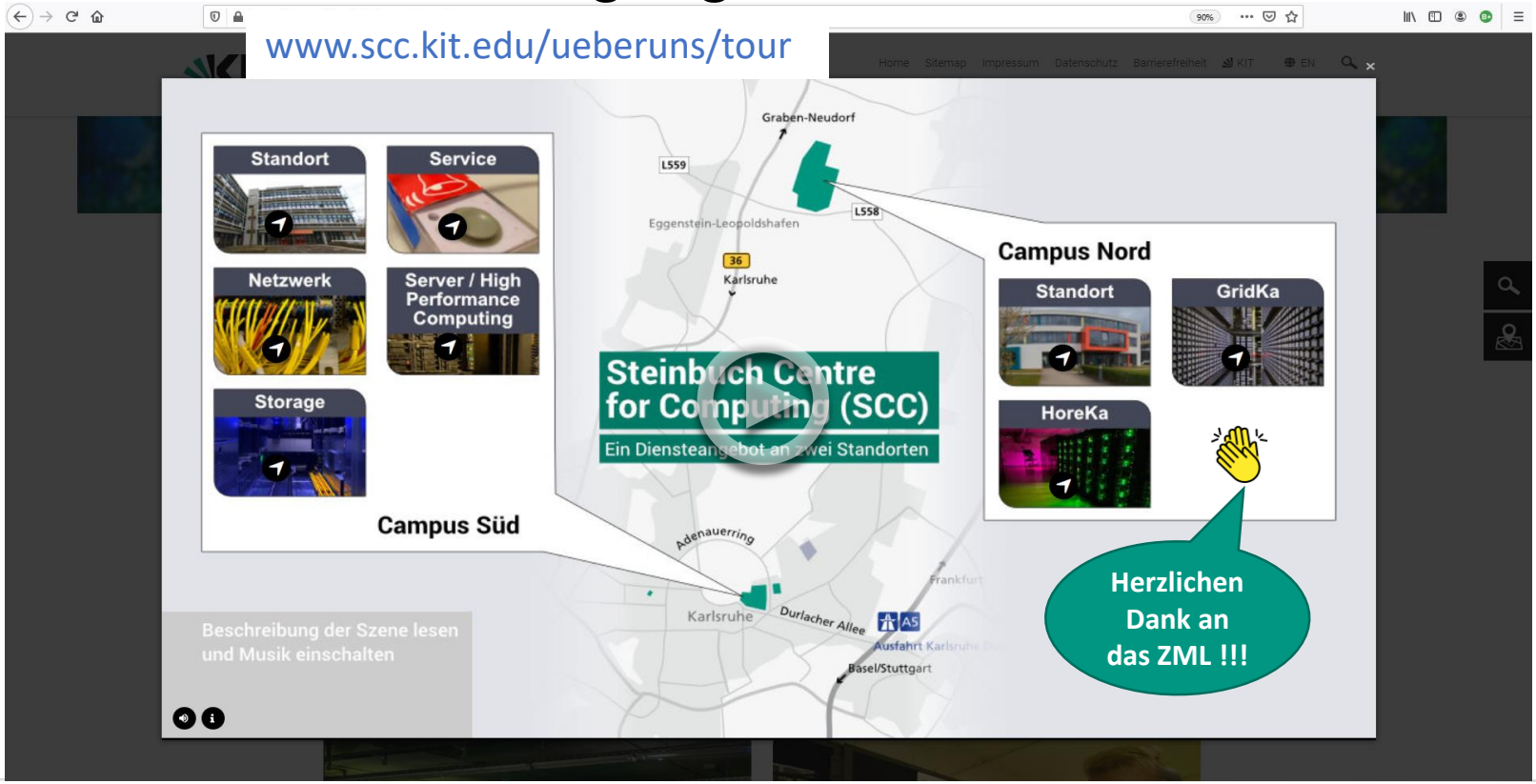
- Zentrale Empfehlung für Stockwerksdrucker in Vorbereitung
  - Vorstellung im IT-EK in 1-2 Monaten
- Wichtige Funktionalität „Follow Me Printing“
  - Authentifizierung über KIT-Card
  - Unterstützt die Ziele der Informationssicherheit
- Notwendige Server-Komponenten zentral betrieben
- Bei entsprechendem Interesse wird ein Rahmenvertrag angestrebt

Ausblick:
Zentrale E-Mail Archivierung

- Bedarf von vielen Seiten an das SCC herangetragen
  - Entlastung des aktiven Postfachs
  - Unkomplizierter Zugriff auf archivierte E-Mails
- Einfache, leicht handhabbare Lösung angestrebt
  - Anforderungen werden derzeit zusammengestellt
  - Mögliche Lösungen werden dann evaluiert
- Weitere Details in einer der nächsten IT-EK-Sitzungen
- Rechtssichere Aufbewahrung von E-Mail-Daten ist hier nicht im Fokus!

Virtueller 360° Rundgang

www.scc.kit.edu/ueberuns/tour



Steinbuch Centre for Computing

Sonstiges / Diskussion