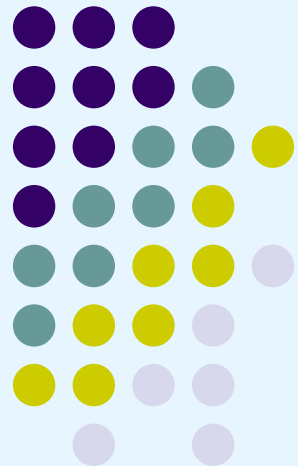
Identitätsmanagement

als Voraussetzung für serviceorientierte, integrierte IuK-Infrastrukturen

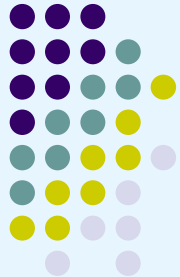
Gerhard Schneider

Rechenzentrum Uni Freiburg

gerhard.schneider@rz.uni-freiburg.de



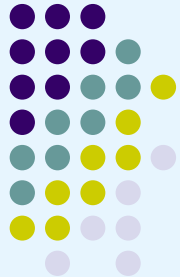
Identitätsmanagement – wozu?



- Das Gehalt zahlt der Staat
- Die Studenten zahlen eh nichts ☺
- Jede Menge Gäste, die „einfach so“ am Wissenschaftsbetrieb teilnehmen
  - Und dabei auch unverzichtbar sind!
- Unorganisiertes Chaos hat sich über Jahrhunderte bewährt

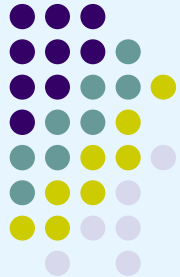
- *Naja, manchmal wird was geklaut*
- *Keiner weiss, wer den mp3-Server betreut*
- *Und häufig erfährt man nicht, was los ist*

Identitätsmanagement – wie?



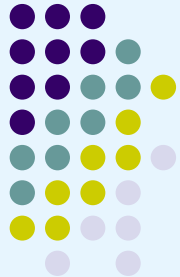
- Sollte unterschieden werden vom Datensammeln!
  - Es nicht wirklich nicht notwendig, alle Aktionen einer Identität zu speichern und 20 Jahre aufzuheben.
- Ein Mensch kann mehrere Identitäten haben – vor allem an der Uni
  - 50% Uni / 50% Drittmittel
  - Mitarbeiter / Gasthörer
- Man muss auch nicht immer wissen, wer sich hinter einer Identität verbirgt.
- Wichtig ist hingegen:
  - Ist die Identität noch gültig?
  - Darf die Identität eine Aktion durchführen?
- Heute: statt theoretischer Überlegungen ein paar funktionierende Beispiele aus der Praxis

Denn die Zeiten ändern sich…



- In „grauer“ Vorzeit:
  - Dürfen Studierende überhaupt ans Internet?
  - Dürfen Studierende denn emails verschicken?
  - Wozu benötigen Studierende einen Rechner-Account?
  - Wer bezahlt die Infrastruktur?
  - Dezentralisierung der DV ist Trumpf!
- Heute:
  - Warum kann das Rechenzentrum nicht mal eben an alle Studierenden eine Mail schicken – die Universität muss Portokosten sparen!
  - Warum führt das Rechenzentrum keine email-Liste aller Professoren?
  - Warum … ?
  - Warum … ?
- Witzigerweise wurden/werden alle diese Fragen von denselben Personen gestellt!
  - Und zwischen „grauer Vorzeit“ und „heute“ liegen vielleicht 4-6 Jahre!

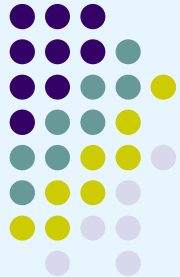
Die Folge: jeder löst das Problem für sich



- Immatrikulation – Aufnahme der Studierenden in eine Datenbank
- Rechenzentrumsaccount – Aufnahme der Studierenden in eine Datenbank
- Lehr- und Lernplattform – Aufnahme der Studierenden in eine Datenbank
- Chipkarten-Schließsystem – Aufnahme der Studierenden in eine Datenbank
- Bibliothek, usw. … …
- Die Daten sind niemals konsistent

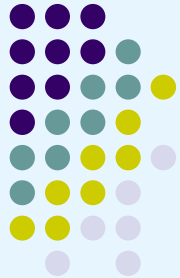
- *Das ist ja nicht so schlimm – schließlich ist es datenschutzrechtlich gut, wenn Daten nicht korreliert sind.*
- Aber man nun hat erkannt, dass man Studierende (= Kunden!!) auch mal erreichen will
- Und die Konsistenzhaltung der Datenbestände kostet echtes Geld (Personal)
  - Beispiel: Exmatrikulation – werden die Türöffnungsberechtigungen gelöscht?

Zentrifugalbewegungen dank fehlender Zentralinstanz



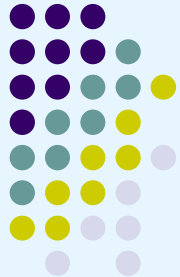
- Jedes System bringt eine eigene Termin-Verwaltung mit
- Jede Neuentwicklung beginnt mit einer eigenen Kalender-Verwaltung
  - Veranstaltungskalender in CLIX
  - Veranstaltungskalender der Fakultät
  - Veranstaltungskalender der Universität
  - Veranstaltungskalender der virtuellen Fachbibliotheken (DFG-gefördert)
- Niemand ist Willens, sich irgendwie einzufügen – und verschärft somit das Problem
  - Die Neuerfindung des Rades macht doch so viel Spaß!
- Welcher arme Nutzer kann in 20 Kalendern die Übersicht behalten?
  - Folge: sie werden ignoriert!

Das Chaos im Rechenzentrum



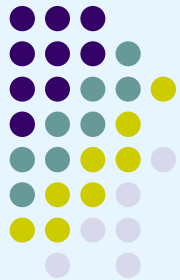
- Früher musste jeder auf die Mainframe
  - Zentrale Anlaufstelle für Logmsg, Mail und die Arbeit
- Heute ist es nicht mehr möglich, Nutzer gezielt zu informieren
  - Mailserver ist autark (falls er genutzt wird)
  - Den Login-Server benutzen nur „wenige“ – und keiner liest die Logmsg
  - Die Homepage des Rechenzentrums wird ignoriert
  - Die Hauszeitung des Rechenzentrums ist unbekannt
  - Und das Datennetz nutzt eh jeder, wie er will
- Witziger Nebeneffekt unseres Funknetzes (und seiner Festnetz-erweiterung sowie der Sicherheitsinseln):
  Nutzer muss sich – dank VPN – beim RZ wieder einwählen
  - Und erhält eine Logmsg
  - Endlich wieder ein Dienst, den man beim Rechenzentrum aktiv beziehen muss – und will! ☺

Das Chaos im Rechenzentrum



- Verschiedene Nutzerverwaltungen für unterschiedliche Systeme
  - Im Freiburger RZ gab es 2001 vier Nutzerverwaltungen
    - Ähnliches gilt für viele Rechenzentren (meines Erfahrungsschatzes)
- Ein Zusammenführen solcher Mehrfach-Verwaltungen ist nicht möglich:
    - Je länger die Experten tagen, desto nachhaltiger der Beweis für die Unmöglichkeit.
  - Angeführte Gründe können sein:
    - jeder möchte die Vorzüge seines Systems vorführen und die Vorzüge sind nicht auf die anderen übertragbar
    - Das alte Chaos ist doch so praktisch, denn die Verwaltungen sind so schön programmiert und richten alles selber auf den Maschinen ein, Änderungen bringen alles durcheinander.
      - Nebeneffekt: der Datenbankrechner aus dem Jahr 1992 muss unter allen Umständen am Leben erhalten werden, sonst geht nichts mehr!
    - Grabenkämpfe zwischen Arbeitsgruppen
    - usw.

Das Chaos lichtet sich

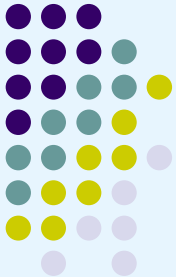


- Keine Lösung in Sicht? Doch!
  - Back to the roots – hin zum alten System einer „dummen“ zentralen Instanz und
  - Anordnung, dass die Rechnersysteme sich bitte von dort die Daten holen und selber entscheiden, was sie damit tun.
    - Vorteil: problemlose Integration neuer Rechner, da die zentrale Instanz deren Eigenarten nicht berücksichtigen muss
    - Entflechtung der organisatorischen Knoten
  - Dienstanweisung: Accounts dürfen nur angelegt werden, wenn sie in der zentralen Instanz vorhanden sind.
- Die Widerstände sind nicht unerheblich
  - Die Funktionalität wird zunächst wirklich schlechter
  - Es ist einiges an „Exportfunktionen“ zu schreiben
  - Und hier lohnt sich der Einsatz externer Unternehmensberater ☺
    - Nur so können alte Zöpfe erkannt und abgeschnitten werden.

Ein Lichtblick

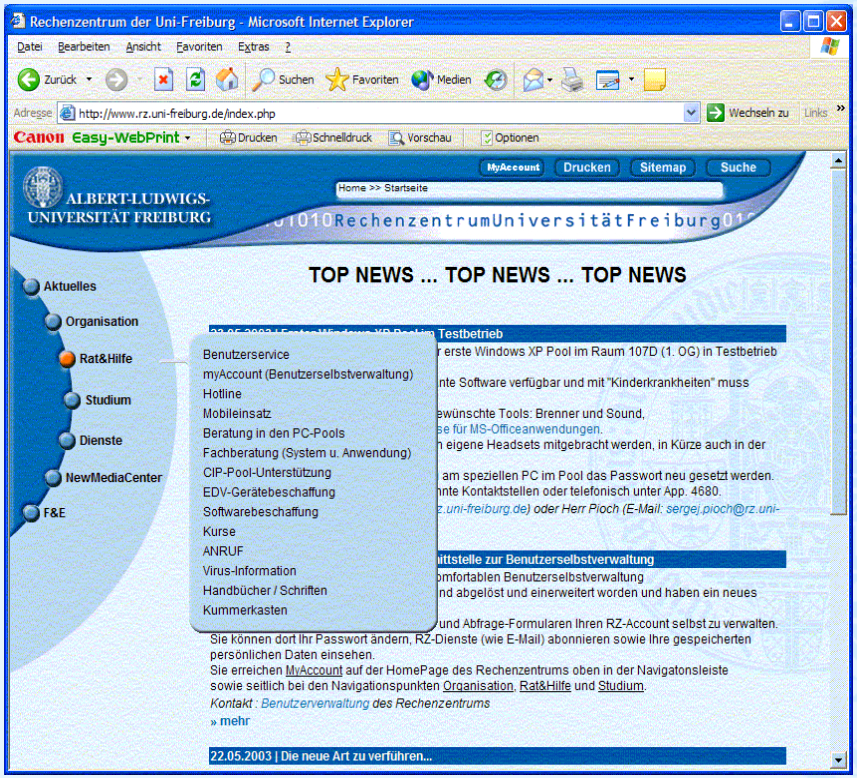
- Das ist ja nichts Neues – also muss es Lösungen geben
- Eine Lösung, die recht einfach ist, heißt LDAP
  - Lightweight directory access protocoll
  - „doofe Datenbank“, die nur Nutzer verwalten kann und sonst zu nichts in der Lage ist.
    - Ich bitte die plakative Übertreibung zu entschuldigen
  - Man kann schnell lesen und nur langsam schreiben
    - Ein Märchen aus alten Zeiten, das die Leistungsfähigkeit eines Notebooks geflissentlich ignoriert
  - Und man kann sogar gegen LDAP authentifizieren (single signon)
- Also Umstellung der Nutzerverwaltung auf LDAP
  - Aber so, dass möglichst wenig RZ-Spezifika fest einprogrammiert werden!
  - Denn vielleicht kann man mit LDAP noch mehr und den Weg darf man sich nicht verbauen

Freiburger Ansätze



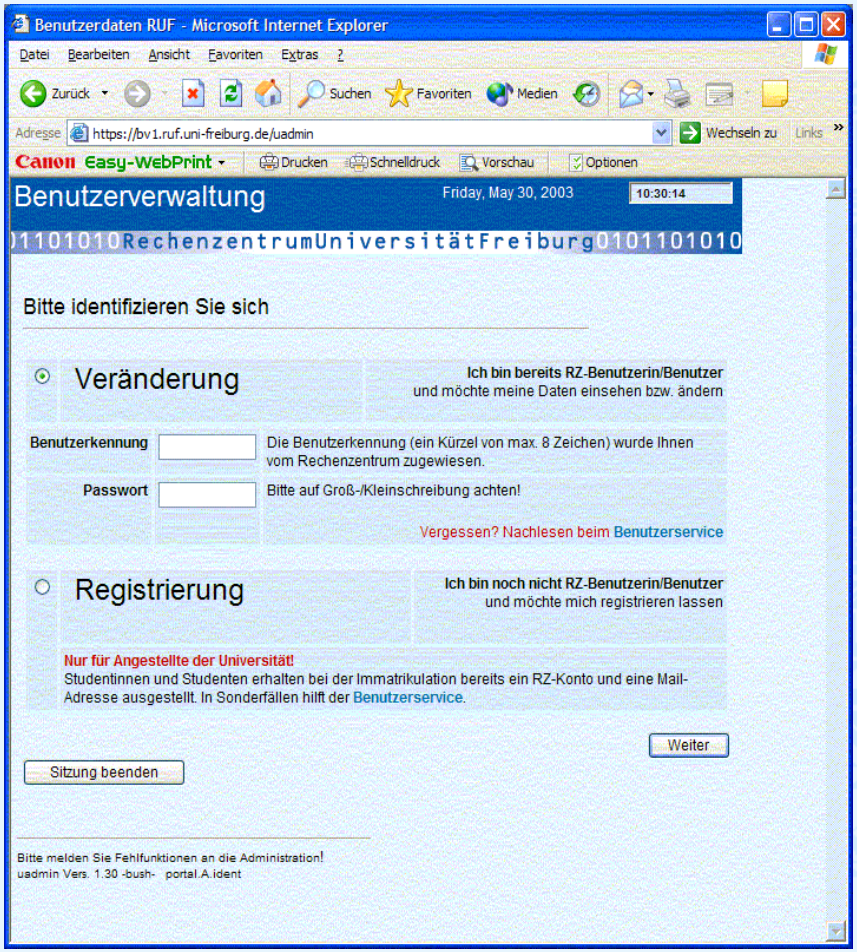
- „Single sign-on“ (ein Passwort für alle Rechner)
  - Scheitert meist an der mangelnden Kooperation der Betriebssysteme
- Freiburger Lösung: Passwortänderung über WWW-Maske, neues Passwort wird jedem einzelnen Dienst „beigebracht“
  - Derselbe Ansatz wie schon beschrieben – Verlagerung der Probleme nach außen erlaubt „einfache“ Lösung
  - Nicht gerade state-of-the-art, aber funktional!
  - Grundlage für die weiteren Lösungsansätze
- Accountvergabe möglichst im do-it-yourself-Verfahren
  - Mitarbeiter sind einem anderem LDAP bekannt!
    - Durch Export der relevanten/unkritischen Daten aus HISPOS
  - Gegen diesen LDAP werden die selbst eingegebenen Daten geprüft und ein Brief mit dem Erstpasswort generiert
    - Zweiter „secure channel“

Benutzerselbstverwaltung „myAccount“



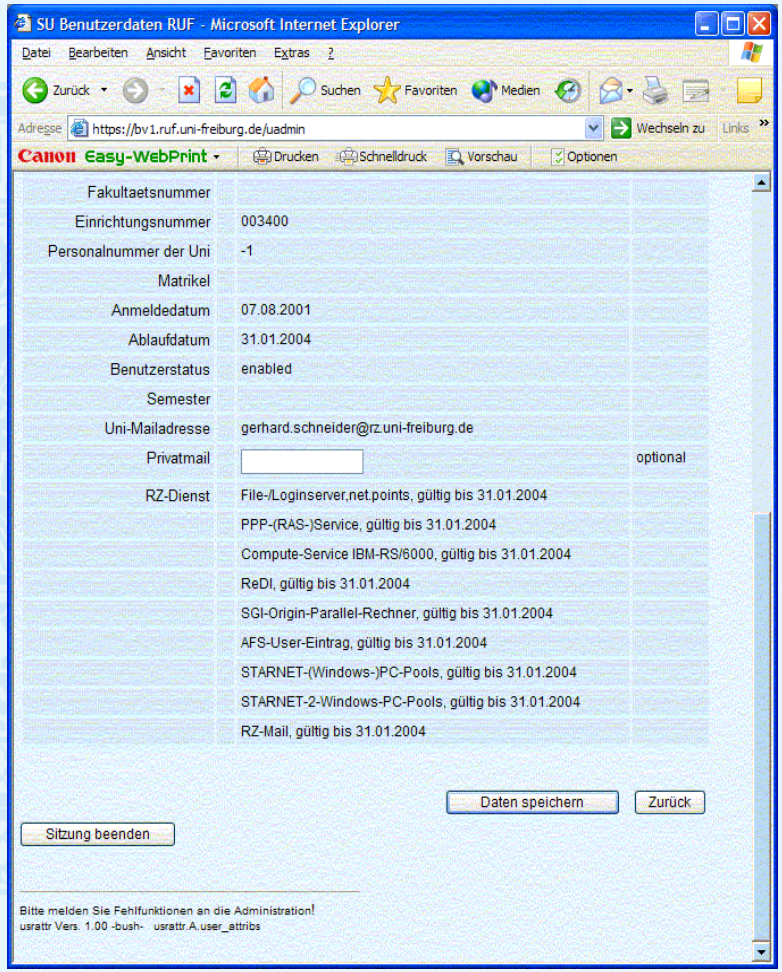
- Je mehr Daten ein Benutzer selbst eingeben kann, desto erträglicher ist der Gesamtaufwand für das Rechenzentrum
- Möglichst eleganter Zugang zu den gespeicherten Daten ist Voraussetzung
- Authentifizierung über RZ-userid und RZ-Passwort ist ausreichend
- Studierende erhalten inzwischen bei der Erstimmatrikulation einen Account

Benutzerselbstverwaltung „myAccount“

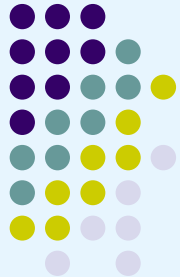


- Eigentlich ein uralter Hut…. Aber man muss es tun
- Diese Maske ist direkt von der RZ-Homepage zugänglich
  - Und damit leicht zu finden.
- LDAP-Daten können so verändert werden
- Nachts laufen Batch-Jobs, die die Änderungen auf die einzelnen Systeme übertragen

Benutzer-Selbstverwaltung „myAccount“



„myAccount“ und die Folgen

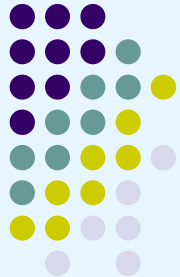


- Import der Daten in die Microsoft ADS
  - Damit Übernahme der Nutzerdaten in die Verwaltung der Instituts-ADS-Inseln
    - Lokale Nutzerverwaltung nicht mehr nötig, nur noch ein „Freischalten“
    - Beim Ausscheiden eines Nutzers automatische Löschung auch im Institut!
- Erkenntnis: man kann offenbar eigene Daten authentifiziert selbst verwalten, ohne großen Aufwand
  - Beispiel: die eigene Telefonnummer
    - Wozu dies über eine Zentrale erledigen?
    - Daraus könnte dann ein Telefonbuch erzeugt werden
      - ☻ Softwarepraktikum für Studenten

„myAccount“ und die Folgen

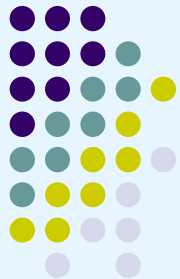
- Man kann nun eine offizielle Mailadresse angeben für Dienstpost
  - Egal, ob die Uni-Adresse oder eine private Mailadresse
  - Diese Mitarbeiter und Studierenden kann man nun per email informieren
  - Spannende Frage: wie überzeugt man Studierende, eine Mailadresse verbindlich festzulegen???
    - Meiner Meinung nach nur über Geld – reduzierte Rückmeldegebühr (eine Verwaltungsgebühr!)
    - Juristen wissen, dass dies unmöglich ist!
- Abonnement von Informationslisten
  - Asta, Fakultät, etc…..

„myAccount“ und die Folgen



- Auch ASTA, Fakultät, etc. wollen Mails verschicken
  - Anfrage ans RZ habe ich immer sehr zurückhaltend beantwortet – wo ist denn der Unterschied zu SPAM?
- Durch Ankreuzen der Aboliste wird Interesse erklärt
  - das Opt-in-Verfahren ist juristisch sauber
  - Bei Erstimmatrikulation wird man darüber aufgeklärt, dass man auf alle relevanten Listen eingetragen wurde
    - „scharf“ wird das erst durch Erklären der zuverlässigen email-Adresse wie vorhin beschrieben
    - Aus der „Rektoratsliste“ kann man sich nicht austragen!
    - Derzeit in Entwicklung ☻ Softwarepraktikum für Studenten
- Dringende Empfehlung: jede Liste sollte sich eine Selbstbeschränkung auferlegen
  - Z.B. max. 10 Sendungen pro Jahr

„myAccount“ und die Folgen



- Weitere Projekte:
- Selbsteintragen in Seminar- und Kurslisten
  - Dummy-Einträge (Micky Maus) und „*ich trag dich mal auf Verdacht ein*“ nicht mehr möglich
- Verwaltung von Leih-Geräten
  - Digitalkamera, etc
  - Weitergabe an andere Unimitglieder nun unmittelbar ohne Rückgabe ans RZ möglich
    - Wenn sich Alt- und Neubesitzer authentifizieren – wozu denn noch das RZ einschalten?
- „Inventarisierung“ von nicht-inventarisierbaren DV-Teilen
  - USB-Speicherstick vom RZ an Mitarbeiter ausgeliehen
  - Dafür ist eine Serien- oder Inventarnummer nicht notwendig, sondern nur eine abstrakte Teilekennung!
    - Vorläuferversion in Göttingen erprobt ☺

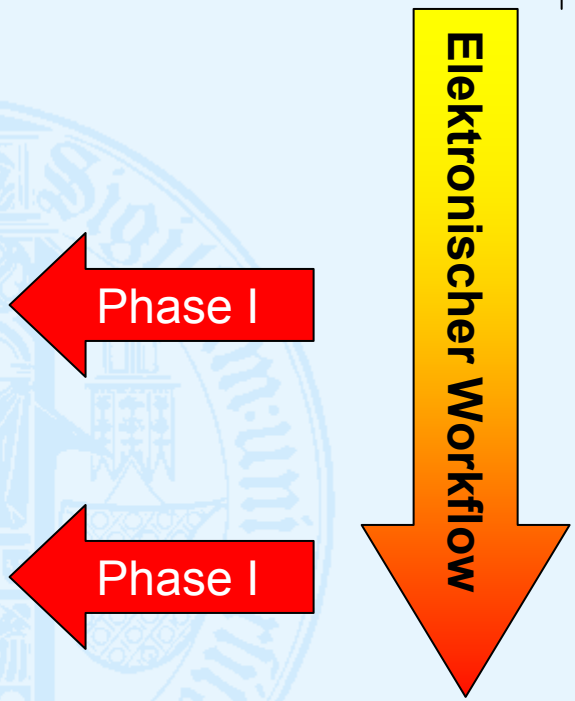
Die Dynamik nimmt zu

- Freiburg hat die Chipkarte
  - Mifare-Chip zum Bezahlen und für Türschließer
  - Cryptochip für Signatur
  - Für Mitarbeiter und Studierende
    - Für Mitarbeiter derzeit wahlfrei
- Aber: *jemand* weiss offenbar, ob die Karte noch gültig ist!
- Und: sie wird in anderen Bereichen eingesetzt!

www.uni-freiburg.de/unicard

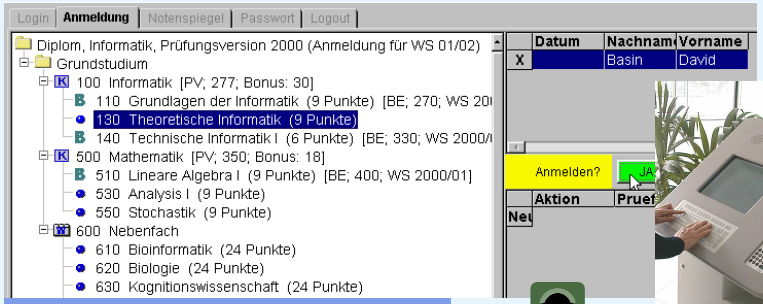
Hauptprozesse der Studierendenverwaltung

- Vorberatung
- Studienplatzvergabe / Zulassung
- Immatrikulation
- **Rückmeldung**
- Studienbegleitende Beratung
- Ausbildung/Lehre (Neue Medien)
- **Prüfungen**
- Exmatrikulation

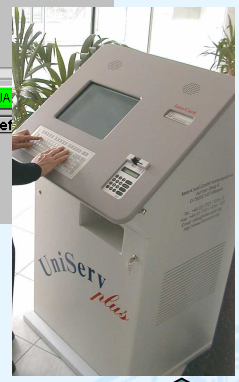


- BAFÖG-Teilerlass
- Service-Funktionen: Bezahlen, Zugang zu Rechnern, Zutritt zu Räumen

Ansicht SB-Station



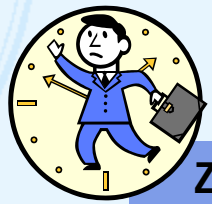
Studierendenverwaltung Prüfungswesen



Authentisierung, Digitale Signatur

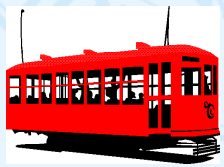
Bibliothek

Zutrittsberechtigung



Zeiterfassung

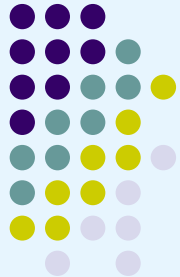
Mensa / Cafeteria Verpflegungsautomaten



Stammkarte Semester-Ticket

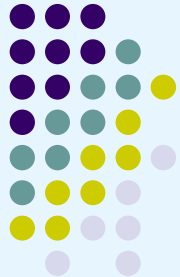
Kopieren Drucken

Identitätsmangement wird greifbar



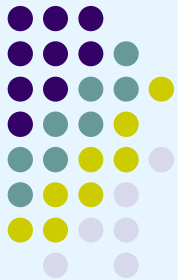
- Ist die KartenID im LDAP gespeichert, so sind RZ-LDAP und Karten-Datenbank synchron
  - Datenabgleich einmal pro Nacht reicht!
  - Und so kann jede Applikation den LDAP befragen, ob eine Karte noch gültig ist
- Wenn das Türschließsystem den LDAP befragt, dann können Berechtigungen sehr schnell widerrufen werden
  - Aufklärung von / Auftrag an Siemens ☺
  - Die Profile verbleiben im Türschließsystem!
- Login ins Funknetz per Unicard
  - Studienarbeit – und ein dickes Lob für den Studenten!
  - Gleichzeitig Basis einer PKI (LDAP-basiert)

Identitätsmanagement wird greifbar



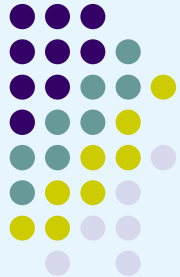
- Die Unicard ist nicht alles
  - Es gibt eine Reihe von netten Diensten, für die sie einfach unfunktionaler Overkill ist
    - Beispiel: Myaccount – dazu reicht userid/passwd
  - Aber ihre Nummer dient zum ID-Management
- Identitätsmanagement soll/muss globales Ziel sein
  - Aber nicht unter dem Aspekt der globalen Datenspeicherung
  - Sondern unter dem Aspekt „darf/darf nicht“
  - Dann können userid/passwd, Unicard, etc wunderbar koexistieren.
  - Und die personalrechtlichen Effekte eines Dienstes können davon unabhängig im Einzelfall verhandelt werden

Was fehlt noch ☹ ☹ ☹ ?



- Aber wie kommen die Daten in den LDAP?
  - Studentensekretariat setzt oft HIS ein
    - Export aus HIS nach LDAP ist machbar
  - Und Daten müssen teilweise zurück nach HIS!
    - Beispiel: Hat unser Studi eine verbindliche Mailadresse angegeben und daher ein Anrecht auf reduzierte Rückmeldegebühren?
- Warum benutzt HIS nicht LDAP als Datenbank?
  - Dann müssten wir weniger basteln!
- Derzeit wird ein Softwaremodell entwickelt (Softwarepraktikum ☺), das „unwichtige“ Daten außerhalb des zentralen LDAPs führt (Tree und Delegation)
  - Macht es für Datenschützer akzeptabler, wenn die kritischen Personaldaten nicht im allgemeinen Zugriff sind

Und die Datenschützer?



- Bemerkenswerter Ansatz der Studierenden im Softwarepraktikum:
  - Account wird mit Personaldaten „verheiratet“
    - Durch Abfragen von Informationen, bis ein Match entsteht, aber keine Datenspeicherung
    - Verbindung über Personalnummer, Matrikelnummer
  - Nutzer kann dann individuell veranlassen, dass/ob die persönlichen Daten aus der Personaldatenbank importiert werden sollen.
    - Ehrlich gesagt: muss ich als RZ wissen, wann der Nutzer geboren ist? Oder wo er/sie wohnt?
    - Freiwilligkeit hilft hier erheblich

Es gibt viel zu tun…
aber es ist lösbar!

Vielen Dank!