
DACHS

DESY ACcess Handling System



Zeuthen 22.9.2009

S. Brinker, C. Kluth

Überblick

- Historie
 - Ziele
 - Systemaufbau
 - Grundlegendes
 - Technik
 - Datenbanken
 - PIP
 - Rollen u. Regeln
 - DARF-DACHS
 - Systemübersicht
 - Meilensteine
 - DACHS-Team
 - Kosten
 - Statistik
 - Ausblick
 - Diskussion
-

Historische Entwicklung

- 2006 – Initiative des Sicherheitsrates
 - von MPS, D5
 - für Beschleuniger, Labore, Kräne etc.
 - Veraltetes HERA Zugangskontrollsystem
 - NORD Hardware aus den Achtzigern
 - 2007 – Projektstart durch M-Bereich zur Ablösung
 - Idee u. Projektleitung: D. Ramert (MPS)
 - 2008 – Einführung eines kommerziellen Systems
 - 6020 von Interflex
 - Zugangskontrollsystem für HERA ab 8/2008
 - Projektleitung → S. Brinker (MPY)
 - Ausweitung auf weitere Beschleuniger u. Bereiche
-

Ziel des Zugangskontrollsystems

- Nur berechnigte und unterwiesene Personen sollen Zugang zu bestimmten Gebieten bekommen
 - Und das möglichst pragmatisch (Freitag, 17 Uhr ...)
 - Unter Beachtung des Datenschutzes
 - In der DESY-Umgebung
-

Was braucht man dazu?

- Eigentlich nur 2 Dinge:
 - Hardware (an Türen, Kartenerstellung,...)
 - Datenbank in der steht, wer wo rein darf

Systemaufbau – Grundlegende Ideen

- Safety → Personeninterlock
 - DACHS hilft mit Infos (BKR, PIII Experimente)
- Security → DACHS
- Kompletter DACHS Ausfall: Türen bleiben zu
- Fluchtwege immer per Klinke zugänglich
- Zugänge immer per Schlüssel möglich
 - für Erste Hilfe durch Technischen Notdienst
- Protokollierung von Zugängen zu Beschleunigern für D3
- Datenschutz in Absprache mit D4, BR
- Selbstorganisation in den Gruppen
 - PIP (teilweise), DARF-DACHS (komplett)

Manuelle Zugangsmöglichkeiten für Notfälle



mit ZZ,
betriebsbereit
(Terminal leuchtet blau)



ohne ZZ,
nicht betriebsbereit
(PIA)

22.9.2009

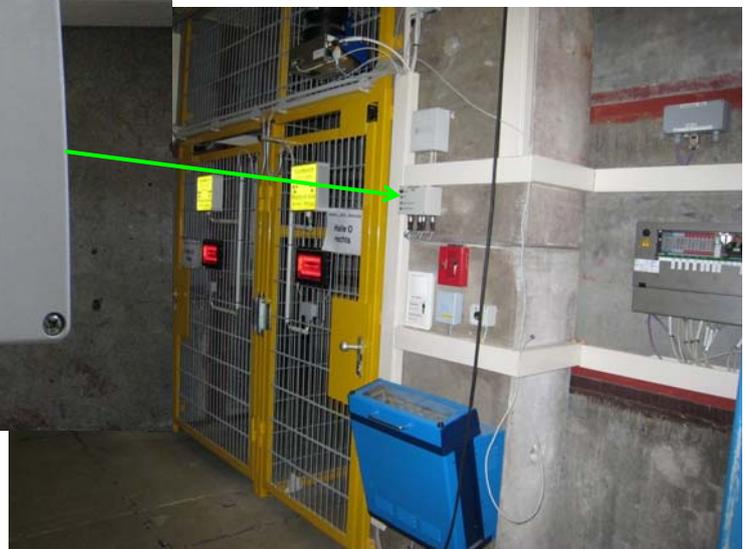
DACHS - S. Brinker, C. Kluth

7

Safety – das Personeninterlock von MPS ist immer das führende System!



PETRA III Accelerator



22.9.2009

DACHS - S. Brinker, C. Kluth

8

Rechnersicherheitsrat

„IT Sicherheitspolitik für DESY“

2. Bestimmung des IT-Sicherheitsniveaus

Wegen der unterschiedlichen Bedeutung der Informations-Technik für die verschiedenen Anwendungen macht es keinen Sinn, ein für alle Anwendungen gleich hohes Sicherheitsniveau anzustreben. Hundertprozentige Sicherheit ist nie zu erreichen. Da Sicherheit auch immer ihren Preis hat, muss es das Ziel sein, ein für die jeweilige Anwendung angemessenes Sicherheitsniveau zu definieren.

2.1 Kriterien

Das anzustrebende Sicherheitsniveau ergibt sich aus der Abwägung folgender Kriterien:

2.1.1 Die zu schützenden Güter und ihr Wert

2.1.1.1 Personenschutz

Die im Bereich des Personenschutzes eingesetzten IT-Systeme dürfen auch im Fehlerfall keine Menschenleben gefährden. An ihre Funktionalität und Verfügbarkeit müssen daher höchste Anforderungen gestellt werden.

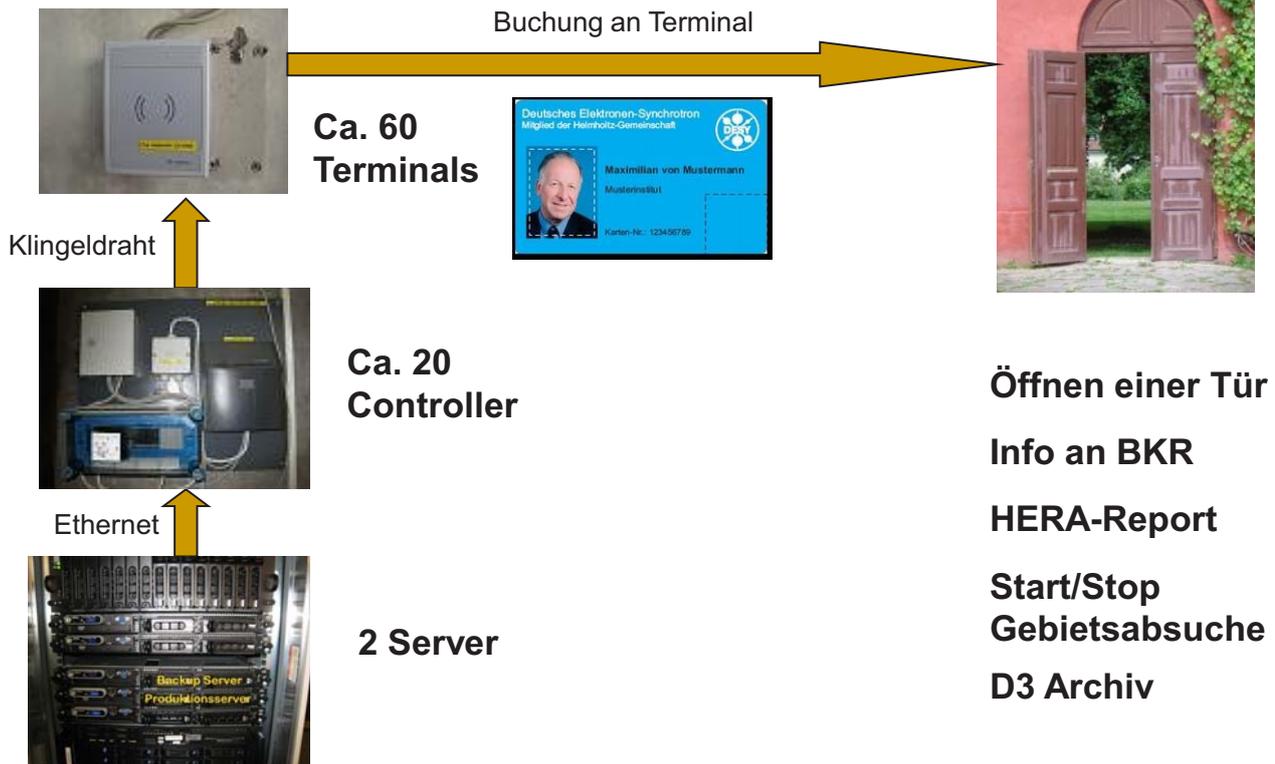
2.1.1.2 Beschleuniger und Experimente

Sowohl die Beschleuniger als auch die Experimente sind ohne Informations-Technik nicht funktionsfähig. Die mit sehr hohem Kostenaufwand geschaffenen Anlagen und die durch einen aufwendigen und kostenintensiven Prozess erzeugten Experimente-Daten sind Güter von sehr hohem Wert.

Technik des Zugangskontrollsystems

- Kommerzielles Security System **6020** von Interflex (kein Safety System)
- Einbettung in den offenen DESY Campus
- Nahfeld RFID Technik
 - *Mifare Classic* Chip, inkompatibel zu EMBL (*Legic*)
- Erweiterbar
 - Zeiterfassung, Bezahlungssystem, Biometrie ...
- Wird eingesetzt in
 - Fußballstadien, Flughäfen ...

Aufbau der Hardware

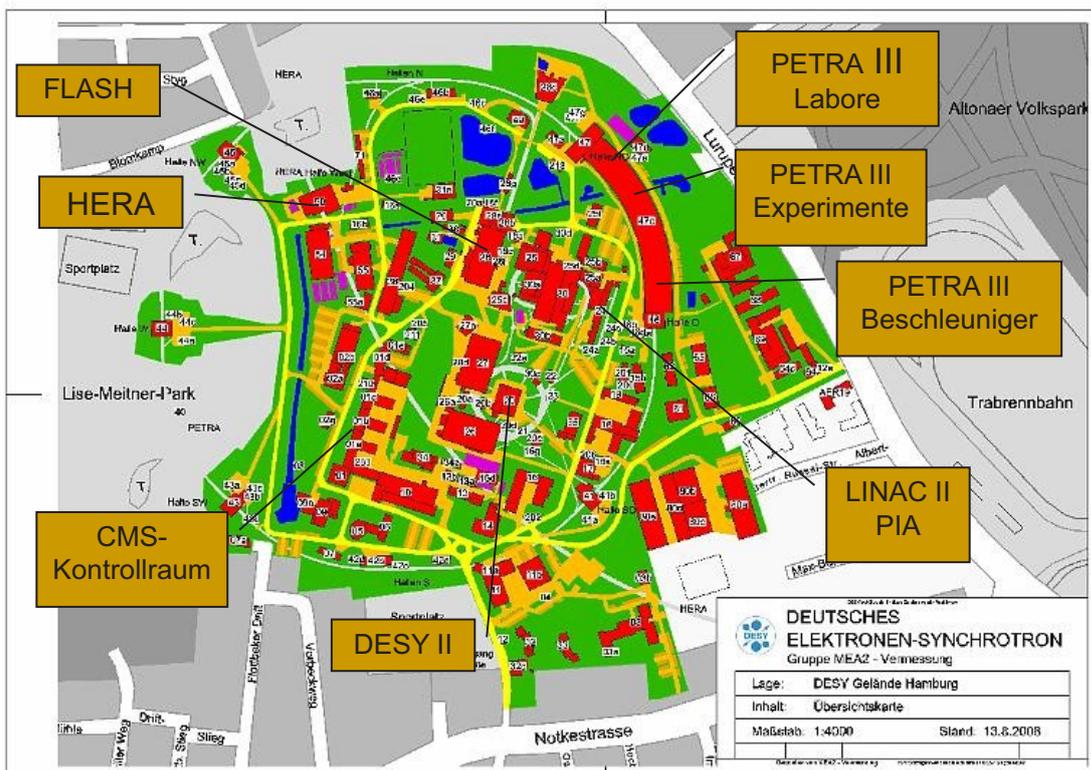


22.9.2009

DACHS - S. Brinker, C. Kluth

11

DACHS am Standort Hamburg



22.9.2009

DACHS - S. Brinker, C. Kluth

12

Systemaufbau – BKR-Applikation zur Unterstützung des Zeitweisen Zugangs

- Führendes System: Personeninterlock
- Beschleunigerbetrieb
 - DACHS zeigt Berechtigungen für ZZ an
 - Keine Wirkung von DACHS auf Türen
 - Handgeschriebenes Protokoll im BKR
- Beschleuniger geerdet u. geschlossen
 - Personeninterlock gibt Türkontrolle an DACHS ab
 - Elektronisches Protokoll für D3 (nur Zugänge)

22.9.2009

DACHS - S. Brinker, C. Kluth

13

Systemaufbau – Unterschiedliche Funktionen der DACHS Terminals

Übersicht über den Einsatz von DACHS Terminals an Türen										
DACHS Terminal Kategorie	Gewöhnliche Zutrittskontrollen				Personeninterlock Türen				Beispiele 3/2009	Bemerkungen
	Info	Zugang	Abgang	Zu- und Abgang	ohne ZZ	mit ZZ	PIL Interface zum Terminal	Gebietsabsuche FS Experimente		
INFO	•								Ausweisausgabe	noch nicht im Einsatz
ZUG		•							Gebäude 20 Zentrum, CMS Kontrollraum	Terminal steuert E-Falle
ABG			•							noch nicht im Einsatz
HERA				•					HERA Hallen	Terminal steuert E-Falle beim Zugang, Abgang per Klinke, Speicherung des Status auf dem Ausweis
ZZ						•			LINAC II, PIA, FLASH	Unterstützung für den BKR bei Zeitweisem Zugang (ZZ), keine Verbindung zur E-Falle
PILD					•		•		PETRA III Schräggänge	Zugang bei aufgehobenem Interlock mit DACHS Ausweis
ZZD						•	•		PETRA III Alte Hallen	Unterstützung für den BKR bei ZZ, Zugang bei aufgehobenem Personeninterlock nur mit DACHS Ausweis
GABS								•	PETRA III Experimente	Starten und Beenden der Gebietsabsuche

22.9.2009

DACHS - S. Brinker, C. Kluth

14

Datenbanken, Personen, Rollen, Rechte Organisation ...

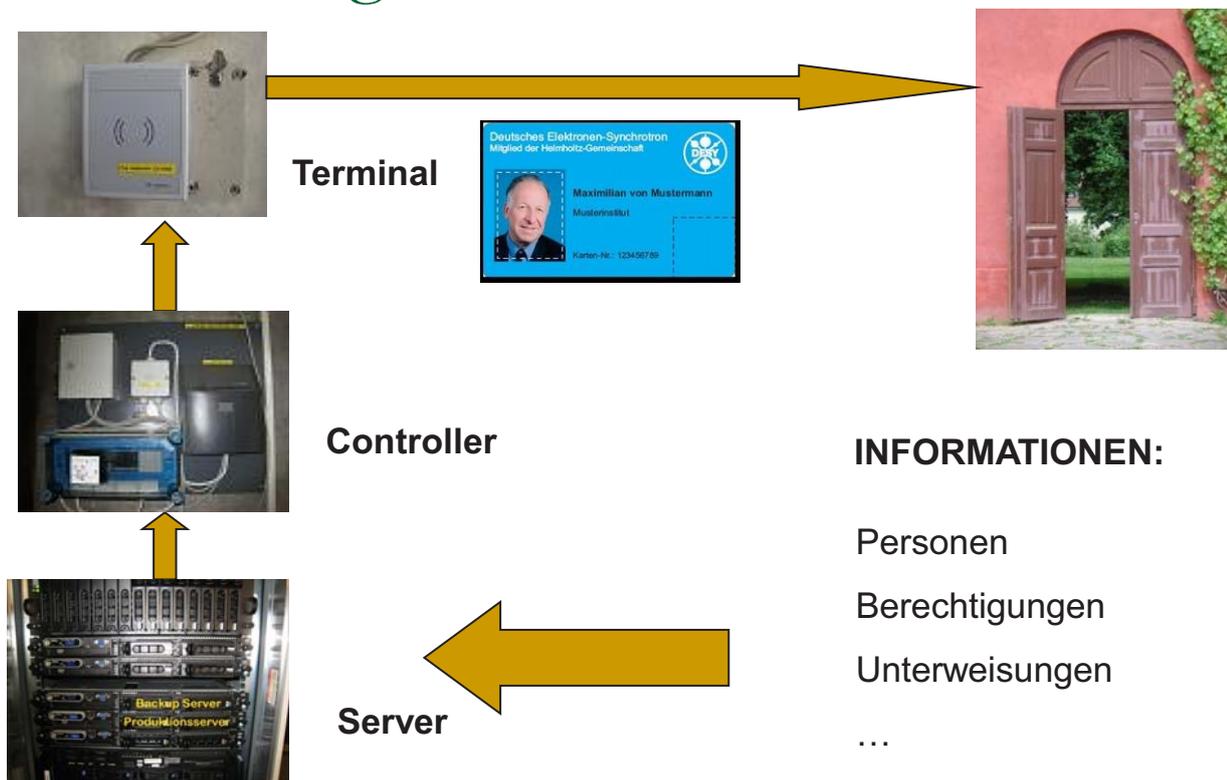
- Was brauchen wir?
 - Rollen und ihre Rechte
 - Gebietsverantwortliche, Gruppenleiter...
 - Festlegung der Voraussetzungen für den Zugang
 - Dezentrale Organisation
 - Benennung von Admins
 - Schulungen
 - Regelmäßige Information
 - Eindeutige Personendaten
 - Workflows

22.9.2009

DACHS - S. Brinker, C. Kluth

15

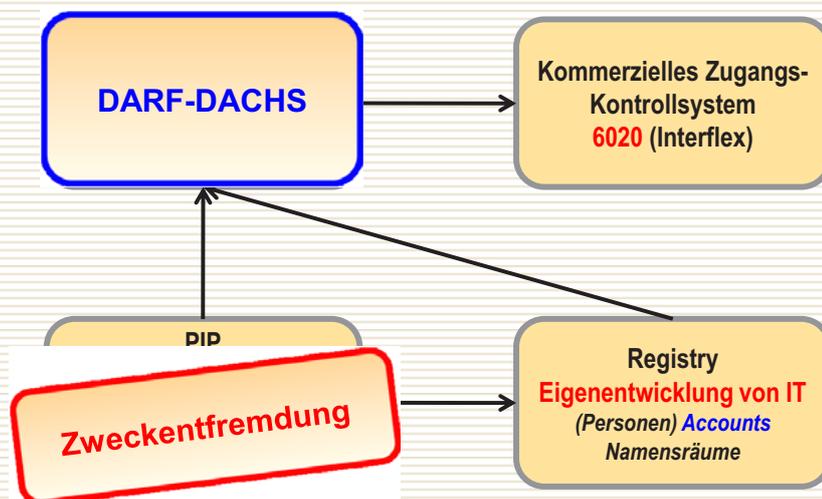
Anbindung an die Datenbanken



22.9.2009

DACHS - S. Brinker, C. Kluth

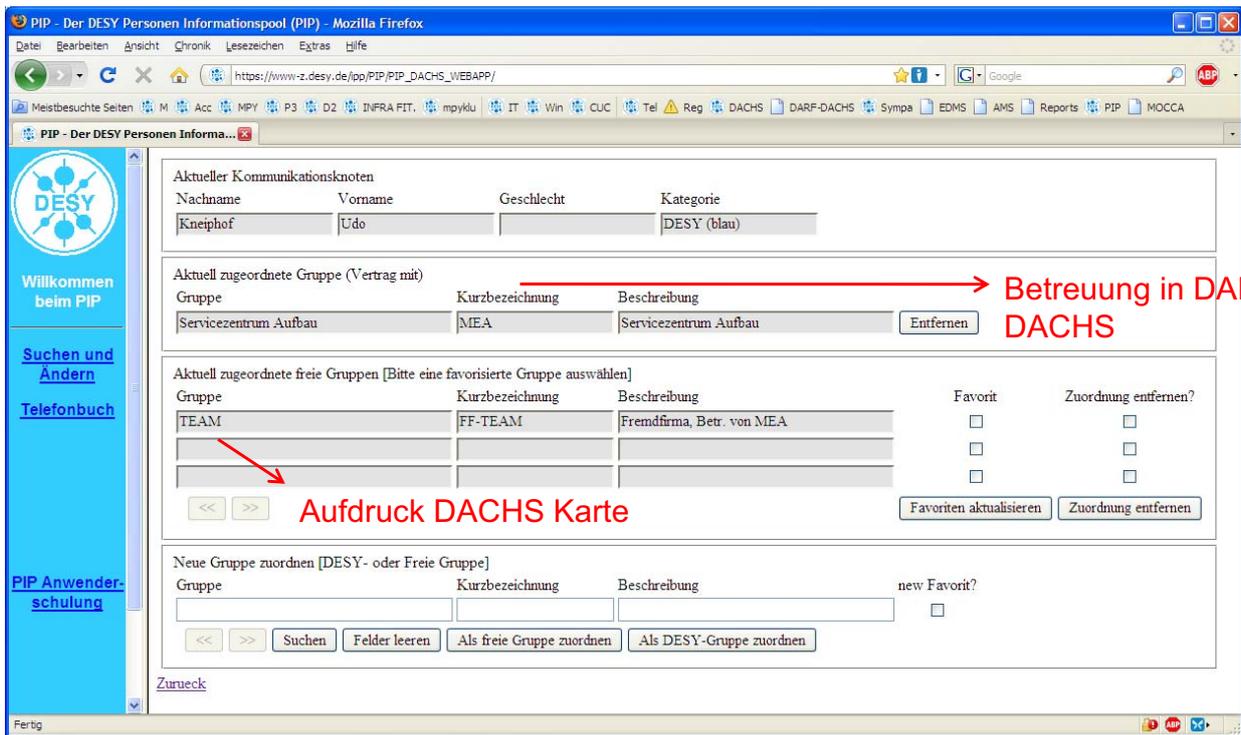
16



PIP im Einsatz für DACHS

- DARF-DACHS nutzt nur PIP Datensätze
 - Gruppen
 - Festlegung der PIP Gruppen durch Bereichsreferenten
 - Personen
 - Diskussion der Aufnahme von Personendaten im CUC
- DARF-DACHS Berechtigungskonzept nutzt PIP-Gruppen
 - DARF-DACHS Admins der 1. PIP-Gruppe betreuen die jeweilige Person
- Kategorien (Farben) der DACHS Karten werden in PIP festgelegt

PIP Screenshot



22.9.2009

DACHS – S. Brinker, C. Kluth

19

Neuer Formularentwurf (CUC) Aufnahme von Personendaten

Formular der DESY Verwaltung (V1)

Anlegen einer Person im PersonenInformationsPool

Version 0.3

Name *	Kluth
Vorname *	Carsten
Geschlecht	m
Geburtsdatum (tt.mm.jjjj) ¹ *	09.11.1959
Geburtsort ¹ *	Osnabrueck

Anforderer *	I. Nikodem
Eintrittsdatum (tt.mm.jjjj)	8.12.1988
Austrittsdatum (tt.mm.jjjj)	

Telefonbucheintrag (i/n) *	j
Standort/Gebäude/Zimmer	Hamburg/30b/451
Telefon-Nr.	2050
Mobil-Tel.-Nr.	-
Sortierung (AG, SRT)	

DESY Vertrag (i/n) *	j
DESY Gruppe **	MPY
Projekt ** / 2. Gruppe	-
Institut auf dem DESY Gelände **	-
Fremdfirma **	-
Externe Person (DESY Bibliothek) **	-

* Pflichtfeld

¹ Daten dienen der eindeutigen Zuordnung der Daten zur Person

** Eine dieser fünf Möglichkeiten muss grundsätzlich ausgefüllt werden

Für auswärtige Personen:

Heimatinstitut	-
Mailadresse	-
Telefon-Nr.	-
Mobil-Tel.-Nr.	-
Fax	-
Kontaktperson bei DESY	-

Hinweise

DESY Vertrag
ja → immer blaue DACHS Karte
nein → nie blaue DACHS Karte

Fremdfirmen

Die beauftragende DESY Gruppe bzw. das beauftragende Institut müssen unbedingt zusätzlich eingetragen werden

Auswärtige Personen

müssen entweder einer DESY Gruppe, einem Projekt oder der Bibliothek zugeordnet werden

Beispiele für Institute auf dem DESY Gelände

EMBL, Universität Hamburg, MPG, XFEL GmbH

Beispiele für Projekte

PETRA III, XFEL, PITZ

Ich erkläre mich damit einverstanden, dass die von mir oben angegebenen personenbezogenen Daten in einem zentralen DESY-Personen-Informations-Pool gespeichert und verarbeitet werden.

Ort, Datum, Unterschrift

22.9.2009

DACHS - S. Brinker, C. Kluth

20

DACHS Karten – Kategorien (DD = DARF-DACHS)

Farbe	Personenkreis	Kartenaufdruck
Cyan	Mitarbeiter von DESY	DESY - <Gruppenkürzel> <Gruppenname>
Grün	Gäste von DESY Gruppen, Mitarbeiter von anderen Instituten	<Name des Instituts> <Kürzel der DD Gruppe>
Gelb	Alle Fremdfirmen	<Fremdfirma> <Kürzel der DD Gruppe>
Weiß	Messgäste von HASYLAB	User Photon Science <Kürzel der DD Gruppe>
Orange	Anonyme Karten für Gruppen Zugang nur für HERA, CMS...	<Kürzel der DD Gruppe> Gast xx
Rot	Anonyme VIP Karten incl. Zugang zu Beschleunigern!	z.B. VIP (PETRA III)

22.9.2009

DACHS - S. Brinker, C. Kluth

21

DACHS Karten – Beispiele

Deutsches Elektronen-Synchrotron
Ein Forschungszentrum der Helmholtz-Gemeinschaft





<Vorname> <Nachname>

DESY - <Gruppenkürzel>

<Gruppenname>

Karten-Nr.: 12345

22.9.2009

DACHS - S. Brinker, C. Kluth

22

DACHS Karten – Beispiele

Deutsches Elektronen-Synchrotron
Ein Forschungszentrum der Helmholtz-Gemeinschaft



Carsten Kluth

DESY - MPY

Beschleunigerphysik

Karten-Nr.: 36893

22.9.2009

DACHS - S. Brinker, C. Kluth

23

DACHS Karten – Beispiele

Deutsches Elektronen-Synchrotron
Ein Forschungszentrum der Helmholtz-Gemeinschaft



MPY

Gast 01

Eingeschränkte Besucher- und Gastkarte

Karten-Nr.: 12345

22.9.2009

DACHS - S. Brinker, C. Kluth

24

DACHS Karten – Beispiele

Deutsches Elektronen-Synchrotron
Mitglied der Helmholtz-Gemeinschaft



<Vorname> <Nachname>

Fa. <PIP-Firmenname>

beauftragt von <PIP-DESY-Gruppenkürzel>

Karten-Nr.: 12345

22.9.2009

DACHS - S. Brinker, C. Kluth

25

DACHS Karten – Beispiele

Deutsches Elektronen-Synchrotron
Ein Forschungszentrum der Helmholtz-Gemeinschaft



<Vorname> <Nachname>

<PIP-Institutsname>

<DARF-DACHS-Admin-Gruppenkürzel in PIP>

Karten-Nr.: 12345

22.9.2009

DACHS - S. Brinker, C. Kluth

26

DACHS Karten – Beispiele

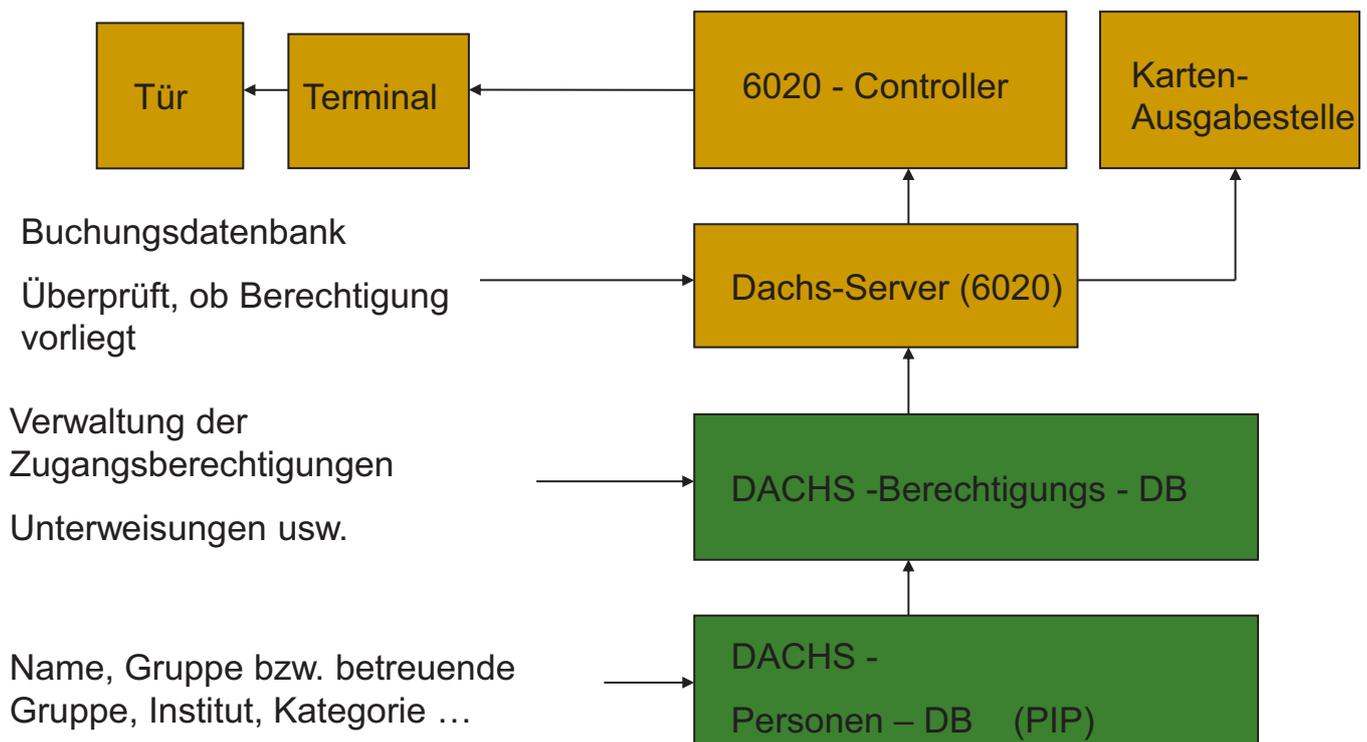


22.9.2009

DACHS - S. Brinker, C. Kluth

27

Grober Aufbau



22.9.2009

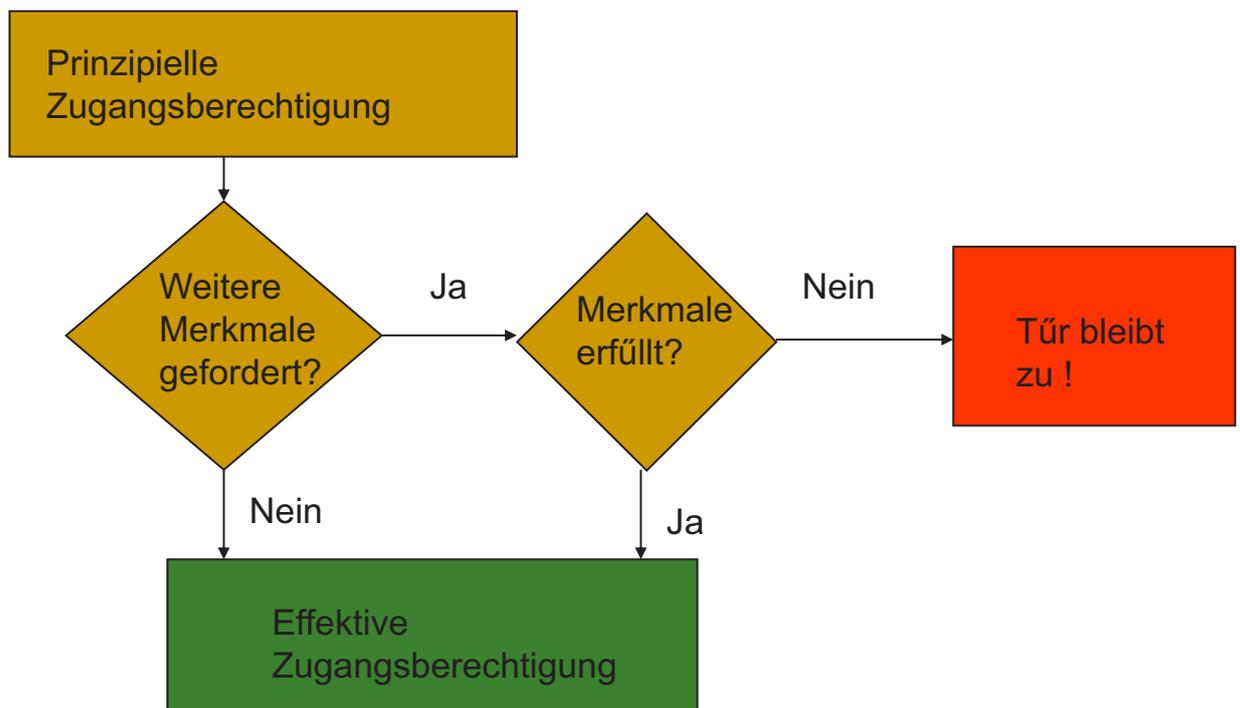
DACHS - S. Brinker, C. Kluth

28

Was wird wo gefordert?

Gebiete	Allgemeine Unterweisungen		Beschleunigerspezifische Unterweisungen		Dosimeter Pflicht
	Strahlenschutz	Sicherheit	Strahlenschutz	Sicherheit	
Modulatorhalle	•	•	Modulatorhalle	Modulatorhalle	•
LINAC II	•	•	LINAC II	LINAC II	•
DESY II	•	•	DESY II	DESY II	•
PETRA III	•	•	PETRA III	PETRA III	•
FLASH	•	•	FLASH	FLASH	•
HERA	Keine Merkmale erforderlich				
CMS	Keine Merkmale erforderlich				

DARF-DACHS



DARF-DACHS Beispiel

The screenshots show the DARF-DACHS web application interface. The left screenshot displays the 'PersonDetails' page for Carsten Kluth, including fields for Lastname, Firstname, OrgUnit, and Card type. Below this, there are two tables: 'Access right' and 'Person property'. The 'Access right' table lists various access rights such as CMS, DESY II, and HERA, along with their validity dates. The 'Person property' table lists properties like 'AllgSi - Allgemeine Sicherheit' and 'HasChemLab - HASYLAB Chemistry Lab'. The right screenshot provides a more detailed view of the 'Access right' table, showing columns for 'Access right' and 'Date', and listing numerous specific access rights for different systems and their validity periods.

22.9.2009

DACHS - S. Brinker, C. Kluth

31

Berechtigungen der Administratoren im DD

Erteilung von Zugangsberechtigungen zu Gebieten										
Stand 1. Dezember 2008										
GRUPPE	NAME	aktiv?	BESCHLEUNIGER / GEBIET							WEITERE GRUPPEN FUER DIE BERECHTIGUNGEN VERGEBEN WERDEN DUERFEN
			Modulartorh.	Linac2	FLASH	DESY	PETRA	HERA	CMS	
DIR	R. Brinkmann	ja	ALLE	ALLE	ALLE	ALLE	ALLE	ALLE	ALLE	alle Gruppen, Sicherheitsverantwortlicher aller Beschleuniger
DACHS Projekt										
MPY	S. Brinker	ja	X	X	X	X	X	X	X	alle Gruppen, Support
	C. Kluth	ja	X	X	X	X	X	X	X	alle Gruppen, Support
Stabsstellen										
D3	N. Tesch	ja	X	X	X	X	X	X	X	
	A. Leuschner	nein	X	X	X	X	X	X	X	
D5	S. Schrader	ja	X	X	X	X	X	X	X	
	A. Hoppe	nein	X	X	X	X	X	X	X	
PR	C. Mrotzek	nein			X	X	X	X	X	
M-Bereich										
MR	A. Gamp	ja	read	read	X	X	X	ALLE		M, MPY, Gebietsverantwortlicher HERA
MBB	M. Bieler	ja	X	X	X	X	X	X		MCS, MDE, MDI, MHF-e, MHF-sl. MKK, MSK, MVS
	P. Hopf	ja	X	X	X	X	X	X		MCS, MDE, MDI, MHF-e, MHF-sl. MKK, MSK, MVS
MCS	R. Bacher	ja	X	X	X	X	X	X		

22.9.2009

DACHS - S. Brinker, C. Kluth

32

Berechtigungsdatenbank DARF-DACHS in Zahlen

Gebiete	> 60
Unterschiedliche Merkmale (Unterweisungen)	> 90
Personen	> 1000
Gruppen	> 50
Administratoren in den Gruppen	> 50
Manuelle Einträge	~ 10.000
Importierte Einträge aus ASIP (PC basierte Unterweisungen bei HASYLAB)	

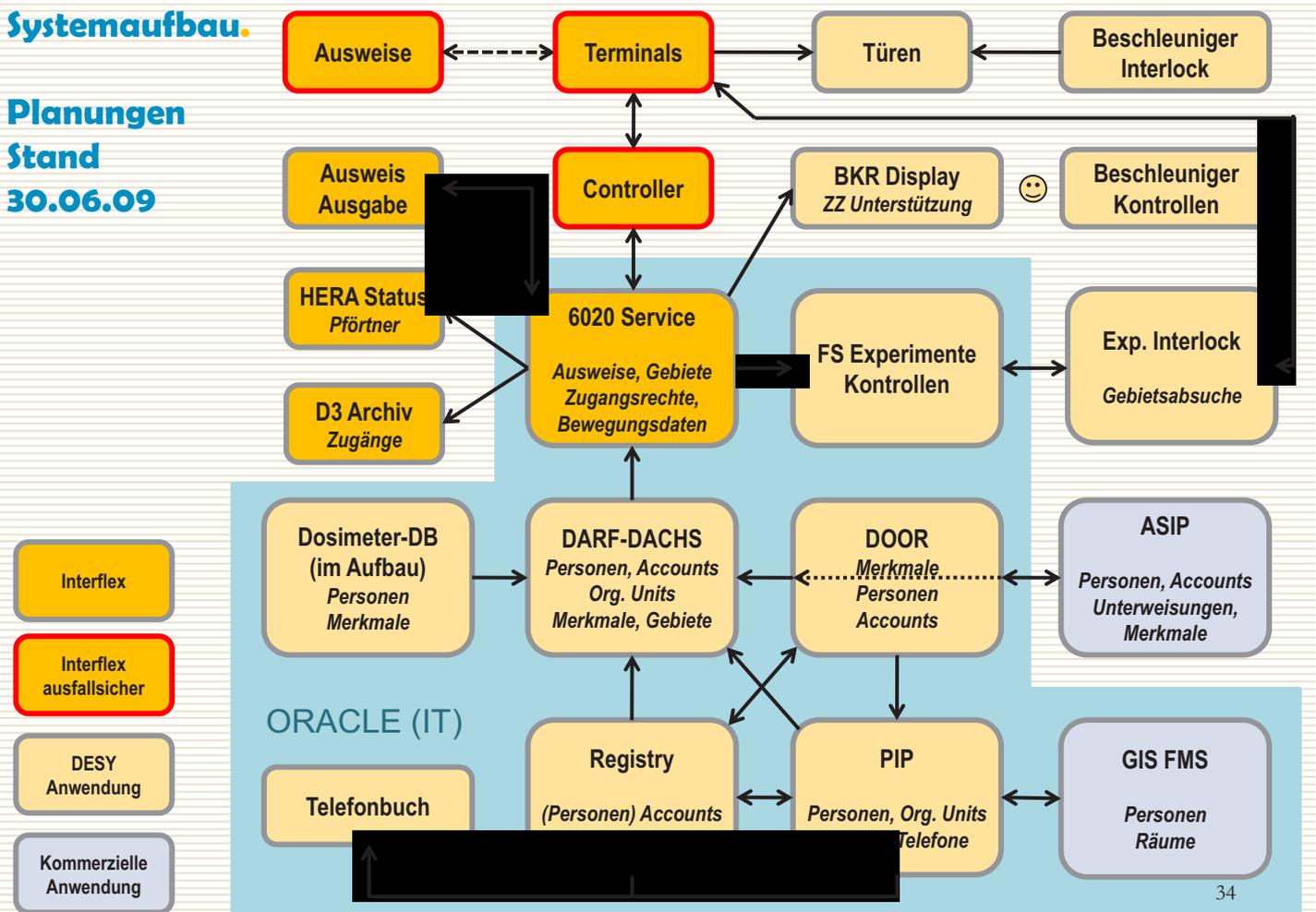
22.9.2009

DACHS - S. Brinker, C. Kluth

33

DACHS Systemaufbau.

Planungen
Stand
30.06.09



Erreichte Meilensteine (1)

- **Betriebsvereinbarung**
 - durch Anhänge sehr flexibel
 - **Inbetriebnahme der kommerziellen Lösung 6020**
 - Zugangskontrollsystem
 - **Inbetriebnahme von DARF-DACHS**
 - Berechtigungsdatenbank
 - Kontinuierliche Weiterentwicklung notwendig
 - **Ablösung der alten HERA Zugangskontrollen**
 - Sichtkontrolle bei Zugängen durch Hauptpförtner
 - Keine Pförtner mehr in den HERA Hallen Süd u. West
 - HERA Report (Rudimentäre Personenverfolgung)
 - Langfristige Protokollierung aller Zugänge für D3
-

Erreichte Meilensteine (2)

- **Einführung von DACHS Karten Kategorien**
 - incl. PIP u. DARF-DACHS Erweiterungen
 - **Hardware Installationen**
 - LINAC II, PIA, DESY II
 - FLASH (Anbindung weiterer Türen in Halle 3 Anfang 2010)
 - **Installation u. Inbetriebnahme CMS Kontrollraum**
 - **Installation u. Inbetriebnahme PETRA III**
 - Teure USV + Notstrom Erweiterungen in den alten PETRA Hallen
 - **BKR Unterstützung für Zeitweisen Zugang (ZZ)**
 - LINAC II, PIA, DESY II, PETRA III, FLASH
 - **Echtzeit Abfrage auf gültige Unterweisungen**
 - **Anbindung DOOR u. ASIP (PC gestützte Unterweisungen)**
-

Statistik August 2009

incl. PETRA III Experimente

- Weitestgehend störungsfreier Betrieb seit August 2008
- Probleme mit HERA Terminals nach Stromausfällen
- Vandalismus, Defekt eines Ausweisdruckers

Beschleuniger Gebiete	6
Experimente Gebiete	> 40
Sonstige Gebiete	4
Terminals	> 60
Dezentrale Controller mit lokaler Intelligenz	> 20
6020 Lizenzen für Karten	3000
Ausgehändigte Karten	> 1300
Buchungen / Monat	> 5000
Fehlgeschlagene Zugänge / Tag	< 1

DACHS Team (1)

Wer	Gruppe	Was	Zeit [h/Woche]
T. Tempel	IT	DARF-DACHS	> 30
S. Brinker	MPY	Organisation	> 15
S. Lessmann-Bassen	FS-BT	PETRA III-Exp.	8
C. Kluth	MPY	Organisation, Server	15
P. Hopf	MBB	Hardware	4
M. Bieler	MBB	Hardware, Betriebsvereinbarung	2
B. Poljanecwicz	MPY	Server	2
G. Fellbaum, W. Parys, Pfortner	V	Kartenerstellung	2

DACHS Team (2)

Wer	Gruppe	Was
D. Ramert	MPS	Grundlegende Planung, Sonderlösungen HERA, HASYLAB
J. Kreuzkamp	IPP	PIP
B. Lange, M. Moe, U. Kirsch	FEPOS	Hardware (Installation, Wartung)
N. N.	MPS	Interface Interlock – DARF-Dachs
J. Doberenz, R. Lami	V	Kartenverwaltung, Personendaten, Betriebsvereinbarung
H. Falkenberg, C. Apfel	IT	Oracle, Dosimeter Datenbank
J.-P. Kurz	FS-EC	Anbindung DOOR, ASIP
H. Förster, M. Steckel, F. Reuther	IT, MDI	Kabel
A. Labbudda	MCS	BKR-Applikation
M. Fleck	FS-EC	Experimente-Kontrollen
Ca. 50 Administratoren	diverse	DARF-DACHS
Ca. 25 Administratoren	diverse	PIP

22.9.2009

DACHS - S. Brinker, C. Kluth

39

Kosten bis Sommer 2009 in k€

■ Interflex	230
□ Erstausrüstung	80
□ PETRA III Acc.	40
□ PETRA III Exp.	90
□ Rohlinge usw.	10
□ Sonstiges	10
■ Kabel verlegen (IT)	10
■ Kabel verlegen (MDI)	10
■ Summe	250
■ DESY Personal	2,5 FTE / Jahr

22.9.2009

DACHS - S. Brinker, C. Kluth

40

Kommende Meilensteine

- Vollständige Inbetriebnahme der Gebietsabsuche bei den PETRA III Experimenten
 - Sehr intensiv diskutierte, letztendlich sehr elegante Lösung MPS System + DACHS als Trigger
 - Erste Tests erfolgreich
 - Personensicherheit verbleibt ausschließlich beim Personeninterlock
 - PETRA III Experimente Labore
 - FLASH Container
 - Einführung günstiger Offline Terminals
 - Vervollständigung der Hardware Installationen
 - DESY II, FLASH
 - Vollständige Inbetriebnahme L2, PIA, D2, FLASH
-

22.9.2009

DACHS - S. Brinker, C. Kluth

41

Geplante Aktivitäten noch in 2009

- Zeuthen
 - PIZ u. Rechenzentrum
 - Mahnwesen in DARF-DACHS
 - Ablösung der HERA Sonderprogrammierung
 - Umstellung auf Interflex Standardlösung
 - Umbau HERA Halle West
 - Anbindung der Dosimeter Datenbank
 - IT baut eine neue DB für D3 auf
-

22.9.2009

DACHS - S. Brinker, C. Kluth

42

Geplante Aktivitäten in 2010

- Bibliothek Hamburg
 - Nach dem Umzug Geb. 1A → 1D
 - Zugang
 - Ablösung des Bibliotheksausweises
 - Upgrade 6020 → 6040
 - Große Umstellung zu Gunsten der Betriebssicherheit
 - Direkte Unterstützung relationaler Datenbanken
 - Web-Techniken
 - Einbindung von EMBL (mittels DOOR?)
-

Weitere Themen

- PC gestützte Beschleuniger Unterweisungen
 - ASIP für alle (Entlastung u.a. von MBB)
 - direkte Anbindung an DARF-DACHS ohne DOOR
 - GKSS (mittels DOOR?)
 - MPG (mittels DOOR)
 - AMTF
 - CMTB
 - CFEL
 - CSSB
 - XFEL
-

URLs

- DACHS (deutsch)
 - <http://dachs.desy.de>
- DARF-DACHS login
 - <https://registry.desy.de/PersonProperties/>
- PIP login (DACHS Support)
 - https://www-z.desy.de/ipp/PIP/PIP_DACHS_WEBAPP/



Vielen Dank für Ihre
Aufmerksamkeit!

Diskussion