

4. IT-Beauftragtenversammlung am 12.11.2012

Partnerschaftliche Zusammenarbeit zwischen SCC und ITB

STEINBUCH CENTRE FOR COMPUTING - SCC



Agenda:

- Begrüßung - Neues aus dem SCC (10')
 - Organisationsänderungen im SCC
 - Herausforderung Budgetkürzung
- SCC-Services: Aktuelles
 - Inbetriebnahme / Aktualisierung / Ausserbetriebnahme (10')
 - Rechnerinfrastruktur HPC-Systeme (15')
 - SCC Service News (5')
- Handlungsstränge kit.edu-Migration: Folge 3
 - Zusammenfassung (5')
 - Ergänzungen: (5')
 - TSM-Dienste
 - Passwortmanagement durch ITB
 - Testkonten
 - Lizenzmanagement für Desktop-Migrationstool FORENSIT
 - Vertrauensstellungen Altdomänen (15')
- Effiziente Gruppenverwaltung im KIT: Organisation u. Technik (20')
- Fragen / Diskussion (20')

IT-Beauftragtenversammlung am 12.11.2012

**SCC-Services: Aktuelles
Inbetriebnahme / Aktualisierung / Ausserbetriebnahme – Andreas Lorenz**

STEINBUCH CENTRE FOR COMPUTING - SCC



SCC-Services: Aktuelles (1)

■ Zertifikatsdienst

■ Erweiterung CA2AD - *Inbetriebnahme*

Automatische Veröffentlichung von Nutzerzertifikaten der KIT-CA im KIT-AD.
SCC-Service-News, heute

■ Nutzerzertifikate – *Änderung*

Nach Änderung der DFN-Policy: Nutzerzertifikat: immer mit Identifizierung;
Serverzertifikat: ohne Identifizierung, aber Antragsteller muss im Besitz eines
gültigen Nutzerzertifikats sein.

<http://www.scc.kit.edu/dienste/kit-ca.php>, SCC-Service-News

■ Druckdienst

■ COPS - *Änderung*

Web-basiertes Druckannahmesystem für PDF- und PostScript-Dokumente.
Zugang via KIT-Accounts.

ITB-Portal, Mail ITB, <http://www.scc.kit.edu/cops>

■ Fileservice / Datenhaltung, nutzerbezogen

■ pBox - *Inbetriebnahme*

Persönliche Speicherbereiche für KIT-Mitarbeiter (Dokumente).

ITEK (z.B. 26.09.12), <http://www.scc.kit.edu/dienste/86439php>

SCC-Services: Aktuelles (2)

- **Serviceaccounts – Inbetriebnahme**
Konten zur Bereitstellung von Diensten
ITEK (z.B. 26.09.12), <http://www.scc.kit.edu/dienste/8637.php>
- **Personenbezogenes Kommunikationsverzeichnis (KV) – Inbetriebnahme**
KIT-Mitarbeiter können ihre persönlichen Daten (Telefonnummer, Standort, Gebäude, Raumnummer, Datenfreigabe) selbst verwalten.
ITEK (z.B. 26.09.12), <http://www.scc.kit.edu/dienste/8641.php>
- **Abkündigung nfs-export GDH – Ausserbetriebnahme**
Abkündigung NFS-Export der globalen Datenhaltung (\$GLOBALHOME) zur Anbindung der FZKA-Windows-Fileserver an HPC-Cluster (CN)
SCC-Meldewesen (06.08.2012)
- **Abkündigung Altdomänen – Ausserbetriebnahme**
ITEK (18.07.2012), SCC-Meldewesen (03.08.2012)

HPC-Systeme am KIT – Status und Strategien

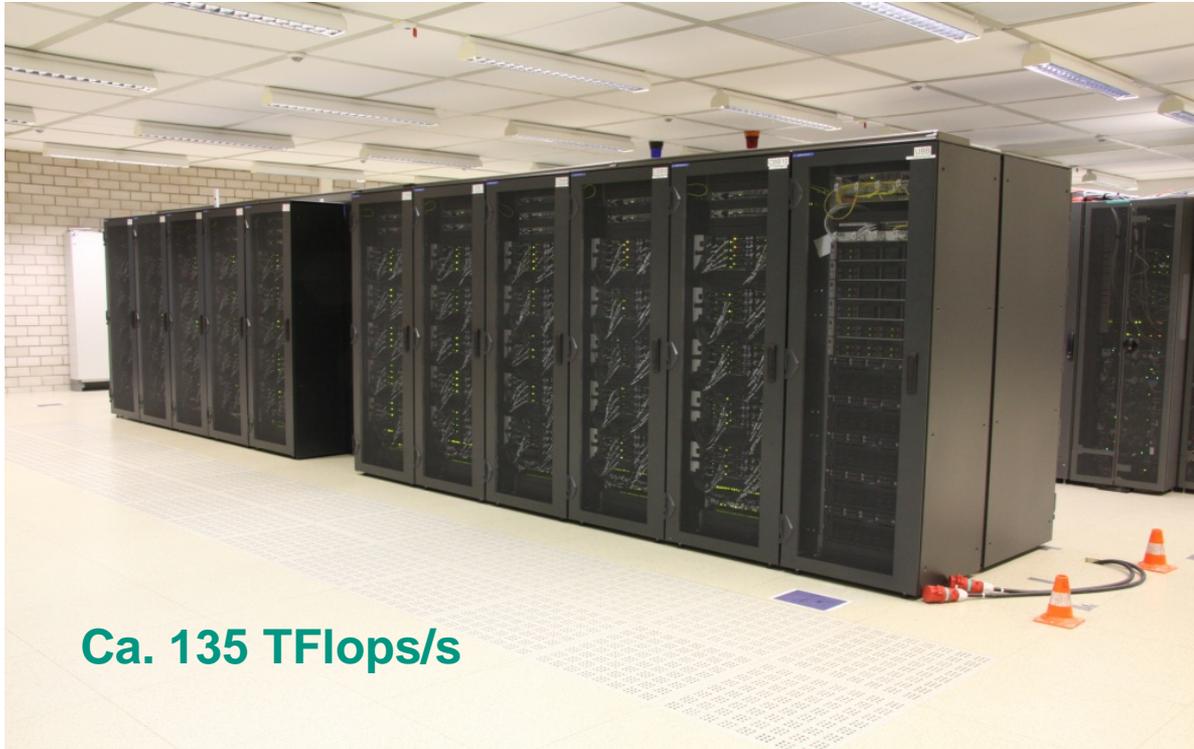
ITB-Versammlung 12.11.2012

Holger Marten

STEINBUCH CENTRE FOR COMPUTING - SCC



InstitutsCluster II



Ca. 135 TFlops/s

- 6.560 CPU-Cores
- 28 TB RAM
- Infiniband
- Spezialknoten für Login, DataMover, etc.

Freigabe zur Nutzung am 4.10.2012

InstitutsCluster II

■ KIT-Beteiligungsmodell (analog IC1)

- Finanzielle Beteiligung durch 17 Institute UB und 7 Institute GFB
- DFG Förderantrag GG Art. 91b in 2011 lieferte nahezu Verdopplung der gesamten Investitionssumme
- Vergabe der Rechenzeit pro Institut / Gruppe *im Mittel* gemäß eingebrachtem Eigenanteil

■ Erweiterung des IC2

- Bis zu 20% des Systems ohne nochmalige Ausschreibung möglich
- Interessenbekundungen etlicher Institute liegen bereits vor
- Planungen bzw. weitere Interessenbekundungen **jetzt**
an H.Marten / H.Gernert, SCC-SCS

Abgekündigte und verbleibende HPC-Systeme

■ Abgekündigt zum Jahresende 2012

- InstitutsCluster IC1
 - Landeshochleistungsrechner XC2 (auch „HP XC4000“)
 - Abgekündigt über Lenkungsausschuss und Gremien
 - Detaildiskussion mit den Projekten laufen
 - NEC SX-8R, SX-9
 - IBM AIX-Cluster
 - OpusIB Cluster
- } Load Leveler „mixed Cluster“

■ Ausweichmöglichkeiten

- InstitutsCluster IC2; *neu! Erweiterung in Kürze*
- KIT-Rechner HC3 (auch „HP XC 3000“); bis ca. 2014
- bwGRiD; KIT-Instanz bis ca. Q3/2013

■ Grid Infrastruktur

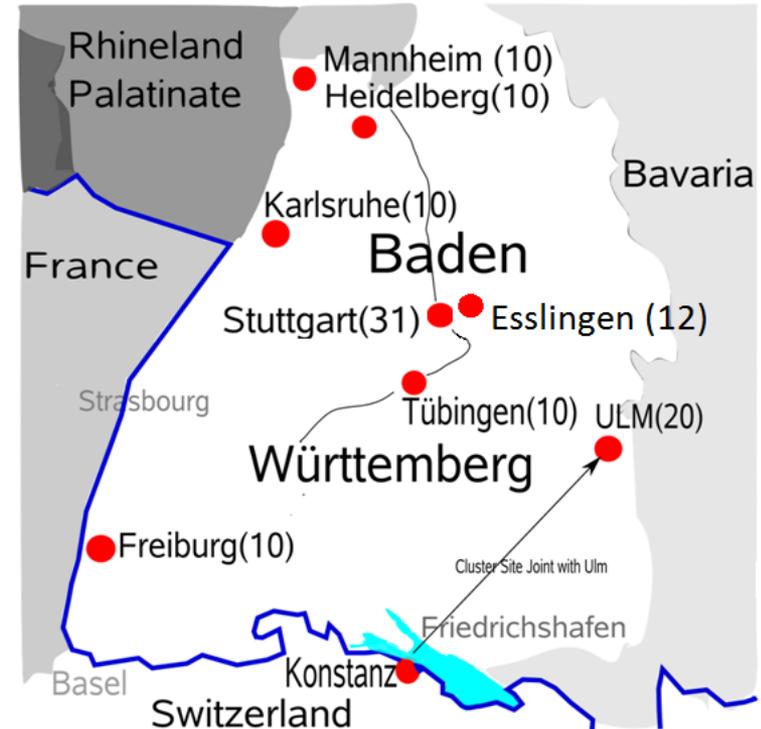
- gefördert durch BMBF (über D-Grid), DFG und MWK BaWü seit Ende 2007
- Projektleitung seit 2010 am KIT / SCC

■ Ressourcen

- 9 Zentren resp. Cluster (●)
- Insgesamt 1.580 Knoten á 8 Cores
→ 12.640 Cores (KIT: 1120 Cores)
- Insgesamt 700 TB Disk, lokal & zentral (KIT: 32 TB lokal & 380 TB zentraler Sp.)
- Globus als gemeinsame Middleware

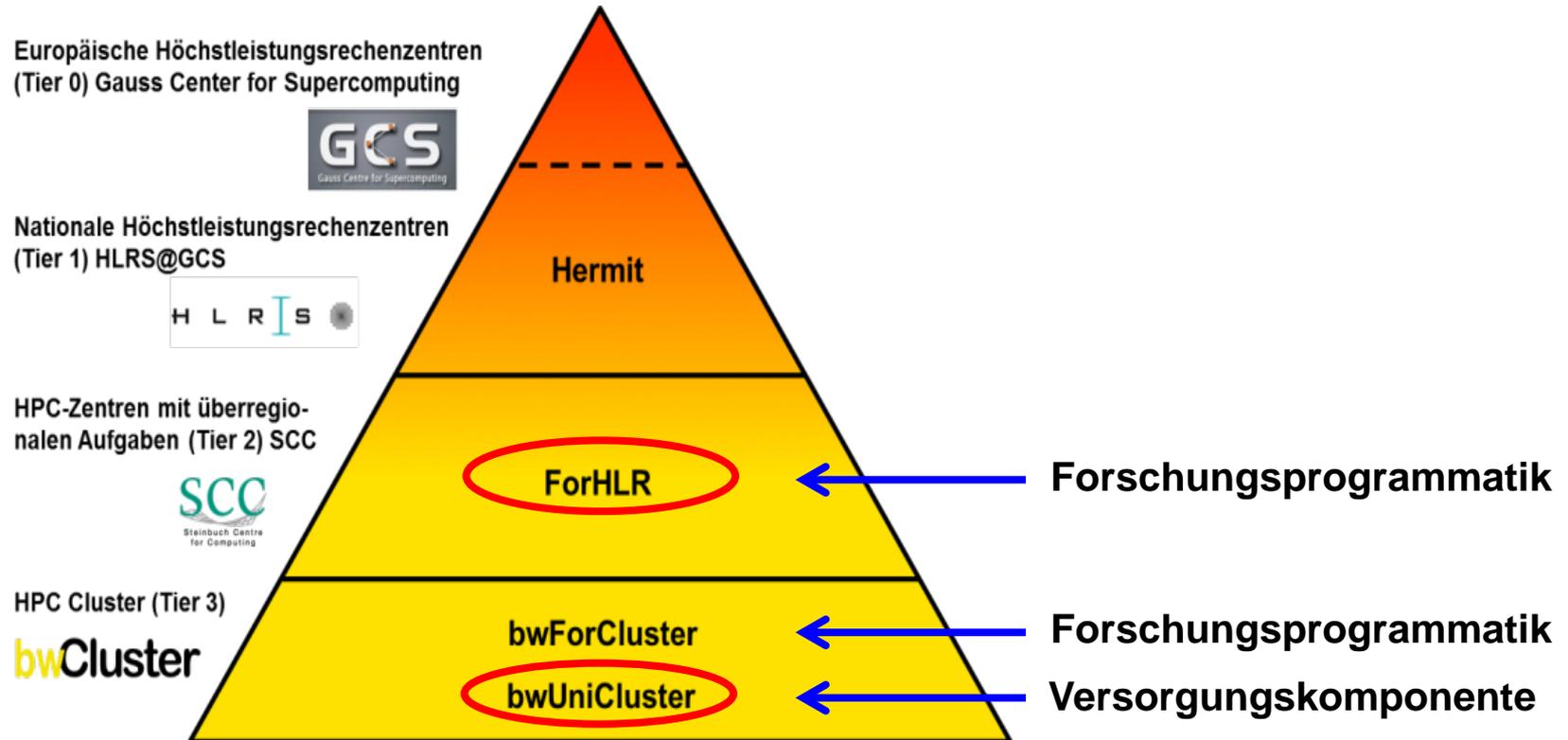
■ Begleitprojekte

- bwGRiD System, bwGRiD Portale, bwGRiD Ergänzende Maßnahmen
- Später: bwIDM, bwLSDF



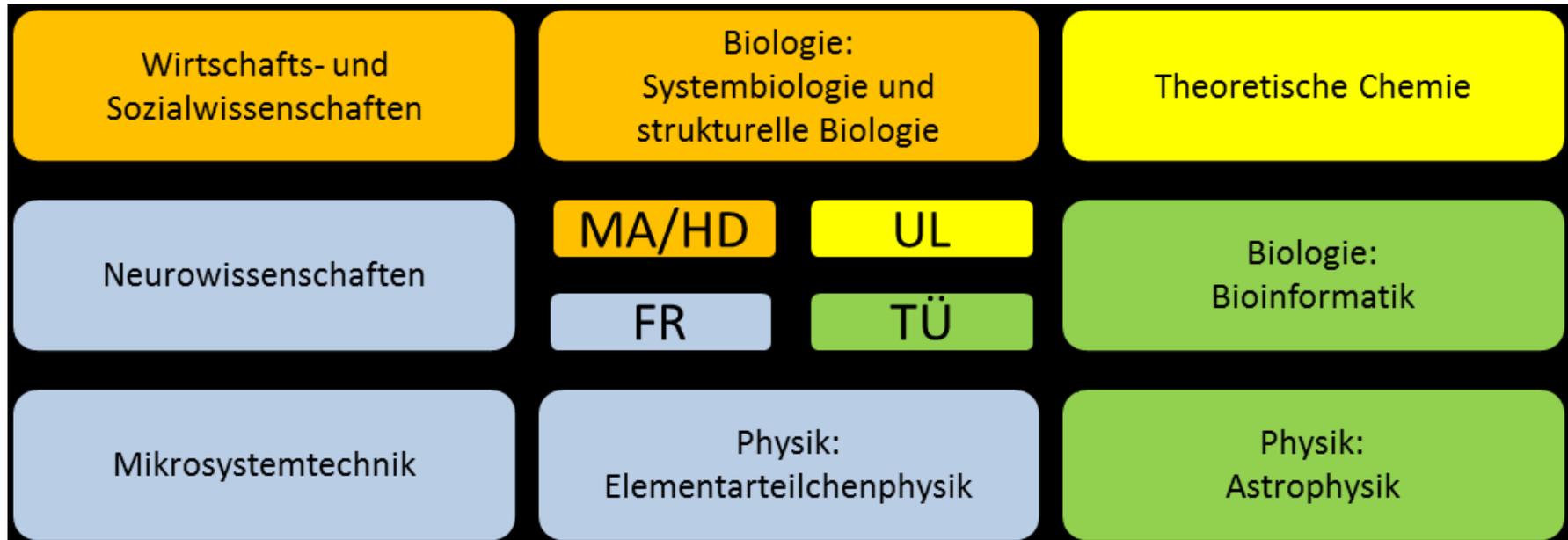
Umsetzungskonzept...

...der Universitäten des Landes Baden-Württemberg für das Hochleistungsrechnen



DFG-Antrag des ALWR-BW in Abstimmung mit MWK, März 2012

bwForCluster (For = Forschungs-)



- DFG Forschungsprogramm (GG Art. 91b)
- 4 Standorte
 - Mannheim/Heidelberg (MA/HD), Ulm (UL), Freiburg (FR), Tübingen (TÜ)

bwUniCluster (Uni = universal- / Universitäts-)

■ Versorgungsrechner GG Art. 143c

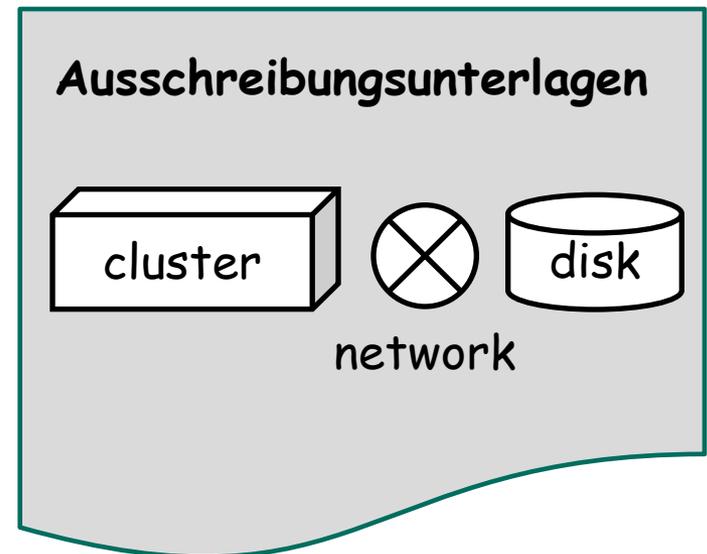
- Standort KIT
- DGF-Antrag März 2012 erfolgreich
- Federführung KIT / SCC

■ Beteiligungsmodell

- Investitionen durch KIT + 7 Unis BW
- Durch DFG-Antrag finanziellen Investitionseinsatz verdoppelt
- Nutzung durch alle Beteiligten
- Umlagemodell für Betriebskosten

■ Ausschreibungsstart in Kürze

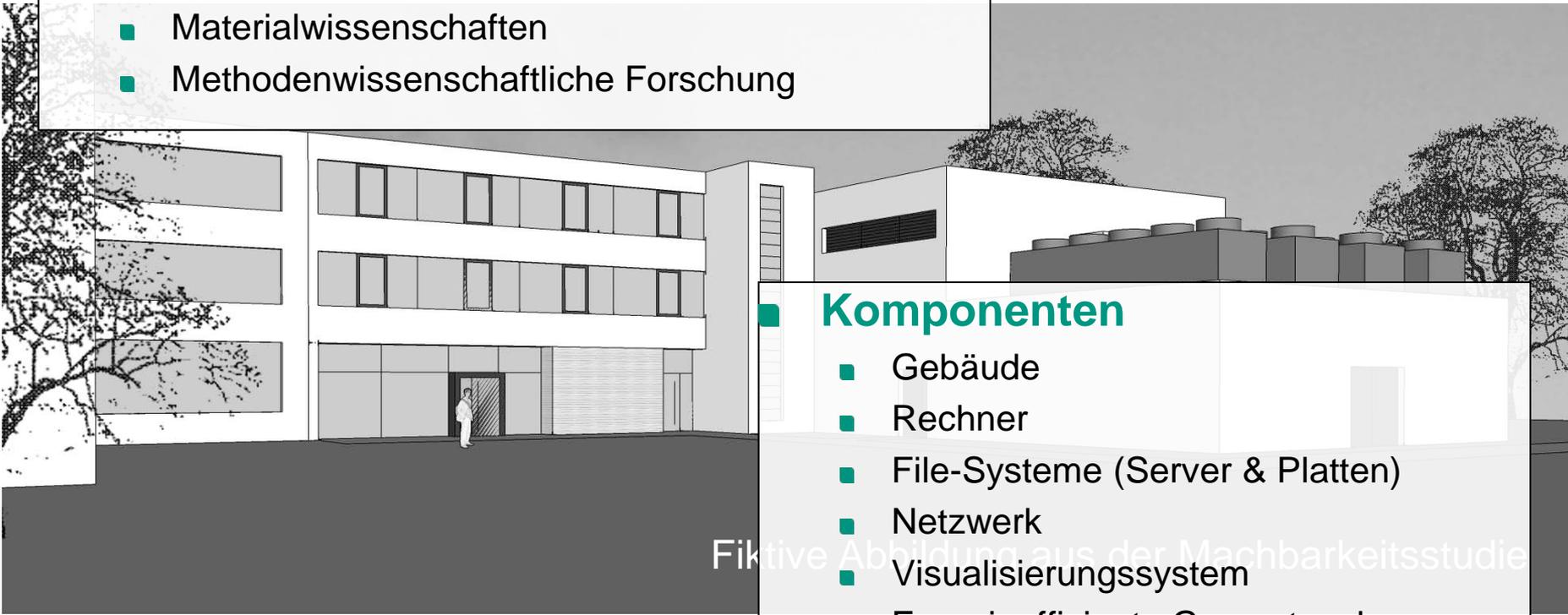
- System soll bwGRiD-Cluster am Standort KIT ablösen (ca. Q3 2013)



ForHLR – Das bwHPC Tier-2 System

■ Forschungsprogramm (GG Art. 91b)

- Umweltforschung
- Energieforschung
- Nanostrukturen und -technologien
- Materialwissenschaften
- Methodenwissenschaftliche Forschung



■ Komponenten

- Gebäude
- Rechner
- File-Systeme (Server & Platten)
- Netzwerk
- Visualisierungssystem
- Energieeffiziente Gesamtauslegung

Fiktive Abbildung aus der Machbarkeitsstudie

ForHLR – **F**orschungs**H**och**L**eistungs**R**echner

■ **Landeshochleistungsrechner BaWü (Tier-2)**

- DFG Forschungsprogramm Art. 91b
- Federführung KIT / SCC
- Positive Bewilligung 26 Mio. € im April 2012
 - Deutscher Wissenschaftsrat, Pressemitteilungen 2012 Nr. 12, 29.5.2012
 - KIT Presseinformation 114/2012, 29.6.2012
 - SCC News 02/2012

- Standort KIT
- Nachfolgesystem für XC2
- 1. Phase in 2013
- 2. Phase inkl. neues Gebäude CN in 2014/15

Zusammenfassung

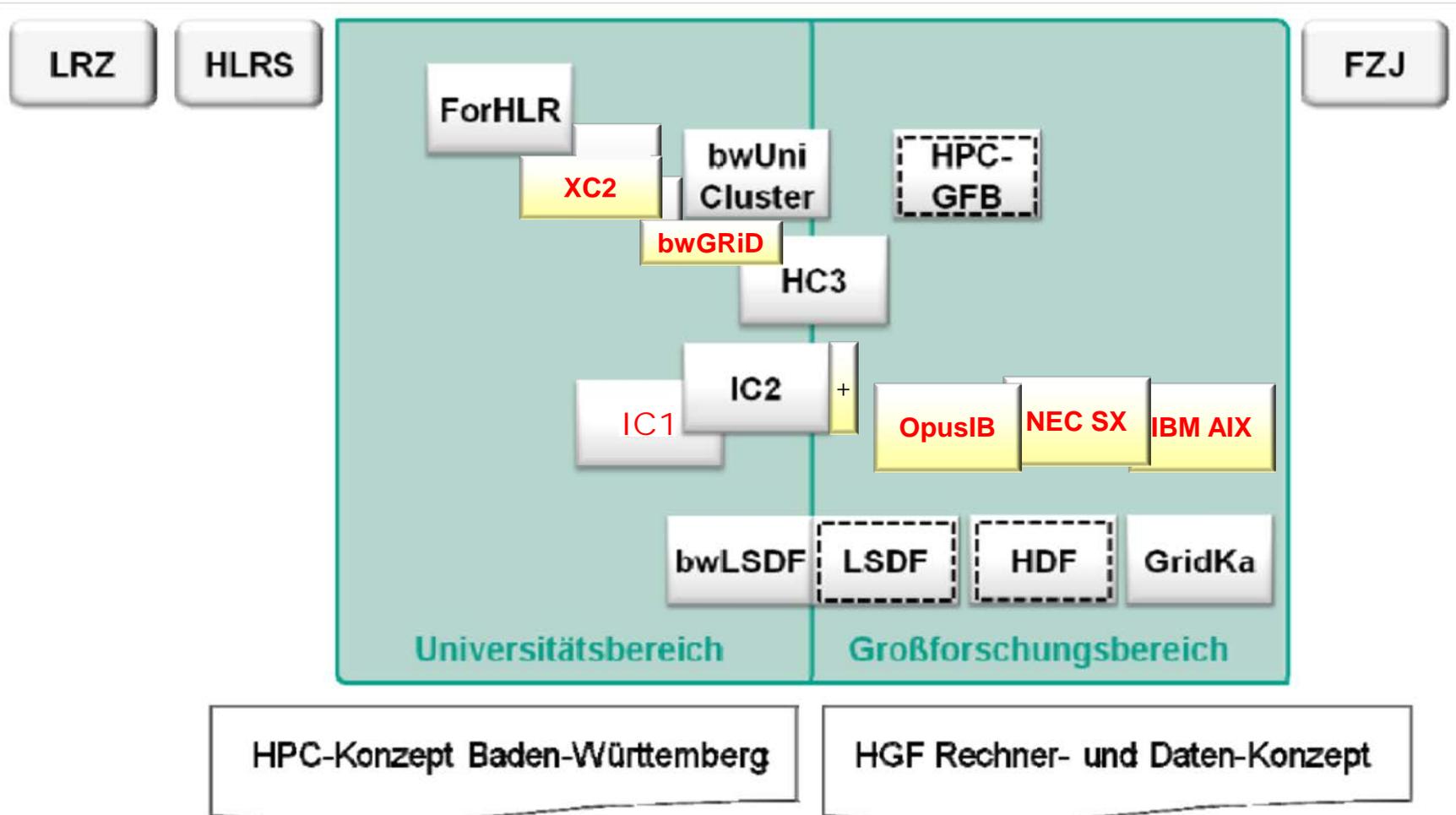


Abbildung 3: Überblick über die HPC- und Datensysteme am KIT

Zusammenfassung

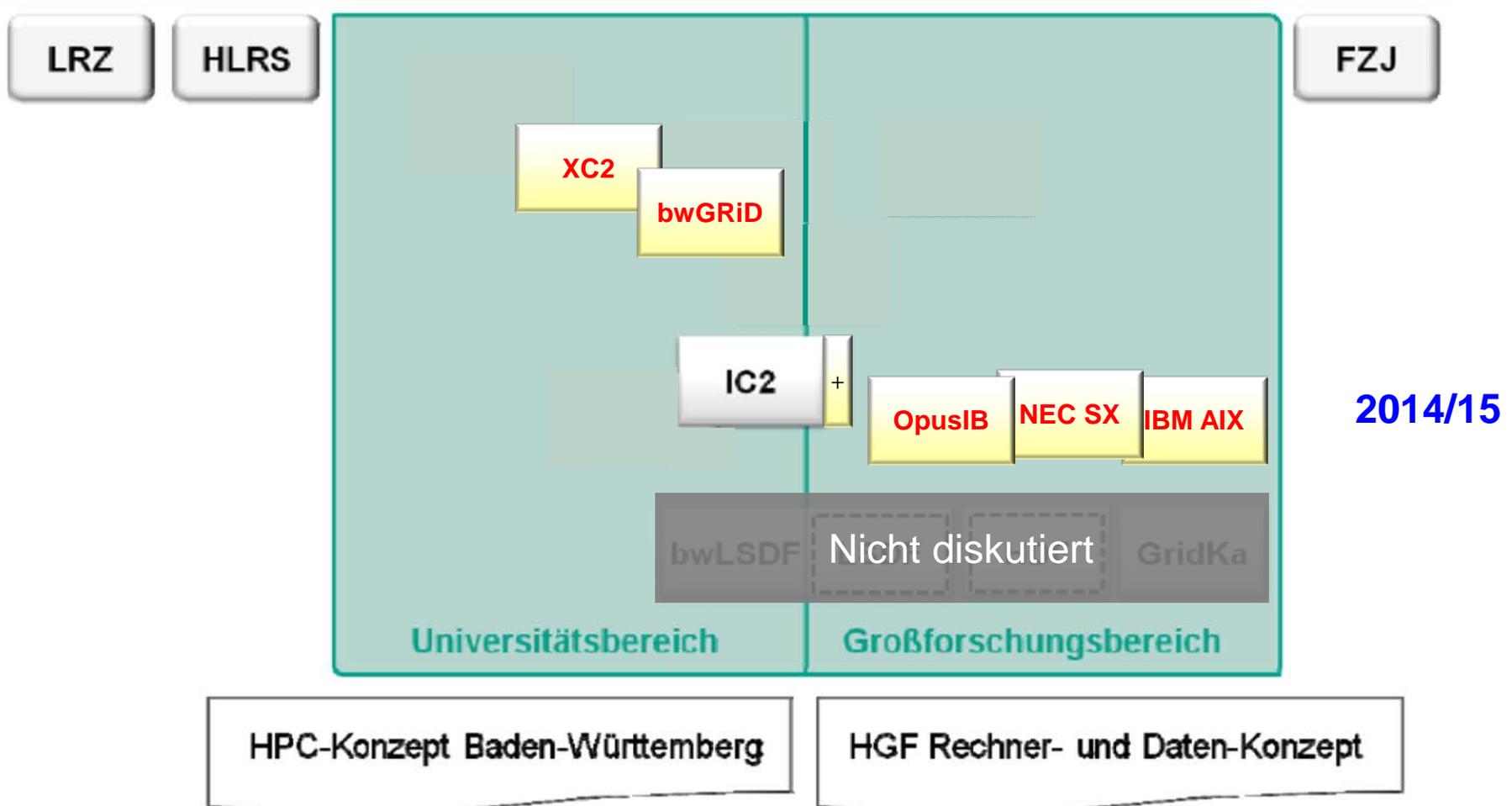


Abbildung 3: Überblick über die HPC- und Datensysteme am KIT

Zusammenfassung

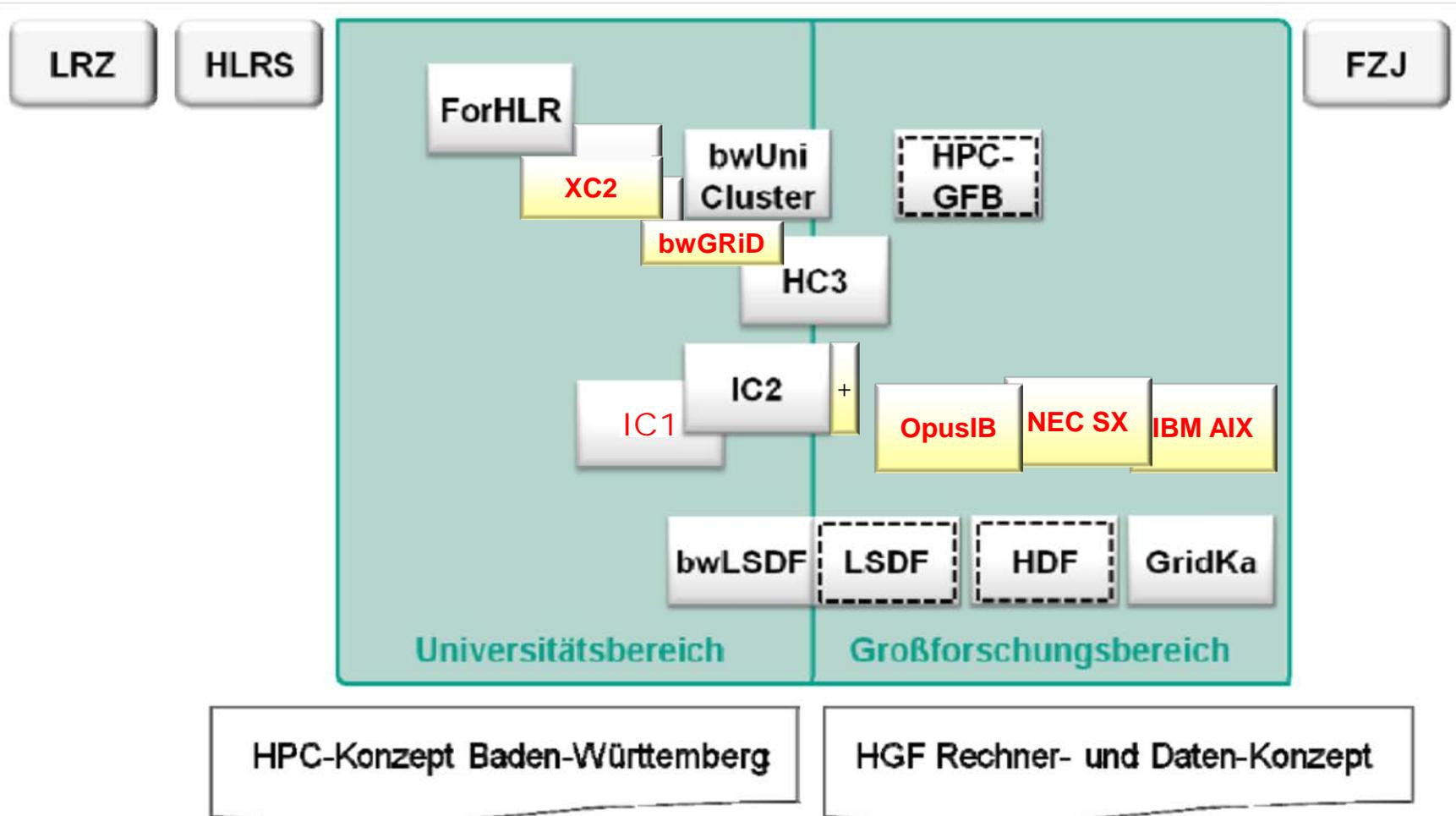


Abbildung 3: Überblick über die HPC- und Datensysteme am KIT

SCC-Services: SCC Service News (1)

- Information zu SCC-Services für alle Nutzer
 - Inbetriebnahme neuer Services
 - Serviceänderungen
 - Abkündigungen/Ausserbetriebnahmen von Services
 - Planungen zukünftiger Dienste
 - Informationen zur kit.edu-Migration
 - IT-Themen mit SCC-Beteiligung, z.B. HW-/SW-Shops

- Zugang mit KIT-Benutzerkonto (Mitarbeiter, Studierende, Gäste und Partner)
- Online- und Druckversion
- Inhalte in Kategorien gebündelt
- Schlagwortsuche
- Als Abonnement via RSS-Feed

- Inbetriebnahme: Heute!
- URL: <https://team.kit.edu/sites/services/scc-servicenews>

SCC-Services: SCC Service News (2)

- Alle Websiteinhalte einblenden
- Alle Artikel**
- kit.edu-Migration**
- Veränderungen**
 - Inbetriebnahmen
 - Änderungen
 - Außerbetriebnahmen
- Nach Diensten**
 - Datenhaltung und -management
 - Desktop- und Arbeitsplatzbetreuung
 - Digitale Medien
 - Drucken & Plotten
 - Kommunikation
 - Netz & Netzzugang
 - Nutzerservice
 - Server & Systeme
 - Sicherheit
 - Software & Anwendungen
 - Wissenschaftliches Rechnen
- Sonstige Hinweise**
- SCC-Dienstangebot**
- RSS-Feed**
-  **Papierkorb**

Alle Artikel

Auf dieser Seite werden aktuelle Informationen über Änderungen an SCC-Services veröffentlicht.

Titel	Textkörper	VeröffentlichtAm	NewsTyp
Kooperative Administration: Ressourcenmanagement (KIT-AD)	Die vom SCC betriebenen Verzeichnisdienste KIT-AD (basierend auf Microsoft Active Directory) und KIT-LDAP (basierend auf OpenLDAP) sind für das Ressourcenmanagement von zentraler Bedeutung. So stehen alle vom IDM verwalteten Benutzerkonten und Benutzergruppen in beiden Verzeichnisdiensten einheitlich zur Verfügung und können von den an den jeweiligen Verzeichnisdiensten angegliederten Diensten genutzt werden. Die OE-Admins haben voraussichtlich am dem 01.07.2012 die Möglichkeit, im KIT-AD eigene Administrationsstrukturen aufzubauen, um hier sowohl die ihnen zugeordneten IDM-Konten und –Gruppen zu nutzen, als auch neue AD-spezifische Computer-, Benutzer-, Gruppen- oder Gruppenrichtlinienobjekte zu verwalten. Siehe: IT-Beauftragtenversammlung Mai 2012: http://www.scc.kit.edu/kooperationen/7656.php	12.11.2012	kit.edu-Migration
Zugang für externe Studierende auf studium.kit.edu möglich	Der Zugang für externe Studierende (Studierende die nicht am KIT eingeschrieben sind) auf das Studierenden-Portal (studium.kit.edu) ist ab sofort (7.11.12) möglich. Die externen Studierenden benötigen hierfür einen Account in der Gäste-und-Partner Verwaltung mit der Rolle „Externer Student“. Eine separate Freischaltung im Studierenden-Portal ist nicht (mehr) notwendig. Nach erfolgreicher Aktivierung des Accounts können externe Studierende sich im Portal anmelden und bestimmte Funktionen (z.B. VABs, Stundenplan, Vorlesungsfavoriten) nutzen. Servicebeschreibung: http://www.scc.kit.edu/dienste/5730.php	07.11.2012	Dienst-Änderung
Automatische Veröffentlichung von Nutzerzertifikaten der KIT-CA im KIT-AD	Vereinfachter Umgang mit Nutzerzertifikaten über "CA2AD" Am 26.10.2012 wurde der Dienst CA2AD aktiv geschaltet. Mit dieser Software werden von der KIT Certification Authority (KIT-CA) ausgestellte und veröffentlichte Benutzer-Zertifikate automatisch in das KIT Active Directory(KIT-AD) eingetragen. Dadurch kann eine gesicherte Kommunikation zwischen zwei KIT-AD-Nutzern statt finden, ohne dass diese im Voraus ihre öffentlichen Schlüssel ausgetauscht haben. Die Zertifikate können von Outlook über die Global Address List (GAL) bezogen werden. Alternativ können Programme wie LDAPSearch verwendet werden, um diese direkt im Active Directory zu suchen. Das entsprechende Feld heißt userCertificate und enthält eine DER formatierte X509 Datei.	31.10.2012	Dienst-Änderung
Nutzerzertifikate: Änderung der DFN-Policy	Die Änderungen der Zertifizierungs-Policy des DFN betrifft die Identifizierung von Nutzern. Um ein Nutzerzertifikat zu erhalten, ist immer eine Identifizierung notwendig. Das bedeutet, dass der Antragsteller sich bei der Registrierungsstelle persönlich identifizieren muss. Um ein Serverzertifikat zu erhalten, ist jedoch keine Identifizierung notwendig. Der	31.10.2012	Dienst-Änderung



News als PDF ▼

Name

PDFs noch nicht verfügbar!

IT-Beauftragtenversammlung am 12.11.2012

Handlungsstränge kit.edu-Migration: Folge 3
Themen – Andreas Lorenz

STEINBUCH CENTRE FOR COMPUTING - SCC



kit.edu-Migration - Übersicht (1)

Bereits betrachtete Themen

(ITB-Versammlungen, IT-Expertenkreissitzungen, AKs ...)

- Desktopmigration
- Ressourcenmanagement
- Clientmanagement
- Mailmigration Exchange
- Mailmigration Cyrus
- Fileservice
- Drucken im SCC
- Poolmigration
- Gruppenverwaltung
- Serviceaccounts
- Gäste und Partnerverwaltung
- Personenbezogenes Kommunikationsverzeichnis
- Migration Webdienste (GFB)
- Drucken im SCC
- NET-Portale – Administration
- Remote Access VPN
- HPC-Dienste
- Linuxintegration – AK
- SCC-Meldewesen
- IT-Grundausstattung
- IT-Sicherheit:
Benutzungsordnung,
IT-Sicherheitskonzept,
IT-Sicherheitsrichtlinie

kit.edu-Migration – Übersicht (2)

Über IT-Expertenkreis neu adressierte Themen

- Migrationsplanungen TSM-Dienste
- Testkonten
- Status Passwortmanagement durch ITB
- Status Lizenzmanagement für das Desktop-Migrationstool
FORENSIT

- Migrationsplanung Lizenzservice Dienste (ist in Vorbereitung)

kit.edu-Migration - TSM-Dienste

- Datensicherung (Backup) und Archivierung mit TSM
- Federführend: SCC-IDA/DADM
- Status: Vorbereitet
- Zugriff auf die Daten im TSM-Server
 - Die Zugriffsrechte der im TSM-Server gespeicherten Daten sind mit dem Knoten (TSM-Nodename) verbunden, von dem die Daten gesichert wurden.
 - Nach einem Rechneraustausch oder der Änderung des Rechnernamens muss das TSM-Team des SCC u.U. dem neuen Rechner oder dem Rechner mit dem neuen Namen wieder Zugriff auf den TSM-Server geben.
- Änderung des Rechnernamens (Windows)
 - Backup: Alle Daten werden erneut gesichert, wenn sich der Hostname ändert.
- ITB-Beteiligung: -
- Zuarbeit seitens ITB: Bitte vor einem neuen Backup mit dem TSM-Team Kontakt aufnehmen, um die Konfiguration client- und serverseitig anzupassen.



kit.edu-Migration - Passwortmanagement

- Federführend: SCC-DEI
- Status: in Abnahme
- Nächste Schritte:
 - Bereitstellung für ITB im November 2012
 - Konten nach PW-Reset neu aktivieren

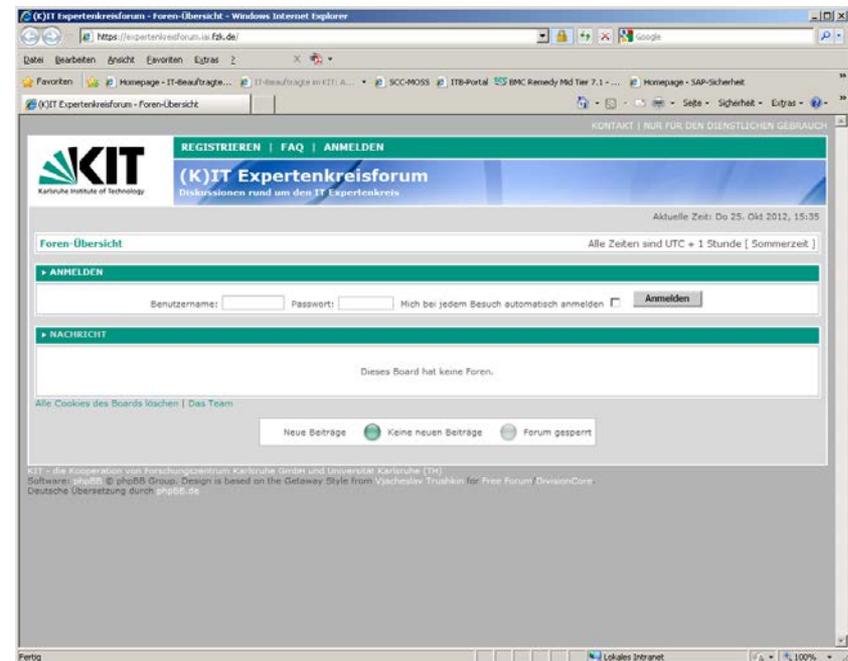
Detailansicht Mitarbeiter

SCC

Name	Vorname	KIT-Konto	E-Mail	
von				
test von der hagen	Patrick	lj5161	patrick.hagen2@kit.edu	<input type="button" value="Neues Passwort"/>
test von der hagen	Patrick	es9776	patrick.hagen3@kit.edu	<input type="button" value="Neues Passwort"/>
test von der hagen	Patrick	zm0996	patrick.hagen4@kit.edu	<input type="button" value="Neues Passwort"/>
von der Hagen	Patrick	of7085	patrick.hagen@kit.edu	<input type="button" value="Neues Passwort"/>

kit.edu-Migration - Testkonten

- IT-Experten wollen während und nach Migrationsphase Dienste prüfen können (QM).
- Federführend: IT-Expertenkreis
- Status: Agenda
- Nächste Schritte: Konkretisierung der Anforderung



kit.edu-Migration – Lizenzen FORENSIT

- Vereinfachtes Lizenzmanagement für ITB für das Desktop-Migrationstool FORENSIT
- Federführend: SCC-CMK
- Status: Sammlung der Anfragen der OEs bis 2.11.2012 (abgelaufen)
- Nächste Schritte: Beschaffung durch SCC, Rechnungstellung für OE, Ablage der Software an zentraler Stelle.
- ITB-Beteiligung: gegeben
- Zuarbeit seitens ITB: erledigt



IT-Beauftragtenversammlung am 12.11.2012

Effiziente Gruppenverwaltung im KIT Organisatorische (und technische) Aspekte

STEINBUCH CENTRE FOR COMPUTING - SCC



Agenda

- Rückblick: Einführung der Gruppenverwaltung
- Dienststeuerung über Gruppen
- Effiziente Organisation

Erinnerung: warum überhaupt eine eigene Gruppenverwaltung?

- Anforderungen der SCC-Fileserver (EMC)
 - Die Fileserver benötigen für Gruppen Unix-Attribute
 - Keine Duplikate, keine Änderung nach Vergabe, etc.
 - Durch ACL im AD nicht realisierbar
- Namenskonventionen müssen eingehalten werden
 - Zeichensatz, Maximallänge, Präfix
 - Durch Verwaltung per MMC im AD nicht realisierbar
- AD als LDAP-Server teils problematisch
 - Schachtelung von Gruppen muss von den Clients interpretiert werden
 - Leider nicht weit verbreitet
 - Objekte können im AD jederzeit verschoben werden
 - Manche Anwendungen verlangen die Angabe fester DNs
 - ACL und Schemaerweiterungen sehr aufwändig
 - MMC als Verwaltungswerkzeug nur auf MS-Plattform
- Schlechte Nachvollziehbarkeit durch fehlendes Audit im AD

Status Gruppenverwaltung

- Vorgestellt auf der 3. ITB-Vollversammlung (2. Mai 2012)
- Hat Pilotphase hinter sich gelassen
- Einführung und Import existierender Gruppen wurden im Juli abgeschlossen
- Über 100 ITB haben sie inzwischen verwendet
 - 600 neu angelegte Gruppen
 - 1900 aktualisierte Gruppen
 - 142 umbenannte Gruppen
 - 50 gelöschte Gruppen
- IDM kann inzwischen Gruppen automatisch auch über die Gruppenverwaltung pflegen
- Gruppen sowohl in KIT-AD als auch KIT-LDAP verfügbar

Und nu?

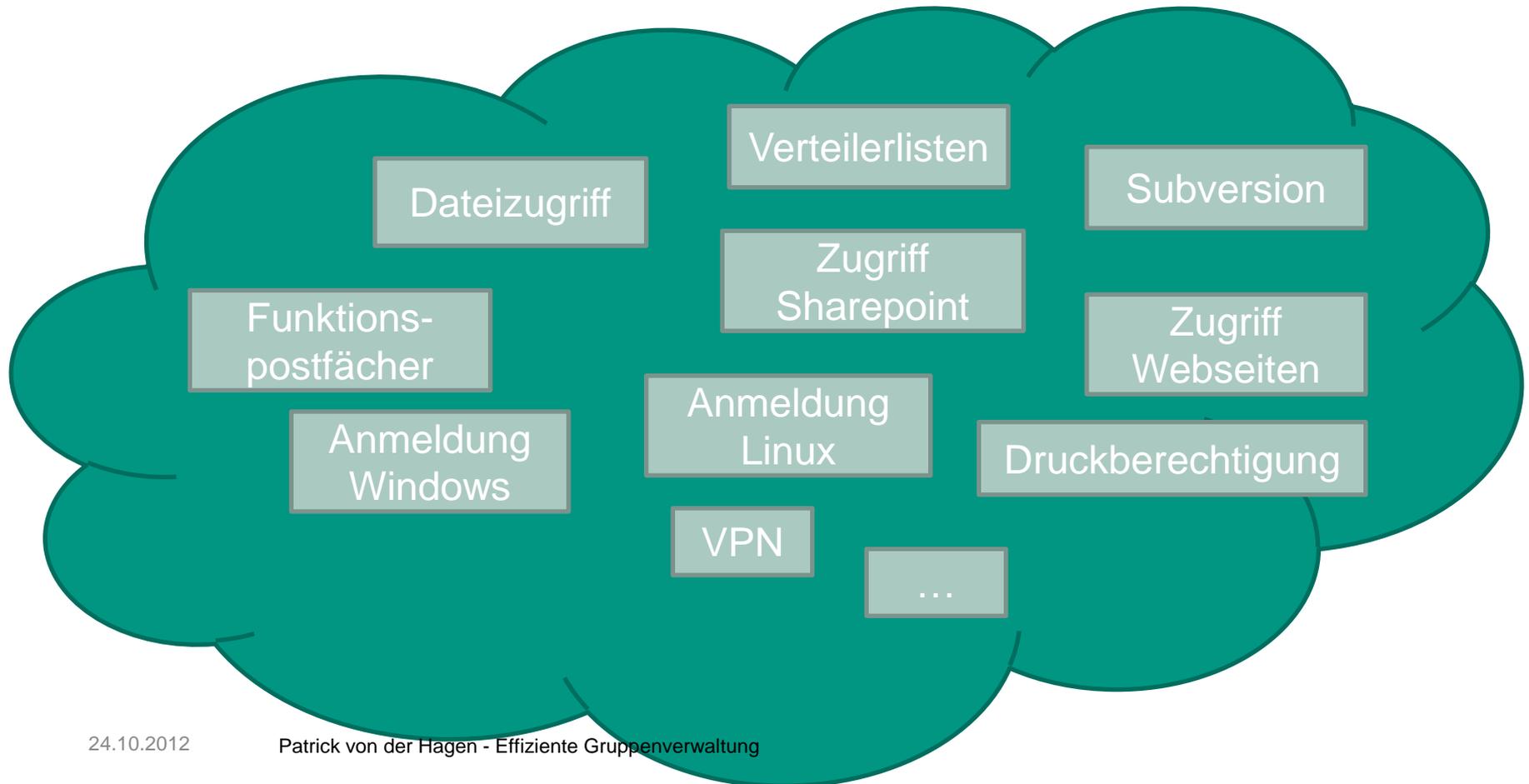
- „Wir haben eine neue Gruppenverwaltung. So what?“
- „Gruppen, Gruppen, Gruppen..... alles ist heute eine Gruppe...“
- „Und wie verwende ich die Gruppen mit...“?

- Fokus bei der Entwicklung
 - Dateizugriff: die Fileserver waren der Hauptgrund für die Entwicklung
 - Verteilerlisten: viele zu importierende Gruppen waren Verteilerlisten

- Aber das ist noch nicht alles....

Gruppen und Dienste

- Viele Dienste nutzen LDAP zu Authentifizierung (Login, Kennwort)
- Viele Dienste können LDAP-Gruppen zur Autorisierung nutzen



Aktuell werden Gruppen selten eingesetzt

- User hat im LDAP/AD ein geeignetes Merkmal
- Dienst konfiguriert „alle Konten mit department=OE“ dürfen auf das Mediawiki zugreifen
- Nachteile
 - Kleinere Einheiten als eine OE werden so nicht unterstützt
 - Wer kann sagen, was ein Mitarbeiter der OE darf?
 - Alle Dienste abfragen?
 - Hoffentlich wird nichts übersehen?
 - Reden wir mal nicht über den Aufwand

Dialog 1

Wer hat eigentlich alles Zugriff auf unser Wiki?

Wieso antwortest Du mit einer Gegenfrage?

Ticket? Wieso Ticket?

Aber wir bekommen in zehn Minuten eine Antwort?

Ach, musst Du das wirklich wissen?

Ist ja schon gut, ich erstelle gleich das Ticket....

Das Wiki wird vom SCC gehostet. Ich muss halt nachfragen.

Naja, wenn der falsche Mitarbeiter jetzt schon im Feierabend ist oder morgen außer Haus.... Aber mehr als zwei Tage waren es bislang selten.

Mit Dienst-Gruppe bzw. „Recht“

- Für jeden Dienst eine Gruppe in der Gruppenverwaltung anlegen
 - „OE-mediawiki-Zugriff“, Beschreibung „Mitglieder dürfen auf wiki.oe.kit.edu zugreifen“
- Der Vhost für wiki.oe.kit.edu wird vom SCC betrieben
 - Apache wertet die Mitgliedschaft dieser Gruppe aus
 - Nur Mitglieder erhalten Zugriff
- Der ITB der OE kann über die Gruppenverwaltung den Zugriff auf den SCC-Dienst regeln

Dialog 2

Welche OE-Mitarbeiter dürfen das Wiki nutzen?

Warum hat Jürgen das Wiki nutzen?

Warum ist er Mitglied in der Gruppe?

Und weshalb hat man ihn eingetragen?

Braucht er den Zugriff denn noch?

Hier ist die Liste

Weil er Mitglied in der Gruppe „OE-mediawiki-Zugriff“ ist

Öhm, weil man ihn da mal eingetragen hat...

Pffftttt.

Tja....

Role Based Access Control, RBAC

- Es existieren leicht unterschiedliche Definitionen, unterschiedliche Begriffe und unterschiedliche Ausprägungen
- Kerngedanke
 - Unterscheidung zwischen Nutzern, Rollen und Rechten
 - Nutzer können Rollen haben, aber keine Rechte
 - Rollen können Rechte haben
 - Rechte werden von IT-Systemen erzwungen
- Übliche Umsetzung
 - Die Nutzer liefert das IDM
 - Die Verwaltung/Organisation definiert Rollen
 - Die Systeme bieten den Rollen Rechte an
 - Diese Rechte werden nur den Rollen zugeordnet, die diese Rechte tatsächlich benötigen
- Gerne verkaufte IDM-Erweiterung
- Erweiterungen möglich, z.B. Konfliktprüfung

Umsetzung in der Gruppenverwaltung

- Technisch keine Unterscheidung zwischen Rollen und Rechten
 - Namenskonventionen?
- Die Gruppe „OE-mediawiki-Zugriff“ ist ein Recht
 - Umsetzung durch Webserver
 - Ggf. Bereitstellung durch Dienstbetreiber
- Zusätzliche Gruppen bilden „Business-Roles“ ab
 - OE-projekt-X
 - Diese Gruppen enthalten Nutzerkonten als Mitglieder
- Die Gruppe „OE-projekt-X“ wird Mitglied in „OE-mediawiki-Zugriff“
 - Ausnutzung der Schachtelung
- Schlüssige Darstellung
 - Nutzer hat Business-Roles „OE-Projekt-X“
 - Business-Role impliziert Recht „OE-mediawiki-Zugriff“
 - Rechte steuern Dienste
- Nachteil: Role-Explosion?

Ansicht einer Gruppe als „Rolle“

Rolle

Gruppe: SCC-DEI-Mitarbeiter

Speichern Abbrechen

Beschreibung: Mitarbeiter der Abteilung DEI

Group ID: 44725

AD-DN: CN=SCC-DEI-Mitarbeiter,OU=Groups,OU=SCC,OU=Staff,OU=KIT,dc=kit,dc=edu

E-Mail: DEI-Mitarbeiter@scs.kit.edu

Erweiterte Suche SCC

Benutzer:

23 items selected Remove all Add all

Berendonck, T	-	Adam, Martina	+
Frank, Robert (-	Ahmed, Usma	+
Gärtner, Thoma	-	Alberto Quiteric	+
Glas, Sabine (s	-	Alef, Manfred (s	+
Heathman, Do	-	Alfinger, Manfre	+
Hör, Hans Pete	-	Ameri, Parinaz	+
Köhler, Jens (d	-	Antoni, Torsten	+
Kühner, Holger	-	Appel, Gunter (+
Labitzke, Seba	-	Assaf, Haidar (+
Nußbaumer, M	-	Atkinson, John	+

Köhler, Jens (da4613)

Gruppen:

0 items selected Remove all Add all

SCC-AbtLeiter	+
SCC-AbtLeiter-Vertretung	+
SCC-ALR	+
SCC-Apache	+
SCC-AppleStore	+
SCC-Autoop	+
scc-biztalk-admins	+
scc-bts-qm-b2b-operators	+
scc-bts-qm-ss0-affiliate-admins	+
SCC-Changemanager	+

Änderungen wirken auch auf:

SCC-DEI-Alle

SCC-redmine-zugriff

Effektive Mitgliederliste:

Berendonck, T

Frank, Robert

Gärtner, Thom

Glas, Sabine (

Heathman, Do

Hör, Hans Pet

Köhler, Jens (

Kühner, Holge

Labitzke, Seba

Nußbaumer, M

Philipp, Micha

Reichert, Heik

Rogge, Carste

Schmidt, Kers

Simon, Michai

Taranu, Irina (

von der Hager

Wandelmaier,

Weiß, Ulrich (

Wenzel, Alvar

Wirtl, Ronny (scc

Mitglieder

Rechte

Speichern Abbrechen

Ansicht einer Gruppe als „Recht“

The screenshot shows a web interface for managing a group. At the top, there are buttons for 'Speichern' and 'Abbrechen'. The group name is 'Gruppe: SCC-redmine-zugriff'. The description is 'Recht: Zugriff auf Redmine'. The Group ID is 47873. The AD-DN is CN=SCC-redmine-zugriff,OU=Groups,OU=SCC,OU=Staff,OU=KIT,dc=kit,dc=edu.

Below this, there is a search section 'Erweiterte Suche' with a dropdown menu set to 'SCC'. There are two main sections: 'Benutzer:' and 'Gruppen:'. The 'Benutzer:' section shows '0 items selected' and a list of users with '+' and '-' icons. The 'Gruppen:' section shows '1 items selected' and a list of groups with '+' and '-' icons.

On the right side, there is a section 'Änderungen wirken auch auf:' which is empty. Below it is 'Effektive Mitgliederliste:' which shows a list of users with '+' and '-' icons.

Three green arrows point to specific parts of the interface: 'Recht' points to the description field, 'Rollen' points to the 'Gruppen:' section, and 'Nutzer' points to the 'Effektive Mitgliederliste:' section.

Nachvollziehbarkeit und Transparenz

- Recht: Wer darf auf das Mediawiki zugreifen?
 - Alle Mitglieder von Projekt X
 - Alle Mitglieder von Projekt Y
 - der OE-Leiter

- Rolle: Was dürfen Mitglieder von Projekt X
 - Zugriff auf das Mediawiki
 - Zugriff auf ein Fileshare
 - Mitgliedschaft im Projekt-Verteiler

Dialog 3

Warum hat Jürgen Zugriff auf das Mediawiki?

Stimmt doch gar nicht, seit einem Monat nicht mehr

Jürgen hat nach wie vor Zugriff auf das Mediawiki, wieso denn das?

Ach ja, stimmt, dann ist das ja in Ordnung

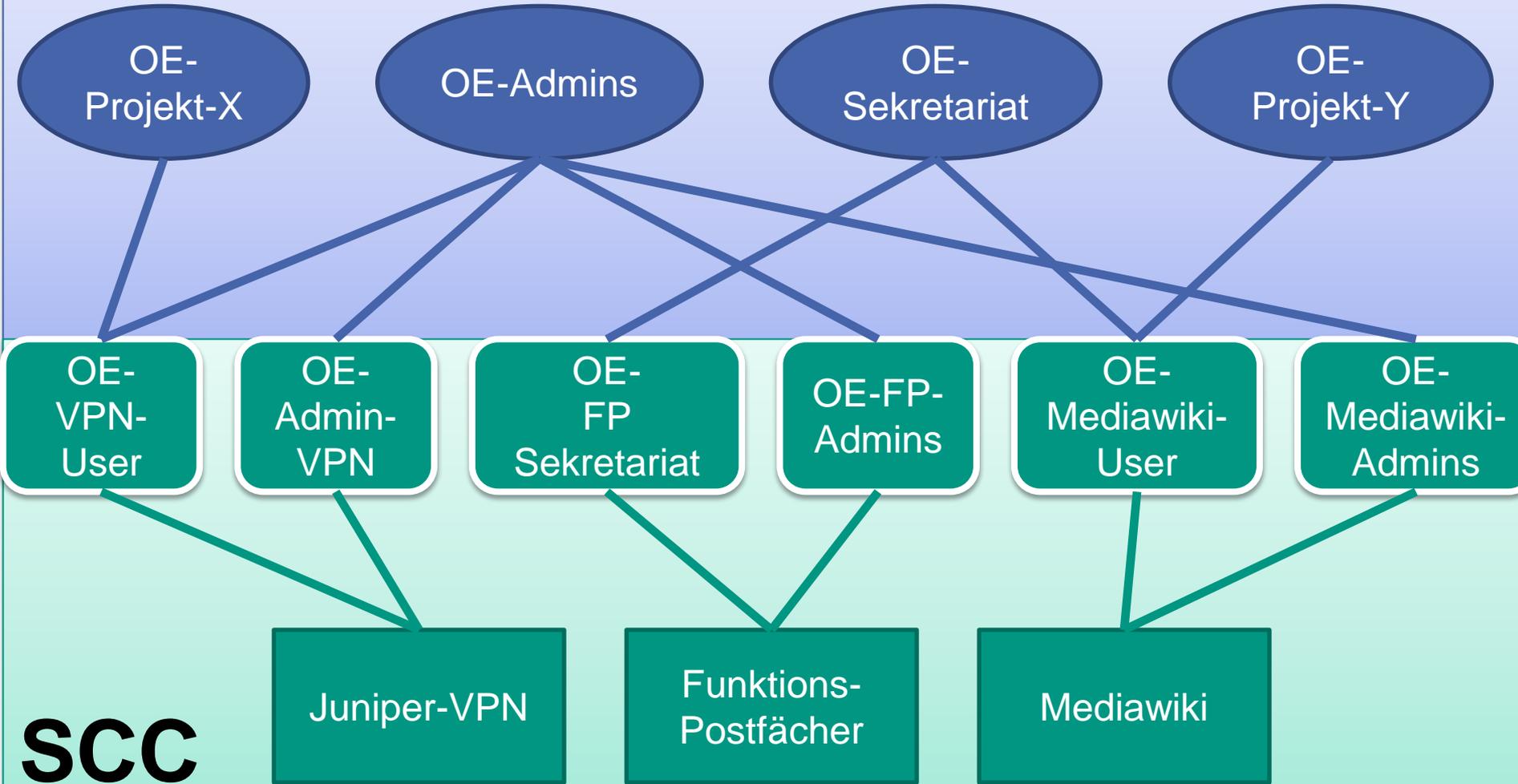
Weil er Mitglied von Projekt X ist

Ups, dann korrigieren wir das doch mal

Er ist halt noch an Projekt Y beteiligt

Verteilung zwischen ITB und SCC

ITB



SCC

Und warum haben wir das nicht schon immer so gemacht?

- Wir bilden Role-Based-Access-Control auf geschachtelte Gruppen ab
- Bisher galt
 - Die Zugriffsrechte im AD waren bislang zu offen
 - Keine geschachtelten Gruppen unter Unix
 - Schachtelung musste jeweils im Client interpretiert werden
 - Unzureichende Kompatibilität
- Inzwischen gilt
 - Änderungsrechte an Gruppen sind feiner
 - Schachtelung wird für OpenLDAP ausgerollt
 - Die ausgerollten Gruppen bieten maximale Kompatibilität zu unseren Diensten

Aktuell in Arbeit durch SCC

- VPN-Zugang
- Funktionspostfächer erhalten automatisch Gruppen zur Verwaltung
- Verwaltung der FS-Admins
- Zugriff auf Web-Dienste

Fazit

- Die Gruppenverwaltung betrifft nicht „nur“ Laufwerke und Verteiler
- Durch den geschickten Einsatz von Gruppen verbesserte Transparenz
 - Für die ITB
 - Und auch für den Changemanager, den Servicedesk,...
- Einmaliger Aufwand beim Einrichten von Diensten für eine OE
- Dauerhafter Nutzen

Fragen / Diskussion

STEINBUCH CENTRE FOR COMPUTING - SCC



Fragen / Diskussion – Informationen für ITB

- Was wurde im Vorfeld gemeldet:
 - Wie sind die Planungen bzgl. Studierenden-Portal?
 - Verantwortung
 - Ressourcen
 - Integration von Anwendungen (z.B. Ilias)
 - Weitere Betriebspunkte:
 - Überführung von AD-Gruppen in zentrale Gruppenverwaltung
 - Eigene php-Anwendungen in OpenText
 - Umstellung Serviceaccounts auf KIT-Namensschema

Herzlichen Dank !

STEINBUCH CENTRE FOR COMPUTING - SCC

