

14. IT-Beauftragten Versammlung am 9. November 2017

Partnerschaftliche Zusammenarbeit zwischen SCC und ITB

STEINBUCH CENTRE FOR COMPUTING - SCC



Agenda

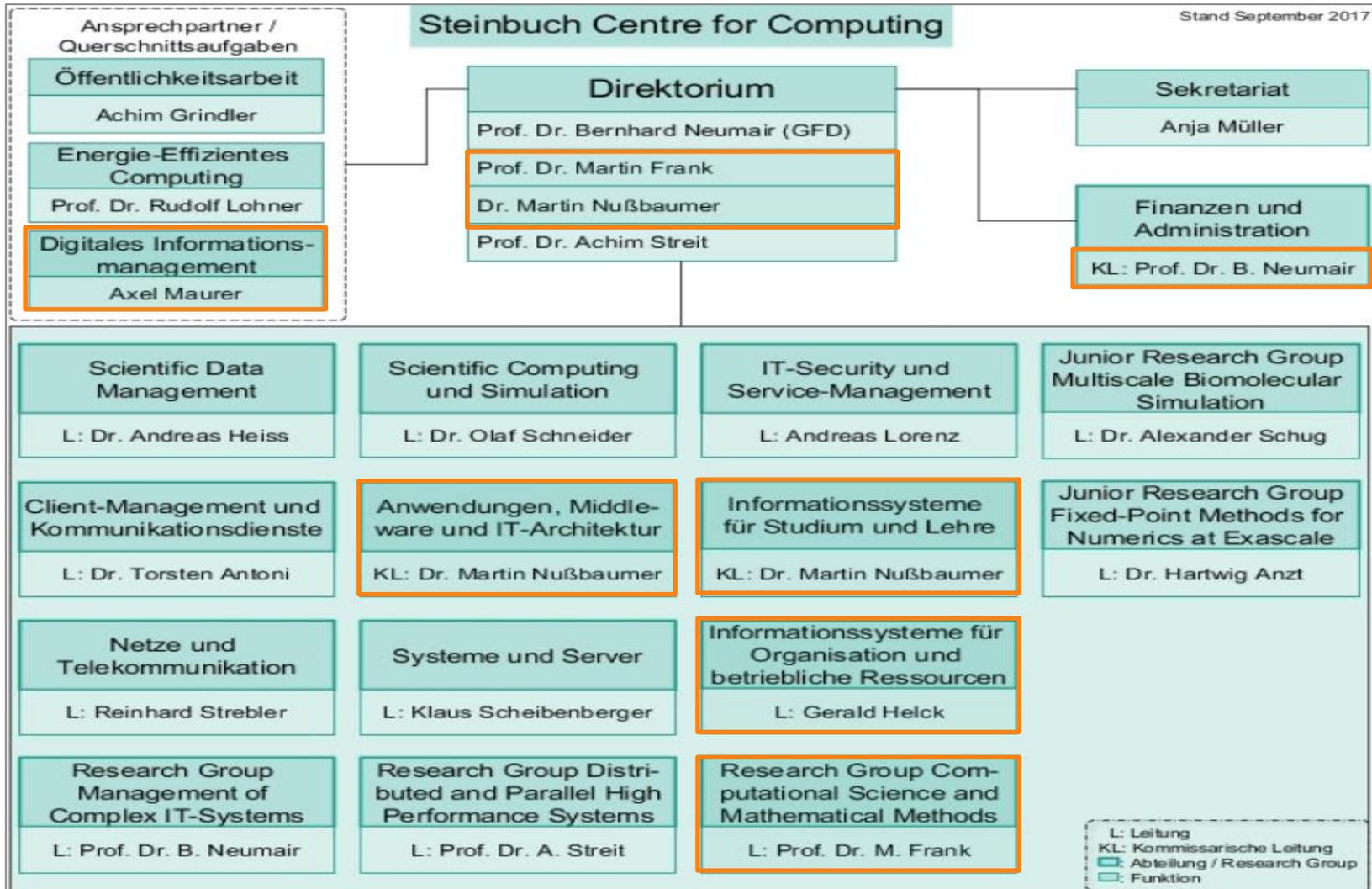
- Begrüßung / Neues aus dem SCC
- Änderungen im SCC - Zusammenführung SCC und ASERV-VIT
- Vorstellung des SAP-Webportals
- Vorhaben Erneuerung KIT-Card
- IPv6 am KIT
- bwSync&Share: Demonstration von OnlyOffice
- Verschiedenes / Diskussion

Begrüßung / Neues aus dem SCC

STEINBUCH CENTRE FOR COMPUTING - SCC



SCC-Organisation – September 2017



Neuer wiss. Direktor am SCC

- Prof. Dr. Martin Frank, vorher RWTH Aachen
- W3-Professur für „Computational Science and Mathematical Methods“
- Mitglied im SCC-Direktorium, Lehre in der Fakultät für Mathematik

- Forschungsschwerpunkte: Numerical methods for kinetic equations and conservation laws, Uncertainty quantification, Application-oriented mathematics, Relevance of mathematics in society

- Start am SCC: 1. September 2017



Änderungen im SCC

Zusammenführung SCC und ASERV-VIT

STEINBUCH CENTRE FOR COMPUTING - SCC



Zur Erinnerung

- Geänderte Bedrohungslage
 - Insbesondere vor dem Hintergrund erfolgreicher Phishing-Angriffe
- Der IT-Sicherheitsbeauftragte hat die Einführung einer Zwei-Faktor-Authentifizierung empfohlen
 - Bei Verarbeitung von Daten mit erhöhtem Schutzbedarf
 - Aktuell: SAP
- Das Präsidium ist der Empfehlung gefolgt
 - SCC wurde mit der Umsetzung beauftragt

Umsetzung

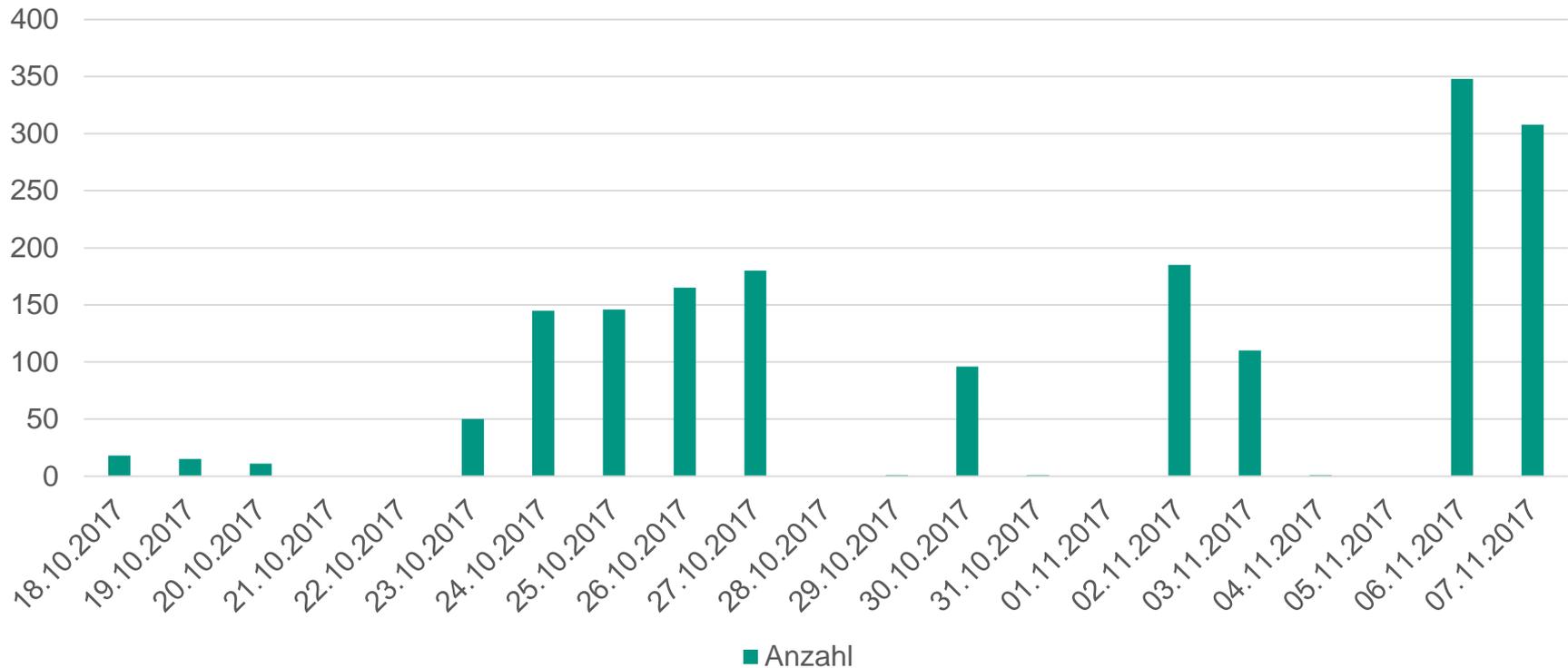
- Präsidiumsbeschluss 27. Februar
- Vorstellung IT-Expertenkreis 23. März
- Vorstellung KIT-ON 18./19. Juli
- Abstimmung mit dem Personalrat 19. September
- Update IT-Expertenkreis 18. Oktober
- Start der Verteilung 19. Oktober
- Information an alle Mitarbeiter 30. Oktober

- Umschaltung SAP-Portale 13. November

Rollout

- Token wurden bislang in 141 von 200 OE aktiviert

Anzahl



Token am KIT (1/2)

- KIT-Token mit Display
 - Time-based One-time Password (TOTP, RFC 6238)
 - 5 Jahre Laufzeit
 - Zeigt Code auf Knopfdruck an

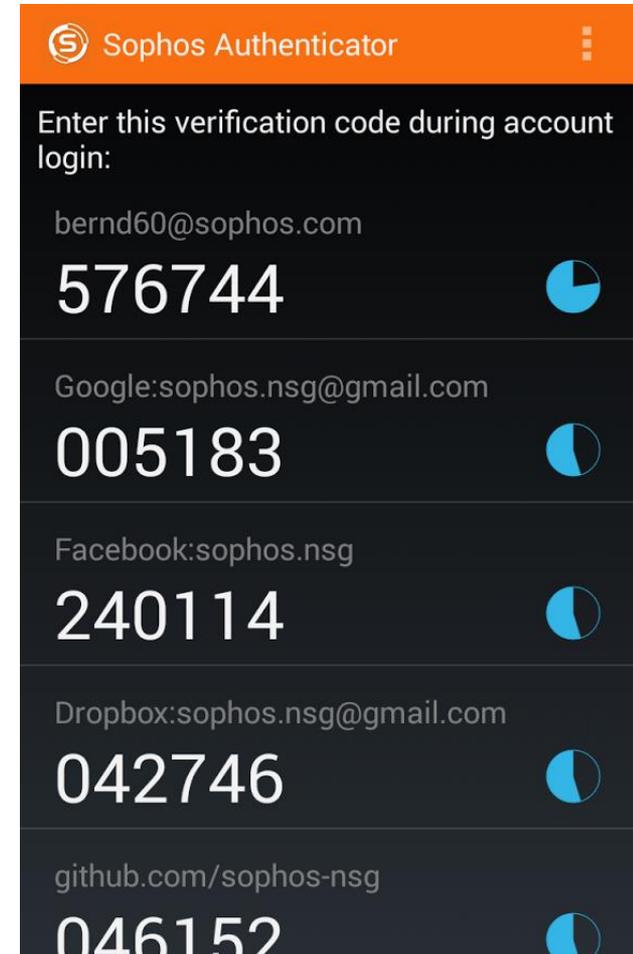
- Hardware-Token mit USB-Anschluss
 - Yubikey 4
 - Teuer und weniger flexibel
 - Leicht, klein, lange Nutzungsdauer
 - Lösung für Sehgeschädigte

- Infineon-Schwachstelle betrifft die Zwei-Faktor-Authentifizierung nicht!



Token am KIT (2/2)

- Smartphone-Apps
 - Getestet z.B.: Lastpass Authenticator, Google Authenticator, Microsoft Authenticator, FreeOTP Authenticator, Sophos Authenticator
 - Gemäß RFC 6238
 - Benötigt keine Internet-Anbindung
 - Vorgesehen insbesondere für GuP und Studierende
- Backup-Liste
 - Im Self-Server unter „neues Token“
 - Ausdruck und sichere Verwahrung!





KIT
Karlsruher Institut für Technologie

SAP-Portal Entwicklungsportal

Wählen Sie einen der verfügbaren Identity-Provider aus

Identity-Provider

[Fortsetzen](#) [Abbrechen](#)

Copyright © SAP AG. Alle Rechte vorbehalten 

Links zur Zwei-Faktor-Authentifizierung

- Anleitungen, Dokumentation
 - <http://www.scc.kit.edu/dienste/2fa>
- Self-Service-Portal
 - <https://my.scc.kit.edu>
 - Direkter Einstieg: <https://my.scc.kit.edu/token>

Vorstellung des SAP-Webportals

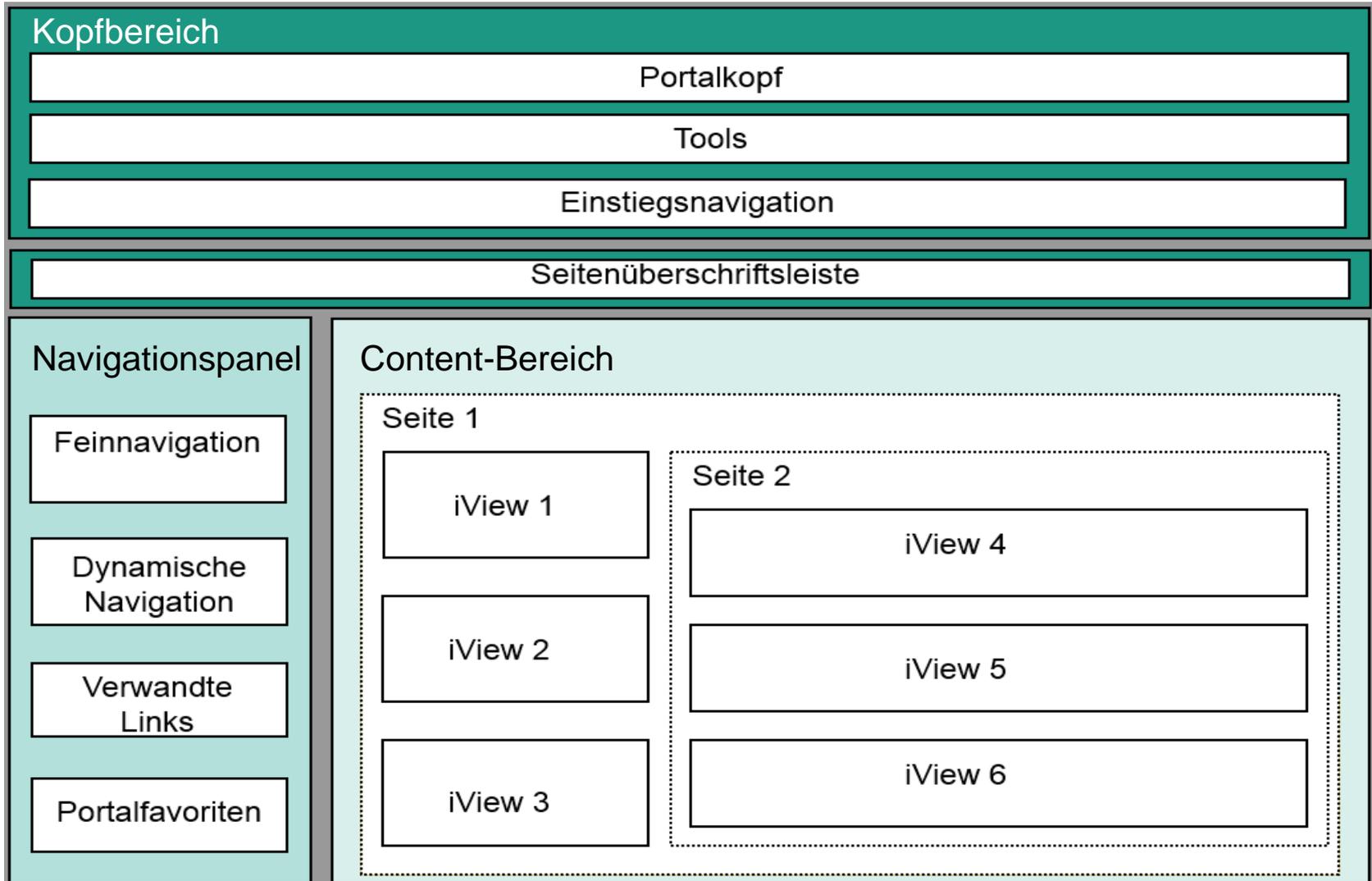
STEINBUCH CENTRE FOR COMPUTING - SCC



Motivation für ein neues Web-Portal

- Aufbau einer benutzerfreundlicheren Oberfläche
 - Verbesserte Menüführung
 - Zusätzliche Verlinkungsmöglichkeiten
 - Einblenden von Nachrichtenpanels
- Browser-unabhängige Nutzung des Portals
 - Versionsunabhängige Nutzung von Microsoft-Explorer und Firefox
 - Unterstützung weiterer Browser, wie Google Chrome, Safari

Grundaufbau Portal



Kopfbereich - Links

[HOME](#) | [ENGLISH](#) | [CHANGE PW](#) | [SYSTEM NACHRICHTEN](#) | [ABMELDEN](#) | [A-Z INDEX](#) | [INTRANET](#) | [KIT](#)



[Startseite](#)

[Employee Self-Services](#)

[Einkaufen](#)

[Willkommen](#)

[Home](#)

Kopfbereich - Systemnachrichten

HOME | ENGLISH | CHANGE PW | **SYSTEM NACHRICHTEN** | ABMELDEN | A-Z INDEX | INTRANET | KIT

root> documents> KIT> sysmsg.html- Edit Online

B Z U

Das SAP-Portal wird vom TT.MM.JJJJ um HHMM bis zum TT.MM.JJJJ um HHMM gewartet und steht in der Zeit nicht zur Verfügung. ...

SCC-IOR

System Message End Date	06.11.2017 12:00:00
System Message HTML	
System Message Start Date	06.11.2017 10:00:00



Benutzer *

Kennwort *

Anmelden

Employee Self-Service

Übersicht

SYSTEM MESSAGES

Das SAP-Portal wird vom TT.MM.JJJJ um HH:MM bis zum TT.MM.JJJJ um HH:MM gewartet und steht in der Zeit nicht zur Verfügung.
SCC-IOR

Systemnachrichten anlegen

Systemnachrichtentext

Dieses System wird vom TT.MM.JJJJ um HH:MM bis TT.MM.JJJJ um HH:MM gewartet und steht in der Zeit nicht zur Verfügung. Bitte um Beachtung!

Servername SID.sap.kit.kit.edu

Mandant 100

Sprache DE

verfällt am 20.11.2017 23:00:00

löschen am 21.12.2017 23:00:00



SAP

Neues Kennwort

Mandant 100

Benutzer testuser

Kennwort *****

Sprache

Menü Bearbeiten Favoriten Zusätze

sm02

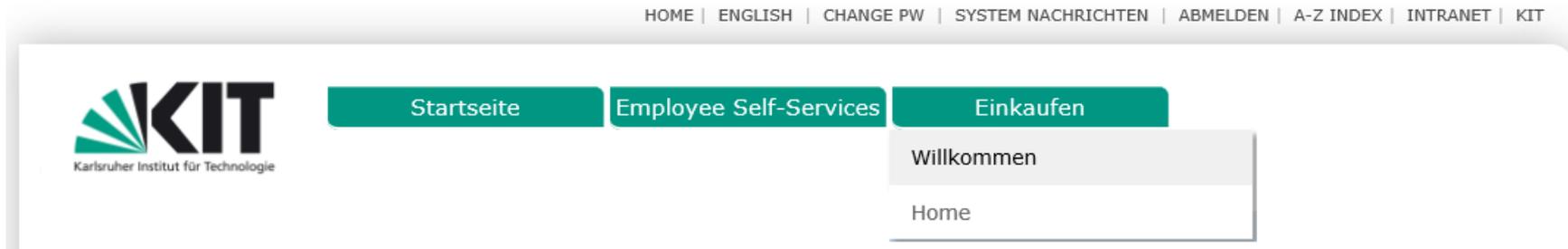
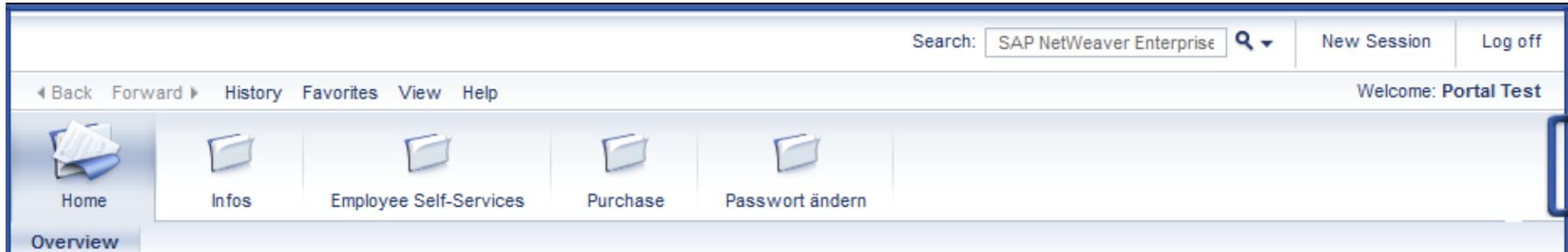
Systemnachrichten

Autor Express-Mag Text

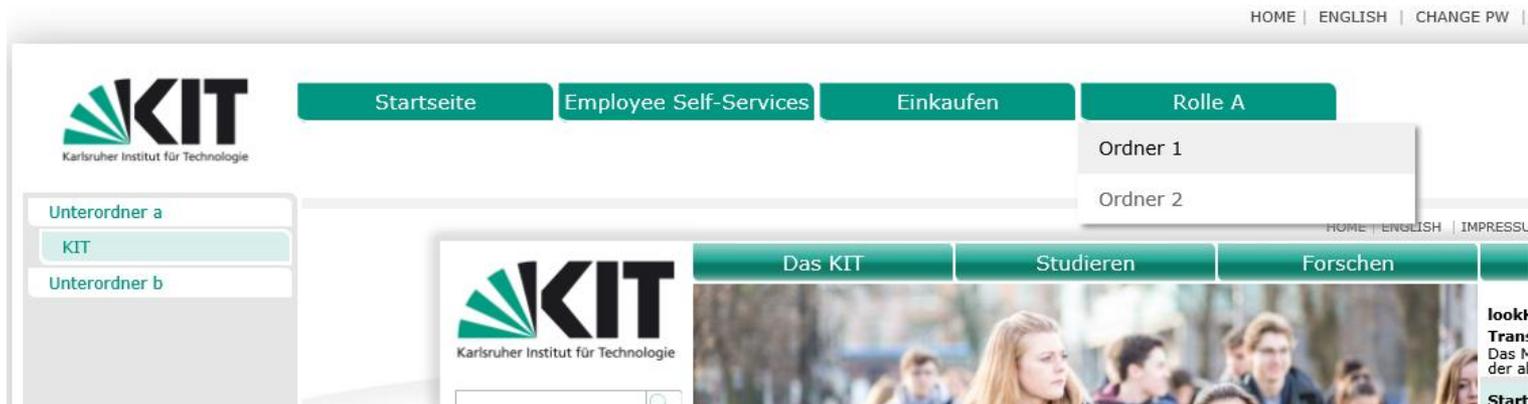
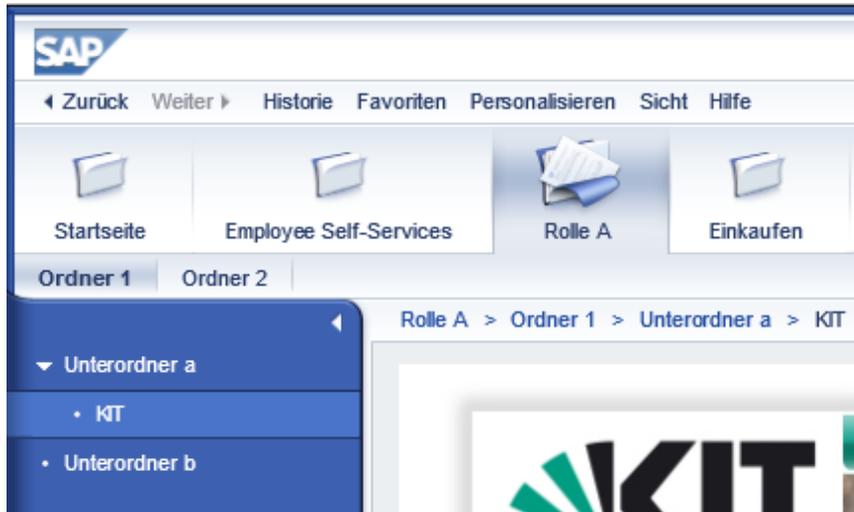
DOGAN-Y

Dieses System wird vom TT.MM.JJJJ um HH:MM bis TT.MM.JJJJ um HH:MM gewartet und steht in der Zeit nicht zur Verfügung. Bitte um Beachtung!

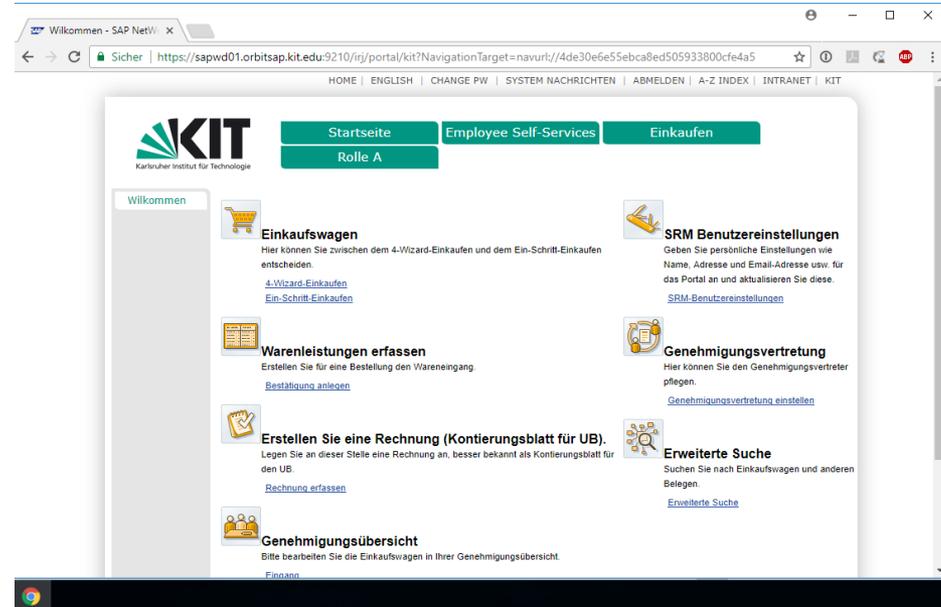
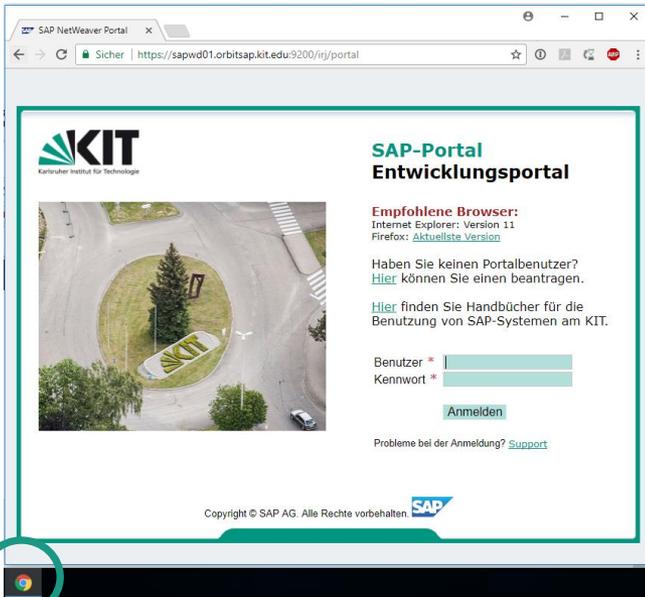
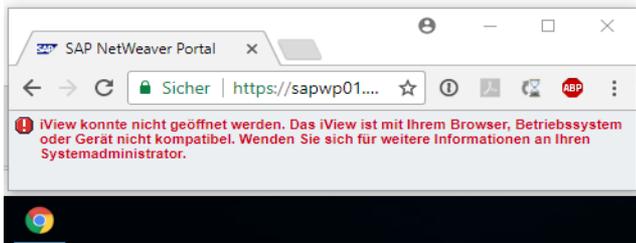
Kopfbereich – Optik – Mouseover



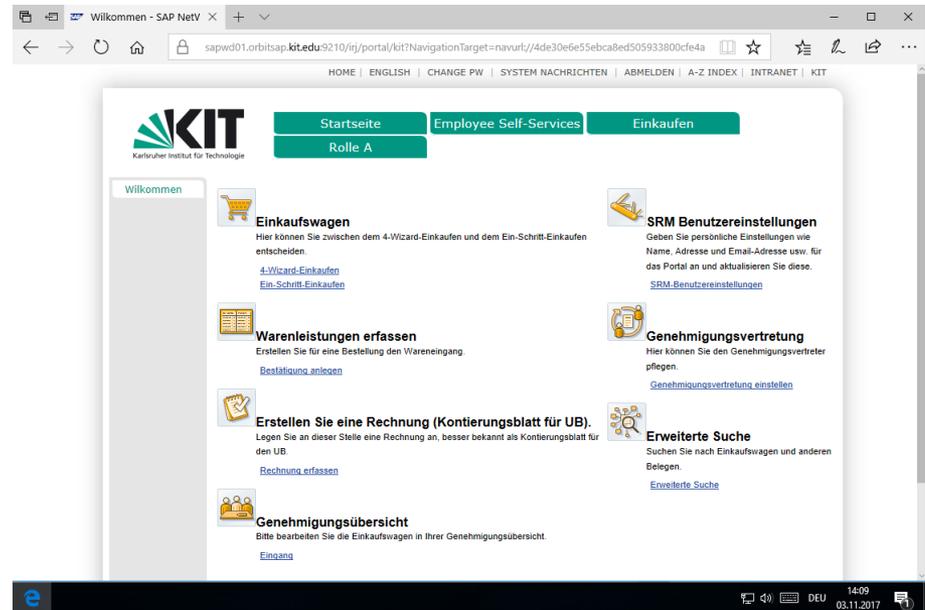
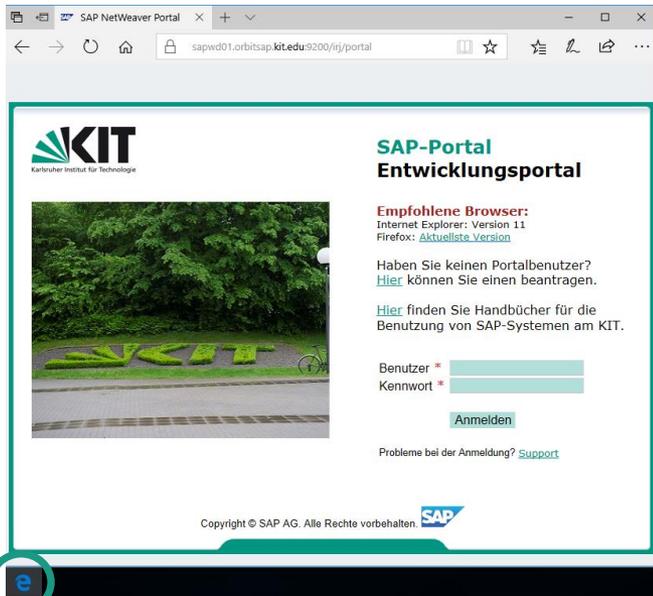
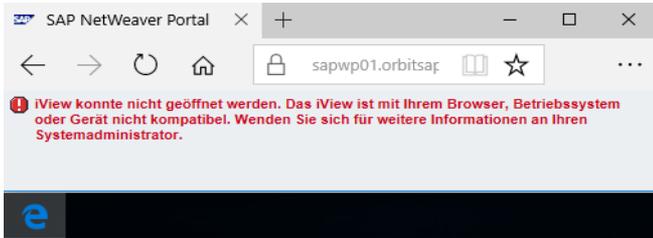
Navigationspanel



Contentbereich- Browserunabhängigkeit - Chrome



Contentbereich - Browserunabhängigkeit - Edge



Startseite – Links und Nachrichten


Aktuellste Version. It then asks 'Haben Sie keinen Portalbenutzer?' and provides a link [Hier](#) to request one. Another link [Hier](#) is provided for finding handbooks. There are input fields for 'Benutzer *' and 'Kennwort *', and an 'Anmelden' button. At the bottom, it says 'Probleme bei der Anmeldung? [Support](#)' and 'Copyright © SAP AG. Alle Rechte vorbehalten.' with the SAP logo." data-bbox="447 426 956 901"/>

KIT
Karlsruher Institut für Technologie

SAP-Portal NetWeaver

Empfohlene Browser:
Internet Explorer: Version 11
Firefox: [Aktuellste Version](#)

Haben Sie keinen Portalbenutzer?
[Hier](#) können Sie einen beantragen.

[Hier](#) finden Sie Handbücher für die
Benutzung von SAP-Systemen am KIT.

Benutzer *
Kennwort *

Probleme bei der Anmeldung? [Support](#)

Copyright © SAP AG. Alle Rechte vorbehalten. 

- Implementierung Portal unter Windows12 abgeschlossen
- Z. Zt. erfolgt das Einbauen von Portal-Patches
- Test durch den Fachbereich steht noch aus
- Dokumentation für Portal wird aktuell aufgebaut
- Produktivstart mit neuer Portaloberfläche zum **Q1/2018** vorgesehen
- Roll-Out neue GUP Gäste- und Partnerverwaltung als Web-Anwendung bereits im **Dezember 2017**

- Weiterer Ausbau Portal
 - Sequentielle Implementierung von Add-ONS in den angeschlossenen IT-Systemen ERP, SRM und BW → dadurch responsives Web-Design umsetzbar
 - Sukzessive weitere Verbesserung des Portals hinsichtlich Bedienbarkeit und Browserunabhängigkeit

VPN-Verschlüsselung

■ Motivation

- In den Web-Portalanwendungen SAP-SRM, SAP-ESS/MSS, SAP-Personentage ist der Datenverkehr verschlüsselt und sehr gut geschützt
- Für SAP-BW und SAP-ERP sind hier zusätzliche Maßnahmen zum besseren Schutz der Kommunikationskanäle erforderlich
- Der Aufbau einer VPN-Verschlüsselung gewährleistet einen gesicherten Transport der Daten

Nutzung VPN für SAP-GUI

- Für die Nutzung von SAP-GUI (Zugriff auf ERP) muss in jedem Fall zuerst eine VPN-Spezial-Verbindung (SAP-VPN) hergestellt werden
 - Es wird unterschieden zwischen innerhalb und außerhalb des KIT

- SAP-VPN
 - Für das SAP-VPN wird das Token der Zwei-Faktor-Authentifizierung benötigt:
<https://www.scc.kit.edu/dienste/2fa.php>
 - Installation und Konfiguration des VPN (OpenVPN-Dienst des SCC):
<http://www.scc.kit.edu/dienste/openvpn.php>

- Zugang innerhalb KIT
 - Realm: @sap
 - Jeder KIT-Mitarbeiter kann dieses VPN nutzen (keine Gruppenvoraussetzung)

- Zugang von außerhalb KIT (Home Office, HIU, ...)
 - Realm: @sap-von-aussen
 - Zugriffsmöglichkeit wird auf Antrag erteilt (Eintrag in Gruppe)

Installation VPN

- Die Installationsanleitung für OpenVPN
<http://www.scc.kit.edu/dienste/openvpn.php>
- Bitte Beachten! Verwenden Sie die Konfiguration für VPN-Spezialzugänge (VPN2VLAN): kit-vpn2vlan.ovpn
- Anmeldung im KIT
Benutzername: <KIT-Account>@sap
z.B. ab1234@sap
Passwort: <KIT-Passwort><Komma><Token>
z.B. 4vzo!81nn/T,639950
- Anmeldung von außen
Benutzername: <KIT-Account>@sap-von-aussen
Passwort: <KIT-Passwort><Komma><Token>
- Gültig ab 20.11.2017

Überblick über Zugriffe auf SAP Webportal und SAP-GUI

was muss der Nutzer beim Zugriff bereithalten?

Anwendung	2FA-Token	Account	SAP-VPN mit 2FA-Token
SRM (Portal)	X	KIT-Account	
BW (Portal)	X	KIT-Account	X
ESS /MSS (Portal)	X	KIT-Account	
Personentage (Portal)	X	KIT-Account	
ERP (GUI)		KIT-Account für VPN	X

Dadurch sind alle SAP-Anwendungen mittels 2FA gesichert

Geplante Änderungen im SAP-Umfeld

- 13.11.2017
Nutzer, die von außerhalb auf das SAP-System zugreifen, werden in einer E-Mail über die sie betreffende Änderungen informiert
- 13.11.2017
ERP-Nutzer und BW-Nutzer, die von innerhalb des KIT zugreifen, werden ebenfalls über sie betreffende Änderungen informiert
- Ab 20.11.2017
Zugriff von außerhalb des KIT über neuen Spezialzugang von außen
- Ab 20.11.2017
Zugriff von innerhalb des KIT über neuen Spezialzugang von innen möglich
- Ab 27.11.2017
kein Zugriff von innen ohne VPN mehr möglich
- Dezember 2017
GuP als Anwendung im SAP-Webportal
- Q1/2018
Optimierung des SAP-Webportals hinsichtlich Nutzung über andere Browser

KIT-Card

Kartentausch mifare Classic nach DESFire

STEINBUCH CENTRE FOR COMPUTING – SCC



UID CHANGEABLE 1K MIFARE



10 X UID card Changeable Writable Proxiable Mifare

Top selling product ★★★★★ Be the first to know

Item condition: New

Quantity:

More
24 sold

Price: US \$18.99

6 watching

100% buyer satisfaction

More than 1000 sold

Shipping: \$40.95 USPS Priority Mail

See details about international shipping
Item location: Mount Pleasant, SC
Ships to: Worldwide



KITCard-Leser

KONTOSTAND

14,44 €

LETZTE TRANSAKTION

- 2,00 €

DETAILS

Herausgeber

KIT

Kartentyp

Mitarbeiter

Kartenummer

158021430447

Kartentechnologie mifare

Classic

- Verschlüsselung mit proprietärem Crypto-1 48 Bit (inzwischen dekodiert mit Sicherheit „nahe Null“)
- Schlüssel teilweise fest und inzwischen bekannt
- Zentrale Verwaltung der Schlüssel beim Kartenchiphersteller
- Karten mit rewritable UID einfach zu kaufen

DESFire EV1/EV2

- Verschlüsselung mit AES 128 Bit
- Alle Schlüssel beim KIT
- UID fälschungssicher (noch)
- Erfüllt ISO/IEC 14443
- Bietet Random UID Funktion
- Nach ISO 15408 (Common Criteria) EAL5+ zertifiziert

Ausgangssituation

- Funktionen der KIT-Card
 - Funktion 1: Chipkarte als digitales Identifikationsmerkmal
 - Funktion 2: Plastikkarte als Sichtausweis

- Sicherheit der KIT-Card
 - *Nach heutigen Maßstäben sind beide Funktionen (teilweise) unsicher*
 - ⊘ Chipkarte mit der eingesetzten Technologie „mifare Classic“ kann gefälscht werden
 - ⊘ Sichtausweisfunktion für Studierende verfügt über keinen verlässlichen Bild-Identifikationsprozess
 - ✓ für Mitarbeiter/innen existiert ein verlässlicher Identifikationsprozess (UB, GFB)

Ziel

- KIT-Card mit verlässlichen Merkmalen in beiden Funktionen soll ab August 2018 flächendeckend umgesetzt sein
 - Verlässliche Kartentechnologie durch Einsatz nach derzeitigem Stand fälschungssicherer Technik mit Verschlüsselung
 - Verlässliche Informationen auf der Karte (Aufgabe der Sicherheitseinrichtungen am KIT → SUM, AServ-CSI)
 - Gegebenenfalls zusätzliche Merkmale zu Erhöhung der Fälschungssicherheit in der Funktion als Sichtausweis
- Kann nur erreicht werden, wenn die derzeit im Einsatz befindliche Karte ausgetauscht wird

1. Die Karte wird dann produziert, wenn die Person zum Austausch vorstellig wird (Produktion „On demand“)
 - Informationen, insbesondere Bild, kann zum Zeitpunkt der Produktion erhoben werden
 - Aufwand zur Prüfung der aufgedruckten Merkmale reduziert sich, wenn beispielsweise das Bild vor Ort erfasst wird
 - Dauer des Kundenkontakts > 5 Minuten (Druckzeit ~ 2 Minuten)
2. Die Karte wird vorproduziert und gegen Vorlage der alten Karte und ggf. Personalausweis/ amtlichem Lichtbildausweis ausgegeben
 - Alle Informationen, die auf die Karte aufgedruckt werden sollen, beispielsweise ein Bild, müssen zum Zeitpunkt der Produktion bereits vorliegen
 - Die sichtbaren (aufgedruckten Merkmale müssen zum Zeitpunkt der Ausgabe geprüft werden
 - Dauer des Kundenkontakts: ca. 1 Minute

Kartenaustausch – Produktion On demand

- Hohe Dauer des Kundenkontakts > 5 Minuten
 - Bei 35.000 auszutauschenden Karten ca. 3.000 Stunden ohne Leerlaufzeiten
- Qualifiziertes Personal mit IT-Kenntnissen, da Erhebung des Bildes während des direkten Kundenkontakts im IT-System erfolgt.
- Lange Wartezeiten beim Austausch aufgrund der langen Kundenkontaktzeiten
- Nur erforderlich und sinnvoll, wenn ein persönliches Bild auf die Karte gedruckt werden soll und dieses nicht bereits vorliegen sollte

Kartenaustausch – vorproduzierte Karten

- Geringe Dauer des Kundenkontakts, ca. 1 Minute
- Geringere Anforderungen an die IT-Kenntnisse der Mitarbeiter/innen
- Verkürzte Wartezeiten
- Das KIT hat in seinem Datenbestand keine Bilder der Mitarbeiter/innen und der Studierenden, die für eine Vorproduktion der Karte genutzt werden könnten.
- Ohne Bild auf dem Ausweis
 - sofort umsetzbar, da alle anderen Informationen zur Produktion der Karte bereits vorliegen
- Mit Bild auf dem Ausweis
 - Erfassung des Bildes über personalisierte Funktion im Portal
 - Vorabprüfung des Bildes auf Verwendbarkeit (Format, Auflösung, etc.)
 - Abklärung mit Datenschutz
 - Kontrolle des Bildes (über amtlichen Lichtbildausweis) bei Ausgabe

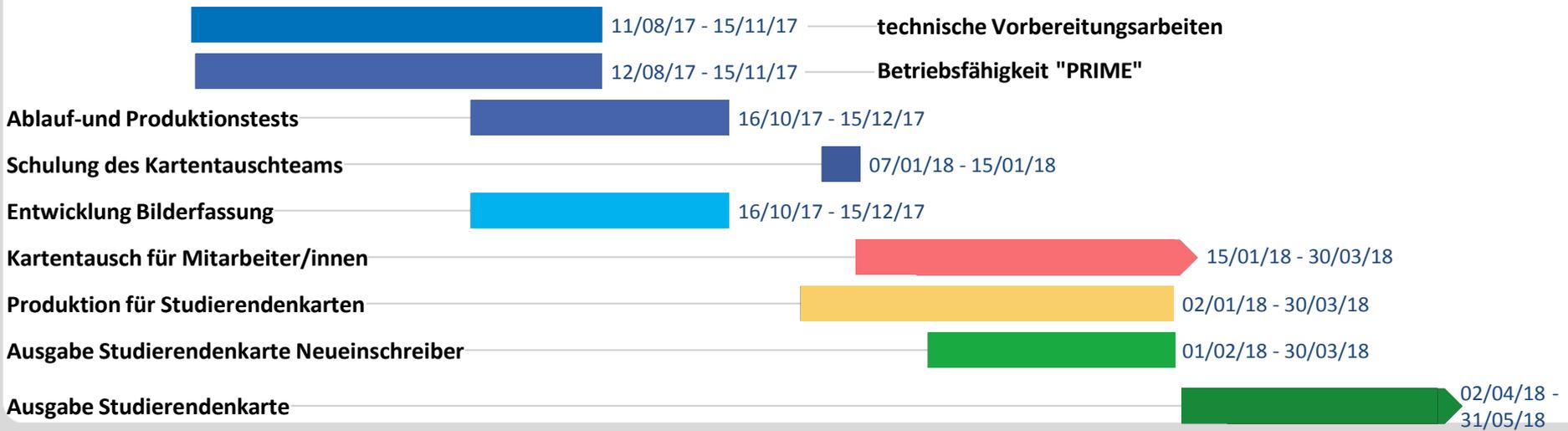
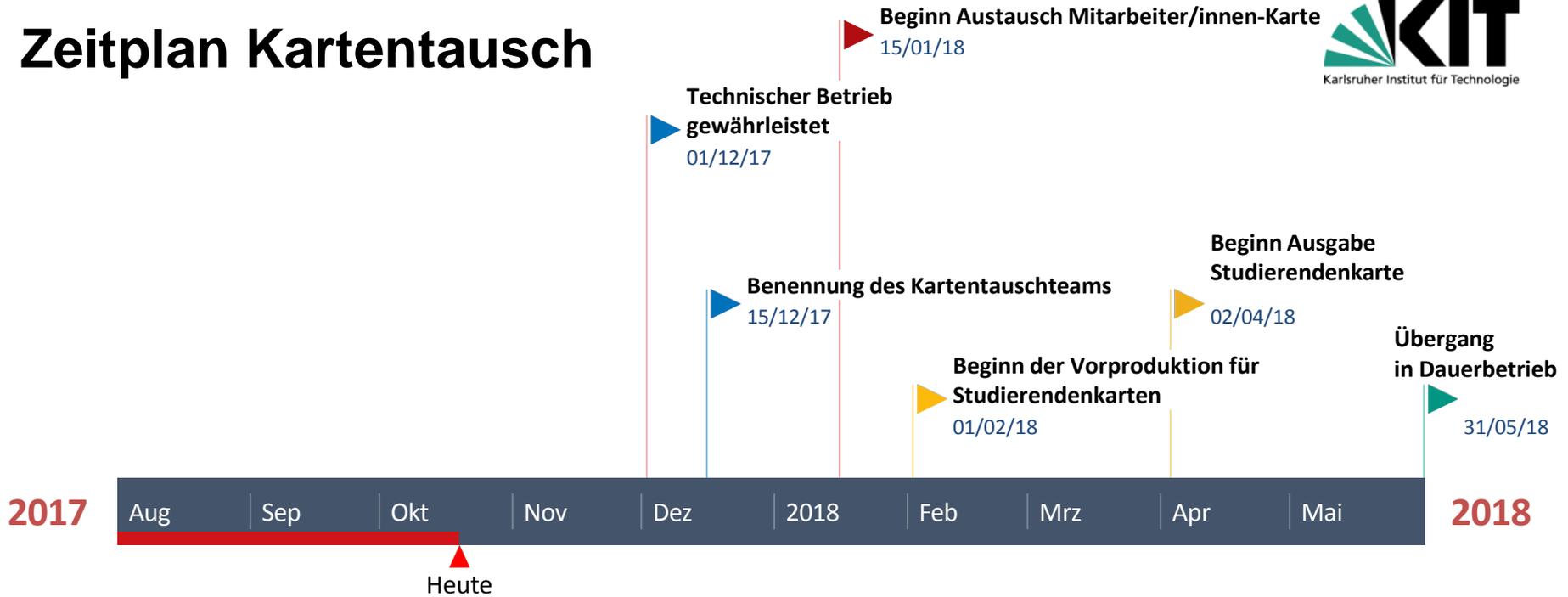
Entscheidung des Präsidiums

- Die KIT-Card soll in Zukunft mit sicherer Technologie ausgestattet werden.
- An einer KIT-Card mit persönlichem Bild wird festgehalten.
- Die DE AServ wird beauftragt, den Austausch der Mitarbeiter/innen-Karte vorzubereiten und zu organisieren.
- Die DE SLE wird beauftragt, den Austausch des Studenausweises auf Basis von vorproduzierten Karten vorzubereiten und zu organisieren.
 - In einer Übergangszeit wird es für die aktuell eingeschriebenen Studierenden Studenausweise ohne Bild geben, um den schnellen Wechsel auf eine neue KIT-Card zu gewährleisten
 - Neu immatrikulierende Studierende erhalten Studenausweise mit Bild.
- Das SCC wird beauftragt alle IT-Belange des Austausches zu betreuen.
- Auftrag an alle beteiligten DEs (SCC, ASERV, BIB, FM, INTL, PPQ, SLE, SUM):
 - Vorlage zur dauerhaften Ausgabe von KIT-Cards an Mitarbeiter/innen und Studierende vorbereiten und untereinander vereinbaren, welche DE die Federführung dabei inne hat.

Zeitplan KIT-Card Tausch

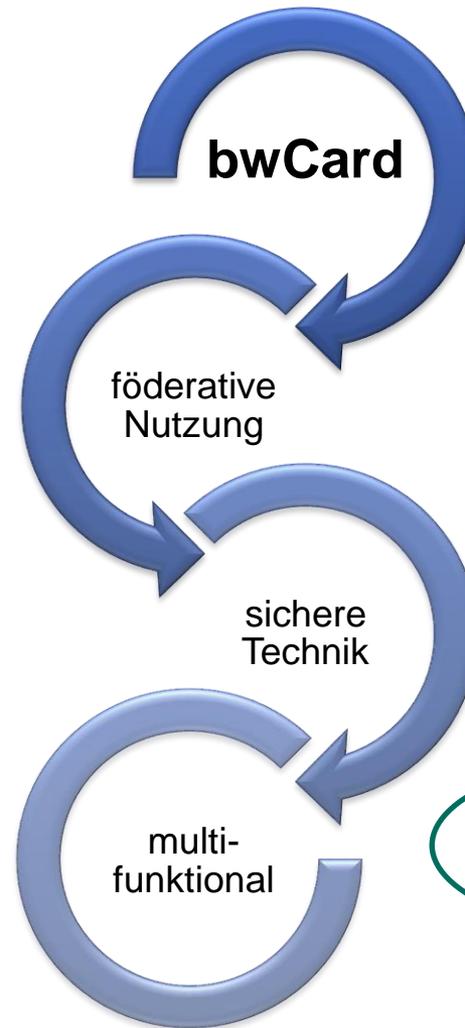
- Kartentausch für Mitarbeiter/innen: 15.01.2018
 - Abschluss technische Anbindungen (Bibliothek, Siport, etc.): 30.11.2017
 - Betriebsfähigkeit des Kartenmanagementsystems: 30.11.2017
 - Ablauf und Produktionstests ab 1.11.2017
 - Schulung des Kartentauschteams ab 6.01.2018
 - **Beginn des Kartentauschs für Mitarbeiter/innen: 15.01.2018**
- Ausgabe Studierendenkarten
 - Ab 1.2.2018 Vorproduktion der Studierendenkarten an den Plätzen für Kartentausch, während eventueller Freizeiten des Kartentauschteams mit zweitem Kartendrucker
 - Ab 15.02.2018 Ausgabe zunächst an Neueinschreiber Sommersemester
 - Ggf. an den Arbeitsplätzen des Kartentauschteams für die Mitarbeiter/innen-Karte
 - **Beginn Ausgabe Studierendenkarte: 01.04.2018**

Zeitplan Kartentausch



KIT-Card im bwCard Konsortium

Stand heute



ulm university universität uulm

EBERHARD KARLS UNIVERSITÄT TÜBINGEN



UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386



Universität Stuttgart



UNIVERSITÄT MANNHEIM

IPv6 am KIT

STEINBUCH CENTRE FOR COMPUTING - SCC



IPv6 am KIT

- Erste Vorstellung im IT-Expertenkreis am 23. Juni 2010
 - Projektgruppe im SCC
 - Vorstellung des Netz-Bereichs
 - Ab Q4/2010 erweiterte Projektgruppe mit KIT-OEs
- Update (21. September 2011)
 - 15 OEs benutzen IPv6
 - World-IPv6-Day erfolgreich
 - Verwaltung von IPv6 DNS-Einträgen möglich (per E-Mail-Request)
 - Nur zentral, nicht mandantenfähig
 - Weiteres Ausrollen von IPv6 für KIT-OEs ist optional
- Update (23. Januar 2013)
 - DNSVS ist IPv6-ready



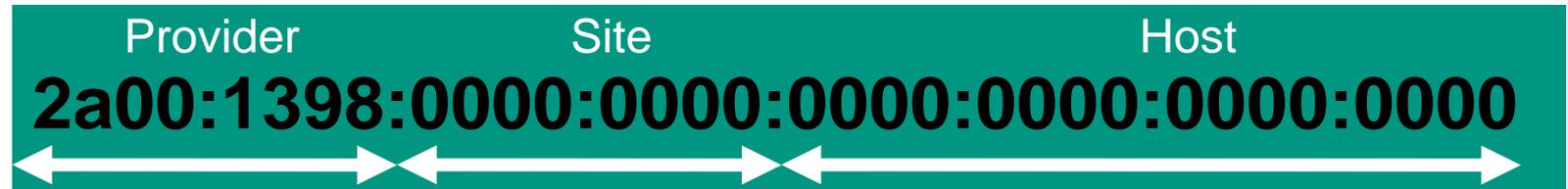
IPv6 am KIT / Stand Oktober 2017

- IPv6 ist Standard-Dienst
- Wesentliche SCC-Dienste über IPv4 und IPv6 nutzbar
- Parallelbetrieb beider Protokolle (Dual Stack)
 - IPv6 ist performanter
 - IPv6 wird seitens der Systeme bevorzugt
 - Dual-Stack noch solange bis die ganze Welt IPv6 spricht
- SCC-Firewall-Dienste für beide Protokolle gleichwertig nutzbar

- Nutzung:
 - ~240 IPv6-Subnetze im SCC genutzt
 - ~60 IPv6-Subnetze von OEs genutzt

IPv6 Adressen und Subnetze

- Format der Adressen:



- Vergebene Subnetze sind immer /64-Netze
- Präfix des KIT: 2a00:1398
- Subnetz-Identifizierung durch die folgenden 4 Bytes (2^{32} Subnetze)
- Subnetze haben grundsätzlich die Größe /64
- Allokationsplan für Subnetze
- Instituts- und OE-Netze
- Zentrale Dienste
- Projekte

KIT IPv6 Adressbereich

- 2a00:1398::/32
 - 2^{96} ($\sim 7,9 * 10^{28}$) mögliche Adressen
- kein Routing von privaten Adressen (wie bei IPv4 10.0.0.0)
- kein NAT (Network Address Translation) mehr
- für jedes Institut/jede OE wird ein Bereich der Größe ::/56 reserviert
 - 256 Subnetze der Standardsubnetzgröße ::/64 möglich

IPv6 am KIT / Identifizierung von Endgeräten

- Verwendung von EUI-64-Formaten
 - MAC-Adresse geht auf dem Host-Teil der IPv6-Adresse hervor
 - Eintrag im DNSVS ist gewünscht

- Verwendung statisch konfigurierter Adressen
 - Beliebige IP-Adresse mit Eintrag im DNSVS

- Verwendung von Privacy Extensions - keine Nachverfolgung möglich
 - Macht nur zusammen mit DAD (Duplicate Address Detection) Sinn
 - Vermeidung des Risikos zufällig identischer IPv6-Adressen

Endgerätekonfiguration

- Endgeräte bringen per Default IPv6 mit
- IPv6 funktioniert, wenn im VLAN konfiguriert (SCC)
- IPv6 bei Endgeräten nicht abschalten/dekonfigurieren!
 - IPv4 ist legacy, IPv6 ist die Zukunft
 - Mit deaktiviertem IPv6 funktioniert der VPN-Dienst des SCC nicht
 - Setzt bei Verbindungsaufbau statische IPv6- und IPv4-Routen im Client
 - IPv6 abgeschaltet: Fehlermeldung -> OpenVPN > Setup schlägt fehl

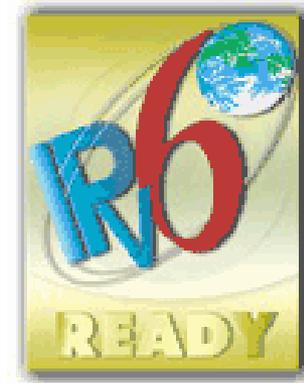
IPv6 am KIT

- DHCP für IPv6 (RFC3315 / RFC6355)
 - Nicht die MAC-Adresse wird zum DHCP-Server übermittelt, sondern der „DHCP Unique Identifier (DUID)“
 - RFC 3315/6355 definiert 3 unterschiedliche Verfahren zur Bildung des DUID
 - Keine MAC/IP-Adresszuordnung – das macht EUI-64!

- DHCPv6 Verfahren
 - Stateless DHCP
 - Übermittlung der DHCP-Optionen an den Client
 - IP-Adresse per SLAC generiert
 - Stateful DHCP für IPv6
 - Übermittlung der IPv6-Adresse und der DHCP-Optionen an den Client
 - SLAC wird nicht verwendet
 - Kein Vorteil gegenüber SLAC mit Stateless DHCP

Zukunft

- Jede KIT-Einrichtung kann IPv6 nutzen
- IPv6 ist in der IT-Grundausstattung enthalten!
- Mail an `netze@scc.kit.edu`
 - OE erhält Mail mit Hinweisen
 - IPv6 wird konfiguriert
- Gründe, abzuwarten, sind nur mental
- Mit Ausrollen des neuen Backbones bekommt jeder IPv6 – es sei denn, es gibt technische Gründe, die dagegen sprechen





- Kollaboratives Online-Editing im Web via bwSync&Share
- Microsoft Office-Formate doc(x), xls(x), ppt(x)
- OpenDocument-Formate odp, odt, ods
- epub, csv
- Änderungen werden jede Minute zurücksynchronisiert
- Umfangreiche Formatierungsmöglichkeiten
- Beschreibung



- Allgemein, u.a.:
 - Owner- und Admin-Übertragung
 - schnellere Synchronisation
 - höhere Performanz der Weboberfläche
- Ausblick:
 - Verschlüsselung (serverseitig)
 - Test-Föderation mit anderen PF-Installationen (u.a. BayernCloud, Hessen-Box) via OpenCloudMesh (CERN)
 - v14: Neues "Look and Feel"

Verschiedenes / Diskussion

STEINBUCH CENTRE FOR COMPUTING - SCC



Herzlichen Dank !

STEINBUCH CENTRE FOR COMPUTING - SCC

