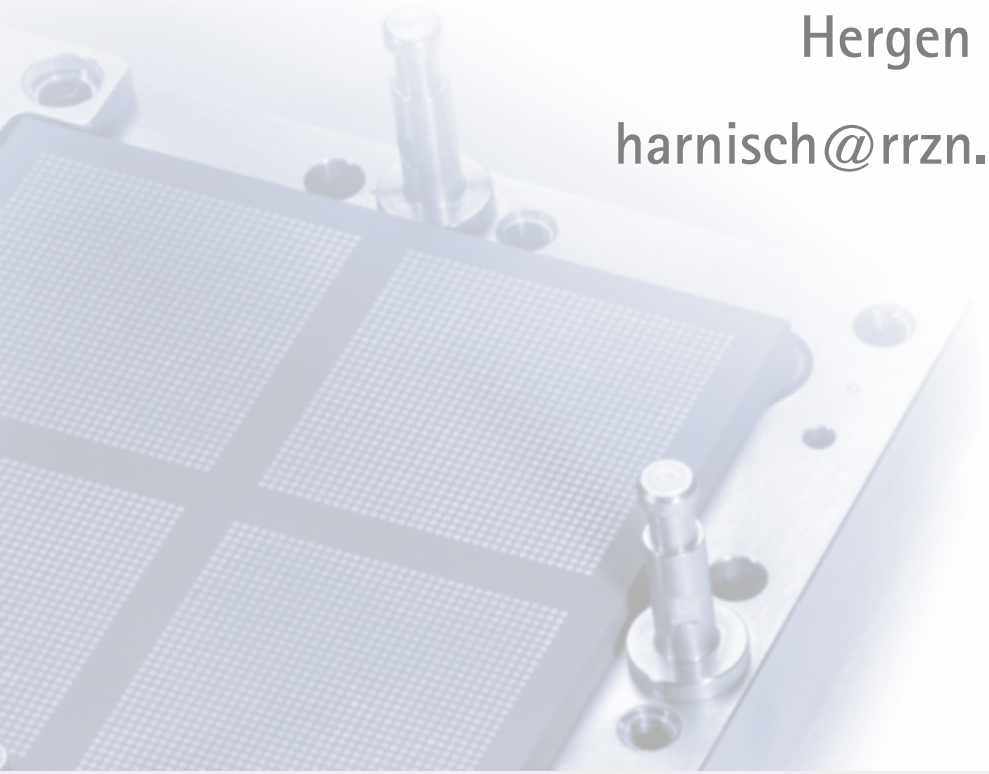
R|R|Z|N

Identitätsmanagement



Hergen Harnisch

harnisch@rrzn.uni-hannover.de

1 Einleitung:

- Zweck
- IdM-Architektur

2 Realisierungsstand

3 Website-Anbindung

4 Pool-Anbindung

5 Planungen

R|R|Z|N

Ist-Situation

neuer Nutzer

- Anmeldung im Institut für Bürorechner
- Anmeldung beim RRZN für WLAN & Email-Adresse (ORG.BEN)
- an StudIP durch `uni-hannover.de`-Email-Adresse

Nutzer geht

- Sperrung durch Institutsadministrator
- Abmeldung / Nicht-Verlängerung im RRZN durch Projektverantwortlichen
- teilweise (selten) laufen Logins aus, teilweise bestehen diese ewig

... und analog für Studierende

Einleitung: Zweck

Ziel

neuer Nutzer

- erhält bei Einstellung/Immatrikulation IdM-Login
- mit IdM-Login eigenständige Freischaltung weiterer Dienste
- Fokus auf zentralen Diensten:
  StudIP, WLAN/VPN, TIB/UB, EMail, CIP-Pools

Nutzer geht

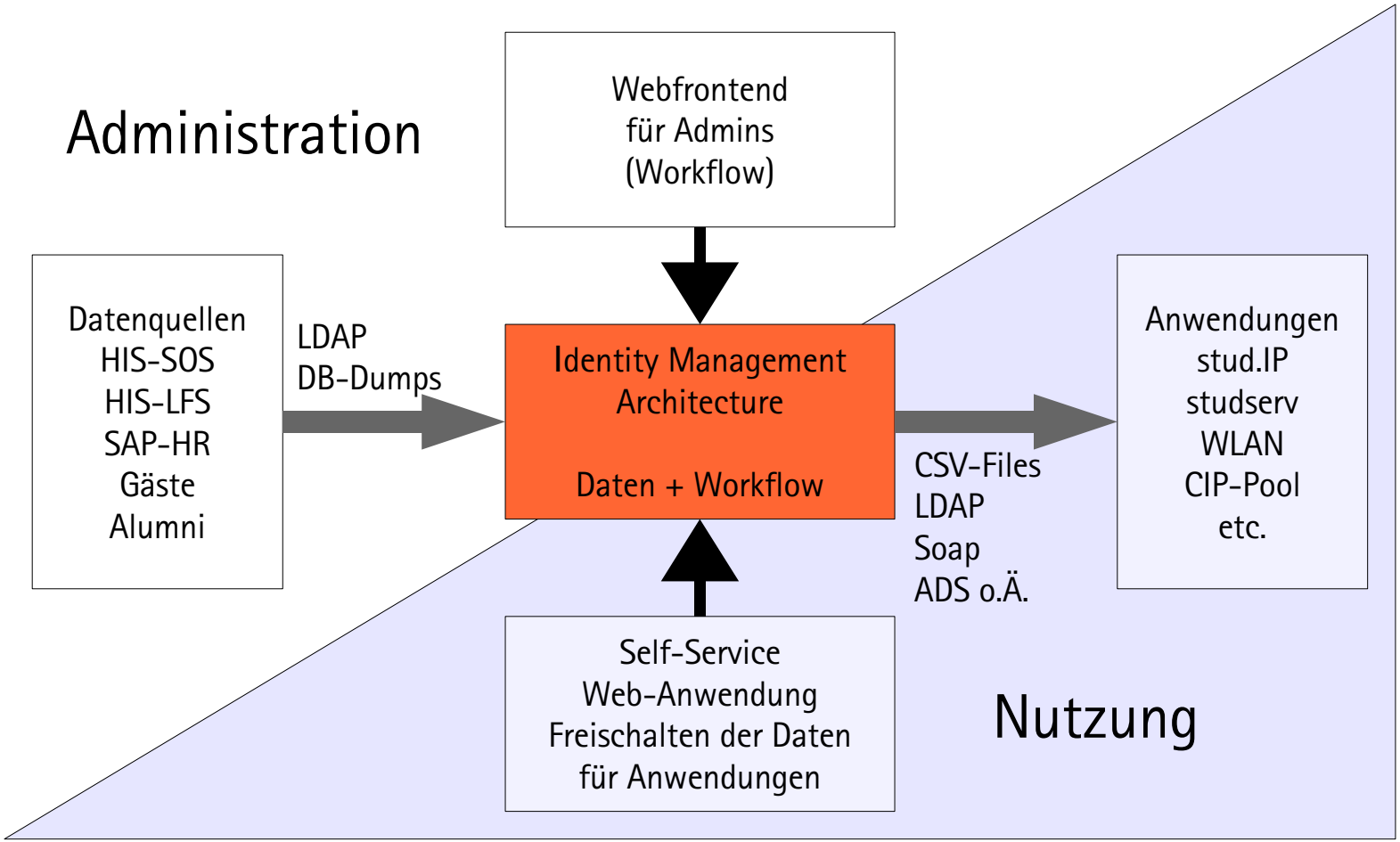
- direkte Zugänge werden gesperrt (z.B. WLAN)
- anderes nach Karenzzeit (z.B. Email)

... und das möglichst automatisch bzw. unaufwändig

Identitätsmanagement

- technischer Begriff
  - Identität meint einen Nutzer und seine IT-Logins & -Berechtigungen
  - zentrales System – Nutzerdatenbank mit Account-Verwaltung
- … natürlich nicht in irgendeinem philosophischen Sinne o.Ä.
- Zweck ist hauptsächlich
  - schnelle, zentrale Einrichtung & Löschung von Zugangsberechtigungen
  - klare, nachvollziehbare Daten über Nutzer
  - aber auch Vereinfachung für Nutzer (Self-Services wie Passwort-Rücksetzungen)

Einleitung: IdM-Architektur



R|R|Z|N

Designprinzipien

- sanfte Einführung (keine radikale Änderung von Prozessen)
- zentrale Authentifizierung, nicht Berechtigungen/Accounting
- nutzerzentriert:
  - Nutzer beantragt Dienste (& Diensteübersicht, Abmeldung)
  - Nutzer muss Datenweitergabe & Nutzungsbedingungen erst explizit zustimmen
- Datenschutz
  - Nutzerzustimmung
  - Verwendung von Pseudonymen
  - Anbindung von Systemen: Datensparsamkeit & Verfahrensbeschreibung
- Workflow, dezentrale Administration
- Stammdatenpflege weiterhin in HIS, SAP

Realisierungsstand

IdM an der LUH

derzeit nur reguläre Studierende im System

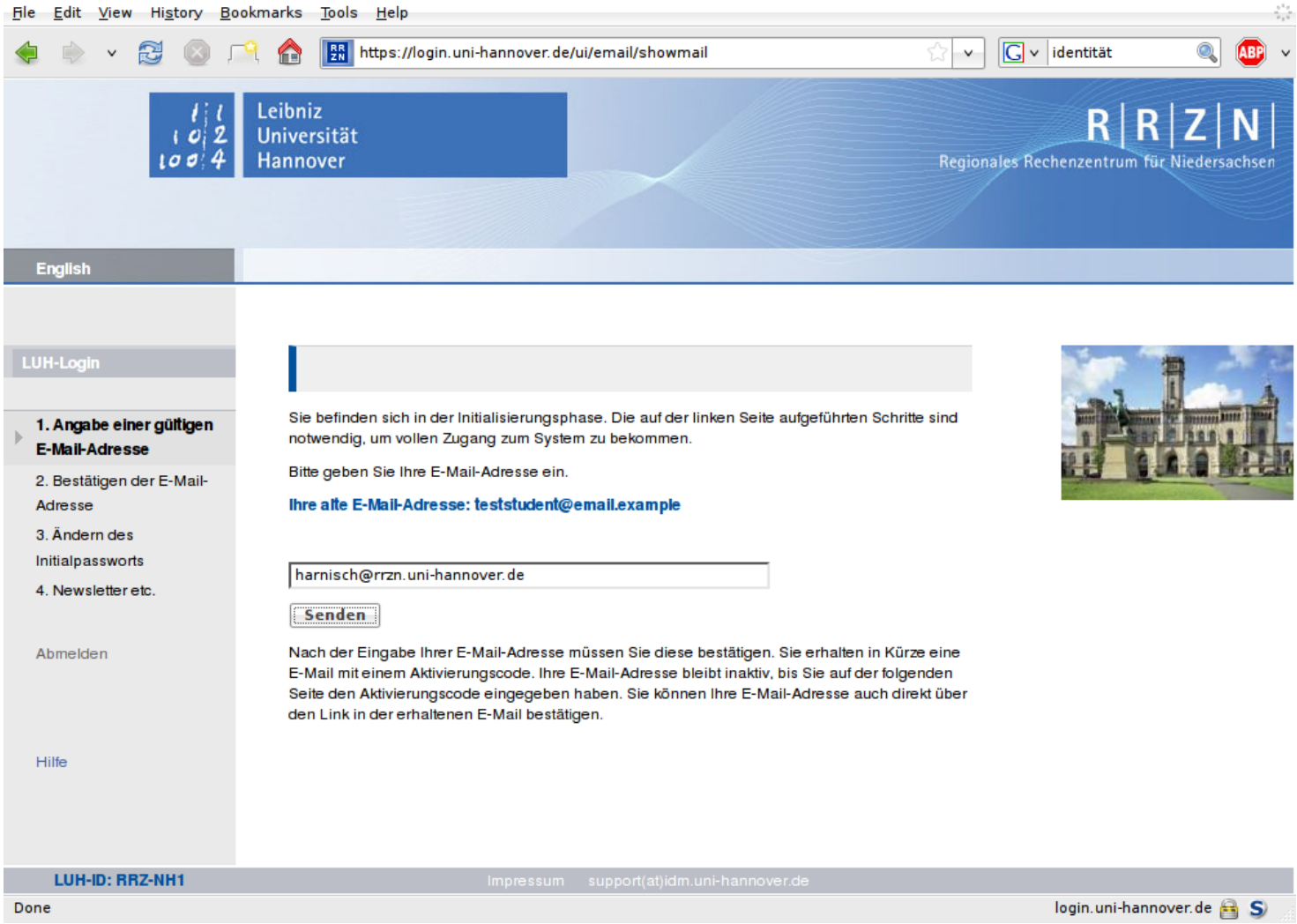
LUH-ID

Jeder Nutzer bekommt eine LUH-ID: RRZ-NH1, denn

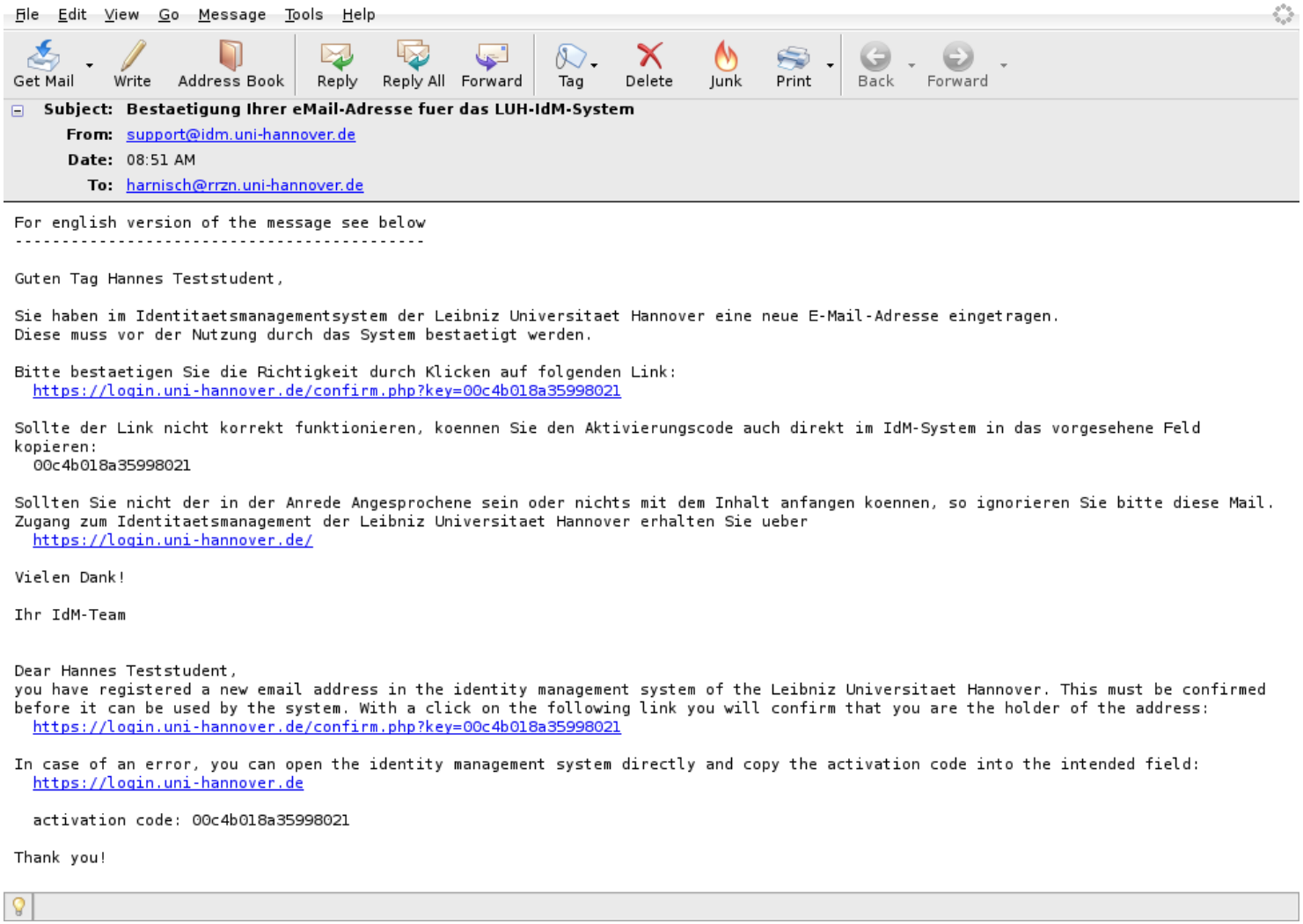
- sie wird nie wieder neu vergeben, also eindeutig
- sie ist kurz (6-stellig)
- enthält eine Prüfziffer
  $\longrightarrow$ Vertipper/-dreher erkennbar
- `meier2` wäre auch nicht schön
- LUH-ID lässt allein keine Rückschlüsse zu auf
  - Name, Geschlecht etc.
  - Student oder Mitarbeiter
  - Länge der Uni-Zugehörigkeit

Prüfprogramme & LUH-ID-Routinen vgl.
`https://login.uni-hannover.de/devinfo/luhid/`

Mail-Adresse



Mail-Adresse



File Edit View Go Message Tools Help

Get Mail | Write | Address Book | Reply | Reply All | Forward | Tag | Delete | Junk | Print | Back | Forward

Subject: **Bestaetigung Ihrer eMail-Adresse fuer das LUH-IdM-System**
From: support@idm.uni-hannover.de
Date: 08:51 AM
To: harnisch@rrzn.uni-hannover.de

For english version of the message see below

Guten Tag Hannes Teststudent,

Sie haben im Identitaetsmanagementsystem der Leibniz Universitaet Hannover eine neue E-Mail-Adresse eingetragen.
Diese muss vor der Nutzung durch das System bestaetigt werden.

Bitte bestaetigen Sie die Richtigkeit durch Klicken auf folgenden Link:
https://login.uni-hannover.de/confirm.php?key=00c4b018a35998021

Sollte der Link nicht korrekt funktionieren, koennen Sie den Aktivierungscode auch direkt im IdM-System in das vorgesehene Feld kopieren:
00c4b018a35998021

Sollten Sie nicht der in der Anrede Angesprochene sein oder nichts mit dem Inhalt anfangen koennen, so ignorieren Sie bitte diese Mail.
Zugang zum Identitaetsmanagement der Leibniz Universitaet Hannover erhalten Sie ueber
https://login.uni-hannover.de/

Vielen Dank!

Ihr IdM-Team

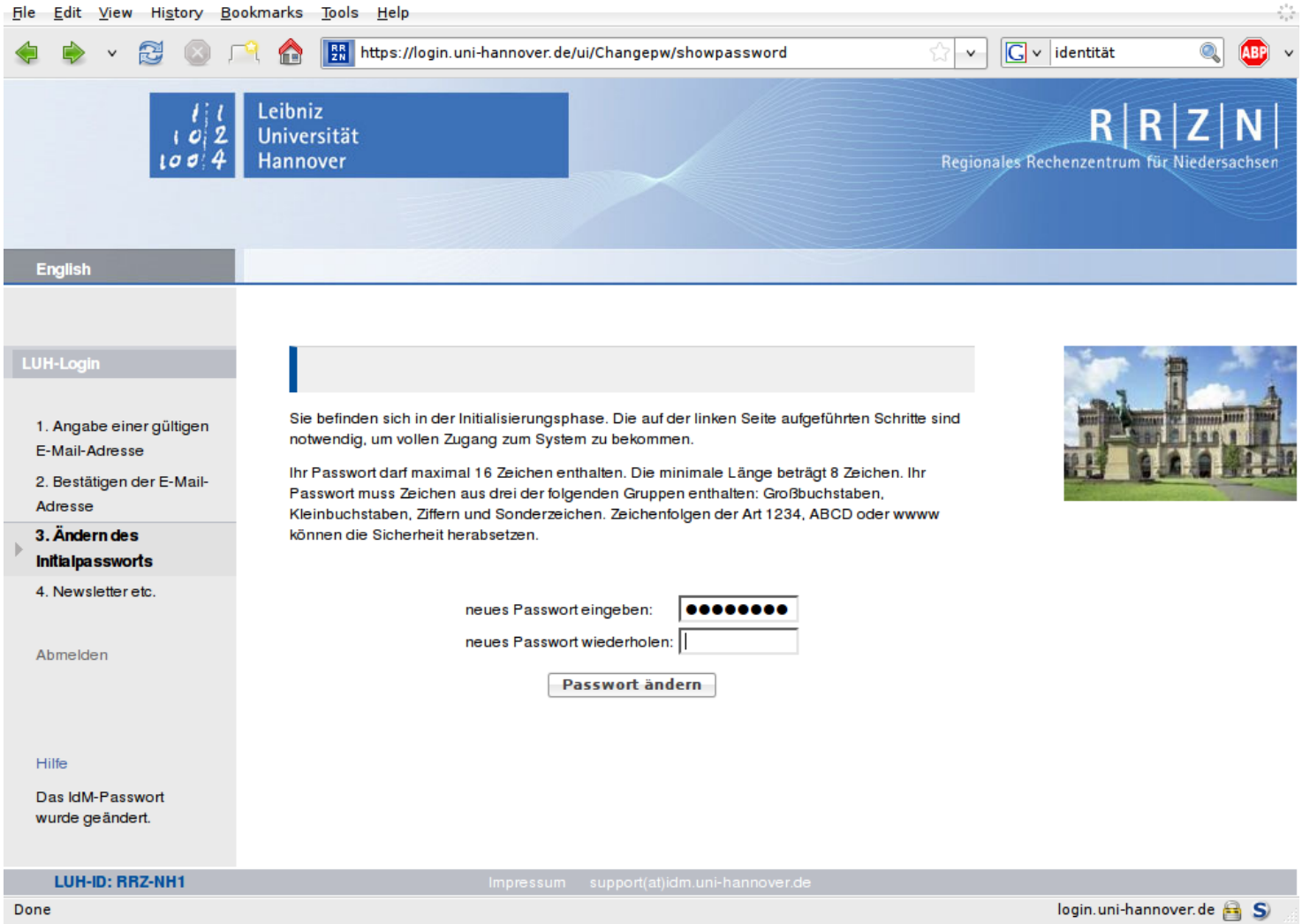
Dear Hannes Teststudent,
you have registered a new email address in the identity management system of the Leibniz Universitaet Hannover. This must be confirmed before it can be used by the system. With a click on the following link you will confirm that you are the holder of the address:
https://login.uni-hannover.de/confirm.php?key=00c4b018a35998021

In case of an error, you can open the identity management system directly and copy the activation code into the intended field:
https://login.uni-hannover.de

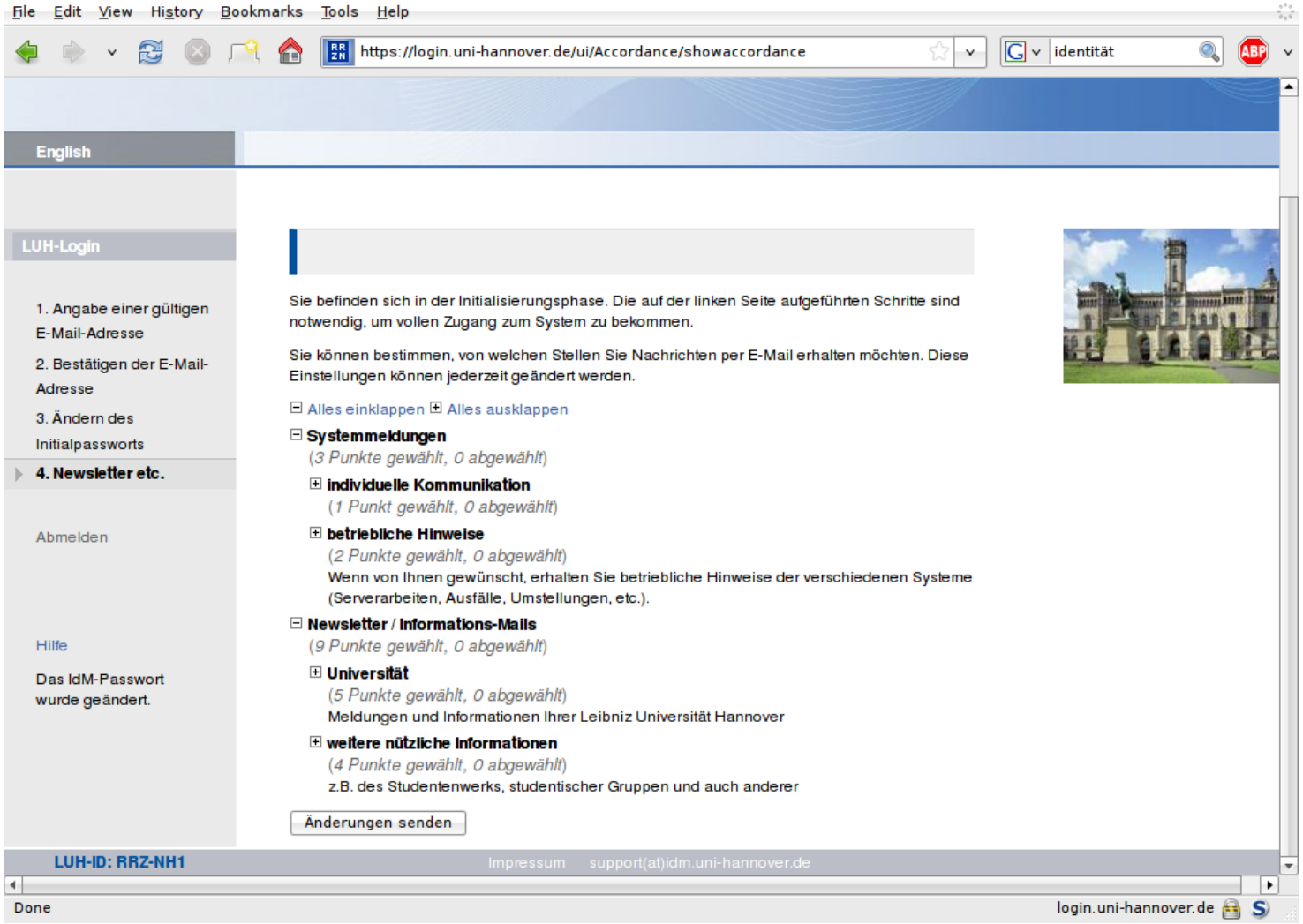
activation code: 00c4b018a35998021

Thank you!

Passwort


File Edit View History Bookmarks Tools Help
https://login.uni-hannover.de/ui/Changepw/showpassword
identität
Leibniz Universität Hannover
R|R|Z|N
Regionales Rechenzentrum für Niedersachsen
English
LUH-Login
1. Angabe einer gültigen E-Mail-Adresse
2. Bestätigen der E-Mail-Adresse
3. Ändern des Initialpassworts
4. Newsletter etc.
Abmelden
Hilfe
Das IdM-Passwort wurde geändert.
Sie befinden sich in der Initialisierungsphase. Die auf der linken Seite aufgeführten Schritte sind notwendig, um vollen Zugang zum System zu bekommen.
Ihr Passwort darf maximal 16 Zeichen enthalten. Die minimale Länge beträgt 8 Zeichen. Ihr Passwort muss Zeichen aus drei der folgenden Gruppen enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen. Zeichenfolgen der Art 1234, ABCD oder wwww können die Sicherheit herabsetzen.
neues Passwort eingeben:
neues Passwort wiederholen:
Passwort ändern
LUH-ID: RRZ-NH1
Impressum
support(at)idm.uni-hannover.de
Done
login.uni-hannover.de

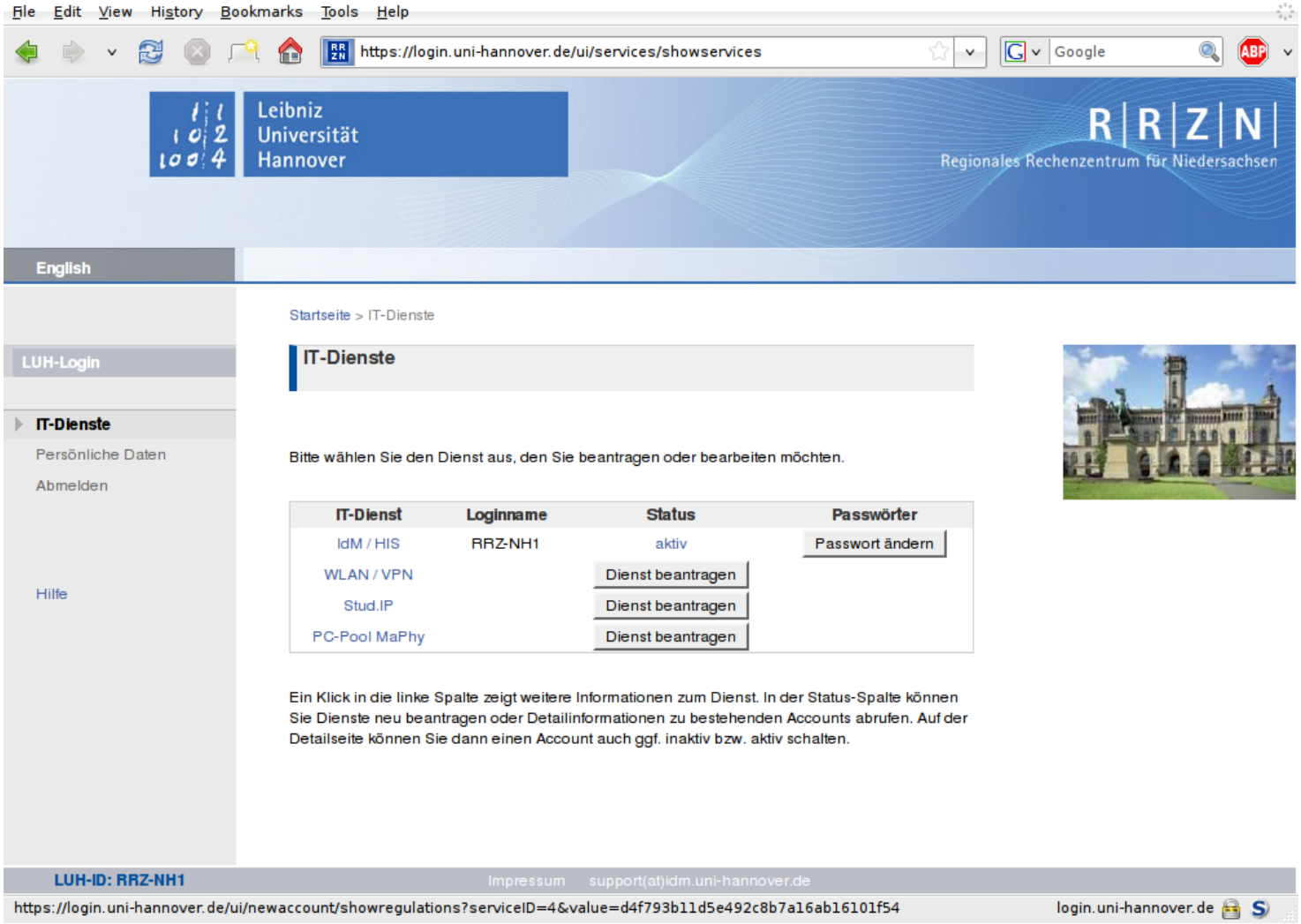
Verwendungszwecke E-Mail-Adresse



Realisierungsstand

1. Anmeldung an Webseite `https://login.uni-hannover.de`
2. Angabe / Korrektur der Mail-Adresse
3. Überprüfung der Mail-Erreichbarkeit
   - login-Seite ist aus unverschlüsseltem UHWLAN erreichbar
   - temporäres WLAN-Account zur UHWLAN-Nutzung für Mail-Abruf
4. Ändern des IdM-Passwortes (komplex wählen)
5. Verwendung der Mail-Adresse für Newsletter?
6. Freischalten für andere Dienste:
   - Stud.IP
   - WLAN / VPN
   - PC-Pools (derzeit nur Mathe-Physik)

Dienstefreischaltung



Dienste-Tabelle

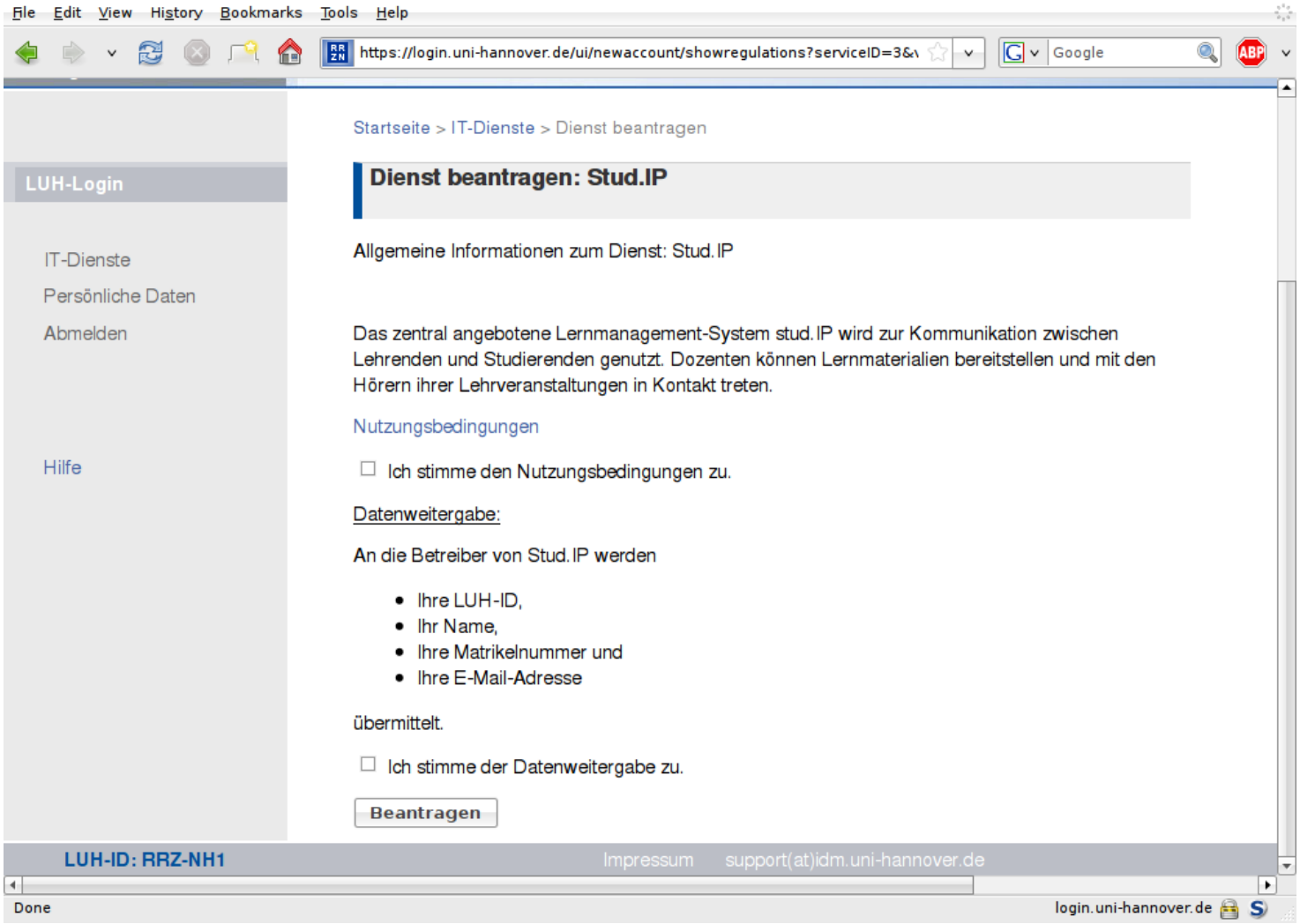
ist das eigentliche Kernstück:

- Übersicht der verfügbaren Dienste
- Informationen zu den Diensten
- Beantragung / Deaktivierung
- Passwort-Rücksetzung

hier später auch Passwort-Zuordnung bei PW-Gruppierung

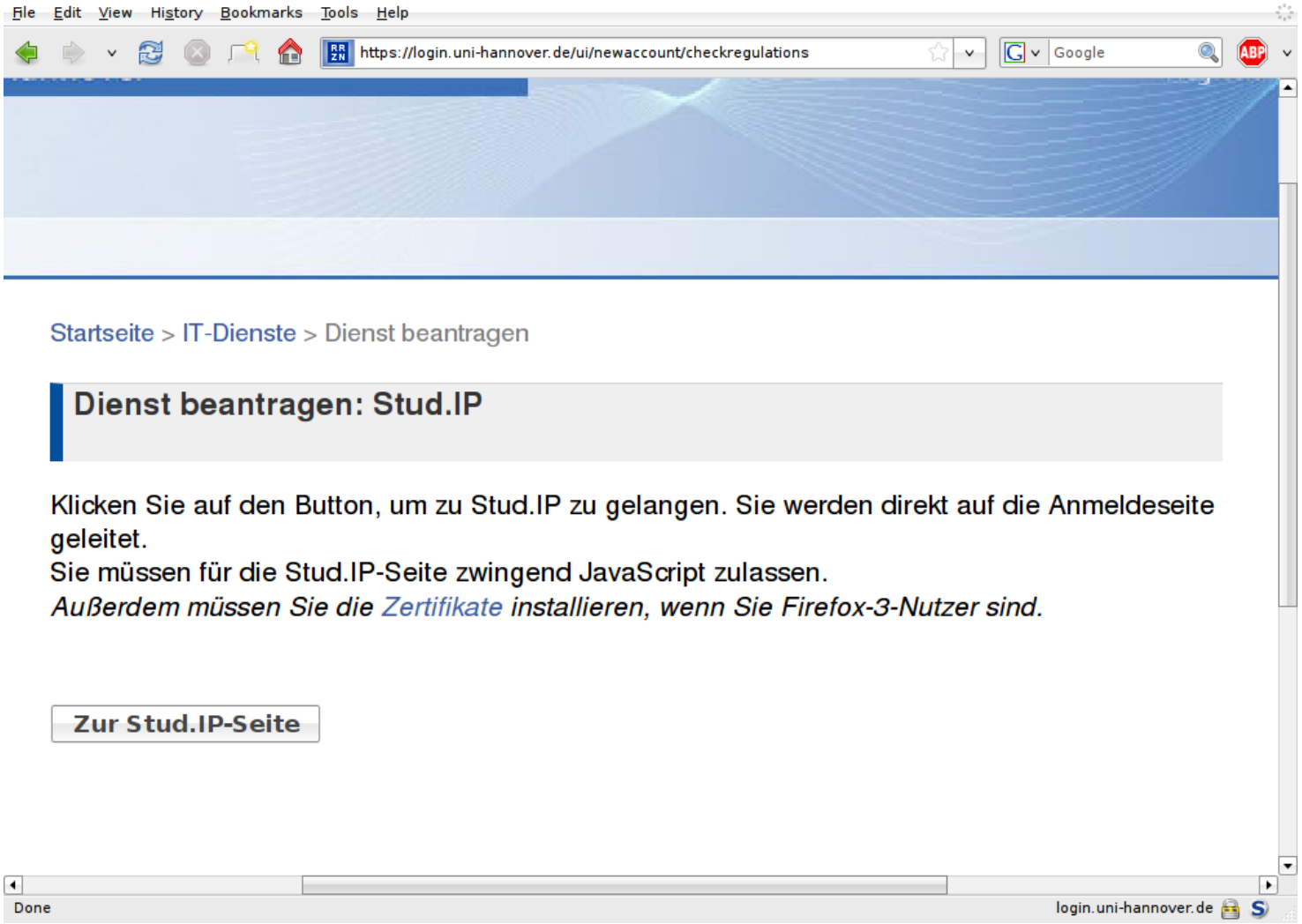
Realisierungsstand

Stud.IP



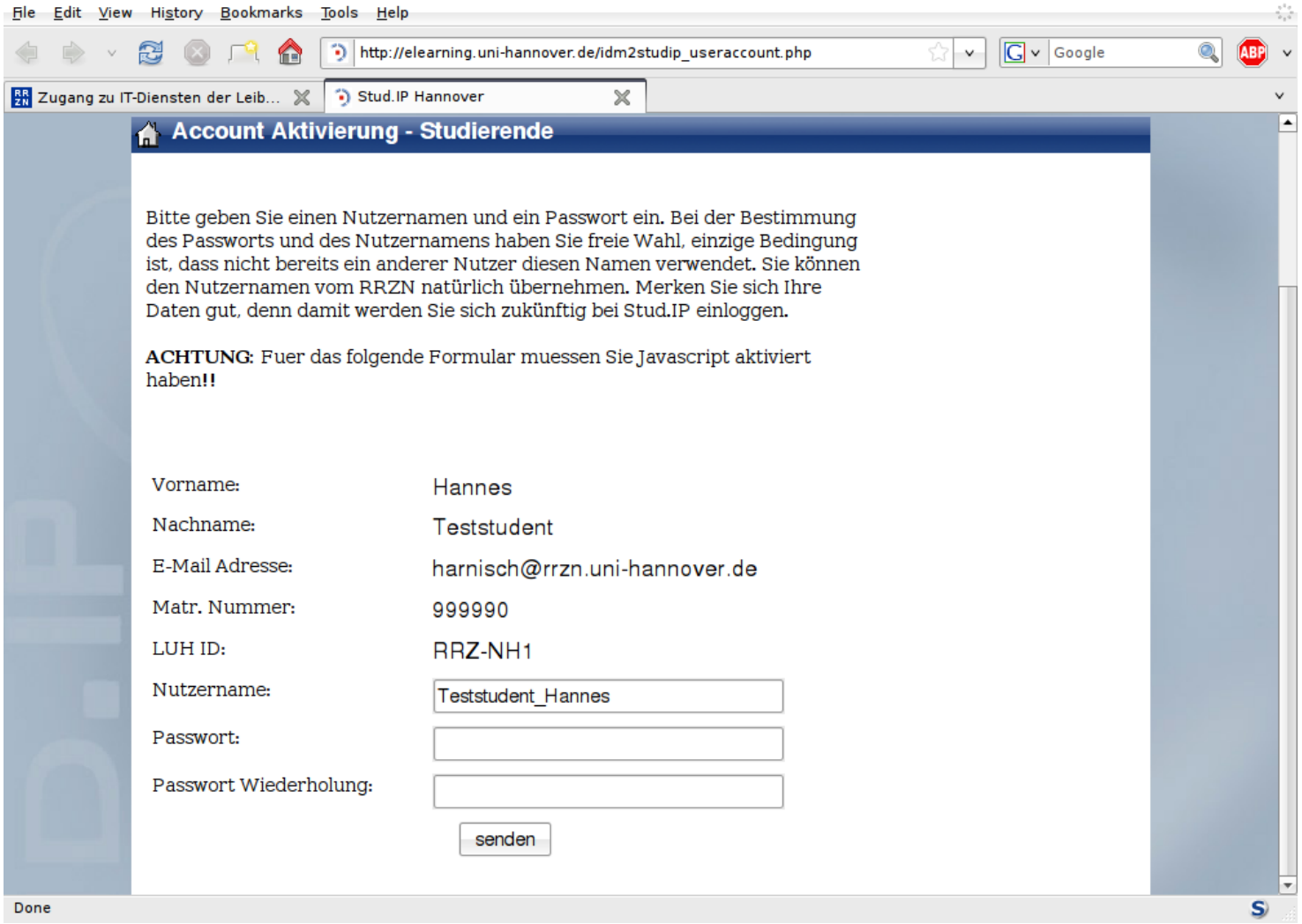
Realisierungsstand

Stud.IP



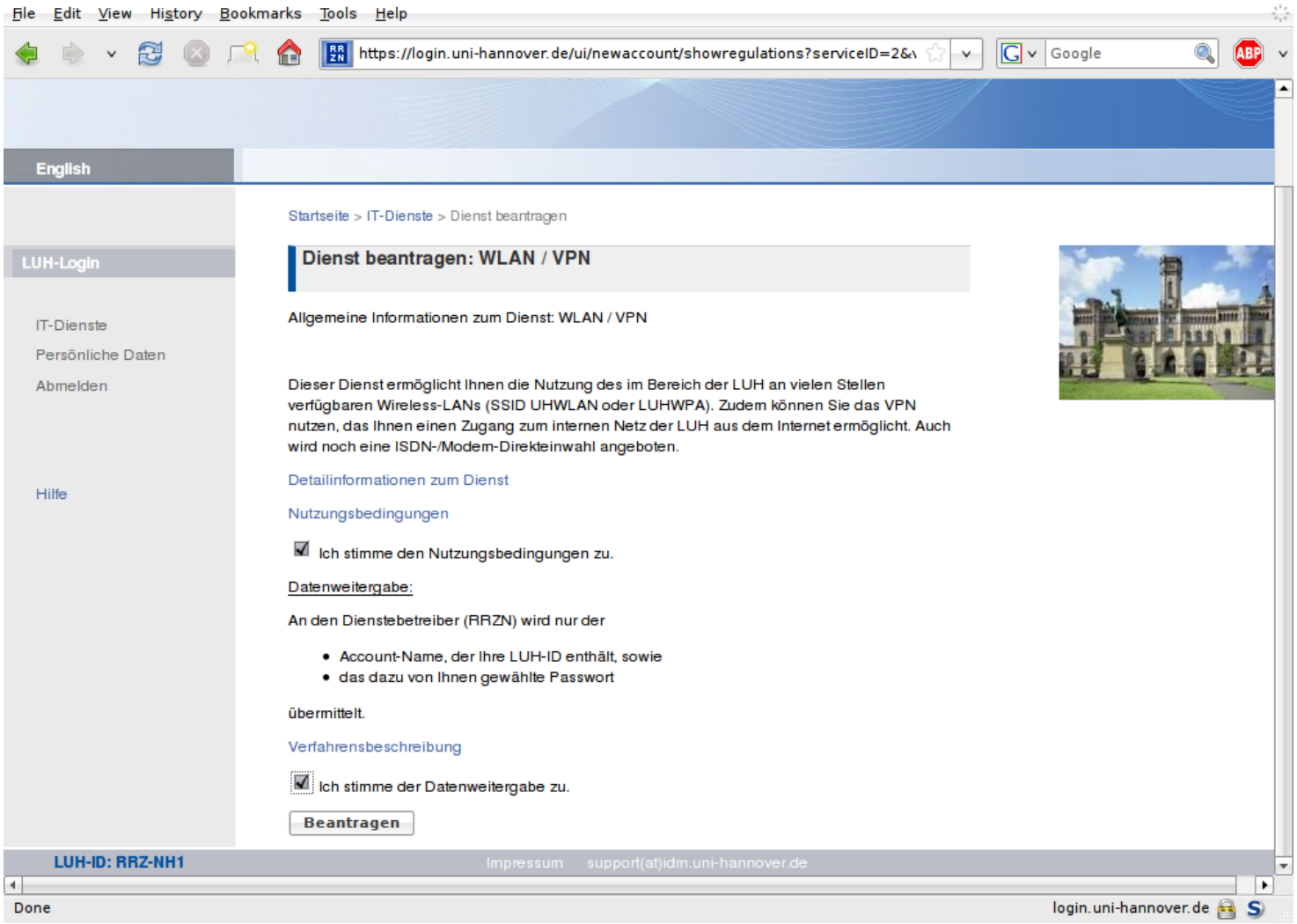
Realisierungsstand

Stud.IP

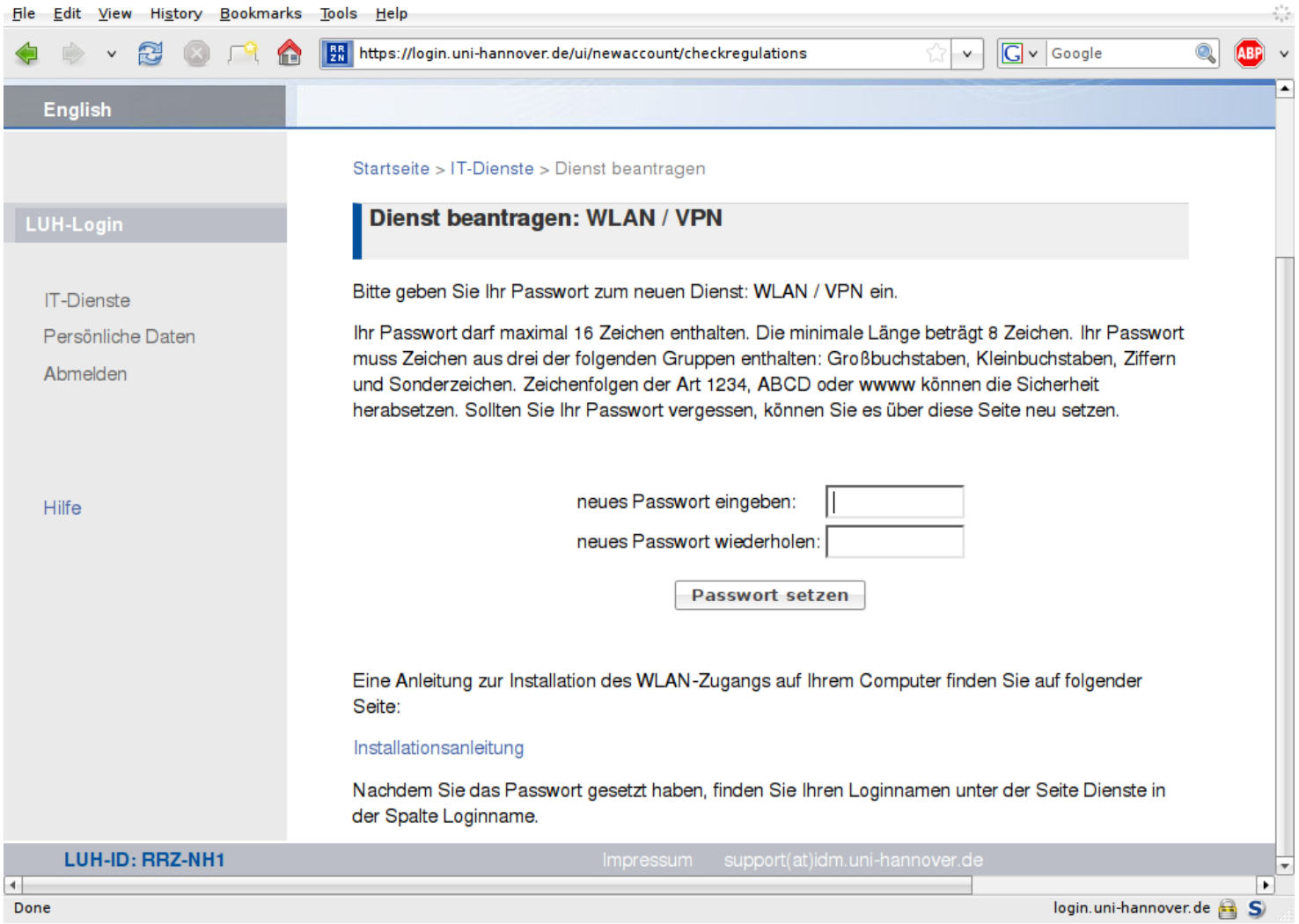


Realisierungsstand

WLAN



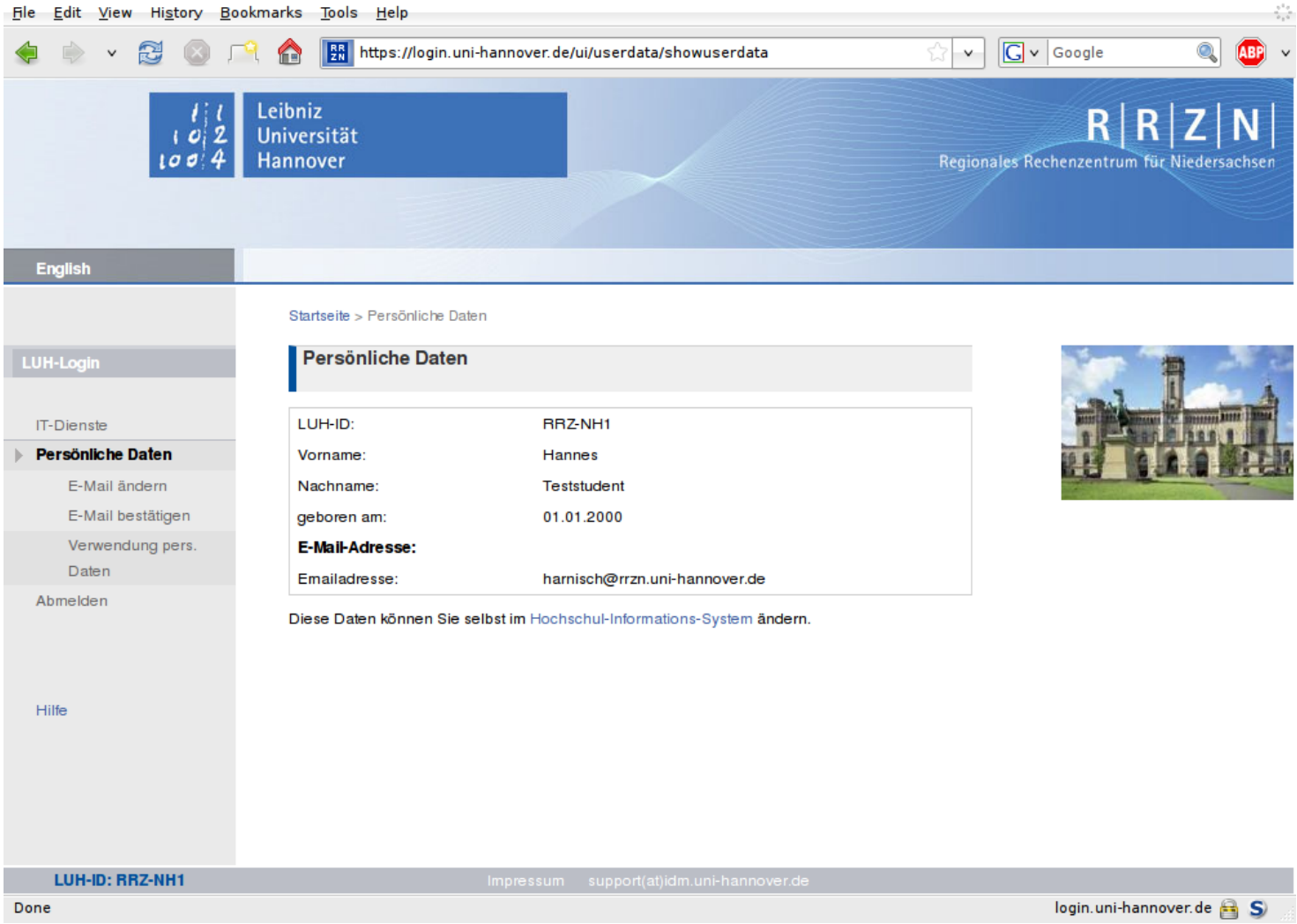
WLAN


File Edit View History Bookmarks Tools Help
https://login.uni-hannover.de/ui/newaccount/checkregulations
Google
English
Startseite > IT-Dienste > Dienst beantragen
LUH-Login
IT-Dienste
Persönliche Daten
Abmelden
Hilfe
Dienst beantragen: WLAN / VPN
Bitte geben Sie Ihr Passwort zum neuen Dienst: WLAN / VPN ein.
Ihr Passwort darf maximal 16 Zeichen enthalten. Die minimale Länge beträgt 8 Zeichen. Ihr Passwort muss Zeichen aus drei der folgenden Gruppen enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen. Zeichenfolgen der Art 1234, ABCD oder wwww können die Sicherheit herabsetzen. Sollten Sie Ihr Passwort vergessen, können Sie es über diese Seite neu setzen.
neues Passwort eingeben:
neues Passwort wiederholen:
Passwort setzen
Eine Anleitung zur Installation des WLAN-Zugangs auf Ihrem Computer finden Sie auf folgender Seite:
Installationsanleitung
Nachdem Sie das Passwort gesetzt haben, finden Sie Ihren Loginnamen unter der Seite Dienste in der Spalte Loginname.
LUH-ID: RRZ-NH1
Impressum
support(at)idm.uni-hannover.de
Done
login.uni-hannover.de

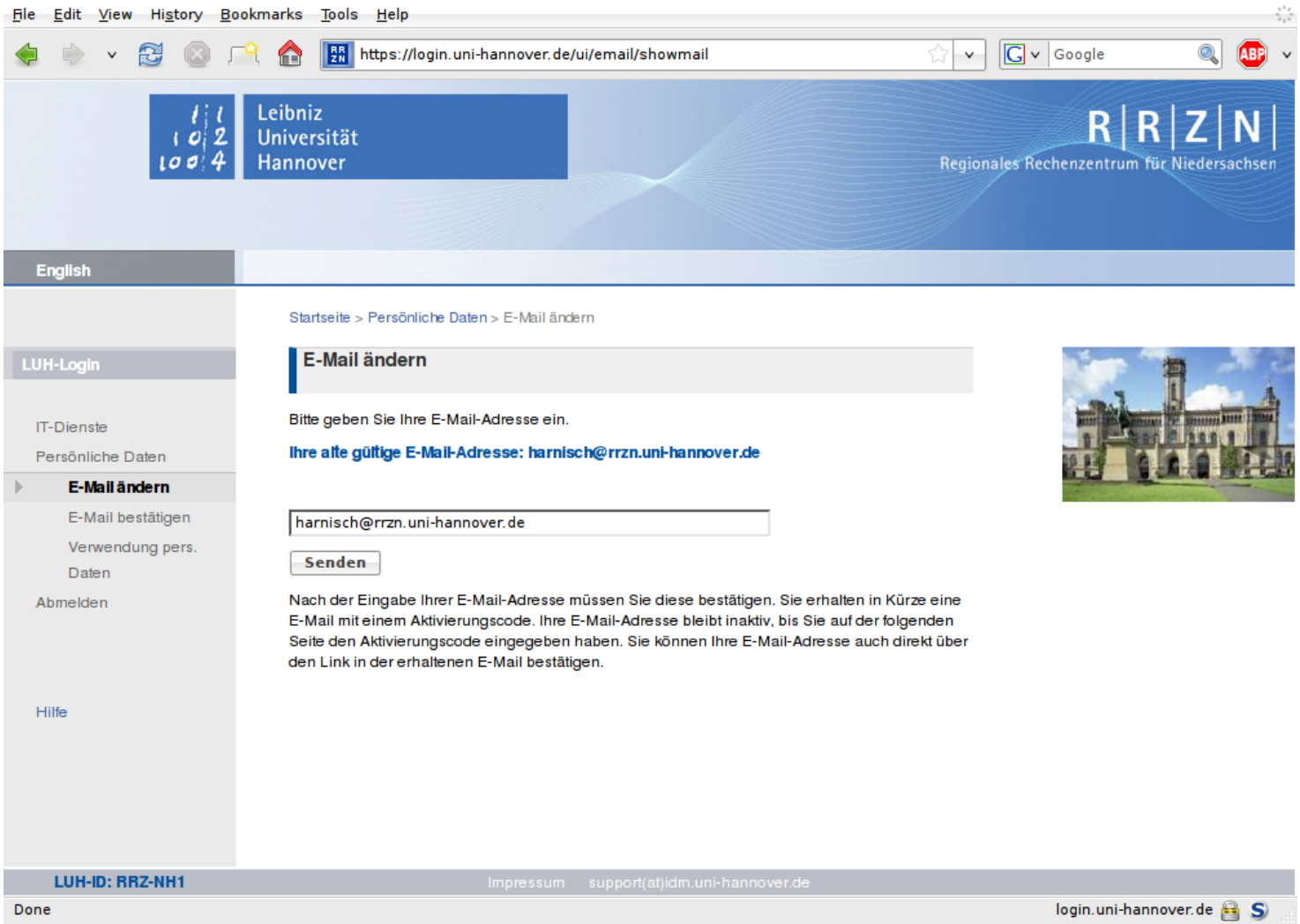
Realisierungsstand

WLAN

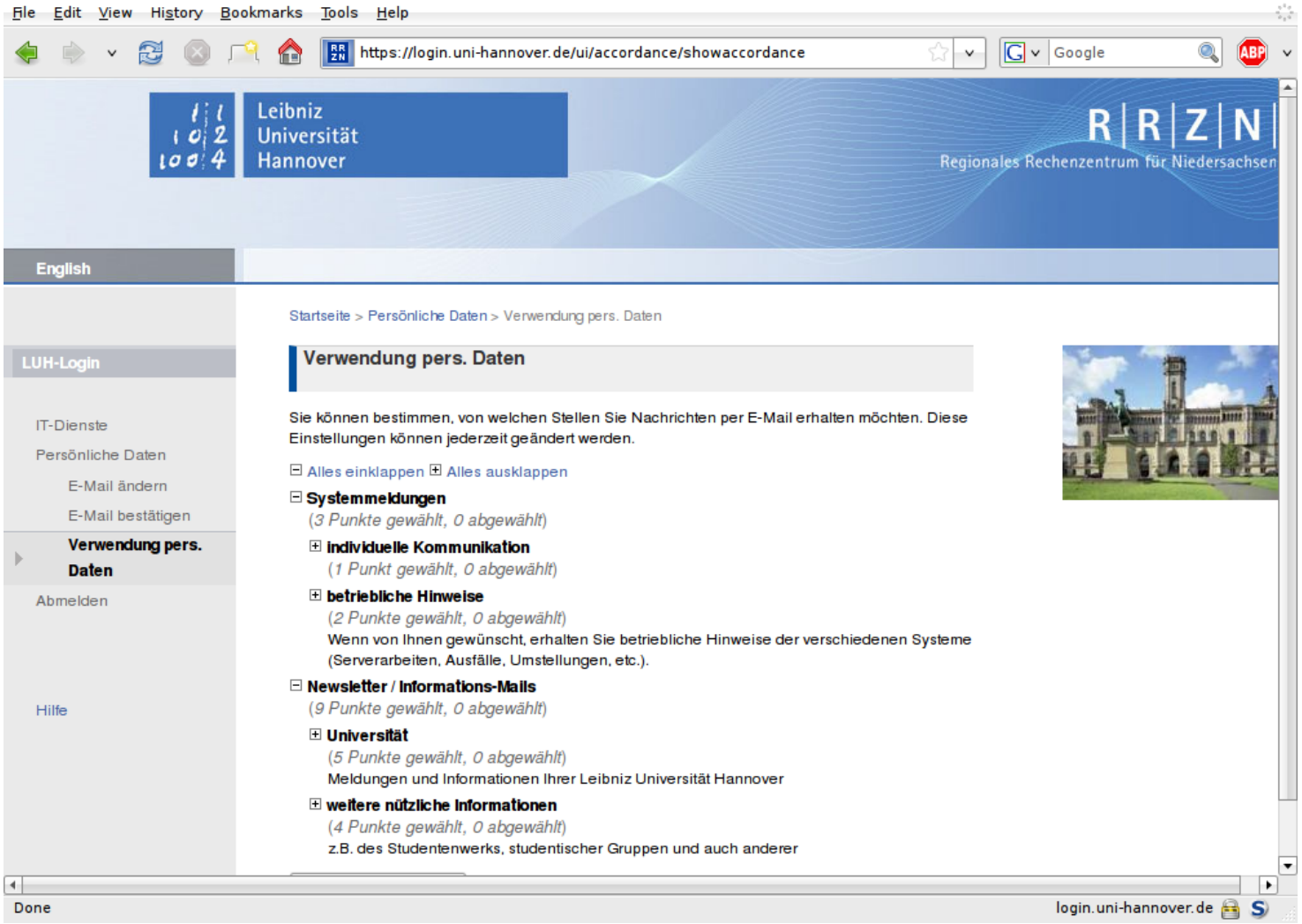
Persönliche Daten



Persönliche Daten



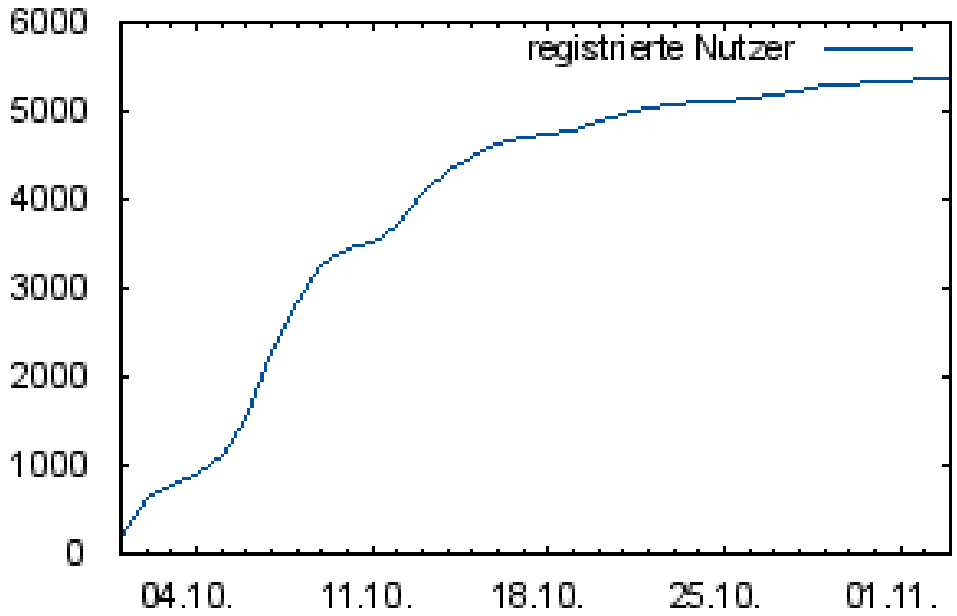
Persönliche Daten



R|R|Z|N

Einführung zum WS 2008/09

- aufgrund knapper Zeit wirklich erst zu Anfang Oktober
- wenige Minuten nach Freigabe erste Nutzer, inzwischen > 5700:



- einige studentische Datenquellen fehlen noch:
  Gasthörer, einige HMT-Studenten, Studienkolleg
- daher Studserv als Alternativweg für WLan, Stud.IP noch möglich

R|R|Z|N

MaPhy und Stud.IP als SP

sind als „Website-Anbindung“ realisiert:

1. Student geht auf IdM-Webseite
2. Knopf dort leitet Ihn mit Post-Daten an SP-Webseite
3. Post-Daten enthalten LUHID und ein LDAP-Passwort
4. Dienst-Webapplikation bindet sich als LUHID mit Passwort an LDAP
5. erfolgreiche Bindung garantiert die IdM-Authentifizierung
6. im LDAP weitere Daten über den Studenten

war nur eine schnelle Lösung

- war schnell zu realisieren, ohne großen Einarbeitungsaufwand
- keine Datenkorrektur möglich, kein Rückfluss ans IdM
- Ausscheiden aus der Uni so nicht abbildbar
- durch SSO-Verfahren mit Abgleichmöglichkeit zu ersetzen

R|R|Z|N

SSO-Verfahren

vielfältige Techniken

- Shibboleth (Internet2, DFN)
- OpenASelect (Alfa & Ariss B.V.), unterstützt u.A. A-Select (Surfnet)
- CAS (Yale University)
- WebAuth (Stanford University)
- Cosign (University of Michigan)
- Pubcookie (University of Washington)
- ...
- OpenID, Cardspace ... (u.A. kommerzielles Umfeld)

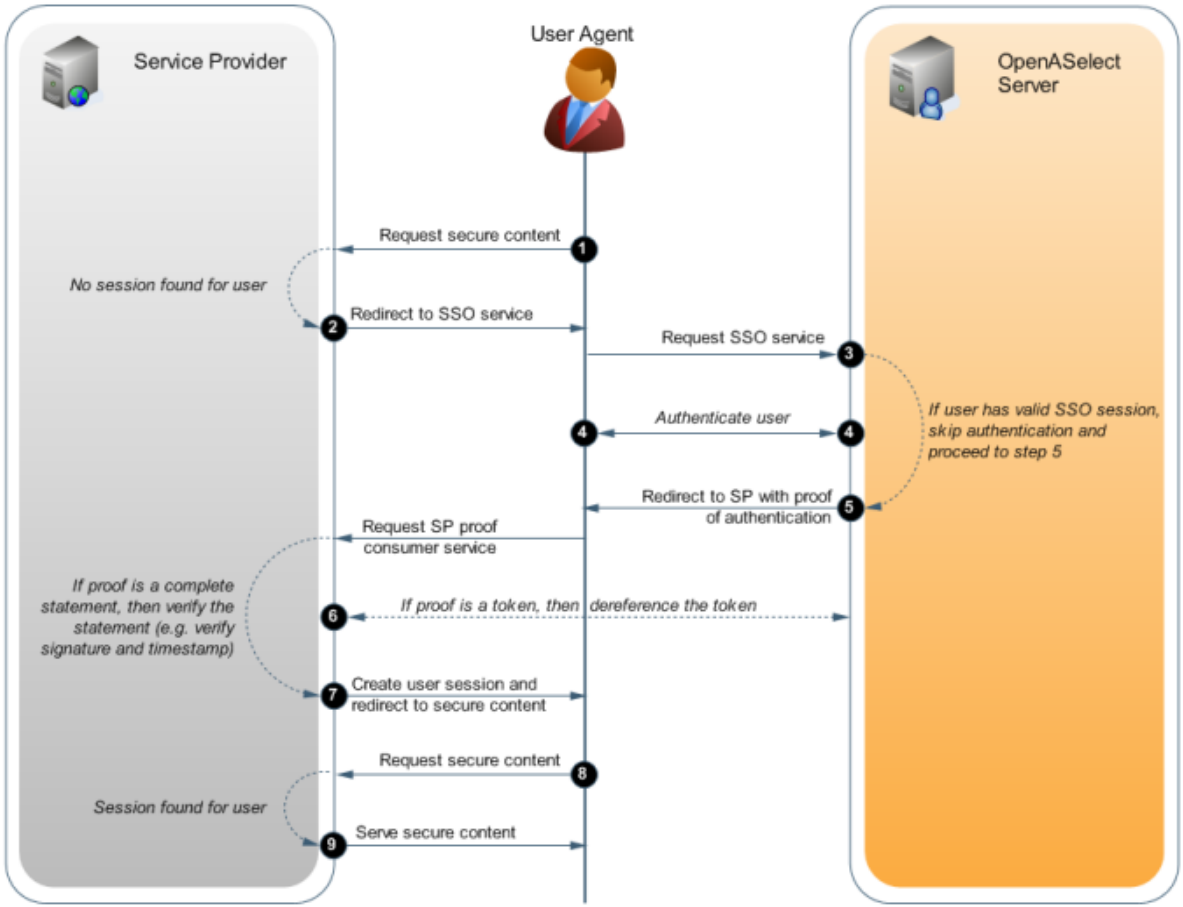
... Shibboleth im DFN-Verbund gesetzt, aber nicht unbedingt uni-intern

Website-Anbindung

- häufig cookie-basierend, Ablauf vgl. Shibboleth (evt. ohne WAYF)

z.B. OpenASelect

Quelle: OpenASelect



- Implementationen in C, Perl, Java; Client häufig als Apache-Modul
- Cardspace-Verfahren scheidet aus, da Ausweiskarte auf Client

R|R|Z|N

SSO Entscheidungskriterien

- Passworteingabe soll nur am IP (IdM) stattfinden, nicht am SP[1]
- Implementationsaufwand bei Website-Betreiber soll gering sein
- Zusatzdaten müssen (mit Nutzerzustimmung) möglich sein
- Ticketweitergabe muss möglich sein (z.B. von Frontend-GUI an SOAP-Backend)
- vollständige Anonymisierung (ohne LUHID) wünschenswert
- Single-Sign-Off schön, aber nicht ganz so wichtig
- auch stufige Verfahren sind denkbar, z.B.
  - einfaches Verfahren in der Uni
  - IP von Shibboleth nutzt dieses Verfahren für DFN-Föderation
  - OpenID-Ausstellung als Angebot für externe Dienste
- Unterstützung von Einmal-Passwörtern, Token o.Ä.

[1] wie es bei Single-Password per LDAP wäre

R|R|Z|N

Zugang PC-Pool

⟶ Pool-Technik recht unterschiedlich, so auch die Anbindung

⟶ häufig nur für Fakultätsangehörige

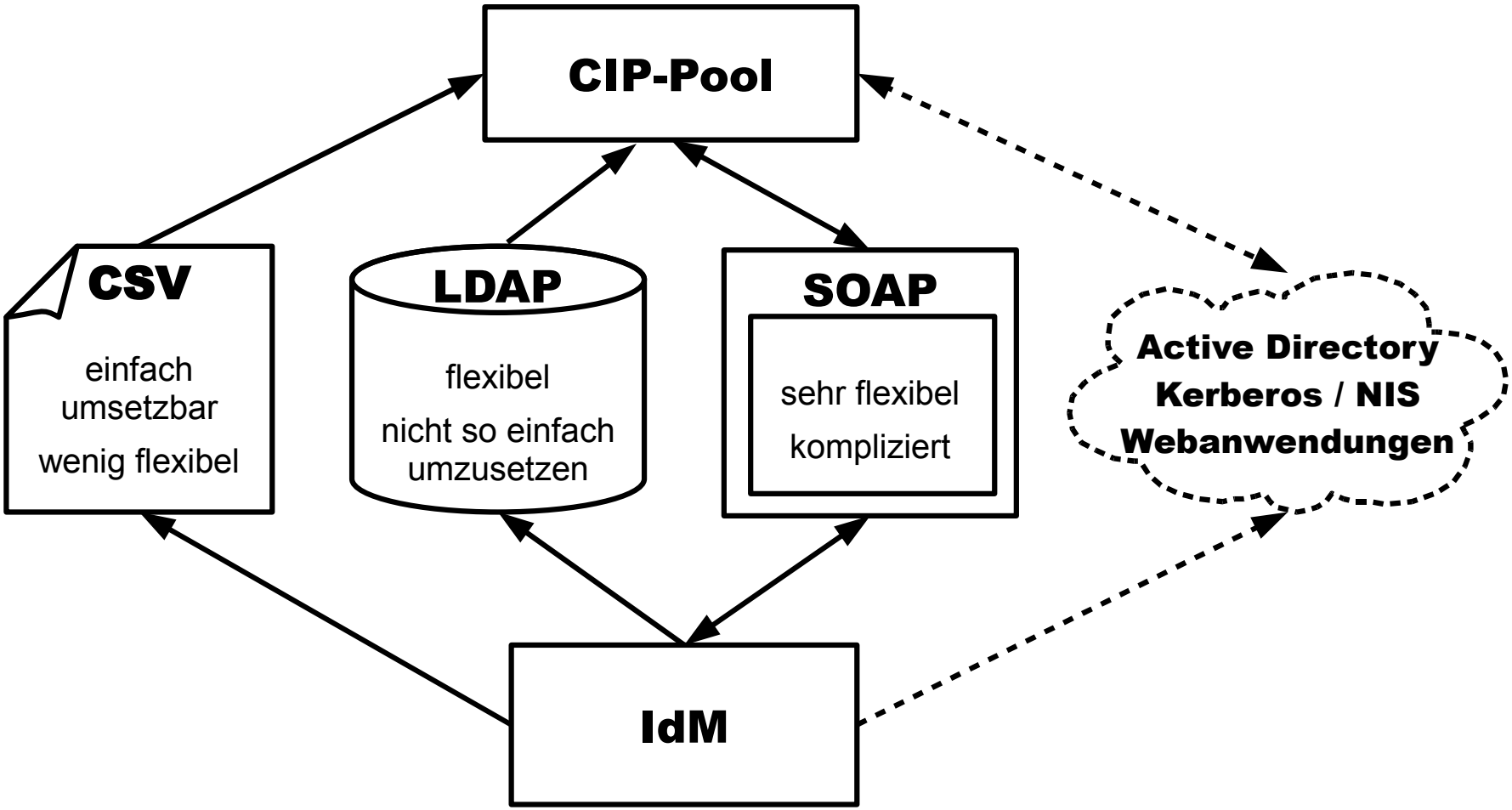
1. Nutzer meldet sich mit IdM-Login an IdM-Webseite an
2. wählt PC-Pool, Beantragung unter Anerkennung (s.o.)

3a. Nutzer gehört zur Fakultät
   - Nutzerkennung/Homeverzeichnis wird angelegt

3b. Nutzer gehört nicht zur Fakultät
   - Nutzer wird um Antragsbegründung gebeten
   - Betreiber erhält Antrag: manuell zustimmen/ablehnen
   - Nutzer wird informiert, ggf. Kennung/Verzeichnis

4. regelmäßiger Abgleich Fakultäts-/Universitätszugehörigkeit

Pool-Anbindung



R|R|Z|N

Probleme und Erläuterungen

- CSV / SOAP mit Beispiel-Clientimplementierung:
  - Anbindung beliebiger („Legacy"-) Systeme
  - Umsetzung auf dem Zielsystem durch Admin
- bei LDAP noch unklar:
  - Pflege der Userverzeichnisse & -dateien beim Anlegen/Löschen
  - Rollenaccounts des Zielsystems, Gruppen
  - Rückfluss zum IdM nötig?

  ⟶ evt. verschiedene Unterbäume je Service
- *geplant:* ActiveDirectory, Kerberos/LDAP; *offen:* NIS, Novell

  ⟶ *Ziel:* zentrale Lösungen als Angebot
- Webanwendungen bevorzugt per SSO

derzeit größtes Problem:

Fakultätszugehörigkeit Studierender
Daten aus HIS geben nur Erstfakultät und Studiengang

R|R|Z|N

Linux/Unix

einheitlich (bereits mit MaPhy realisiert):

- LUHID als Username: `rrz-nh1`, Homeverzeichnis `/home/r/r/rrz-nh1`
- numerische id (uidNumber) einheitlich ab 10.000 ⟵ auch studserv

Ziel

- zentrales Kerberos oder gekoppelte Realms
- unterstützt durch (zentrales / dezentrales) LDAP

Problem

- zusätzliche lokale Nutzer (uidNumber < 5.000)
- zusätzliche lokale Anforderungen
- Einrichtung Home-Verzeichnisse

R|R|Z|N

Windows

Ziel

- zentrale Domäne mit Untergliederung in OUs für PC-Pool-Betreiber
- Forest-Bildung mit eigenständigen Domänen

Probleme / Fragen

- Domänenhierarchie scheidet aus Sicherheitsgründen aus
- wie eigenständig sind OUs gestaltbar?
- „Details“: z.B. Zuordnung neu aufgenommener Clients in OU
- reicht Forest-Bildung aus?
- Problem der Homeverzeichnis-/Profileinrichtung bleibt

Planungen

Noch kein echtes Identitätsmanagement:

- derzeit nur wenige zentrale Dienste angebunden
- auch nur Studenten im System, Mitarbeiter fehlen noch

konkret geplant u.A.

- Umstellung der alten Studserv-WLAN-Accounts auf IdM
- zentrales Adressbuch (mit Studierenden nach individueller Datenfreigabe)
- Anbindung HIS, PC-Pools exemplarisch
- Passwort-Rücksetzung & -Reduzierung, Single-Sign-On
- exemplarische / testweise Umsetzung Web-SSO

zu lösende Probleme

- fehlende Fakultätszugehörigkeit in HIS-SOS
- schlechte Datenlage in HIS-LSF (und ohne „externe“ Einrichtungen)
- viele unterschiedliche Datenquellen
- Benennung und Pflege dezentraler Ansprechpartner / Admins
  derzeit z.B. Problem bei Security-Kontakten & DNS/IP-Ansprechpartnern
- …

zu berücksichtigen

- lokale Zusätze (Gruppen, Nutzer)
- auch dezentrale Datenpflege, Genehmigung
- „einsammeln“ von Alt-Beständen an Account-Daten

R|R|Z|N

Zeitrahmen

SS08	Projektstart
zum WS08/09	Anbindung WLan/VPN, Stud.IP, PC-Pool MaPhy provisorisch
im WS08/09	Anbindung HIS-LSF-Webseite, Studierenden-Rechner; PC-Pool MaPhy verbessern, exemplarisch Windows-PC-Pool; Adressbuch Studierender (Web & LDAP); Erschließung weiterer Datenquellen Studenten (Gast, SK, HMT)
im SS09	Anbindung PC-Pools (zunächst nur einfache Workflows); Support Newsletter und ähnlicher Mailverteiler; Adressbuchausbau mit Organisationsstruktur (auch SOAP); Erschließung erster Datenquellen Mitarbeiter
ca. SS09	SSO-Funktionalitäten für ausgewählte Webseiten
...	
ab SS11	Regelbetrieb

aber Zeitplan ist ehrgeizig ...