

27. IT-Beauftragten Versammlung am 15. Mai 2024

Partnerschaftliche Zusammenarbeit zwischen SCC und ITB

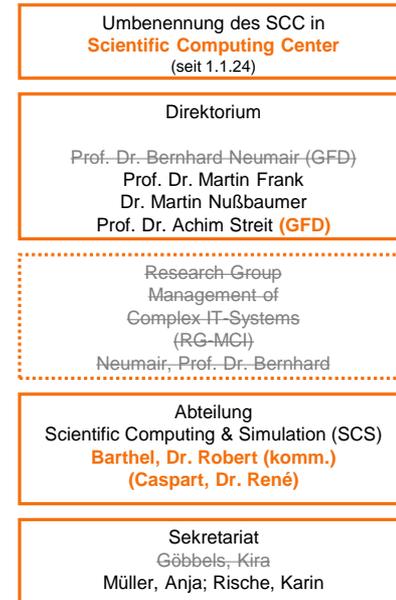
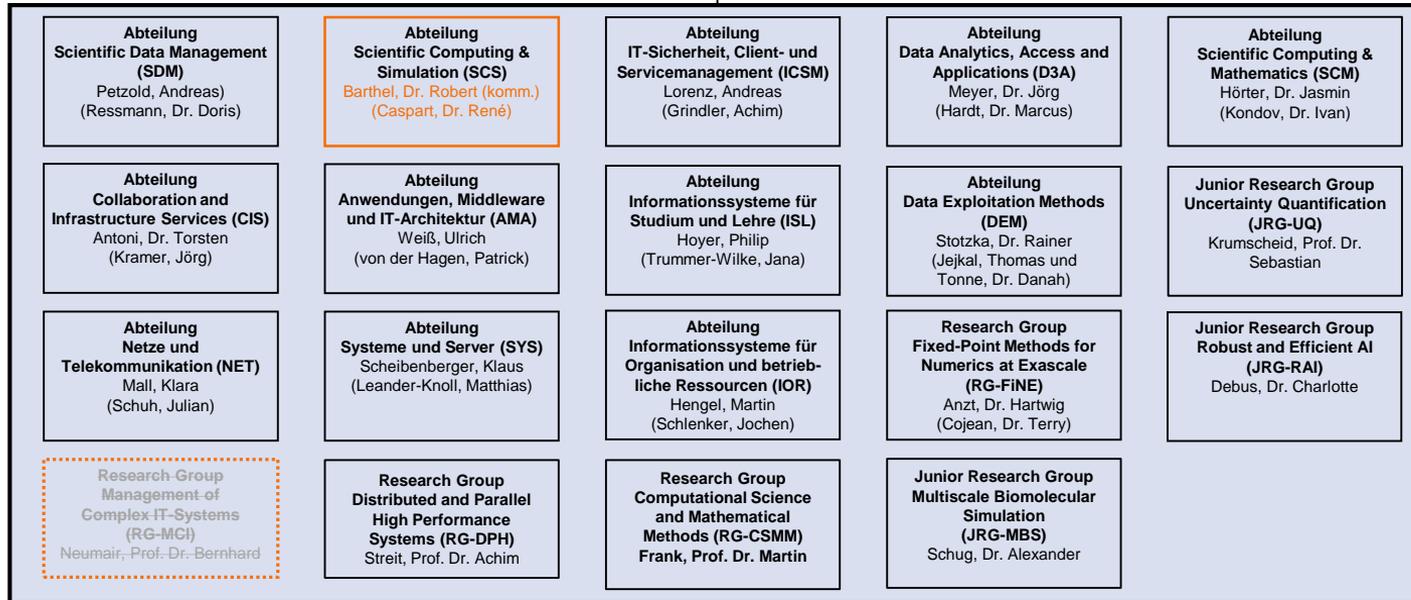
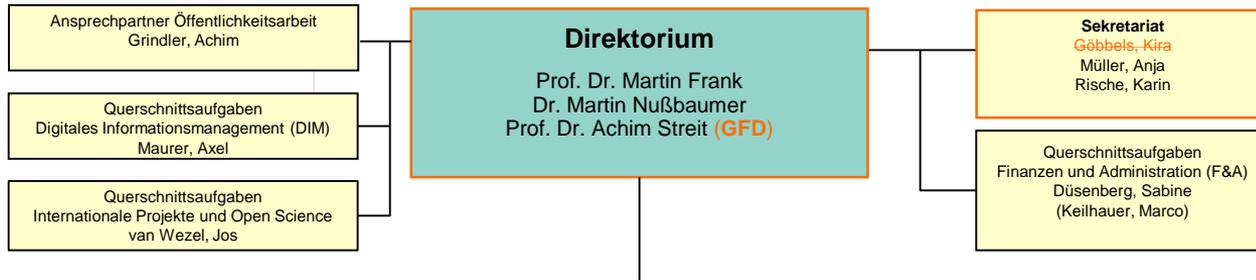


Agenda

- Begrüßung & Neues aus dem SCC
- Cloud-Service *Microsoft M365* am KIT
- Entwicklungen und Neuheiten in bwIDM
- Einführung von HISinOne STU
- bwJupyter für die Lehre - Pilotphase und Perspektiven
- Aktuelles rund um das User Portal (UP)
- IT-Sicherheit
- Kurzinformationen / Sonstiges

Begrüßung & Neues aus dem SCC





Cloud-Service *Microsoft M365* am KIT

Torsten Antoni, Uli Weiß



On-Premises- & Cloud-Dienste

 50.000 Postfächer

 750 Share-Point Sites

 20.000 Projekte

 Fileserver OE & Anwgd. 1,4 PB

 bw Sync & Share

 HIFIS

 bwCloud

 Overleaf

 zoom

 Rainbow

 DATEV

 ATlassian

 Microsoft 365

Software/Anwendungen verlagern sich von On-Premises zu SaaS
Anwender-Bedarfe für zeitgemäße Umsetzung im KIT vorhanden

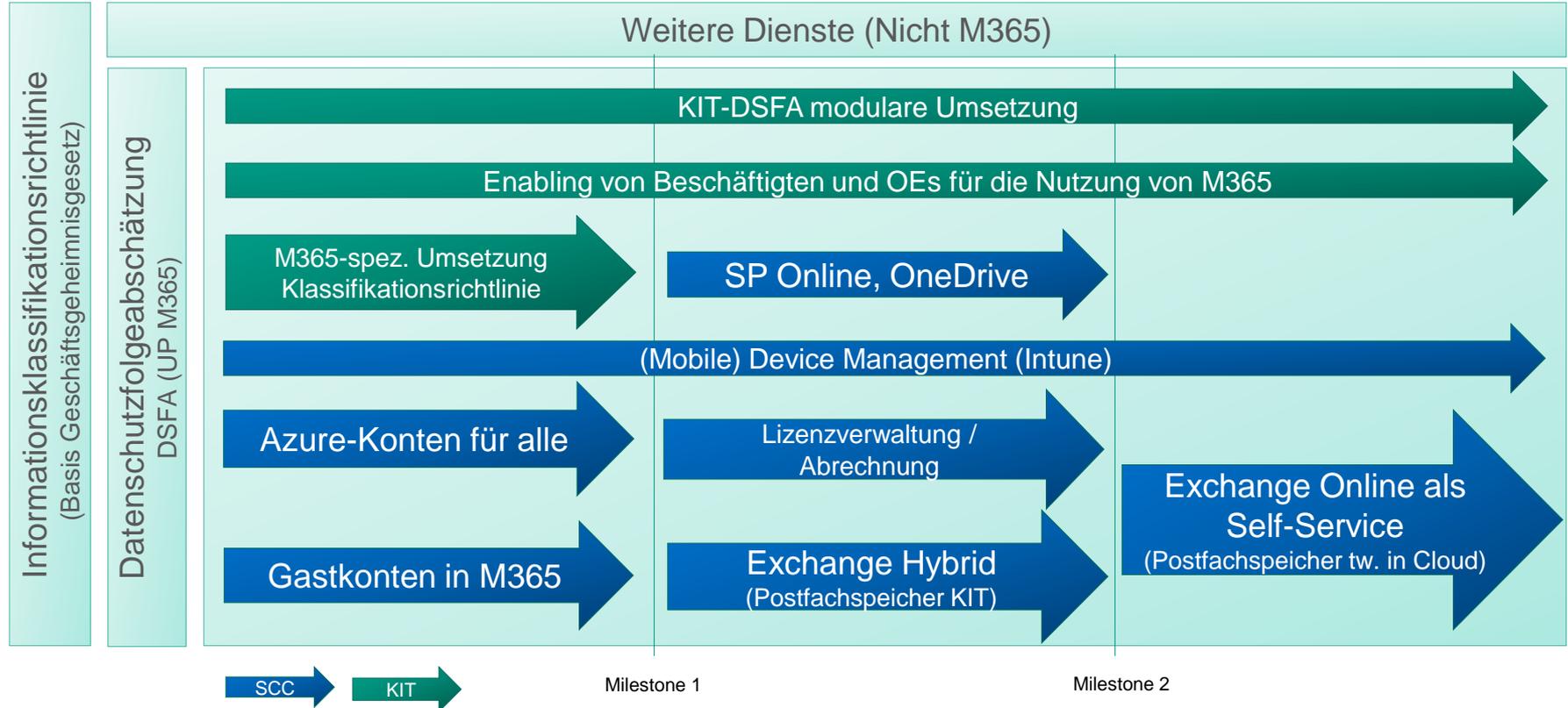
M365 ergänzt KIT SW-Portfolio bietet zusätzliche Features



Master 1

Master 2

Roadmap M365 für Mitarbeitende des KIT



Muster-DSFA

- Vorarbeiten (Rechtsgrundlagen, Definition Nutzungsszenarien,...)
 - DSGVO, Bundes-, Landesdatenschutzgesetz,...
- Risikobewertung (Identifizierung, Klassifizierung, Szenarien,...)
 - Geheimdiensttätigkeiten, Identitätsdiebstahl, Höhere Gewalt
- Empfehlungen zur Risikominimierung
 - 13 „Muss“- und 17 „Soll“-Empfehlungen zu unterschiedlichen Themen (bspw. Datenminimierung, Speicherbegrenzung,...)
 - Datensparsame Konfiguration von Endgeräten, Löschfristen, MDM, MAM

Präsidiumsbeschluss

- Ein Präsidiumsbeschluss zur „erweiterten Nutzung von M365 am KIT“ ist in Vorbereitung
- Ziel:
Bereitstellung von M365 für alle Mitarbeitenden bei Ausgewogenheit zwischen maximal möglicher Funktionalität und Datenschutz, sowie Informationssicherheit
- Erstellung einer Dienstvereinbarung zu M365 unter Einbeziehung der relevanten Gremien, inkl. Personalrat

Informationsklassifikationsrichtlinie

- Wird derzeit für das KIT erstellt
 - Zuständig: RECHT, DSB, ISB
 - Leitung ISB

- Wir erwarten ein Ergebnis mit 3-5 Klassifikationsstufen für Dokumente
 - öffentlich bis streng vertraulich
 - Plus Regeln, wie mit entsprechenden Informationen umgegangen werden muss
 - Wo dürfen Dokumente abgelegt werden
 - Wie wird der Zugriff geregelt
 - ...

- Gültig auch für Nicht-M365 Dienste

Microsoft M365 am KIT Die Module im Überblick



Gastkonten

M365-Gastkonten sind Verknüpfungen zu externen Identitäten (Azure- u. Microsoft-Konten, Google-Konten, E-Mailadresse etc.)

Unterschiede zu GuP-Konten

- Einfache Verwaltung:
Jeder M365-Benutzer kann Gäste in sein Team einladen
- Höherer Datenschutz:
Gast erhält bei Anmeldung am KIT-Mandanten explizite Auflistung der für andere Personen sichtbaren Daten
- Hohe Informationssicherheit
 - Eingeschränkte Funktionen im KIT-Mandanten
 - Gast interagiert nur innerhalb seiner Gruppe und sieht nur für ihn freigegebene Informationen
 - Kein Zugriff auf On-Premises-Dienste des KIT

"Azure-Konten für alle"

■ Motivation

- einheitlicher Kontenstamm für On-Premises- und M365-Dienste
- Betrifft aktuell nur für Beschäftigte des KIT
- Für Lizenzierung von Office 365 notwendig

■ Datenschutz und Datensicherheit mit DSB und ISB geklärt

- Zu synchronisierende Attribute
- Nutzbare Dienste

■ Umsetzung nach PS-Beschluss/Dienstvereinbarung

Lizenzverwaltung und Abrechnung

- M365 Campus-Lizenz
 - Aktuell A3-Lizenzen, dies beinhaltet On-Premises-Lizenzen und 100 TB + 50 GB pro A3-Lizenz Speicherplatz
 - Teil des zentralen Softwareportfolios
- Ein verursachergerechtes Abrechnungsverfahren für Lizenzen außerhalb der Campus-Lizenz und auch für weiteren Speicherplatz wird entwickelt
- Eine mögliche zentrale Lizenzenerweiterung (bspw. Umstieg auf A5-Lizenzen) ist abhängig von Funktionalitäts- (IT-Sicherheit, Telefonie,...) und Wirtschaftlichkeitsabwägungen

SharePoint / OneDrive

SharePoint Online

- Basis für weitere Dienste (z.B. OneDrive, Office-Integration, MS-Datendienste)
 - Weiterentwicklung: Neue und erweiterte Funktionalitäten
 - Collaboration für Interne & Gäste (Ablösung bisheriger externen Benutzerverwaltung)
 - Ist in MS-Teams integriert und kann so bereits genutzt werden
-
- Nutzung SharePoint Online oder SharePoint On-Premises
 - On-Premises Betrieb auch weiterhin vorhanden
 - Entscheidung in Abhängigkeit von Klassifizierungsstufe

Es erfolgt keine automatische Migration der bestehenden Sites in die Cloud!

SharePoint / OneDrive

OneDrive

- Basis für weitere Dienste (z.B. Whiteboard, Teams Chat, etc.)
- (persönlicher) Cloudspeicher für Office Dokumente (Austausch mit internen und externen Personen)
- Verwendungsmöglichkeiten
 - Webzugang, Sync-Client (Windows/Mac) oder App (iOS/Android)
 - Ausprägungen werden noch definiert
- Zukünftig zusätzlicher Datendienst mit neuen Features unter scc.kit.edu/dienste/daten

Mobile Device Management (Intune)

Mobile Application Management (MAM)

- Policies für spezielle Apps auf Mobilgeräten (iOS/Android)
 - Teilen von Dokumenten nur über die M365-Teilen-Funktionen
 - Nicht über Telegram...
- Vorteil: erfordert keine Geräteverwaltung

Mobile Device Management (MDM)

- Anforderungen von KIT-OEs zur Verwaltung von iPads & iPhones
 - Inventarisierung, zentrale Lizenzbeschaffung, unpersonalisierte Laborgeräte, etc.
- Zunächst Fokus auf Mobilgeräte Android, iOS, iPadOS & MacOS (Windows-Geräte zunächst weiterhin mit OPSI, AD, Gruppenrichtlinien)
- Zunächst Überprüfung von Gerätezustand (z.B. Patchstatus)
 - Potentiell Kriterium für „conditional access“, z.B. „Zugriff von FIMA auf SAP nur von verwalteten und gepatchten Geräten“

Exchange Hybrid/Online

Motivation

- up-to-date Sicherheitsfeatures sind in Exchange Online verfügbar
 - MFA fürs Postfach, besserer Schutz vor Phishing-Angriffen
- immer mehr Anwendungen funktionieren nur noch mit Exchange Online
- andere M365-Dienste sind ohne Exchange Online eingeschränkt, weil Funktionen fehlen

Migrationsplan

- Hybridstellung
 - "Vertrauensstellung" zwischen Exchange Online und Exchange On-Premises
- Synchronisation aller Exchange-Empfänger-Objekte (Postfächer, Verteilerlisten, Kontakte,...)
 - M365-Dienste wissen damit, dass der M365-Benutzer ein Exchange-On-Premises Postfach hat
 - vollständiges Adressbuch für Exchange-Online-Benutzer
- Migration nach Exchange Online

Aktueller Stand

- Hybridstellung/Synchronisation teilweise
 - hybride Teams-Besprechungen mit Videokonferenz-Geräten
 - Kalender in MS-Teams
 - Teams-Präsenzanzeige in Outlook

Betriebs- und Supportkonzept

■ Betrieb

- Betriebsteams für die einzelnen M365-Dienste
- Regelmäßiger Austausch zwischen den Betriebsteams
 - Wichtig wegen starker Verzahnung der Dienste
- Strategieguppe
 - Bindeglied zwischen SCC und ISB/DSB
 - Ansprechpartner für die Betriebsteams bei relevanten Änderungen an den Diensten

■ Support

- Über die üblichen Wege, wie auch bei On-Premises-Diensten
 - Ticketsystem
 - Webseiten
 - ...

Status Quo

- Informationsklassifikationsrichtlinie & Präsidiumsbeschluss
 - in Arbeit
- Hybridstellung MA-Konten (für bisherige M365-Nutzende)
 - flächendeckend seit Mitte März
- Gastkonten fertig
- Exchange Hybrid
 - begonnen
- Demo-Umgebung mit „Soll-Zustand“
 - Q2 2024
- OneDrive/SharePoint Online
 - Q2 Pilotphase mit eingeschränkter Nutzergruppe (SCC + ausgewählte OEs)
 - Q3 flächendeckende Ausrollung

Zusammenfassung

- Das SW-/Dienstportfolio wird mit M365 um zusätzliche Dienste erweitert
- Nutzende verantworten die Auswahl/Nutzung der Dienste gemäß Informationsklassifikation
- SCC bietet für alle Schutzbedarfe entsprechende Dienste an

Microsoft M365 am KIT

Fragen & Diskussion

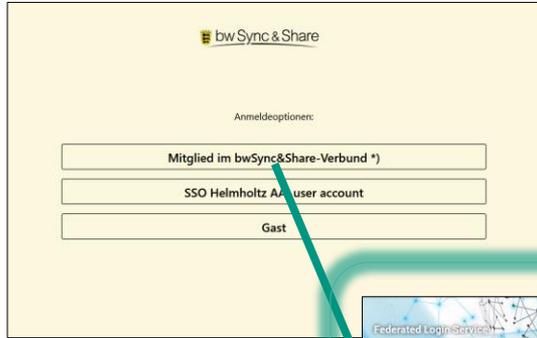


Entwicklungen und Neuheiten in bwIDM

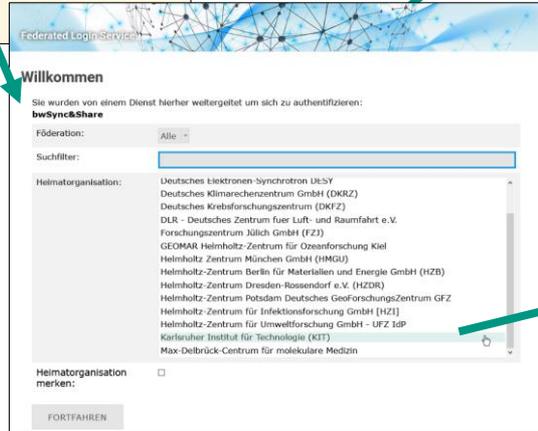
Uli Weiß



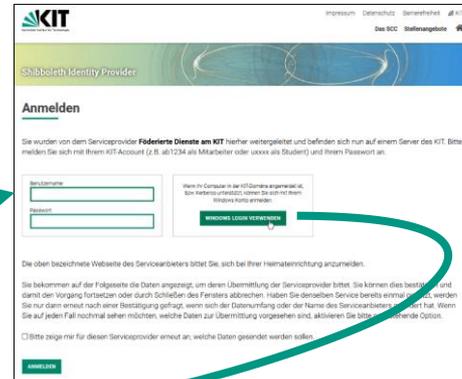
Dienst-Login mit Heimataccount



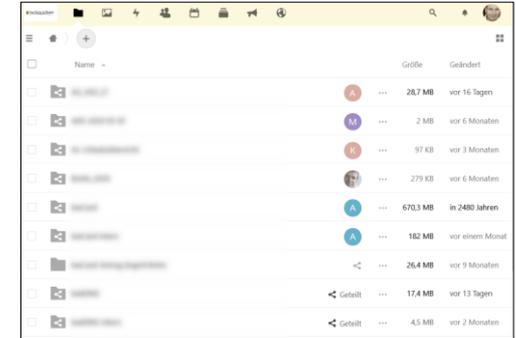
Service



RegApp AAI-SW



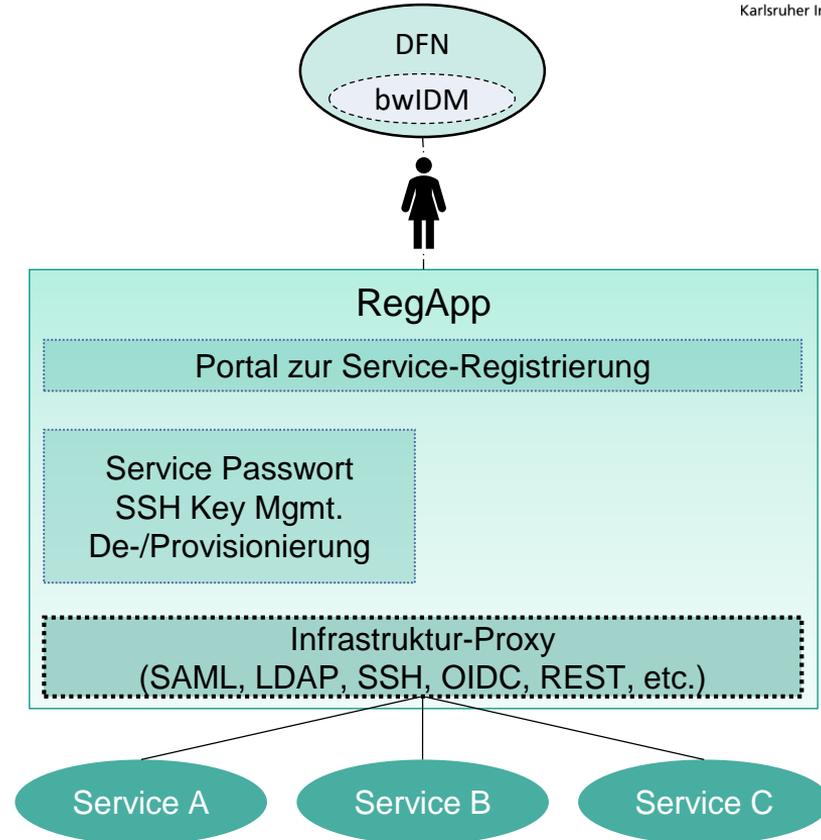
Heimat IdP



Service

RegApp – AAI-Software

- Zentraler Betrieb am SCC
- bwIDM
 - Derzeit > 50.000 Benutzer
 - KIT-Services sind daran angeschlossen
- Funktionsumfang sehr groß
- Entwicklung am KIT



RegApp – Features

■ Basisfunktion als Community AAI für Single Sign-On Umgebungen

- Provisionierung und Deprovisionierung (Benutzeridentitäten)
- Transparente Anbindung von SAML-Föderationen
- SSO Protokoll-Proxy OIDC ↔ SAML
- Infrastruktur-Proxy für LDAP-Dienste

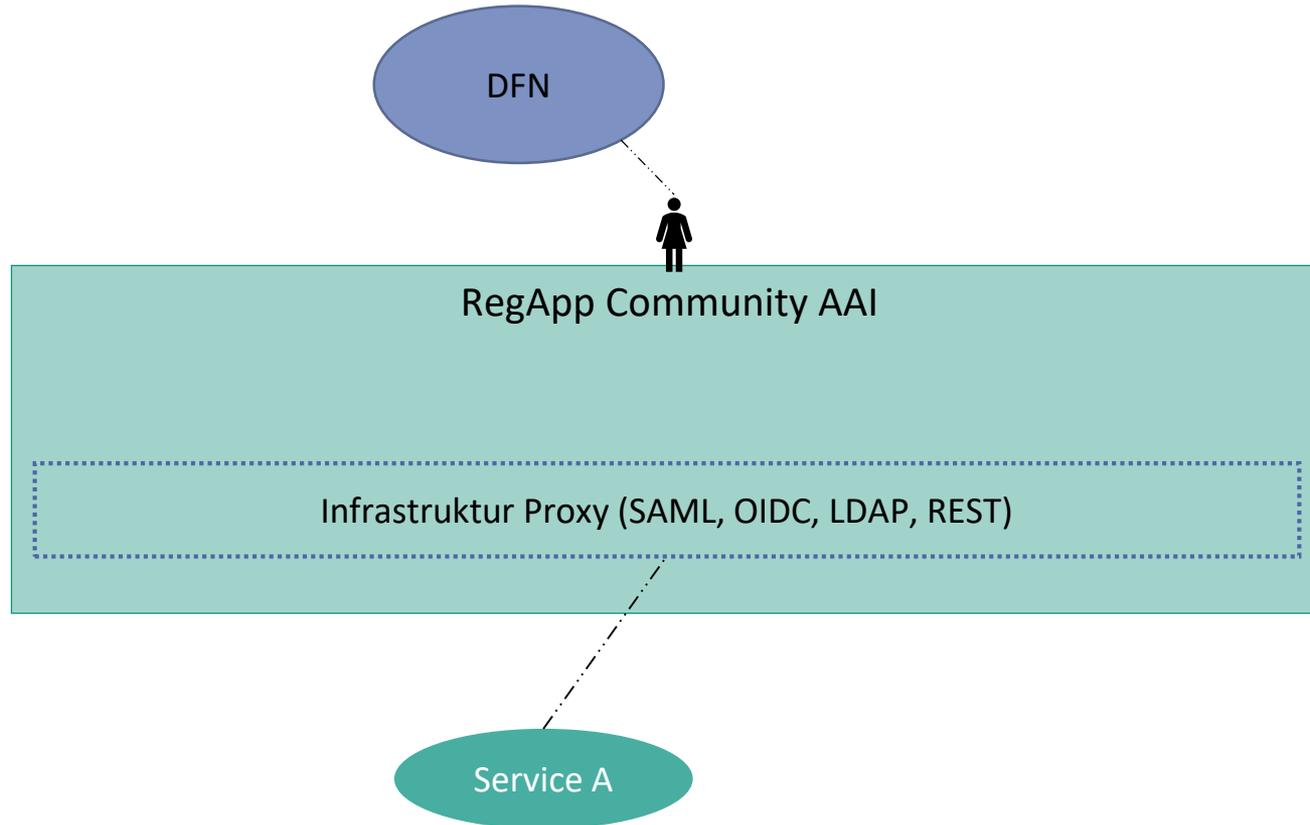
■ Weitere Funktionen

- Zweifaktor-Authentifizierung
- Endnutzerportal zur Service-Registrierung
- Hinterlegen von SSH-Schlüsseln

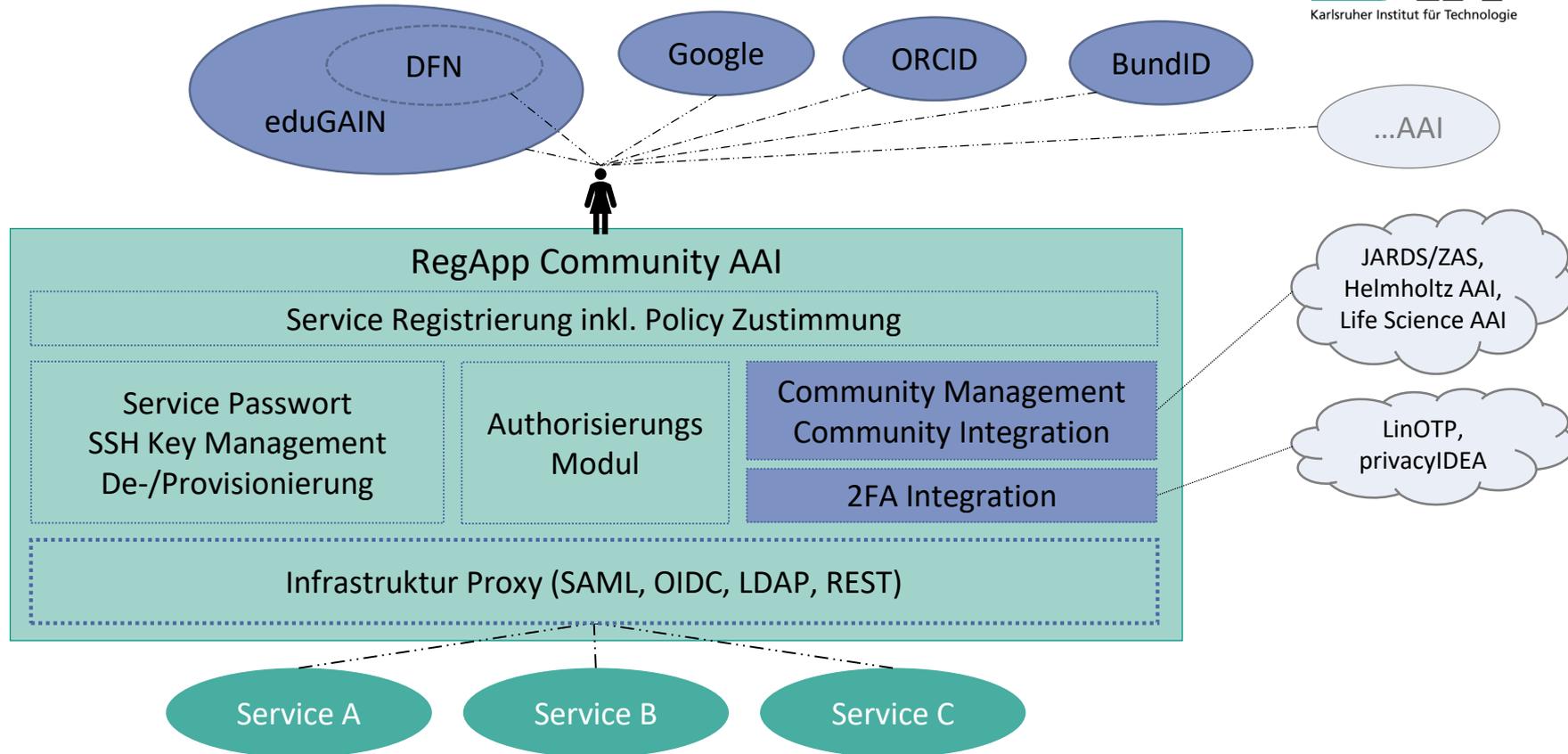


Authentication and Authorisation for
Research and Collaboration
aarc-project.eu

RegApp – Weiterentwicklung



RegApp – Weiterentwicklung



Autorisierung via Community Management



VO-Manager / Principal Investigator (PI)

Erstellt Projekt

Beantragt
Service/Ressource

Lädt Projekt-
mitglieder ein

Verwaltet Projektmitglieder

HPC-Admin (z.B. HoreKa)

Freigabe Projekt
auf Ressource

Service-Admin (z.B. LSDF, Gitlab)

Freigabe Projekt
auf Ressource

Projektmitglieder

Nehmen
Einladung an

Führen Projektarbeiten
durch

RegApp-Erweiterung: Integration **bund** ID

- BundID besteht im Wesentlichen aus zwei Funktionen
 - Ein zentrales Konto zur Identifikation bei Online-Anträgen
 - Ein Postfach für den Empfang von Bescheiden und Nachrichten
- Kerndomäne in der Nutzung im OZG

- Für Hochschulen interessante Self Services bei Vorgängen, an denen **typischerweise ein Personalausweis vorgezeigt** werden muss
 - Passwort des Hochschulkontos zurücksetzen bei Verlust
 - Beantragung persönlicher Email-Zertifikate
 - Adressdaten für Bibliotheksnutzung
 - De-Registrieren von 2FA-Authentifikatoren bei Verlust von Token/Smartphone

Technische Ausgestaltung Erweiterung der föderierten Login-Dienste

Federated Login Service - FeLS (TEST)

Willkommen

Sie benötigen ein gültiges Benutzerkonto bei einer teilnehmenden Organisationen, um föderierte Dienste nutzen zu können.
Wählen Sie Ihre Heimatorganisation aus und klicken auf "Fortfahren" bzw. drücken die Returnntaste.

Suchfilter

-  Karlsruhe Institute of Technology (KIT) - Test
Heimatorganisation merken

FORTFAHREN

Oder nutzen Sie einen alternativen Anbieter:



Google



bund ID
BundID



iD
ORCID

Wie sieht's für die Anwendenden aus (Bund IdP)



id.bund.de/de/welcome

Willkommen bei der BundID

Für Online-Anträge müssen Sie Ihre Identität nachweisen. Mit der BundID haben Sie verschiedene Optionen, dies zu tun. Im Video unten werden Ihnen die Funktionen und Vorteile der BundID näher erklärt.

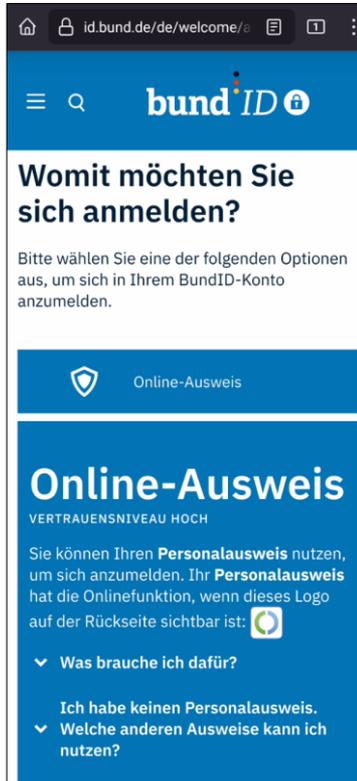
Nutzen Sie jetzt in wenigen Schritten die BundID für Ihren Online-Antrag.

KONTO ERSTELLEN

ANMELDEN

ZURÜCK

Wie funktioniert die BundID?



id.bund.de/de/welcome/

Womit möchten Sie sich anmelden?

Bitte wählen Sie eine der folgenden Optionen aus, um sich in Ihrem BundID-Konto anzumelden.

Online-Ausweis

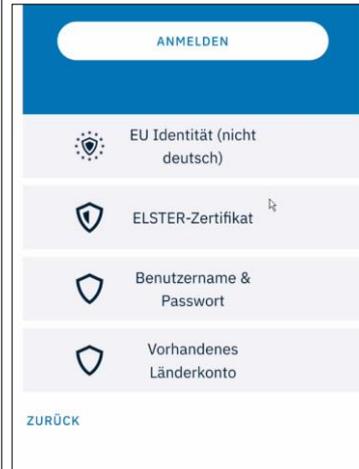
Online-Ausweis

VERTRAUENSNIVEAU HOCH

Online-Ausweis

Sie können Ihren **Personalausweis** nutzen, um sich anzumelden. Ihr **Personalausweis** hat die Onlinefunktion, wenn dieses Logo auf der Rückseite sichtbar ist:

- Was brauche ich dafür?
- Ich habe keinen Personalausweis.
- Welche anderen Ausweise kann ich nutzen?



ANMELDEN

- EU Identität (nicht deutsch)
- ELSTER-Zertifikat
- Benutzername & Passwort
- Vorhandenes Länderkonto

ZURÜCK



id.bund.de/de/welcome/

Haben Sie alles für die Anmeldung?

Bitte halten Sie Folgendes bereit, um sich mit Ihrem Online-Ausweis anzumelden. Unsicher wie es geht? [Hier finden Sie ein Erklärvideo dazu.](#)

- Ihren Online-Ausweis
- Ihre persönliche 6-stellige PIN oder die 5-stellige Transport-PIN
- Ihr Smartphone oder Kartenlesegerät
- Installierte und geöffnete AusweisApp auf Ihrem Smartphone und Ihrem Laptop/PC



id.bund.de/de/welcome/

Ihren Online-Ausweis

Ihre persönliche 6-stellige PIN oder die 5-stellige Transport-PIN

In einer anderen App öffnen

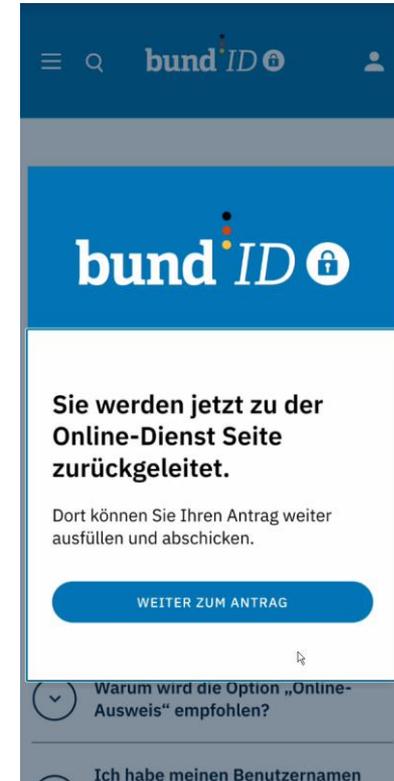
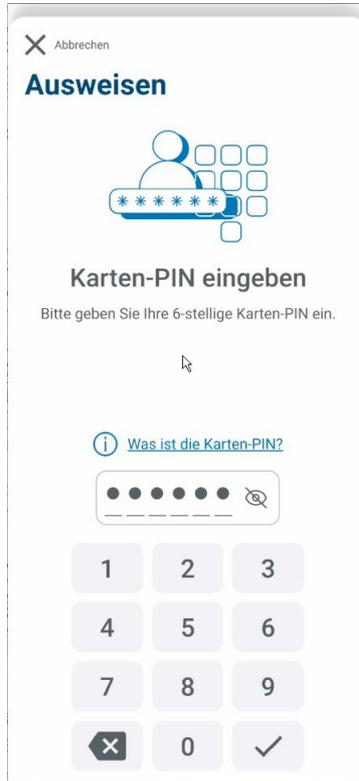
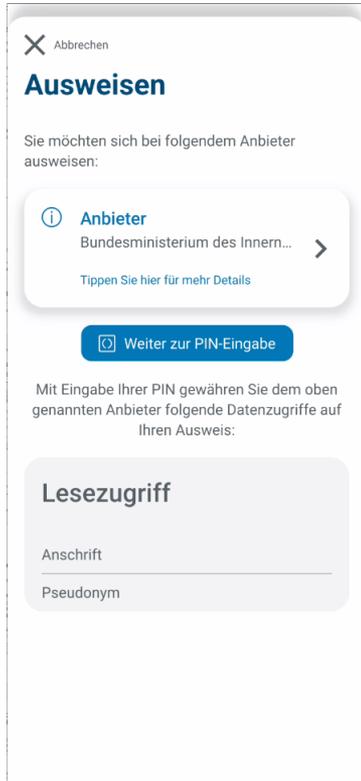
Möchten Sie Firefox verlassen, um diesen Inhalt anzuzeigen?

ABBRECHEN ÖFFNEN

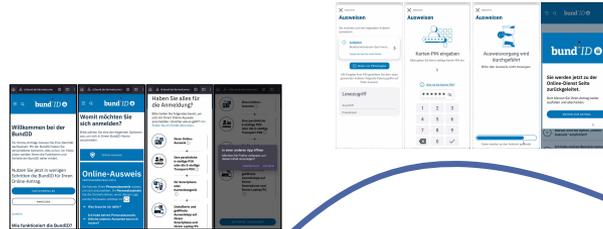
geöffnete AusweisApp auf Ihrem Smartphone und Ihrem Laptop/PC

WEITER MIT AUSWEISAPP

Wie sieht's für die Anwendenden aus (Ausweis-App)



Aus Dienst-Sicht



Gelieferte Attribute & Werte des Personalausweis	
Name	Wert
Unbekanntes Attribut	VI...NA
Vertrauensniveau	STORK-QAA-Level-4
Strasse	FIKTIVE STR. ...
PLZ	76133
Postkorb ID	fac0...03b6
Geburtsdatum	19...-06-10
Email	uli.weiss@kit.edu
Geburtsort	IRGENDWOIMNORDEN
Vorname	ULRICH
Nationalität	DE
Bereichsspezifisches Personenkennzeichen	kHz...Yx8
Ausweisart	eID
Gültigkeit	2021.7.1
Anrede	1
Wohnort	KARLSRUHE
Nachname	WEIß

Dienstanbindung aus Nutzendensicht

Scientific Computer Center

Änderung des Passworts für Ihr KIT-Benutzerkonto

Sie haben Ihr Passwort zu Ihrem KIT-Benutzerkonto vergessen? Sie können entweder zum SCC-ServiceDesk gehen, sich dort ausweisen und Ihr Kennwort zurücksetzen lassen, oder alternativ die Anmeldung mit Personalausweis durchführen.

Wenn Sie Ihr KIT-Benutzerkonto bereits mit der BundID verknüpft haben, können Sie Ihr Passwort nach Anmeldung mit BundID im Folgedialog neu setzen.

MIT BUNDID ANMELDEN

RegApp (transparent)
Weiterleitung Bund-IdP

RegApp (transparent)
Mapping KIT-Account
Attribute an Dienst

Scientific Computing Center

kd1927 abmelden

Änderung des Passworts für Ihr KIT-Benutzerkonto

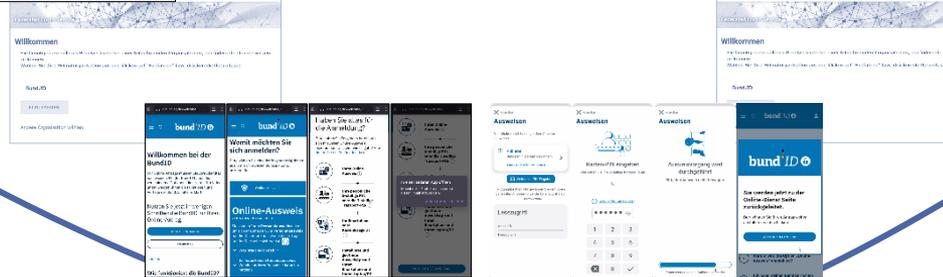
Passwortänderung

Benutzerkennung:

Neues Passwort:

Neues Passwort (Wiederholung):

Ändern



Technische Ausgestaltung Erweiterung der föderierten Login-Dienste

Federated Login Service - FeLS (TEST)

Willkommen

Sie benötigen ein gültiges Benutzerkonto bei einer teilnehmenden Organisationen, um föderierte Dienste nutzen zu können.
Wählen Sie Ihre Heimatorganisation aus und klicken auf "Fortfahren" bzw. drücken die Returnntaste.

Suchfilter

-  Karlsruhe Institute of Technology (KIT) - Test
- Heimatorganisation merken

FORTFAHREN

Oder nutzen Sie einen alternativen Anbieter:

 Google

 bund ID
BundID

 ORCID

Schwierigkeit:
Anmeldung BundID mit PA/eAT
erfordert Lesegerät oder
Smartphone mit Ausweis-APP.

→ Ausführung auf Smartphone
erforderlich

RegApp – im Einsatz



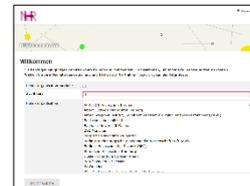
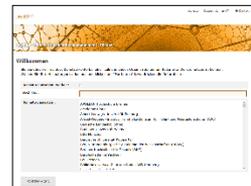
universität freiburg



bwIDM



NFDI4ing



Fragen & Anmerkungen

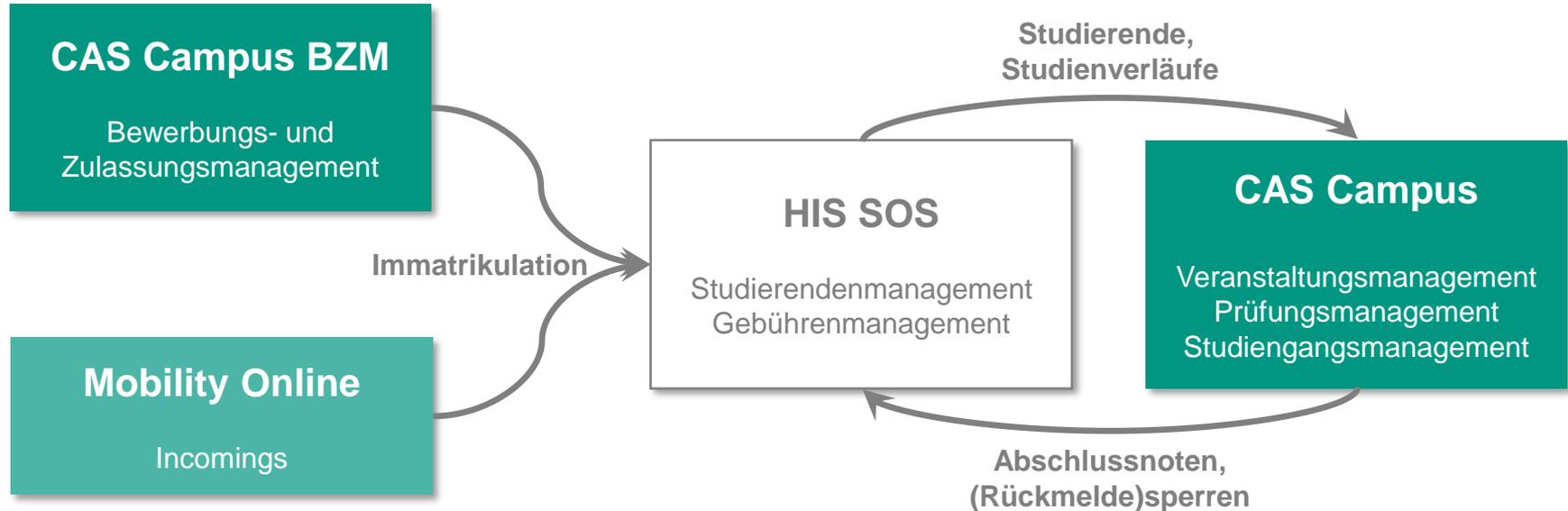


Einführung von HISinOne STU

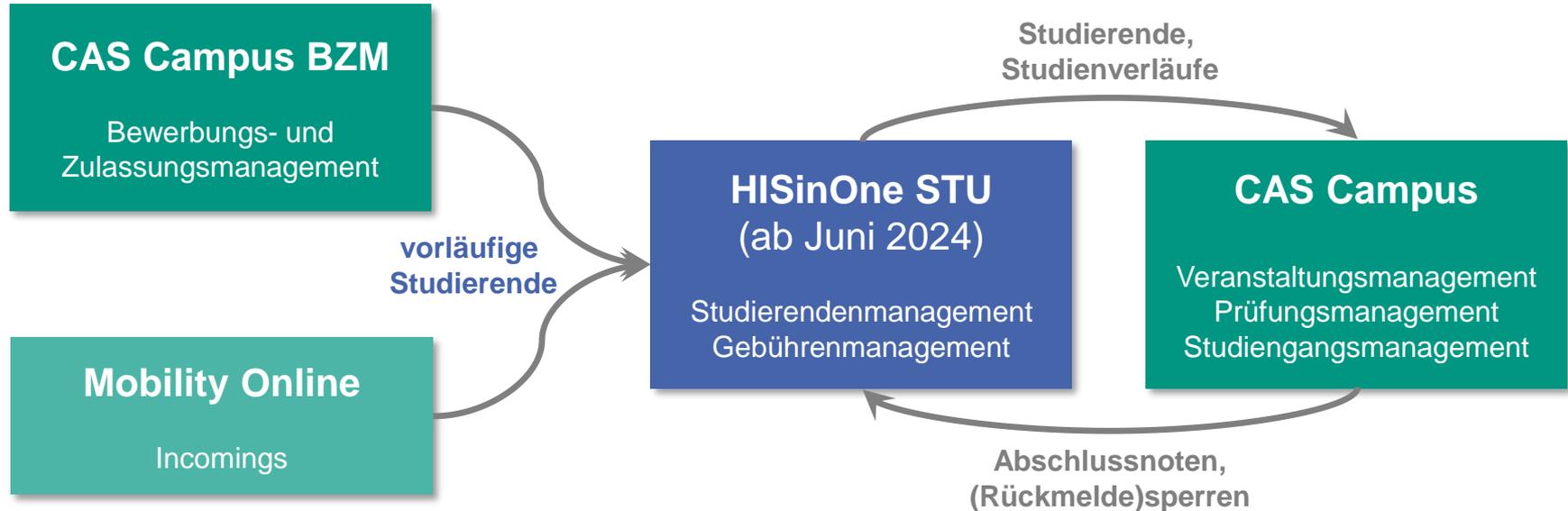
Philip Hoyer (hoyer@kit.edu)



Campus Management am KIT



Campus Management am KIT



Neuerungen mit HISinOne

- Neuer Status "Vorläufige/r Studierende/r" bei Start des Immatrikulationsprozesses
 - Eingeschränkter KIT-Account als vorläufiger Studierender: ILIAS-Zugang, E-Mail, Studierendenportal (**ohne** CAS Campus), **keine** KIT-Card, **keine** Bescheinigungen
 - Voraussetzungen (u.a.) für Immatrikulation und vollwertigen KIT-Account: Gebühren, Krankenversicherung, ggf. nachzureichende Unterlagen
- Neuer Prüfzifferalgorithmus für Matrikelnummer
 - Letzte Ziffer der Matrikelnr. ist Prüfziffer (123456**7**)
 - Ab Matrikelnr. X neuer Algorithmus (i.d.R. alle ab WS 23/24 immatrikultierten Studierende)

Neuerungen mit HISinOne

- Zahlungsverarbeitung direkt in HISinOne und Kommunikation über LOK (ohne SAP)
 - KIT-Bankverbindung auf Briefen bitte beachten!
Briefvorlagen unter kit-cd.sts.kit.edu/briefe (rechte Spalte)
 - IBAN für Studiengebühren: **DE07 6600 0000 0066 0015 35**
- Neuerungen und Veränderungen im Studierendenportal
 - Rückmeldung und Bezahlung durchführen – Veränderte Oberfläche
 - Kontaktdaten bearbeiten – Veränderte Oberfläche
 - Anträge stellen (später) - NEU
 - Einwilligungen erteilen - NEU

Weiteres Vorgehen

- Derzeit laufen Schulungen für SLE und INTL mit Fachberatern von HIS zum Thema Studierenden- und Gebührenmanagement
 - 1. Block in KW 17 (erledigt)
 - 2. Block in KW 20 (aktuell)

- Produktivnahme von HISinOne in ~~KW 21 (Pfingstwoche)~~ KW 24 (ab 10.06.)
 - **In dieser Woche steht weder SOSPOS, noch HISinOne zur Verfügung!**
 - CAS Campus / BZM läuft weiterhin wie gewohnt

bwJupyter für die Lehre – Pilotphase und Perspektiven

Dr. Jasmin Hörter





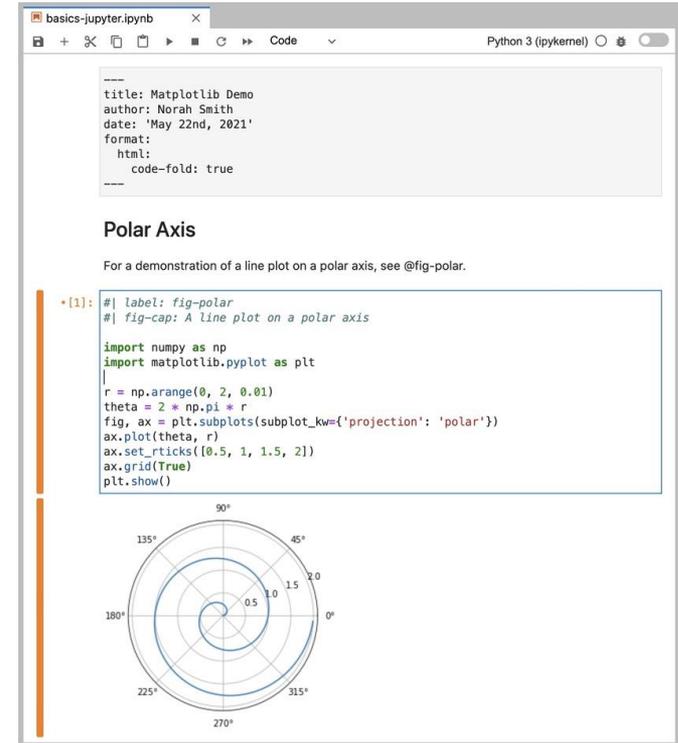
Ein Jupyter „Notebook“ ...

... ist kein „Laptop“, also kein Gerät, sondern:

- eine **web-basierte interaktive Software-Umgebung**, die aus einer Liste von Eingabe- und Ausgabezellen besteht, die jeweils Programmcode, Text und Plots enthalten können.

Warum Jupyter auch für die Lehre einsetzen?

- entspricht dem internationalen wissenschaftlichen Standard
- Geräteunabhängig einsetzbar
- unterstützt ca. 40 Programmiersprachen, u.a. **Julia**, **Python**, **R**
- open-source und somit frei verfügbar



bwJupyter für die Lehre

- Förderung im Rahmen des Dialogprozesses „Hochschulen in der digitalen Welt“
- Ziel: Aufbau eines Landesdienstes „bwJupyter für die Lehre“
- Projektteam: KIT (federführend) und Uni Stuttgart
- Erweitertes Projektteam/Pilotnutzer: Unis Heidelberg, Tübingen, Ulm, Hochschule Karlsruhe
- Fördervolumen: 801.350 Euro
- Projektlaufzeit 01.04.24-31.12.25

AP1: Pilotphase und technische Evaluation (Pascal Schuhmacher, SCC)

AP2: Nutzungsanforderungen und Bedarfe (Uni ST)

AP3: Niederschwellige Integration in die forschungsnaher Lehre (Uni ST)

AP4: Technischer Betrieb und Produktionsinfrastruktur (Klaus Scheibenberger, SCC)

AP5: Aufbau Supportstruktur

AP6: Projektmanagement (Jasmin Hörter, SCC)

bwJupyter – der neue Landesdienst

Ziel

- forschungsnahe Lehre in den Bereichen HPC, KI und Data Science mit Hilfe niederschwellig einsetzbarer Lehrtools

Konzept

- bestehende Dienste und Infrastrukturen nutzen (Pilot auf UC2, Integration in bwCloud-Umgebung)
- wenige Standorte betreiben den Dienst, alle bw-Hochschulen profitieren
- Communitybuilding und First-Level-Support an den jeweiligen Hochschulen
- Finanzierung über Umlagemodell

Pilotphase am KIT im Sommersemester 2024

- Pilot ist planmäßig zum SS24 gestartet
- 3 Notebook-Varianten wählbar:
 - CPU-Basispaket Python
 - CPU-Data Science-Umgebung mit Python, R und Julia
 - GPU-Jupyter für rechenintensive KI-Modelle mit Tensorflow und Pytorch
- Im WS24/25 wird die Pilotphase auf weitere bw-Hochschulen ausgeweitet



20 Lehrveranstaltungen mit ca. 1500 Nutzenden werden bedient



Zugriff ist auf angemeldete Lehrveranstaltungen beschränkt, Authentifizierung mit KIT-Account



Informationen unter [SCC-Dienste scc.kit.edu/dienste/jupyterhubpilot](https://scc.kit.edu/dienste/jupyterhubpilot)

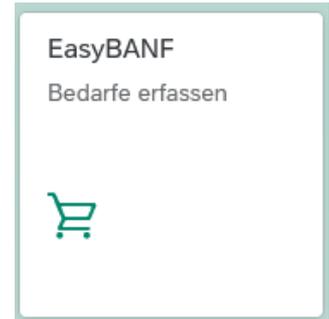
Aktuelles rund um das User Portal (UP)

Martin Hengel



Aktuelles rund um UP – easyBANF

- Pilotbetrieb beginnt mit ausgewählten Organisationseinheiten ab dem 22.05. (zunächst Freitextbestellungen)
- Gesamtproduktivsetzung mit Katalogbestellungen und Nicht-Einkaufsprozessen geplant für Ende Juni 2024
- Informationen (u.a. zu Online-Schulungen) werden laufend auf den Hilfewebseiten von UP ergänzt



Aktuelles rund um UP – ESS/MSS

- Neue App „Meine Zeitbuchungen“ mit verbesserter Usability (ersetzt bisherige aus dem SAP-Webportal stammende Oberfläche)
- Neue App „Meine Gleitzeitampel“ (provisorischer Name) für Mitarbeitende und Vorgesetzte
- Möglichkeit zur Einrichtung von Vertretungen in der Inbox



Aktuelles rund um UP – Beantragung von Berechtigungen

- Ablösung der bisherigen PDF-Formulare durch einen geführten Antrag mit digitalen Workflow auf Basis des Finanzstellenbaumes und Organisationsmanagements
- Neue App „Meine Berechtigungen“ und weitere Verbesserungen in Planung

Antrag zur Vergabe von Berechtigungen auf das User-Portal (UP)

2 Allgemeine Angaben 2 Berichtswesen 1 Warenkörbe und Rechnungen 4 Gäste- und Patrimonienstellung 1 Personentage (nur GFA) 2 Fertigstellen

Berechtigungen für Heugel, Martin (h4149@kit.edu) in der OE SCC - Scientific Computing Center festlegen

Hier werden Berechtigungen für SRM und die automatisierte Rechnungseingangsbearbeitung (AREB) beantragt. Aktuell ist noch nicht die Beantragung für Berechtigungen für die easyBANK, den Nachfolger für das SRM, möglich. Beachten Sie bitte die Regelungen der aktuellen Beschaffungsrichtlinie (<https://www.kit.edu/187.php>), insbesondere die Regelungen zu berechtigten Personen (3.1) und zur Beschaffung von Gefahrstoffen (3.8). Mehr Informationen zur automatisierten Rechnungseingangsbearbeitung finden Sie unter <https://www.kit.edu/1176.php>

Berechtigung	Aktion	Berichtswesen	Kostenstelle
Anlage von Warenkörbe für eigene OE	Neuvergabe	Einheit in Finanzstellenplan	
Berechtigung	Aktion		
Sachliche Richtigezeichnung von Lieferantenrechnungen	Aktion		
Berechtigung	Aktion	Berichtswesen	Kostenstelle
Freigabe von Gefahrstoffen	Neuvergabe		6188, 6190
Berechtigung	Aktion		
Erste Budgetgenehmigung von Warenkörben und Lieferantenrechnungen	Aktion		
Berechtigung	Aktion	Berichtswesen	PSP-Element
Abschließende erste Budgetgenehmigung für einzelne PSP-Elemente bei Warenkörben	Neuvergabe		
Kostenstelle	Personentage		
6331	02.00022211 (open-00137963)		
Berechtigung	Aktion		
Optionale zweite Budgetgenehmigung für Warenkörbe	Aktion		

Zurück Weiter Abbrechen

- Aufforderung zur Kennwortänderung
- Sicherheit beim Versenden von E-Mails
- Disaster-Recovery-Konzept für die neue a2DNS-Infrastruktur



Aufforderung zur Kennwortänderung

- Wer wurde angeschrieben?
 - ITBs und betroffene Benutzer
 - Ca. 1200 Benutzer
- Was wurde empfohlen?
 - Betroffene Benutzer sollen ihr Kennwort zweimal in Folge ändern
 - Über my.scc.kit.edu
- Warum?
 - RC4-Abschaltung in 12/2023 → fehlender AES128/256 Hash für Verschlüsselung angeforderter Kerberos Tickets
 - Ohne Kennwortänderung kein Zugriff auf Ressourcen, die zur Authentifizierung ausschließlich Kerberos verwenden

Sicherheit beim Versenden von E-Mails

12.04.2024

Mehr Sicherheit beim Versenden von E-Mails

Das SCC überprüft nun auch interne E-Mails, die eine potentielle Gefahr für die IT-Infrastruktur am KIT bedeuten können. Ein besonderes Gefahrenpotential ist beim Versand von bestimmten Dateien in Form von Mailanhängen gegeben.



E-Mails mit potentiell gefährlichen Dateien im Anhang werden schon seit langer Zeit beim Senden nach extern oder beim Empfang von extern geblockt (Siehe auch [Policy-Veränderung an den Maileingangssystemen](#)), denn diese Dateien, etwa Office-Dateien, die Makros enthalten, werden häufig von Angreifern genutzt, um Schadsoftware (sogenannte Makroviren) einzuschleusen. Um dieses beliebte Einfallstor für Angreifende zu schließen, wird das SCC die Sicherheit bei der E-Mail-Kommunikation innerhalb des KIT erhöhen und beispielsweise Mails auf solche potentiell gefährlichen Dateien überprüfen und ggf. blockieren. Das Mailrouting für KIT-Postfächer wird dazu angepasst.

Ab Dienstag, den 23. April 2024, werden dann auch die E-Mails, die von KIT-Postfach zu KIT-Postfach versendet werden, überprüft. Ab diesem Zeitpunkt werden also E-Mails mit potentiell gefährlichen Dateien im Anhang abgelehnt und erreichen damit die Zieladressen nicht mehr.

Das betrifft insbesondere E-Mails mit folgenden Anhängen

- RTF-Dateien oder
- Word/Excel-Dokumente mit Makros (*.docm und *.xlsm)



Disaster-Recovery-Konzept für die neue a2DNS-Infrastruktur



[SCC](#) > [Dienste](#) > [Arbeitsumgebung](#) > [Netzzugang \(Internet, WLAN, VPN\)](#) > [Domain Name Service \(DNS\)](#) > [mehr](#)

Domain Name Service (DNS)

Kontakt: dns-betrieb@scc.kit.edu

Der Domain Name Service für das KIT beinhaltet den Betrieb der DNS-Server, die Bereitstellung des Self-Service-Portals DNSVS und die Durchführung der Domain-Registrierung für durch KNN genehmigte Domains.

Der Domain Name Service ist vergleichbar mit einem Telefonbuch. Jedes Gerät im KIT-Netzwerk erhält automatisch oder manuell eine IP-Adresse zur Kommunikation. Damit beispielsweise ein Browser den entsprechenden Server hinter einer Webseite erreicht oder eine EMail zugestellt werden kann, wird im Hintergrund der Name auf die entsprechende IP-Adresse aufgelöst. Hierzu werden am KIT von der Abteilung Netze und Telekommunikation DNS-Server betrieben. Zu unterscheiden sind hierbei die autoritativen Nameservern, welche die DNS-Einträge des KIT weltweit bereitstellen, und den Resolvern, welche für ein Endgerät am KIT das globale DNS-System abfragen.

Eintragungen in das DNS-Systemen am KIT können von IT-Betreuern am KIT über das am SCC entwickelte Self-Service-Portal DNSVS vorgenommen werden. Neue Subdomains **<subdomain>.kit.edu** oder Domains außerhalb des Namensraums unterhalb von **kit.edu** müssen vom Gremium Karlsruhe Names and Numbers (KNN) genehmigt werden.



Kurzinformationen / Sonstiges

- bwGitLab – GitLab als Landesdienst
- bwSync&Share - Freischaltung von Apps
- VMware am SCC - Quo vadis?
- Anhang
 - Infoveranstaltungen / Arbeitskreise
 - Neues zu IuK-Diensten und Infrastruktur



GitLab als Landesdienst – bwGitLab

Klaus Scheibenberger



- Im Rahmen des Dialogprozesses „Zukunftslabor Hochschulen in der digitalen Welt wurde der Projektantrag *Landesdienst GitLab* gestellt.
 - **Ziel:** Aufbau eines landesweiten GitLab-Dienstes
 - Federführend HD, KIT/SCC als Kooperationspartner
 - Antrag wurde Mitte April bewilligt
- Standorte für (zentrale) GitLab-Installationen sind HD und KIT
 - Einbindung der am SCC bereits laufenden Installation (*GitLab am KIT*)
- Projektstart 01.07.2024
- Abstimmung mit GitLab bzgl. Lizenz-Fragestellung (Thema Landeslizenz) wurde bereits initiiert.

Ergänzung weiterer Apps in bwSync&Share?

Klaus Scheibenberger



Apps in der Nextcloud von bwSyncAndShare?

- bwSync&Share nutzt aus der Nextcloud Enterprise Subscription die **Nextcloud Files Subscription**
 - Weitere Subscriptions sind *Groupware*, *Talk*, *Nextcloud Office*
- Im Umfang der **Files-Subscription** sind Apps wie beispielsweise *Contacts* (darin integriert auch *Circles*) und *Photos* verbunden (siehe [Übersicht](#)).
 - Für diese Apps leistet Nextcloud im Rahmen von bwSync&Share daher auch Support!
- Diese sind auch installiert, Circles wurde aber erst wieder Ende August 2023 freigegeben, nachdem massive Instabilitäten behoben waren.
- Auch die **Federation-App** (*Federation Sharing*) ist Teil der Files Subscription
 - Aber: Im Hintergrund werden zwischen den beteiligten Instanzen Benutzerverzeichnisse ausgetauscht!
 - “... trusted Nextcloud servers, which allows the trusted servers to **exchange user directories** and **auto-complete** the names of external users ...” (siehe [hier](#)).
 - Das ist der „technische“ Grund *Federation Sharing* nicht zuzulassen.
 - Das Teilen über Instanzen hinweg ist für Nutzer nicht selbsterklärend: “... *Click the share icon, and then enter the username and URL of the user on the remote Nextcloud server...*” (siehe [hier](#)).

Erweiterung um Apps

- **Primäres Ziel:** Stabiler Betrieb!
 - Bekannt: Es gibt im Dienstbetrieb nach wie vor Instabilitäten durch DB-Probleme.
 - Nextcloud arbeitet daran:
 - In Nextcloud Hub 8 wird die Struktur angepasst werden (u.a. DB sharding) um diese Probleme zu beheben.
- In 2023 wurde die *Deck* App (Projektverwaltung; *Kanban*) als ein erster Test für weitere Apps installiert
 - Ziel: Sukzessive Erweiterung der Funktionalitäten (*Deck* war eine Entscheidung von uns als Betreiber.)
 - Es kam dann Mitte Juli 2023 zu massiven Performanzproblemen, die zunächst nur durch Abschaltung der App behoben werden konnten.
 - Aber: Da diese App nicht Teil der Files sondern der Groupware Subscription war/ist, muss der Support für diese Subscription separat hinzugekauft werden.
 - Es wurde eine Sonderkondition dann nur für *Deck* getroffen (da Talk und Mail nicht genutzt werden).
 - Erst im September 2023 konnte *Deck* wieder freigegeben werden.

Kosten, Ressourcen, ...

- Die Erweiterung durch Apps birgt die Gefahr von zusätzlichen **Instabilitäten** für den Dienst.
- Die Absicherung durch Zukauf von Nextcloud Support erhöht die **Kosten**.
 - Und: Absicherung heißt nicht die Vermeidung/Verhinderung von Problemen, sondern (nur) Unterstützung bei der Behebung/Lösung von auftretenden Problemen!
- Die personellen Ressourcen (im aktuelle Betrieb) sind stark begrenzt.
 - Tests (vieler) zusätzlicher Apps und insbesondere die Behandlung von Störungen würde den personellen Aufwand zusätzlich erhöhen.
 - Und die Erfahrung zeigt: Die (Last-)Stabilität zeigt sich immer erst im realen Betrieb.
- Demgegenüber stellen sich aber auch Fragen bzgl. sich überschneidender Funktionalitäten, z.B.:
 - Braucht man zusätzlich *Mail* (App) wenn man Exchange mit entsprechenden Mail-Clients nutzen kann: *OWA* (Web), *Outlook*, *Thunderbird* und Clients (for mobiles)?
 - Braucht man zusätzlich *Talk* für Chat wenn man *Matrix* hat?
- Unter den Randbedingungen: Was kann man (evtl. sogar mehrfach) betreiben/bereitstellen?
 - „Was macht man selbst und was nicht“. (Auch das gehört auch zu *Digital Sovereignty*)

VMware am SCC – Quo vadis?

Klara Mall



Was bisher geschah – VMware by Broadcom

- Massive Veränderungen im Portfolio
 - Fokus auf wenige Bundles
 - Nur noch Softwaremiete
 - Keine EDU-Preisliste, Rabatte auf Verhandlungsbasis
 - Auswirkungen bei kleinen Kunden heftiger als bei großen

- Unsicherheiten bei Kunden
- Große Unzufriedenheit bei der Community
- Schlechte Presse
- Erste Klagen in Europa / Deutschland

VM-Umgebung am SCC

- (Noch) kein Grund für Panik
 - Lizenzvertrag bis Ende 2025
 - VMware-Lizenzen heute nur ein kleiner Teil der Gesamtkosten einer VM
- VMware ablösen? Schwierig
 - Umgebung zu groß für Proxmox-artige Ansätze
 - Workloads wie SAP oder Exchange erfordern zertifizierte Infrastruktur
 - Echte Alternativen (z.B. Nutanix) nicht zwingend günstiger

VMware am KIT

- Vorschlag: Austausch mit VMware-Betreibern am KIT
- Ziele:
 - Evaluierung von Alternativen
 - Knowledge Sharing
 - Gemeinsamer Einkauf?
 - Gemeinsamer Betrieb von Infrastruktur?
- Bei Interesse gern Kontakt zum VM-Team (vm-team@lists.kit.edu)

Infoveranstaltungen / Arbeitskreise

Anhang



Infoveranstaltungen / Arbeitskreise

Thema	Termine	Uhrzeit	Ort / Anmeldung
Werkzeuge zur Administration von kit.edu	Dienstag, 18.06.2024	13:30 – 15:30 Uhr	MS Teams SCC_ITB-Info-AdminKitEdu 
Netzverwaltung am KIT	Mittwoch, 26.06.2024	09:30 – 11:00 Uhr	MS Teams SCC_ITB-Info-AdminKITnet 
Grundunterweisung IT-Sicherheit / Teil 1	Donnerstag, 18.07.2024 Donnerstag, 14.11.2024	13:30 – 15:30 Uhr	FTU; Online 
Grundunterweisung IT-Sicherheit / Teil 2	Dienstag, 30.07.2024 Mittwoch, 27.11.2024	09:00 – 13:00 Uhr	FTU; Online 
Arbeitskreis Clientmanagement	Mittwochs <ul style="list-style-type: none"> • 19.06.2024 • 07.08.2024 • 09.10.2024 • 04.12.2024 	09:00 – 10:00 Uhr	MS Teams SCC_AK-Clientmanagement 

Neues zu IuK-Diensten und -Infrastruktur

Anhang



Neues zu IuK-Diensten und -Infrastruktur

Thema	Detail	Protokoll/ Präsentation / Change	Dienst
Serverhousing am SCC	Konzept: Ausblick auf Angebot für KIT-Einrichtungen am CS und CN, Kosten, Bestellung, ...	 	
KIT-AD: Deaktivierung Computerkonten	Alte Computerkonten wurden Anfang Dezember 2023 deaktiviert (350 Rechner betroffen);		
KIT-AD: Anmeldenamen von KIT Konten für Beschäftigte werden vereinheitlicht	Änderung des UPN; Anpassung des Anmeldenamens für Beschäftigten-Konten am KIT => <ab1234>@kit.edu	 	
KIT-AD: Verteilung von Datenschutzeinstellungen für Windows 10 und Windows 11	Zur Verbesserung von Datenschutz und Informationssicherheit auf Windows 10/11 Geräten werden im KIT-AD Gruppenrichtlinien zu „Win 10 sicher konfigurieren“ umgesetzt		
KIT-AD: Abschaltung alter Verschlüsselungsalgorithmen	Abschaltung TLS 1.1; Unterstützung von Cipher Suites mit Status recommended oder secure.		
MS Update Service	keine Updates mehr für Windows 7, Windows 8/8.1, Windows Server 2008/R2, Windows Server 2012/R2		

Neues zu IuK-Diensten und -Infrastruktur

Thema	Detail	Protokoll/ Präsentation / Change	Dienst
Forschungssoftware	KIT-internes Projekt zur Forschungssoftware www.rse-community.kit.edu	 	
Externer IT-Support für Arbeitsplatz-Endgeräte	Vorstellung des neuen/alten Rahmenvertragspartners TechniData	 	
KIT-Postfach: Internes Mailrouting	Änderung Mailroutings für interne Mails in der KIT Exchange Server Umgebung		
KIT-Postfach: Mehr Sicherheit beim Versenden innerhalb des KIT	Erweiterte Überprüfung von E-Mails auf Spam, Phishing und potentiell gefährlichen Anhängen. Freigabe für externen Zugriff auf smtp.kit.edu ohne VPN		

Neues zu IuK-Diensten und -Infrastruktur

Thema	Detail	Protokoll/ Präsentation / Change	Dienst
Zentraler Fileservice	Informationen zu Ransomware-Strategie; OE-Interne Aufteilung der Kontingente; Umstellung S3 auf IAM-Konten; OE-Veränderungen und Konsequenzen	 	  
Zentraler Fileservice	Änderung des Snapshot-Zeitpunkts für \\scfcs.scc\service		
KI: Microsoft Copilot	Nutzung von MS Copilot am KIT	  	
KI: LLMs zur Unterstützung von administrativen Prozessen	Lokal betriebene LLMs zur Erschließung von Anwendungsmöglichkeiten zur Unterstützung von administrativen Prozessen (AIFB, SCC)	 	

Neues zu IuK-Diensten und -Infrastruktur

Thema	Detail	Protokoll/ Präsentation / Change	Dienst
KIT-CA: Zertifikate	Status und Diskussion; DFN-PKI vs. GÉANT TCS/Sectigo vs. Let's Encrypt; ...		
KIT-CA: CA-Portal für Anträge	Zertifikatsanträge über CA-Portal statt über SCC Ticketsystem (seit 3.5.24) - portal.ca.kit.edu		
KIT-Internet: Firewall Einstellungen	Konfigurationsänderung: Sperrung von Ports für eingehenden Datenverkehr		
SAP: User Portal (UP)	User Portal (UP) – up.scc.kit.edu – ersetzt SAP-Webportal		

Neues zu IuK-Diensten und -Infrastruktur

Thema	Detail	Protokoll/ Präsentation / Change	Dienst
JupyterHub für die Lehre	Start der Pilotphase zum SoSe 2024		
GitLab Pilotbetrieb	Ende der Pilotphase; Betrieb von git.scc.kit.edu wurde zum Ende des WiSe am 31.03.24 eingestellt;		
ILIAS	Umstellung der Usernames in EPPN-Format		
CAS-Campus	Umstellung der internen Userbezeichnungen		

Vielen Dank für Ihre
Aufmerksamkeit !!!

Schöne Pfingsten 😊

i Nächste ITB-Versammlung
Mittwoch, 27.11.2024, 9:30 – 11:30 Uhr

