Erfahrungen mit dem Betrieb des IBM Tivoli Identity Managers (ITIM) an der RWTH Aachen

Guido Bunsen**, Michael Gebhardt, Michaela Schraad**
{bunsen,gebhardt,schraad}@rz.rwth-aachen.de

Rechen- und Kommunikationszentrum
Rheinisch-Westfälische Technische Hochschule Aachen
http://www.rz.rwth-aachen.de

Inhalt

1. **Einführung**
   - Ausgangslage, Ziele, Architektur
2. **Erfahrungen: Identitätsmanagement des RZ**
   - Überblick, Freischaltprozess für Studierende
   - Quellsysteme: Anbindung der „HR-Feeds“
   - Zielsysteme: Provisionierung neuer Dienste
   - Wandel, Aufwände, Fazit
3. **Ausblick: RWTH-Identitätsmanagement**
   - Was fehlt noch für die RWTH?
   - .. und über die RWTH hinaus.
4. **Zusammenfassung**

1. Einführung

1. **Einführung**
   - Ausgangslage, Ziele, Architektur
2. **Erfahrungen: Identitätsmanagement des RZ**
   - Überblick, Freischaltprozess für Studierende
   - Quellsysteme: Anbindung der „HR-Feeds“
   - Zielsysteme: Provisionierung neuer Dienste
   - Wandel, Aufwände, Fazit
3. **Ausblick: RWTH-Identitätsmanagement**
   - Was fehlt noch für die RWTH?
   - .. und über die RWTH hinaus.
4. **Zusammenfassung**

Die RWTH Aachen in Zahlen

Professoren:	414
Mitarbeiter:	4.669 [1)]
Studenten:	30.800 [2)]
Studienkurse:	ca. 80
Fakultäten:	9
Organisationseinheiten:	ca. 650
Lehrstühle:	ca. 350
Budget (total):	545.1 Mio. Euro [3)]
Eingeworbene Mittel:	142.3 Mio. Euro [3)]

ca. 750 Promotionen p.a. ca. 5.000 Neueinschreibungen p.a.

⇨ hohe personelle Fluktuation ⇨ heterogene Vorstellungswelten

[1)] in 2004
[2)] im WS 2002/2003
[3)] in 2003

Quelle: RWTH Aachen 03/2004, Dez. Planung, Entwicklung und Controlling

Ausgangslage, Beweggründe

Steigende Zahl von Dienstleistungen mehrerer Dienstleister

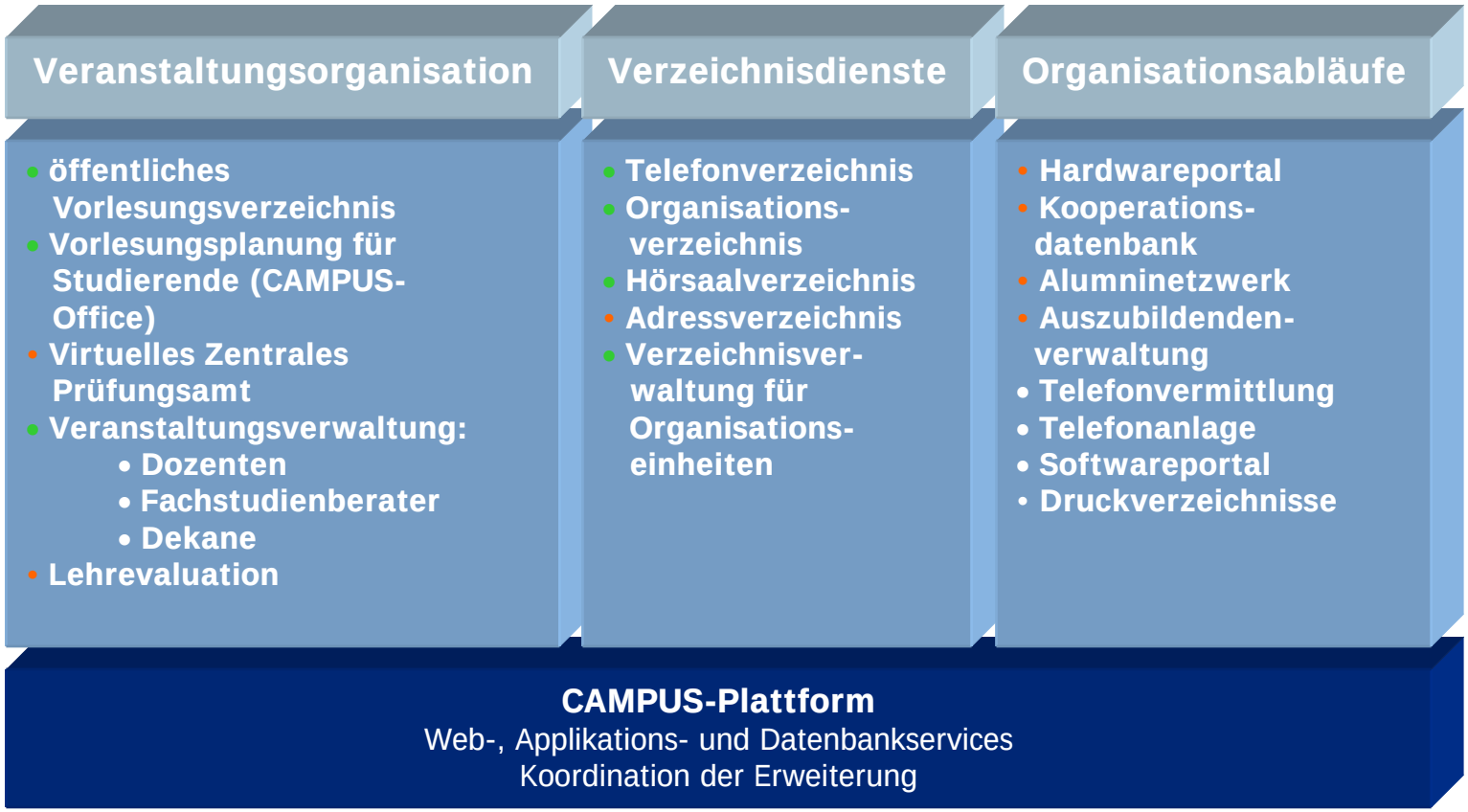
- **Rechen- und Kommunikationszentrum**
  - Traditionelle Dienste, neue Lehr- und Lernformen
- **Bibliothek**
  - Elektronische Medien, Zugänge zu kostenpflichtigen DB
- **elektronische Verwaltungsabläufe (z.B. CAMPUS-Informationssystem)**
  - Telefonbuch, Hörsaalverwaltung, Bestellportale, ...
  - Terminkalender, Belegung von Kursen, virtuelles Prüfungsamt, ...

Herausforderung

- **Mehrfache Registrierung von Personen**
  - Konsistenz, Mehrarbeit
  - Löschung von Diensten nach Ausscheiden (z.B. aus Lizenzgründen)
- **Rechtsverbindlichkeit**
- **Zeit ist bei der Bereitstellung von Diensten durchaus kritisches Element**

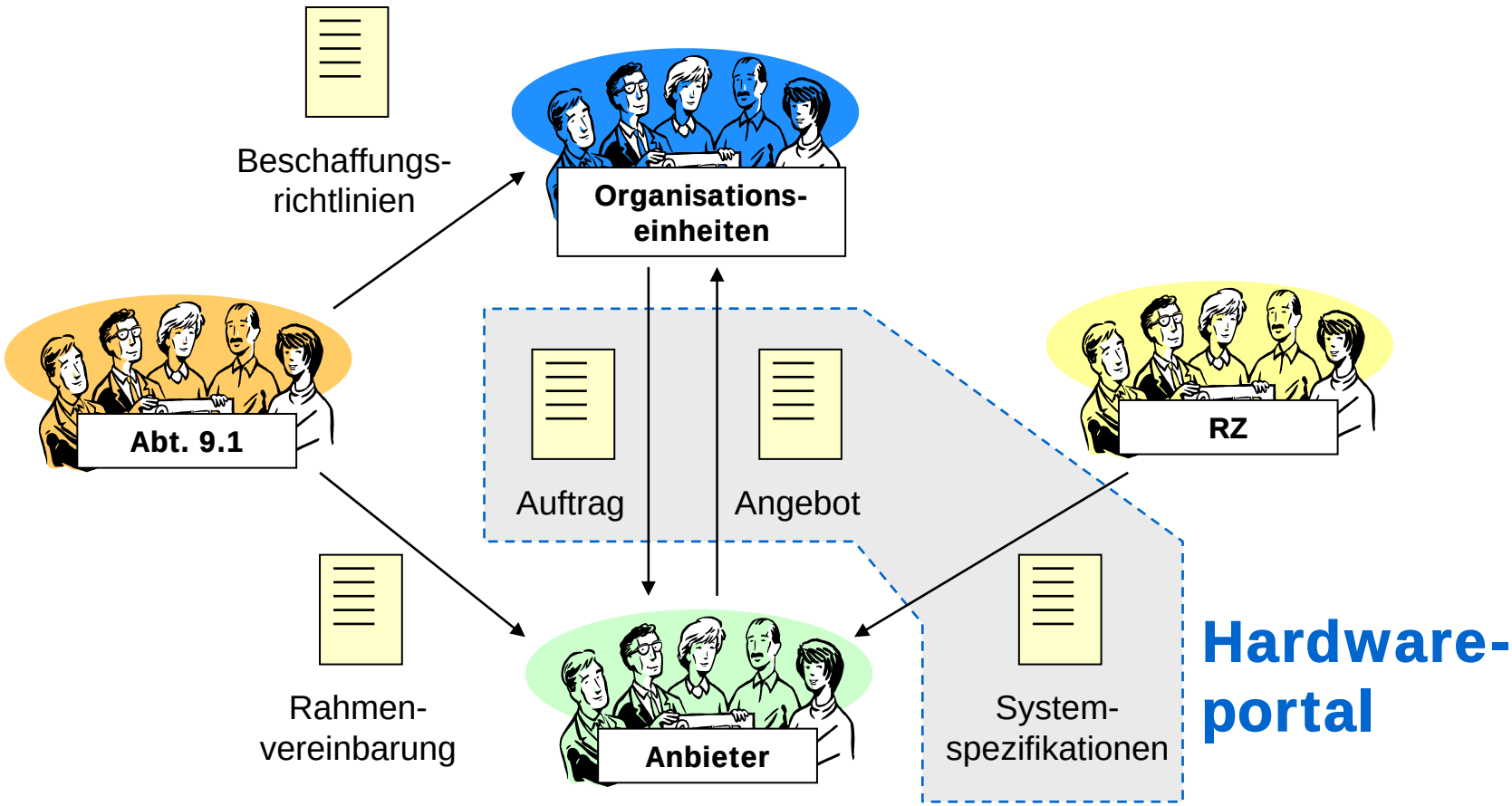
Eigenverständnis / -darstellung des RZ als moderner Dienstleister!

Dienstleistungen mehrer Anbieter: CAMPUS-Informationssystem



ZIEL: integrierte Dienstleistungen

Beispiel 1: Informationsfluss Hardwareportal
(vereinfacht)



Beispiel 2:
Virtuelles Zentrales Prüfungsamt

- **Früher:**
  - Anmeldung im ZPA erforderlich
  - Anmeldelisten an Dozenten (Diskette), Nachmelder
  - Notenaushang (Datenschutz?)
  - Notenliste an ZPA (Diskette), Korrekturen
  - Bescheinigung im ZPA abholen
- **Mit VZPA**
  - Anmeldung online (Studierender, Dozent)
  - Notenerfassung online
  - Prüfungsleistung online

- **Ersparnis/Komfortgewinn**
  - 2 Besuche beim ZPA entfallen
  - Aktuelle Sicht für Studierende und Dozenten
  - Diskette mit Anmeldeliste und Notenliste entfällt
  - Kein Notenaushang erforderlich

- **Integrationsprinzip:**

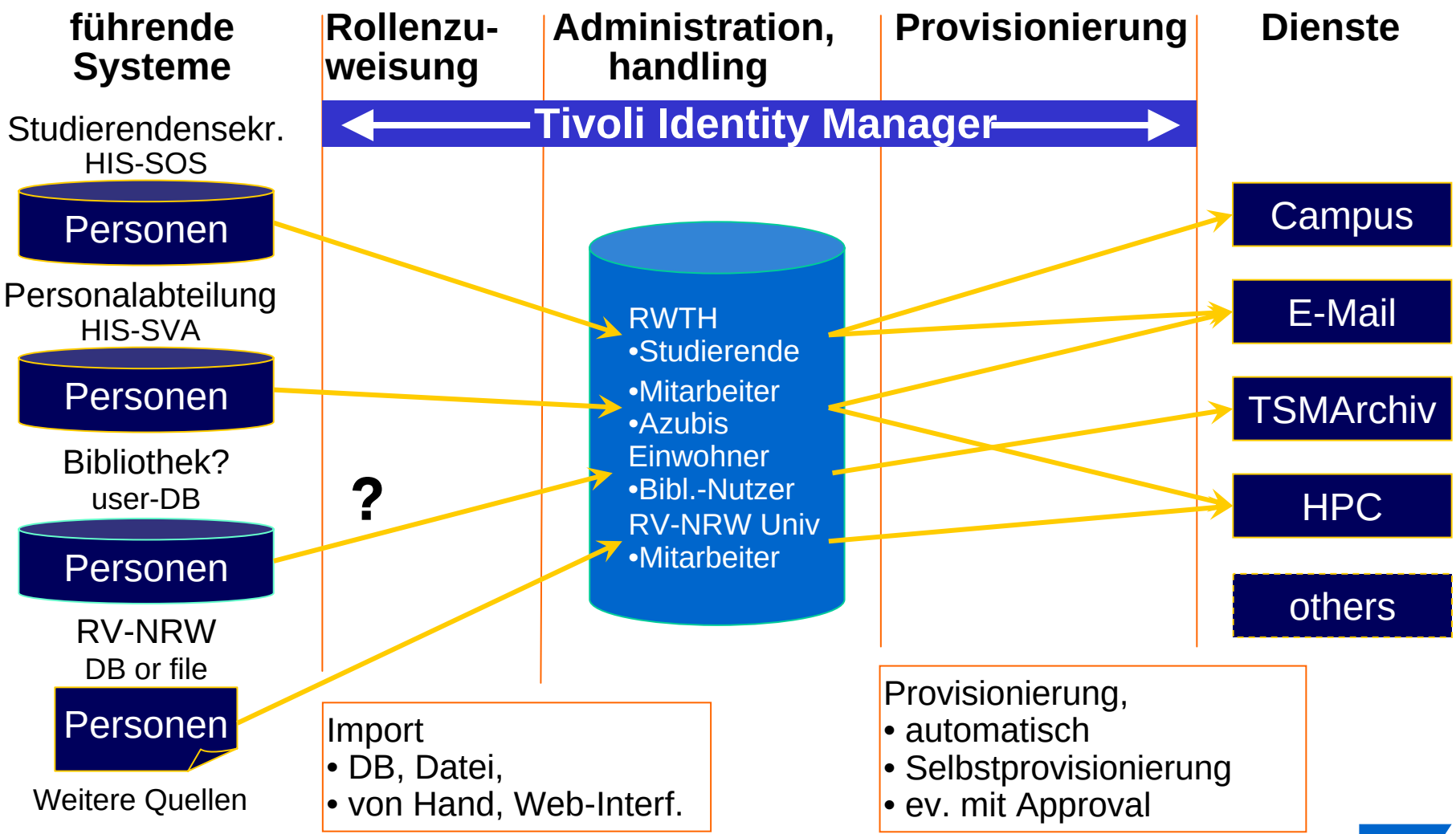
Zugriff auf relevante Daten ersetzt hin und her von Daten

Integration bringt die wesentlichen Komfort- und Effizienzgewinne

Erwartungen und Ziele

- **Definierte Prozesse**
  - Durchsetzung von Policies
  - Rechte sollen rechtzeitig wieder entzogen werden
  - Änderungen sollen nachvollziehbar sein (Auditing)
  - Mehr Transparenz und Überblick für Dienstleister und Kunden
- **Kostensenkung**
  - Vermeidung von Mehrfacharbeit/Mehrfacherfassung
- **Mehr Produktivität in der Hochschule**
  - Nur noch eine Anlaufstelle für Kunden (zentrales Helpdesk)
  - Schnellerer Zugang zu webbasierten Diensten und Netzdiensten
  - Betreiber von Diensten sollen von Benutzerverwaltung befreit werden

Architektur: Identitätsmanagement



2. Identitätsmanagement des RZ

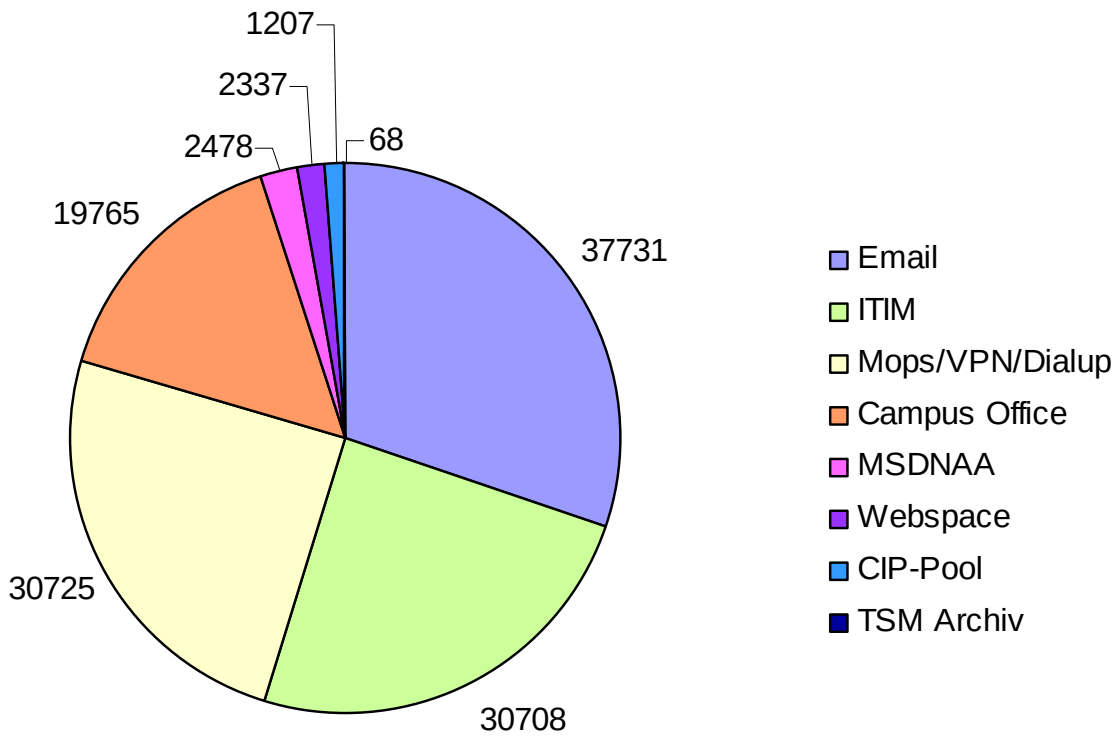
1. **Einführung**
   - Ausgangslage, Ziele, Architektur
2. **Erfahrungen: Identitätsmanagement des RZ**
   - Überblick, Freischaltprozess für Studierende
   - Quellsysteme: Anbindung der „HR-Feeds“
   - Zielsysteme: Provisionierung neuer Dienste
   - Wandel, Aufwände, Fazit
3. **Ausblick: RWTH-Identitätsmanagement**
   - Was fehlt noch für die RWTH?
   - .. und über die RWTH hinaus.
4. **Zusammenfassung**

Durch ITIM provisionierte Dienste

- **Produktiv**
  - ITIM-Accounts
  - Email @{|rz.|post.}rwth-aachen.de
  - CampusOffice
  - Einwahldienste (Radius, VPN / WLAN, Uni-DSL, DFN@Home)
  - CIP-Pool
  - TSM-Archiv
  - MSDNAA
  - Webspace

- **In Planungs- oder Realisierungsphase**
  - Condor / RWTH-Grid
  - IXI / UMS
  - Unix Cluster
  - Dienste in anderen Fachbereichen

Verteilung der 125042 Accounts



Freischaltprozess

- **Freischaltcode (einmal PIN)**
- **Versand mit Studienbescheinigung nach Immatrikulation**
- **Freischaltung mit Java Web-Appl. in 4 Schritten:**
  1. Eingabe von Matrikelnummer und Freischaltcode
  2. Auswahl einer Emailadresse aus einer Vorschlagsliste und Veröffentlichung ja/nein
  3. Bestätigung, dass Angabe korrekt
  4. Auslieferung von Username, Passwort, Emailadresse Eintragung in User-Objekt über ITIM-Java-API

Freischaltung Login - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse https://services.rz.rwth-aachen.de/unlock/ Wechseln zu Links

RWTH

Hier erhalten Sie in vier Schritten eine Email-Adresse, eine Benutzerkennung und ein Passwort. Dazu benötigen Sie Ihre Matrikelnummer und Ihren **Freischaltcode**. Diesen haben Sie vom Studierendensekretariat zusammen mit Ihren Immatrikulationsunterlagen erhalten.
Bitte halten Sie Papier und Bleistift bereit, um die Daten, die Sie mit der Freischaltung erhalten, notieren zu können.

Login - Schritt 1 von 4

Matrikelnummer: (siehe Studentenausweis)

Freischaltcode: (siehe Immatrikulationsunterlagen)

Einloggen Zurücksetzen

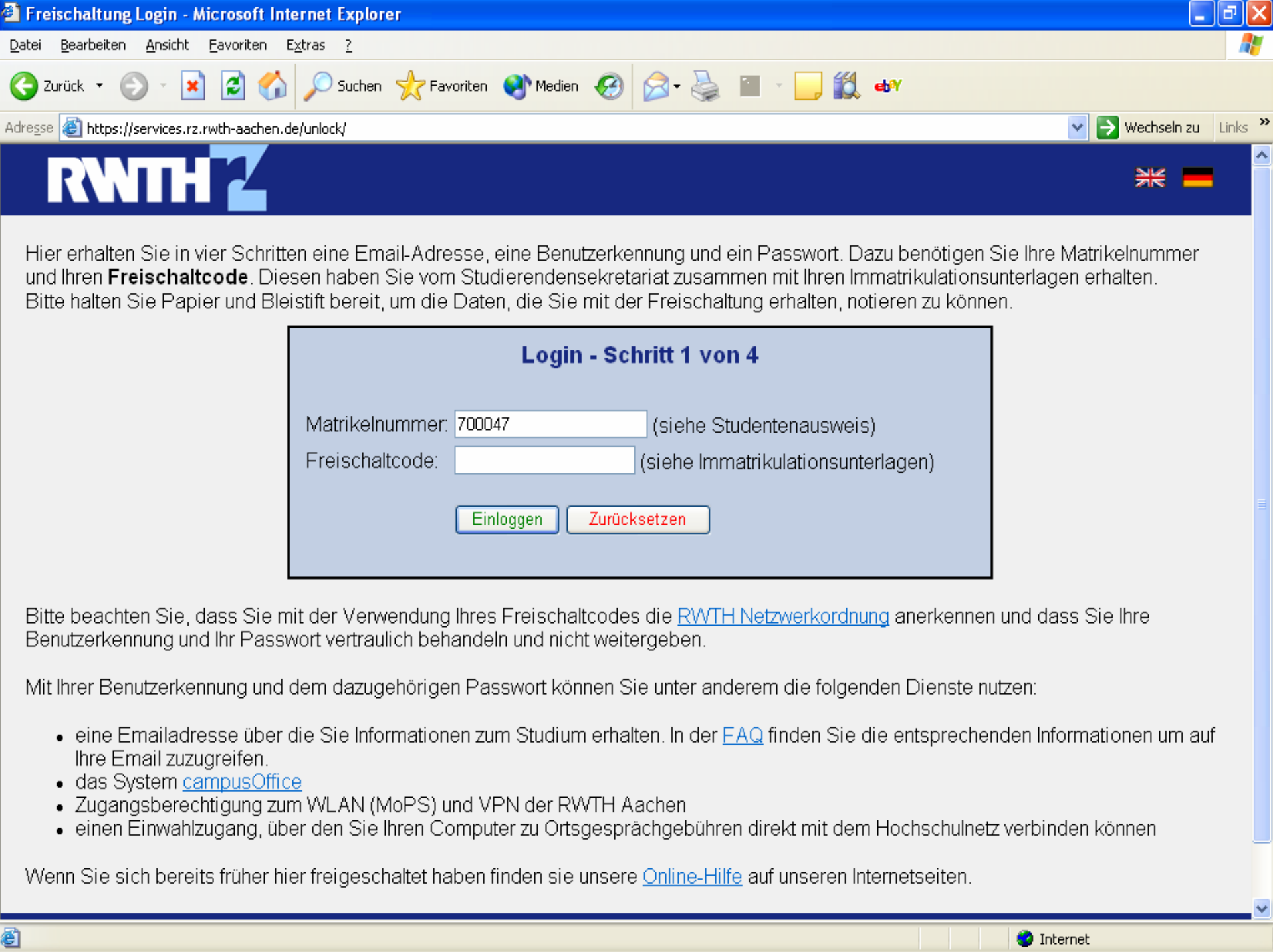
Bitte beachten Sie, dass Sie mit der Verwendung Ihres Freischaltcodes die RWTH Netzwerkordnung anerkennen und dass Sie Ihre Benutzerkennung und Ihr Passwort vertraulich behandeln und nicht weitergeben.

Mit Ihrer Benutzerkennung und dem dazugehörigen Passwort können Sie unter anderem die folgenden Dienste nutzen:

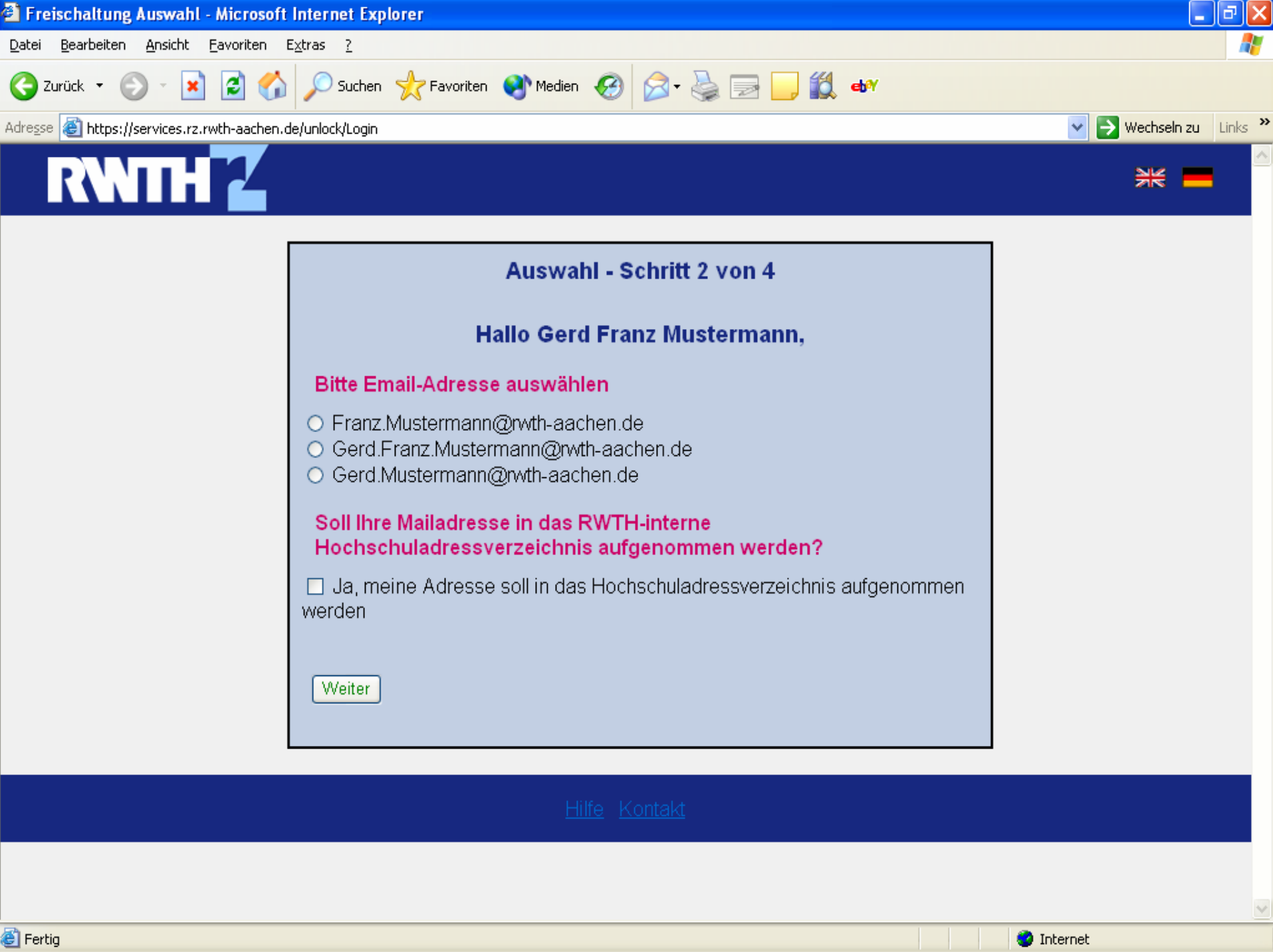
- eine Emailadresse über die Sie Informationen zum Studium erhalten. In der FAQ finden Sie die entsprechenden Informationen um auf Ihre Email zuzugreifen.
- das System campusOffice
- Zugangsberechtigung zum WLAN (MoPS) und VPN der RWTH Aachen
- einen Einwahlzugang, über den Sie Ihren Computer zu Ortsgesprächgebühren direkt mit dem Hochschulnetz verbinden können

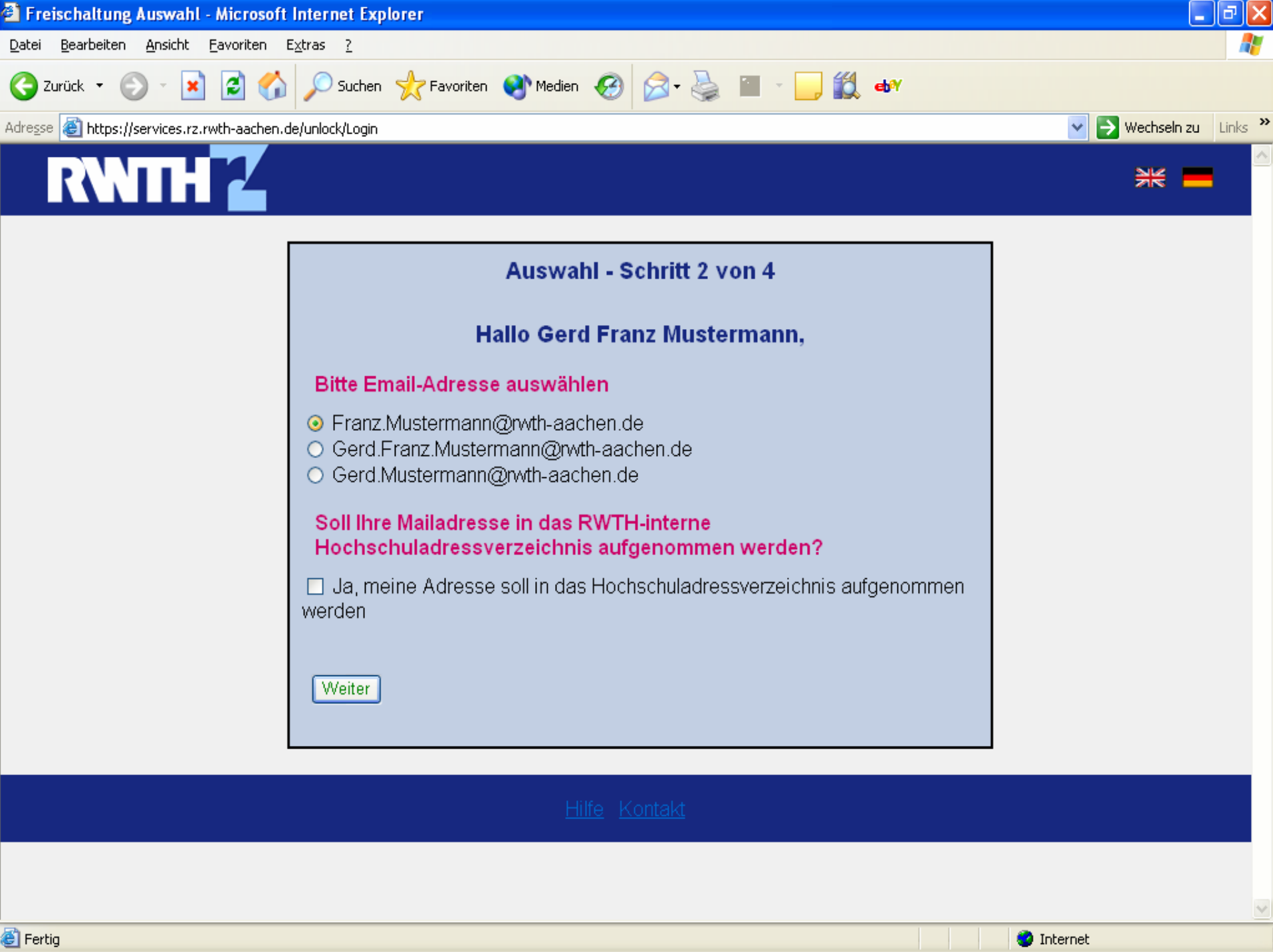
Wenn Sie sich bereits früher hier freigeschaltet haben finden sie unsere Online-Hilfe auf unseren Internetseiten.

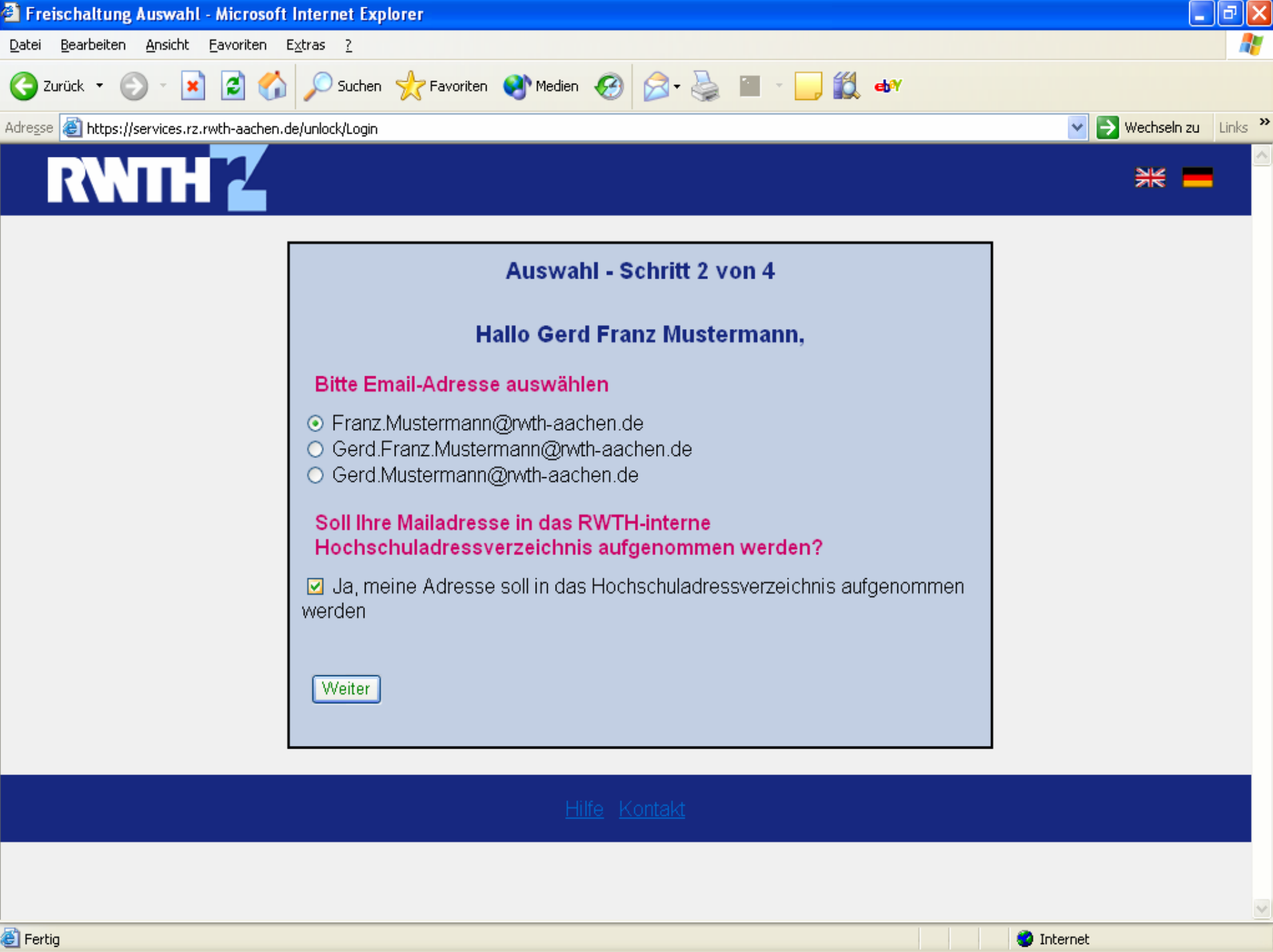
Fertig Internet

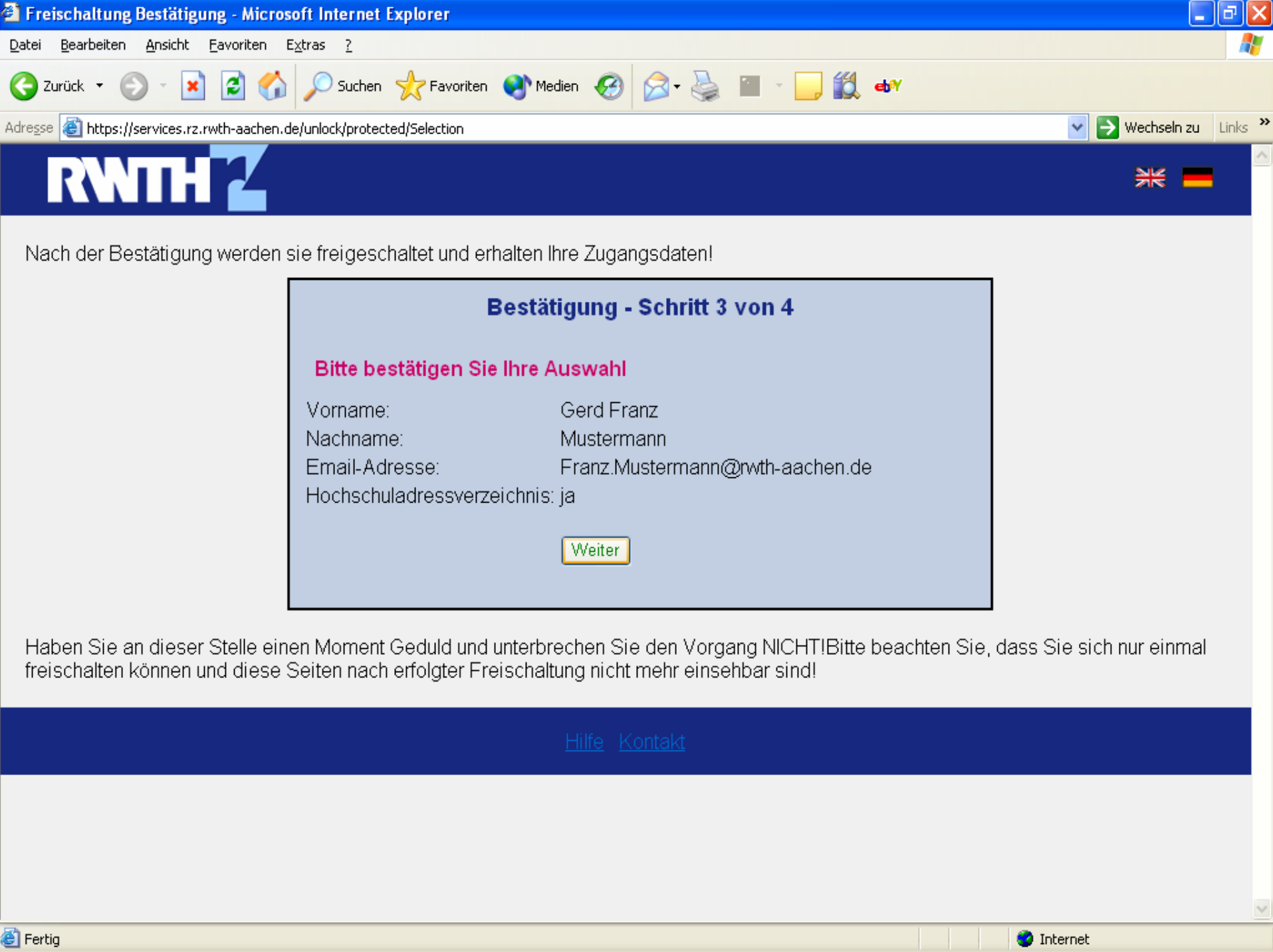

Freischaltung Login - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/unlock/
Wechseln zu Links
RWTH
Hier erhalten Sie in vier Schritten eine Email-Adresse, eine Benutzerkennung und ein Passwort. Dazu benötigen Sie Ihre Matrikelnummer und Ihren Freischaltcode. Diesen haben Sie vom Studierendensekretariat zusammen mit Ihren Immatrikulationsunterlagen erhalten.
Bitte halten Sie Papier und Bleistift bereit, um die Daten, die Sie mit der Freischaltung erhalten, notieren zu können.
Login - Schritt 1 von 4
Matrikelnummer: 700047 (siehe Studentenausweis)
Freischaltcode: (siehe Immatrikulationsunterlagen)
Einloggen Zurücksetzen
Bitte beachten Sie, dass Sie mit der Verwendung Ihres Freischaltcodes die RWTH Netzwerkordnung anerkennen und dass Sie Ihre Benutzerkennung und Ihr Passwort vertraulich behandeln und nicht weitergeben.
Mit Ihrer Benutzerkennung und dem dazugehörigen Passwort können Sie unter anderem die folgenden Dienste nutzen:
eine Emailadresse über die Sie Informationen zum Studium erhalten. In der FAQ finden Sie die entsprechenden Informationen um auf Ihre Email zuzugreifen.
das System campusOffice
Zugangsberechtigung zum WLAN (MoPS) und VPN der RWTH Aachen
einen Einwahlzugang, über den Sie Ihren Computer zu Ortsgesprächgebühren direkt mit dem Hochschulnetz verbinden können
Wenn Sie sich bereits früher hier freigeschaltet haben finden sie unsere Online-Hilfe auf unseren Internetseiten.
Internet


Freischaltung Login - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/unlock/
Wechseln zu Links
RWTH
Hier erhalten Sie in vier Schritten eine Email-Adresse, eine Benutzerkennung und ein Passwort. Dazu benötigen Sie Ihre Matrikelnummer und Ihren Freischaltcode. Diesen haben Sie vom Studierendensekretariat zusammen mit Ihren Immatrikulationsunterlagen erhalten.
Bitte halten Sie Papier und Bleistift bereit, um die Daten, die Sie mit der Freischaltung erhalten, notieren zu können.
Login - Schritt 1 von 4
Matrikelnummer: 700047 (siehe Studentenausweis)
Freischaltcode: (siehe Immatrikulationsunterlagen)
Einloggen Zurücksetzen
Bitte beachten Sie, dass Sie mit der Verwendung Ihres Freischaltcodes die RWTH Netzwerkordnung anerkennen und dass Sie Ihre Benutzerkennung und Ihr Passwort vertraulich behandeln und nicht weitergeben.
Mit Ihrer Benutzerkennung und dem dazugehörigen Passwort können Sie unter anderem die folgenden Dienste nutzen:
eine Emailadresse über die Sie Informationen zum Studium erhalten. In der FAQ finden Sie die entsprechenden Informationen um auf Ihre Email zuzugreifen.
das System campusOffice
Zugangsberechtigung zum WLAN (MoPS) und VPN der RWTH Aachen
einen Einwahlzugang, über den Sie Ihren Computer zu Ortsgesprächgebühren direkt mit dem Hochschulnetz verbinden können
Wenn Sie sich bereits früher hier freigeschaltet haben finden sie unsere Online-Hilfe auf unseren Internetseiten.
Internet


Freischaltung Auswahl - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
https://services.rz.rwth-aachen.de/unlock/Login
Wechseln zu
Links
RWTH
Auswahl - Schritt 2 von 4
Hallo Gerd Franz Mustermann,
Bitte Email-Adresse auswählen
Franz.Mustermann@rwth-aachen.de
Gerd.Franz.Mustermann@rwth-aachen.de
Gerd.Mustermann@rwth-aachen.de
Soll Ihre Mailadresse in das RWTH-interne Hochschuladressverzeichnis aufgenommen werden?
Ja, meine Adresse soll in das Hochschuladressverzeichnis aufgenommen werden
Weiter
Hilfe
Kontakt
Fertig
Internet


Freischaltung Auswahl - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
https://services.rz.rwth-aachen.de/unlock/Login
Wechseln zu
Links
RWTH
Auswahl - Schritt 2 von 4
Hallo Gerd Franz Mustermann,
Bitte Email-Adresse auswählen
Franz.Mustermann@rwth-aachen.de
Gerd.Franz.Mustermann@rwth-aachen.de
Gerd.Mustermann@rwth-aachen.de
Soll Ihre Mailadresse in das RWTH-interne Hochschuladressverzeichnis aufgenommen werden?
Ja, meine Adresse soll in das Hochschuladressverzeichnis aufgenommen werden
Weiter
Hilfe
Kontakt
Fertig
Internet


Freischaltung Auswahl - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
https://services.rz.rwth-aachen.de/unlock/Login
Wechseln zu
Links
RWTH
Auswahl - Schritt 2 von 4
Hallo Gerd Franz Mustermann,
Bitte Email-Adresse auswählen
Franz.Mustermann@rwth-aachen.de
Gerd.Franz.Mustermann@rwth-aachen.de
Gerd.Mustermann@rwth-aachen.de
Soll Ihre Mailadresse in das RWTH-interne Hochschuladressverzeichnis aufgenommen werden?
Ja, meine Adresse soll in das Hochschuladressverzeichnis aufgenommen werden
Weiter
Hilfe
Kontakt
Fertig
Internet


Freischaltung Bestätigung - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/unlock/protected/Selection
Wechseln zu Links
RWTH
Nach der Bestätigung werden sie freigeschaltet und erhalten Ihre Zugangsdaten!
Bestätigung - Schritt 3 von 4
Bitte bestätigen Sie Ihre Auswahl
Vorname: Gerd Franz
Nachname: Mustermann
Email-Adresse: Franz.Mustermann@rwth-aachen.de
Hochschuladressverzeichnis: ja
Weiter
Haben Sie an dieser Stelle einen Moment Geduld und unterbrechen Sie den Vorgang NICHT!Bitte beachten Sie, dass Sie sich nur einmal freischalten können und diese Seiten nach erfolgter Freischaltung nicht mehr einsehbar sind!
Hilfe Kontakt
Fertig
Internet

RWTH

Achtung: Ihr Login und Passwort werden nur hier angezeigt. Bitte unbedingt NOTIEREN! Bei Verlust bitte beim RZ-Helpdesk melden.

Freischaltung erfolgreich!

Bitte unbedingt notieren

Email-Adresse:	Franz.Mustermann@rwth-aachen.de
Login für Mailserver:	gm078034+rwth-aachen.de
Login für alle anderen Dienste:	gm078034
Passwort für alle Dienste:	2A86ZVkm

Weitere Informationen

Webmailer:	http://webmail.rwth-aachen.de
POP3/IMAP-Server:	mailbox.rwth-aachen.de
SMTP-Server:	relay.rwth-aachen.de
Einwahl-Telefonnummer:	0241 / 88721

Ihr CampusOffice Zugang, Ihre Email-Adresse und Ihr Einwahlzugang (WLAN, VPN, Einwahl) werden in wenigen Minuten aktiv sein.

2.1 Quellsysteme

führende Systeme

Rollenzu-weisung

Administration, handling

Provisionierung

Dienste

Tivoli Identity Manager

Studierendensekr.
HIS-SOS
Personen

Personalabteilung
HIS-SVA
Personen

Bibliothek?
user-DB
Personen

RV-NRW
DB or file
Personen

Weitere Quellen

?

RWTH
•Studierende
•Mitarbeiter
•Azubis
Einwohner
•Bibl.-Nutzer
RV-NRW Univ
•Mitarbeiter

Campus

E-Mail

TSMArchiv

HPC

others

Import
• DB, Datei,
• von Hand, Web-Interf.

Provisionierung,
• automatisch
• Selbstprovisionierung
• ev. mit Approval

Gespeicherte Personenattribute

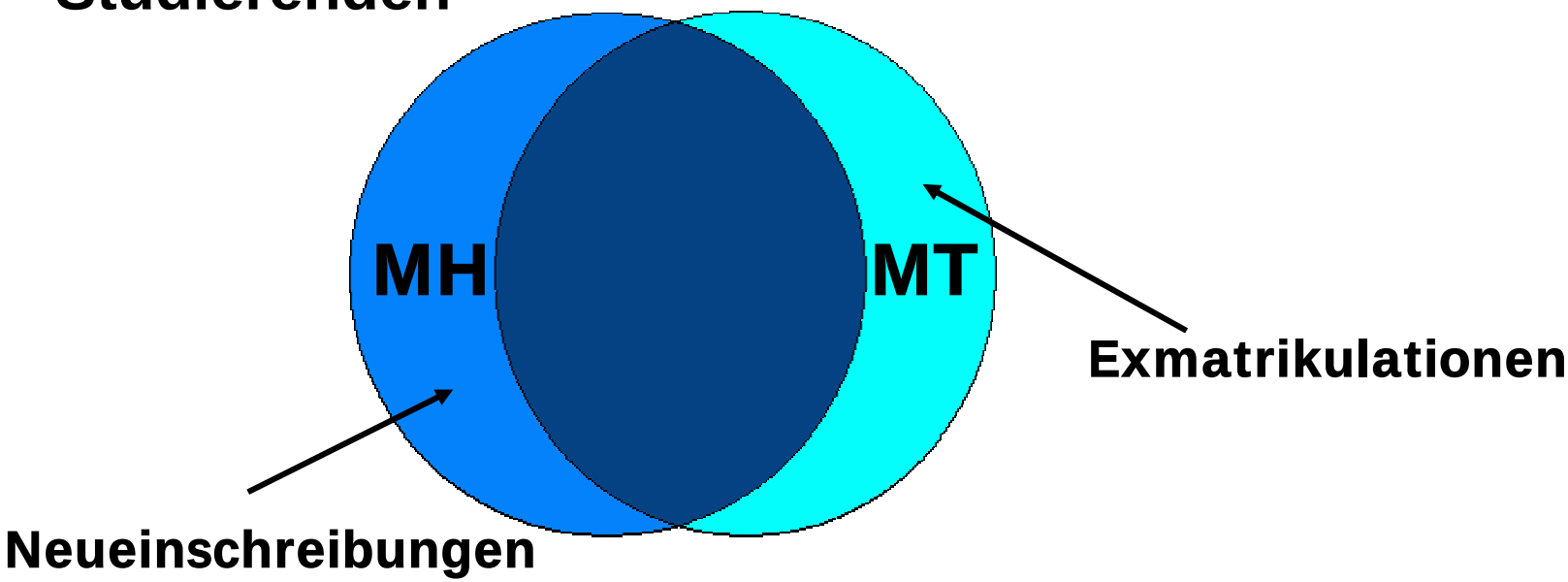
- **Prinzip**
  - So wenig wie möglich
  - So viel wie nötig
- **Konkret**
  - Name
  - UID (ohne Semantik), Passwort
  - Emailadresse
  - Anschrift oder Institutszugehörigkeit
  - Verlinkung mit HR-Systemen (SOS, SVA, Alumni, etc)

HR-Feed HIS/SOS

- **HTTPs-Fileupload über Browser/Java-Servlet**
  - Einfach und sicher
  - firewallfreundlich
- **CSV-Datei mit allen Studierenden (z.Z. >30.000)**
- **Bis zu 3 mal wöchentlich (je nach Bedarf, Anstoß durch ZHV Dez 7)**
- **Enthaltene Informationen:**
  - Matrikelnummer
  - Name, Anschrift
  - Freischaltcode (einmal PIN, per Postweg an Stud.)

Ablauf des HIS/SOS Abgleiches

- **Bildung der Mengen MH bzw. MT aus den Matrikelnummern in HIS/SOS bzw. ITIM**
- **Die Differenzmengen MH-MT und MT-MH liefern die neu immatrikulierten und exmatrikulierten Studierenden**



Ablauf des HIS/SOS Abgleiches

- **Abbildung zwischen ITIM u. HIS/SOS über 2 Attribute:**
  - Matrikelnummer
  - Statusfeld
- **Für neue Stud. werden neue Identitäten angelegt**
  - rwthreplicationcode: SOS;123456
  - rwthreplicationstatus: SOS;active
- **Exmatrikulierte Stud. werden markiert, Identitäten und Abbildung bleiben erhalten:**
  - rwthreplicationcode: SOS;123456
  - rwthreplicationstatus: SOS;deleted

Ablauf des HIS/SOS Abgleiches

- **Programmlauf benötigt unter 4 Minuten, kann also problemlos mehrfach täglich laufen.**
- **Vorteile:**
  - kurzfristig realisierbar, auch ohne Stagingtabellen etc.
  - Konsistenz der Daten gegenüber Stagingtabellen
  - Weniger Vorbehalte als bei Direktanbindung
  - Bei erneuter Immatrikulation wird die alte Zuordnung wieder hergestellt.
  - Eine Person in ITIM kann mehren Identitäten in führenden Systemen zugeordnet sein

Ablauf des HIS/SVA Abgleiches

- **Problematik:**
  - hohe Überlappung mit HIS/SOS (Hiwis, Doktoranden)
  - Lösung in ITIM auf Basis des Namensvergleichs kann nicht so gut sein wie eine Lösung an der Quelle, also bei der Einstellung
  - Keine Verteilung von Freischaltcodes/PINs bei der Einstellung
  - Personaldaten sind politisch sensitiv (Personalrat)

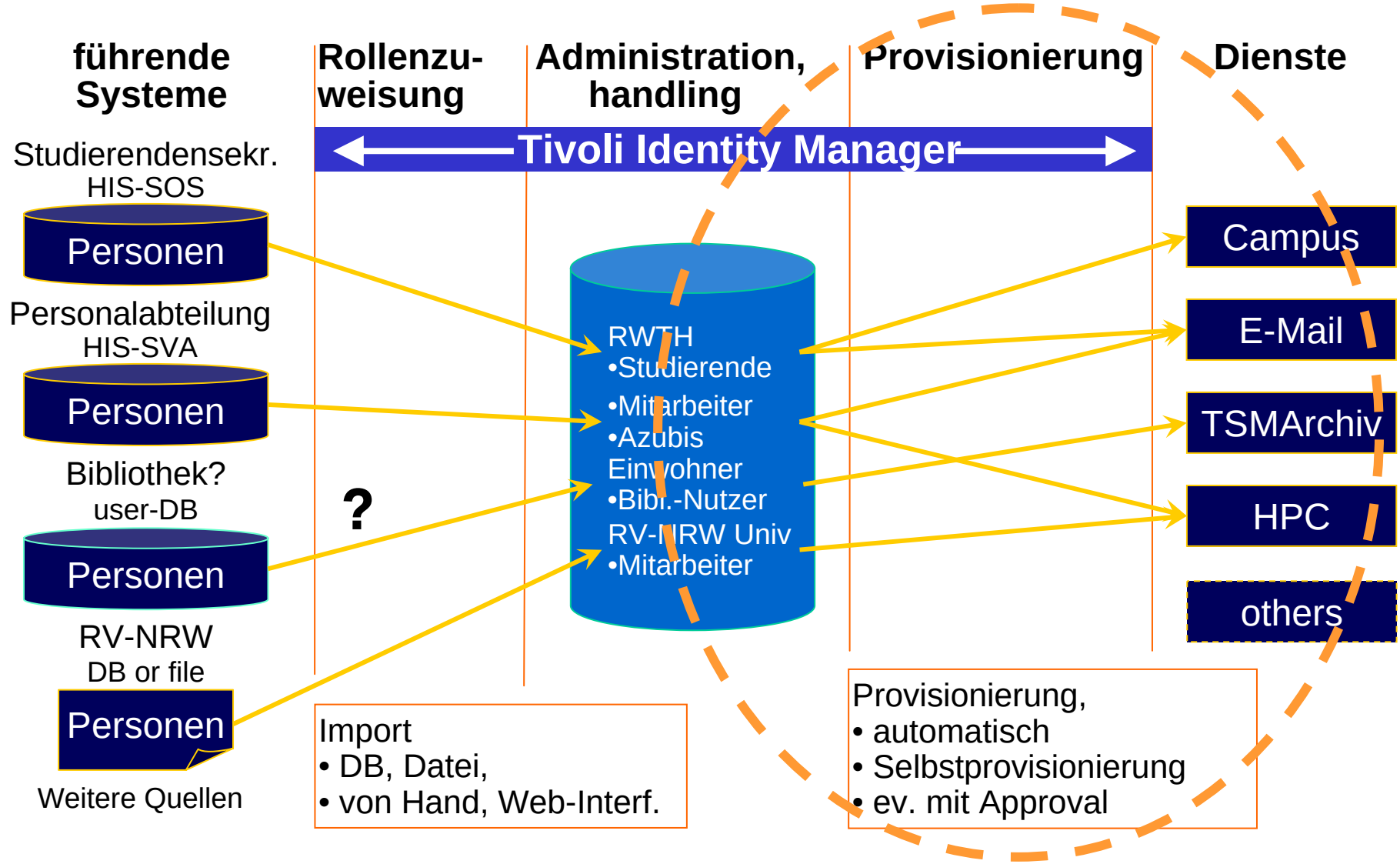
Ablauf des HIS/SVA Abgleiches (2)

- **Vorläufige Lösung:**
  - Übermittlung aller Änderungen in HIS/SVA beschränkt auf:
    - TH-Personalnummer, Name, Institutszugehörigkeit
  - Nutzung der Daten nur bei Vergabe der Rolle „Mitarbeiter“ und zum Entzug dieser Rolle
  - Datenumfang reicht **nicht** aus um Personen in ITIM anzulegen
  - Datenumfang ist gut genug, um vorhandene Personen zu Mitarbeitern zu machen.
- **Entgültige Lösung: später**

Ablauf des HIS/SVA Abgleiches (3)

- **Mitarbeiterstatus an vorhandene Person zuweisen:**
- **Abbildung zwischen ITIM u. HIS/SVA über Attribute:**
  - TH-Empfängernummer
  - Statusfeld
- **Neue Attribute für Person in ITIM:**
  - rwthreplicationcode: SVA;654321
  - rwthreplicationstatus: SVA;active
- **Javaanwendung für Statusänderung mit Parameter:**
  - ITIM-UID, Passwort, TH-Empfängernummer

2.2 Zielsysteme



Regeln für die Provisionierung

- **Fragen zur Ermittlung von Provisionierungsregeln**
  - Welche Parameter werden benötigt
  - Wie werden die Parameter für Accounts gebildet
  - Wer darf Dienste nutzen
  - Wer muss ggf. zustimmen
  - Wer muss ggf. weitere Informationen liefern?
- **Konfiguration in LDAP-Schema und ITIM-Weboberfläche**
- **Dienste können „stateless“ oder „statefull“ sein**

Beispiele

- **Online-Dienste**
  - Zweck: VPN, WLAN, Einwahl, DFN@Home, UniDSL
  - Nutzung: durch alle Studierenden und Mitarbeiter
  - Parameter: UID, Passwort
- **TSM-Archiv**
  - Zweck: Nutzung des Bandroboters
  - Nutzung: durch Mitarbeiter
  - Parameter: IKZ, archivedelete, backupdelete, clientcompression, cn, eraccountstatus, eruid, keepmp, locked, maxnummp, nodetype, tsmdomainmembership, validateprotocol, eraccountcompliance, mail, sn

Beispiel

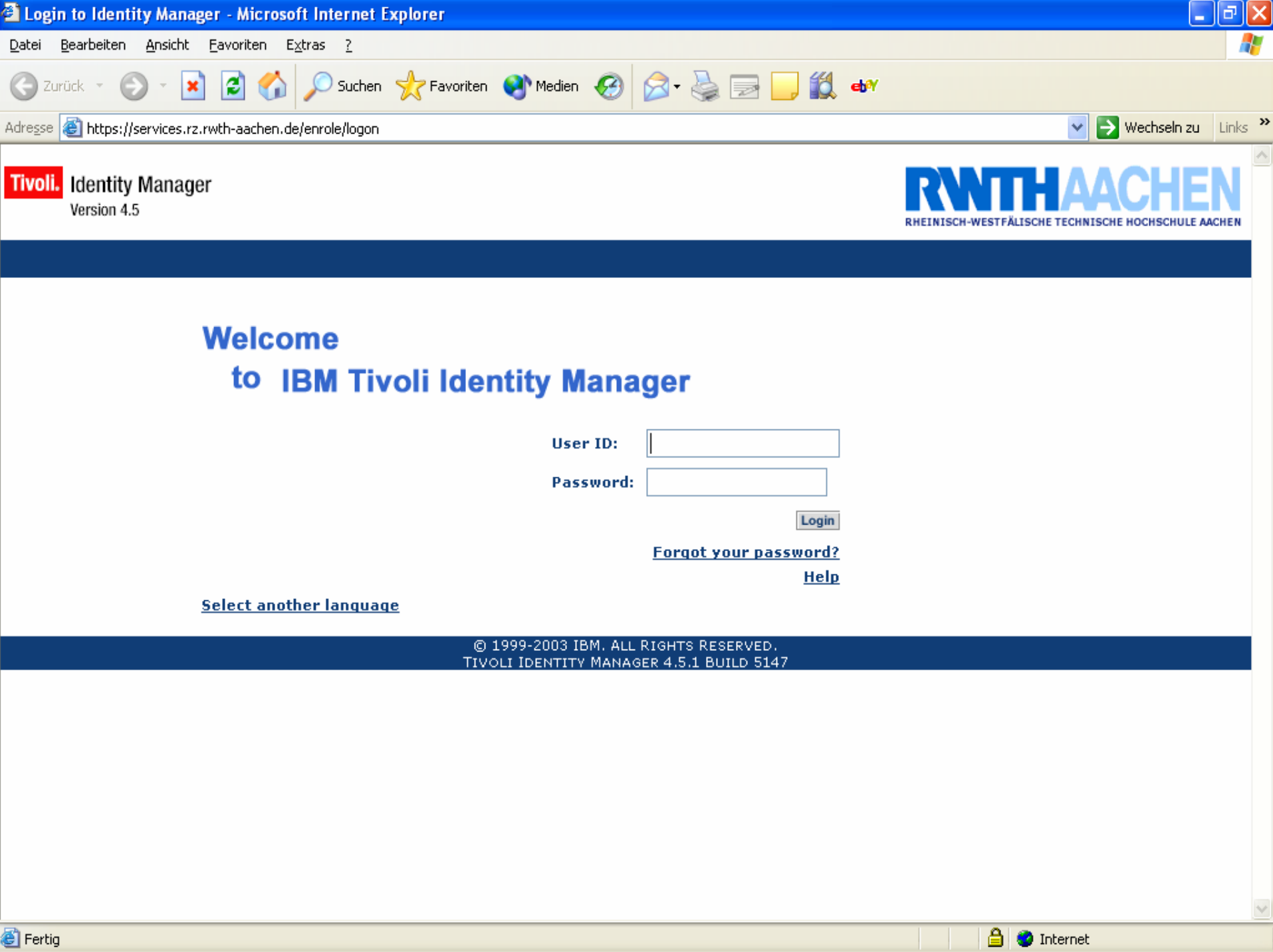
- **Email**
  - Zweck: Email
  - Nutzung: Mitarbeiter, Studierende, Alumni
  - Parameter: UID, Passwort, Mailadresse, Weiterleitungsadressen, Mailaliases, Maildelivery-Option
  - Weitere Parameter werden im Mailsystem gepflegt:
    - Abwesenheitsnotiz
    - Adressbuch
    - Quotierung
    - Mailfilter

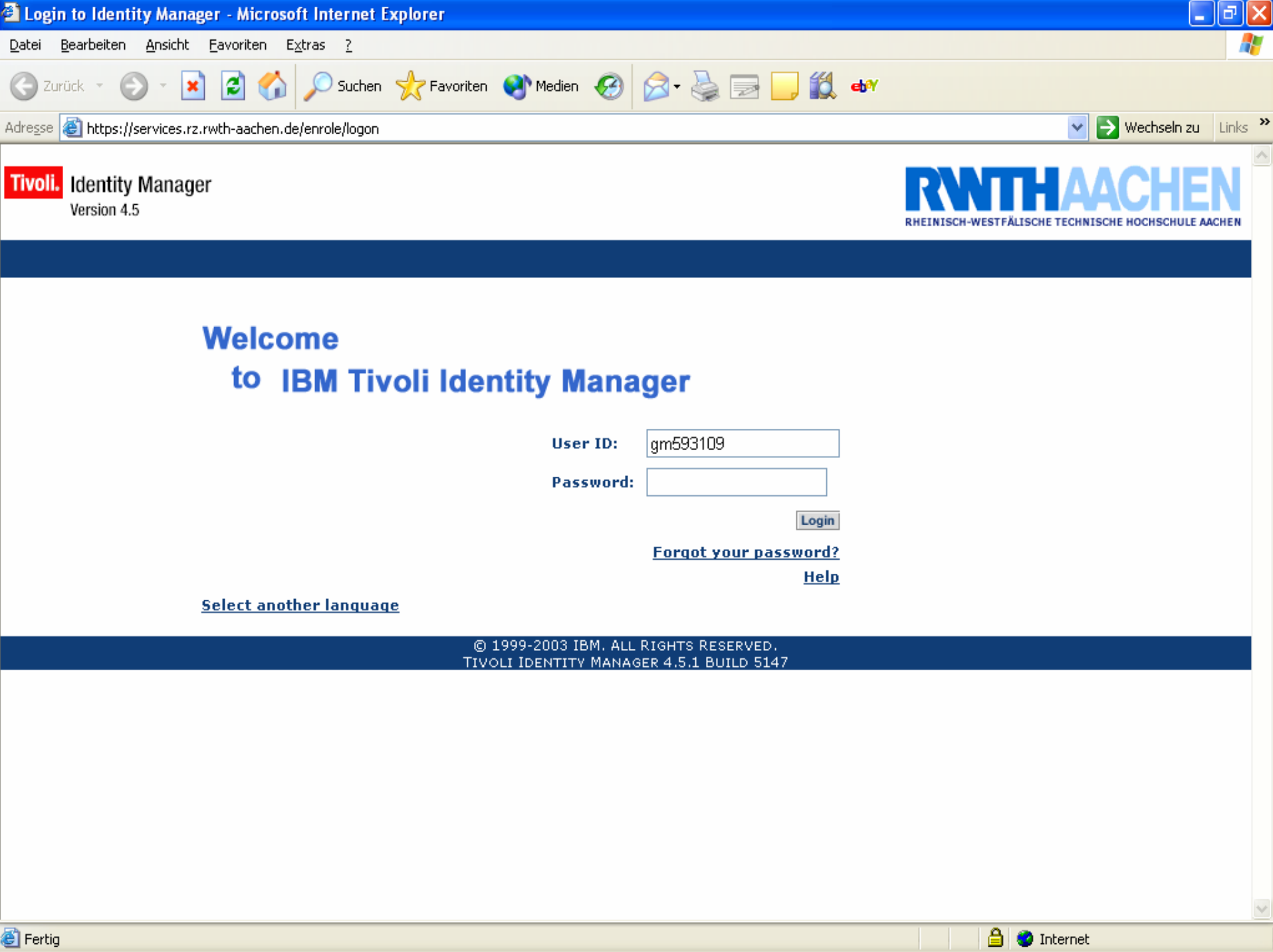
Konfiguration der Agenten

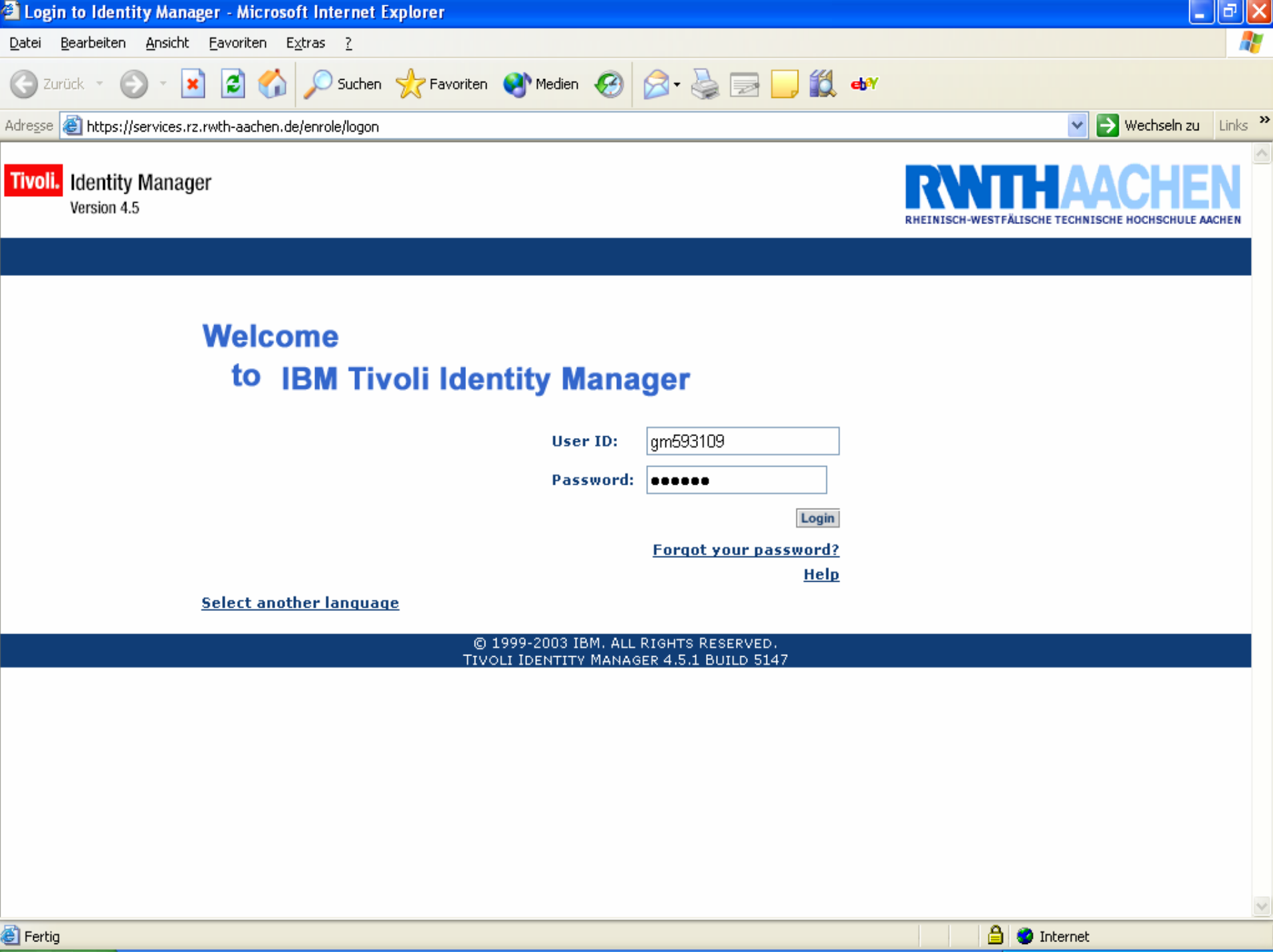
- **Agenten führen die Provisionierung in den Zielsystemen per HTTPs/DSML durch:**
  - Add Request
  - Delete Request
  - Change Request
  - Reconciliation
- **Agenten für:**
  - Windows 2000
  - Solaris / Unix
  - Universalagent: IBM Directory Integrator (IDI)

IBM Directory Integrator (IDI)

- **(fast) universelles Werkzeug zur Konvertierung von Datenbeständen**
- **Assemblylines mit einer Vielzahl von Connectoren oder Eventhandlern. Beispiele:**
  - LDAP
  - SQL (JDBC)
  - CSV
  - DSML
- **Hooks in Java oder JavaScript**
- **Graphische Programmierung**


Login to Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/logon
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
Welcome
to IBM Tivoli Identity Manager
User ID:
Password:
Login
Forgot your password?
Help
Select another language
© 1999-2003 IBM. ALL RIGHTS RESERVED.
TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147
Fertig
Internet


Login to Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Medien
Adresse
https://services.rz.rwth-aachen.de/enrole/logon
Wechseln zu
Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
Welcome
to IBM Tivoli Identity Manager
User ID:
gm593109
Password:
Login
Forgot your password?
Help
Select another language
© 1999-2003 IBM. ALL RIGHTS RESERVED.
TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147
Fertig
Internet


Login to Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/logon
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
Welcome
to IBM Tivoli Identity Manager
User ID: gm593109
Password: ••••••
Login
Forgot your password?
Help
Select another language
© 1999-2003 IBM. ALL RIGHTS RESERVED.
TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147
Fertig
Internet

IBM Tivoli Identity Manager - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse https://services.rz.rwth-aachen.de/enrole/change_password Wechseln zu Links

Tivoli. Identity Manager
Version 4.5

RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

HOME | REPORT | HELP | Logout

User ID: gm593109

You Are Here: Home > Manage Password

- Manage Passwords
- Manage Accounts
- Access To Do List
- View Pending Requests
- View Completed Requests
- Access Personal Information
- Delegate Authority
- Password Challenge Response

Change | Create Password

New Password

Confirm Password

Create Password

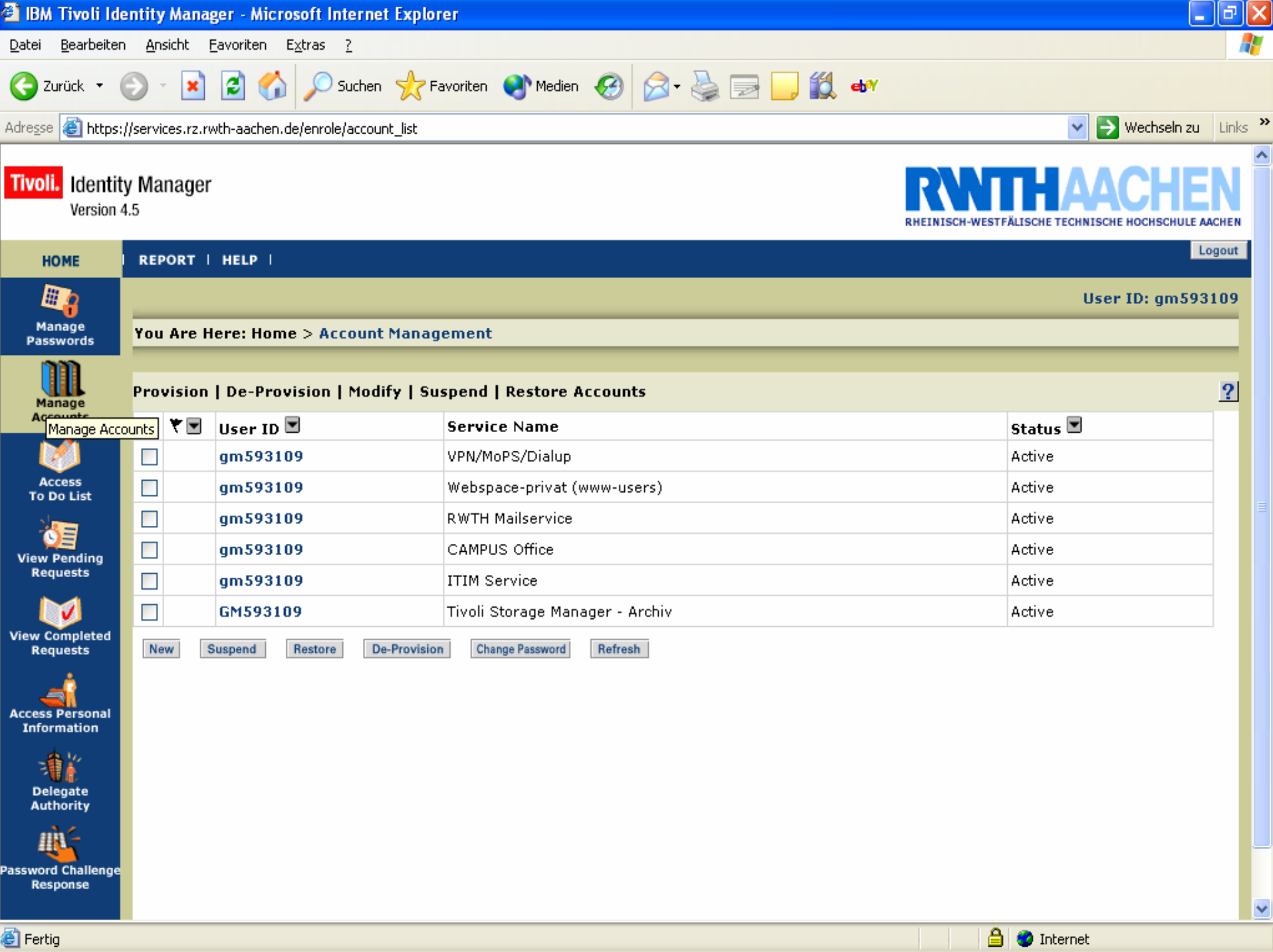
Effective Date 12 13 2004 18:30 Schedule Immediately

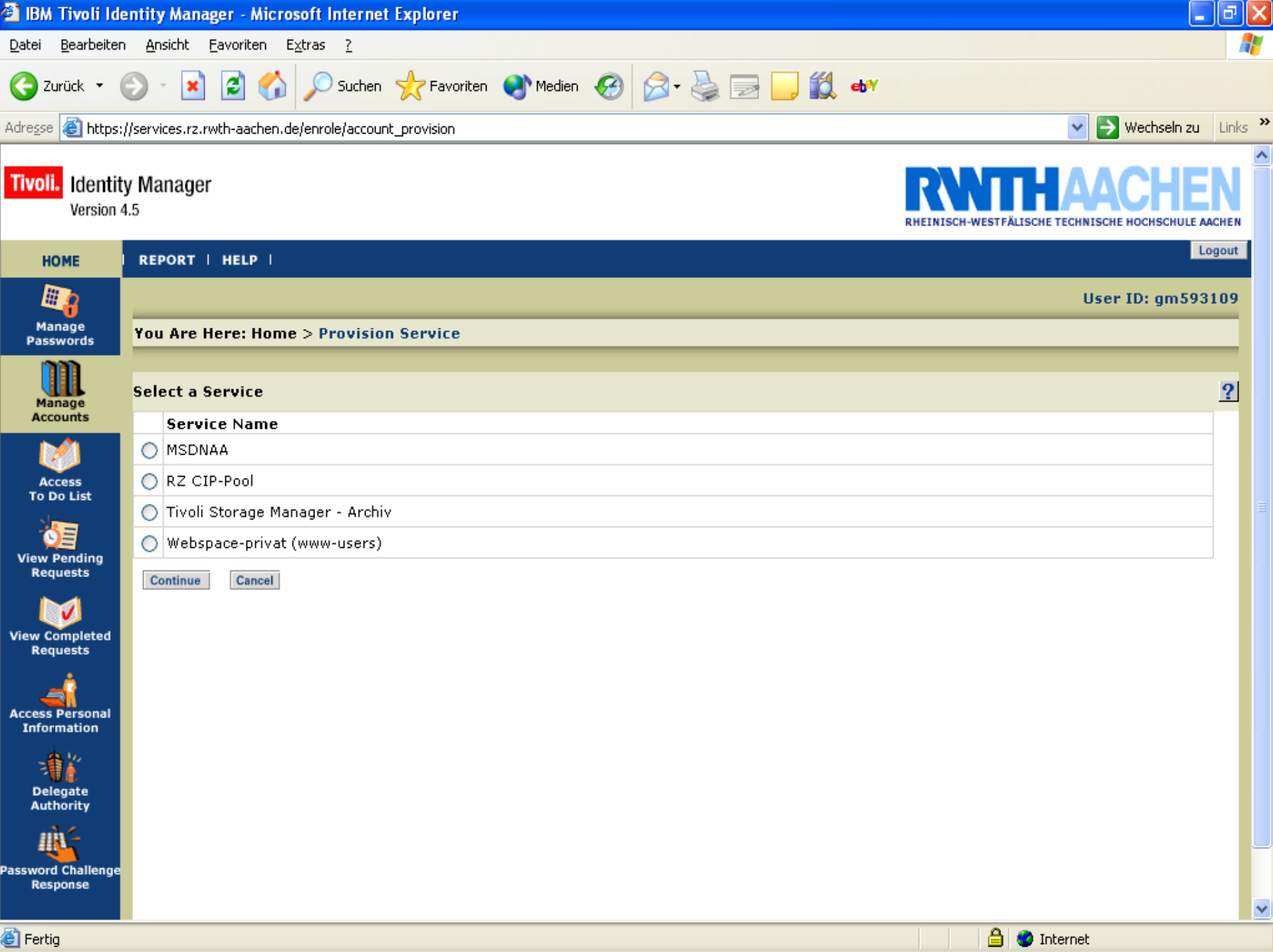
	Rules	Service	Login	Status
☑		VPN/MoPS/Dialup	gm593109	Active
☑		CAMPUS Office	gm593109	Active
☑		RWTH Mailservice	gm593109	Active
☑		Tivoli Storage Manager - Archiv	GM593109	Active
☑		Webspace-privat (www-users)	gm593109	Active
☑		ITIM Service	gm593109	Active

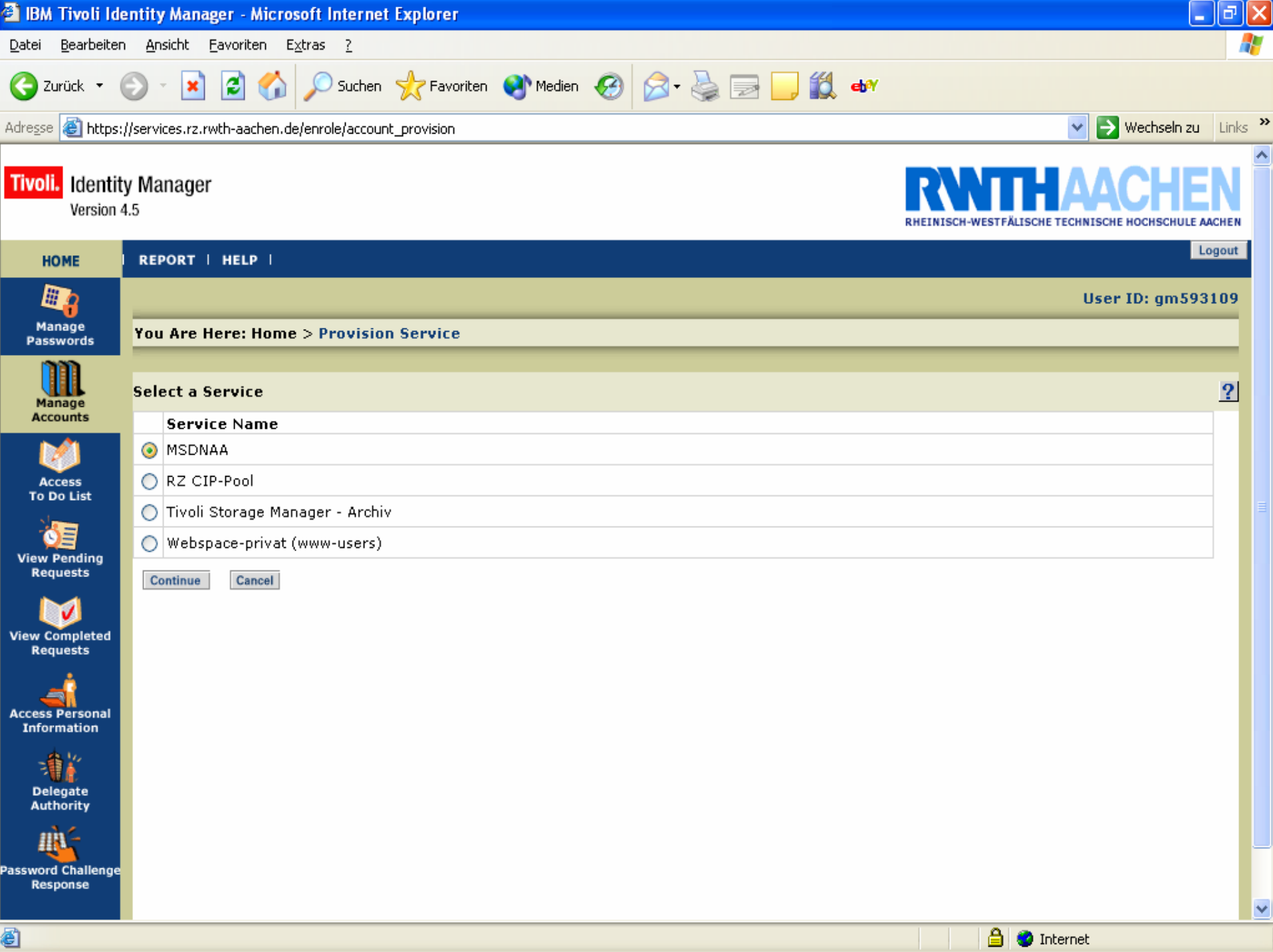
Submit Reset

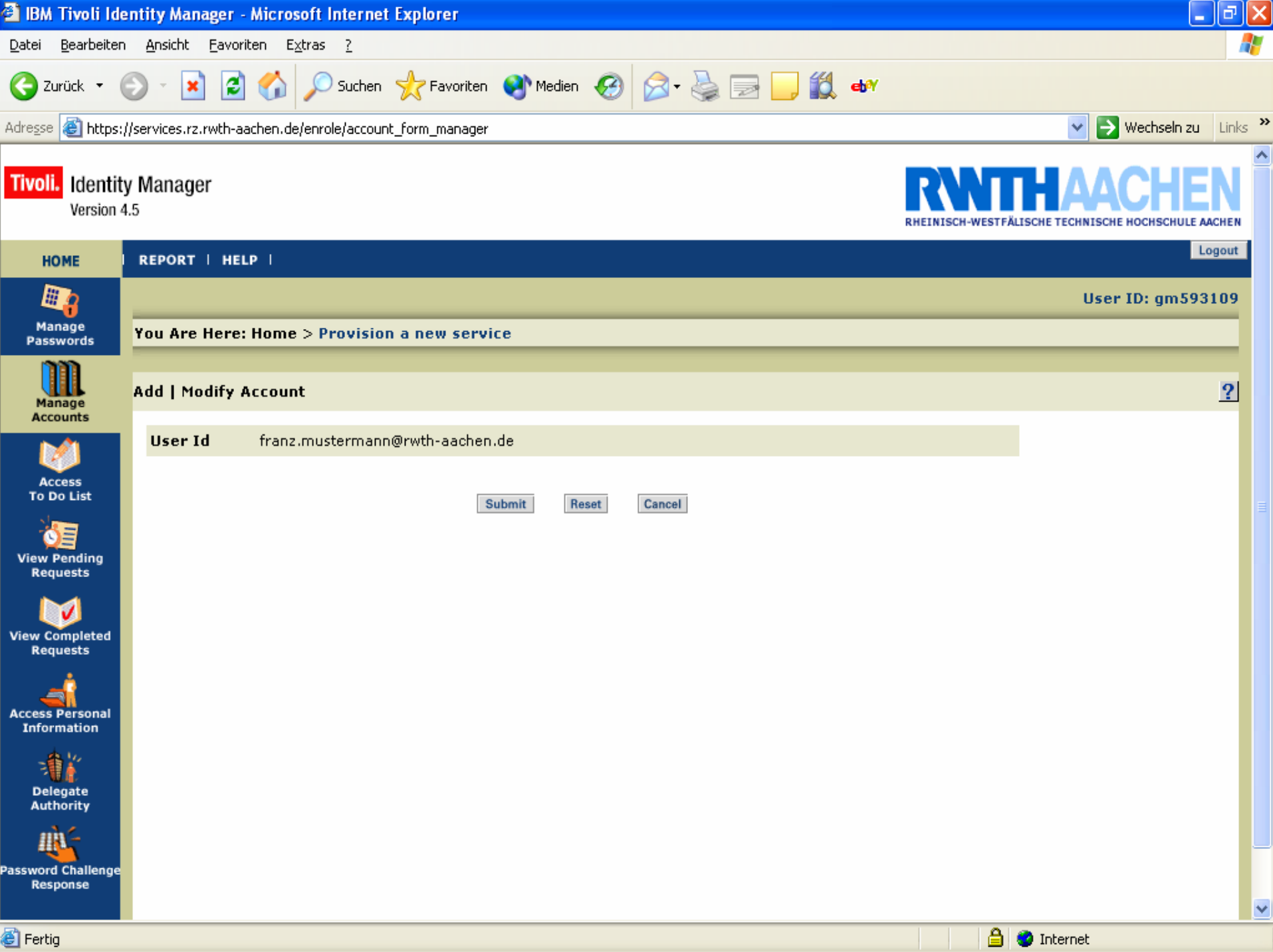
View Combined Password Rules

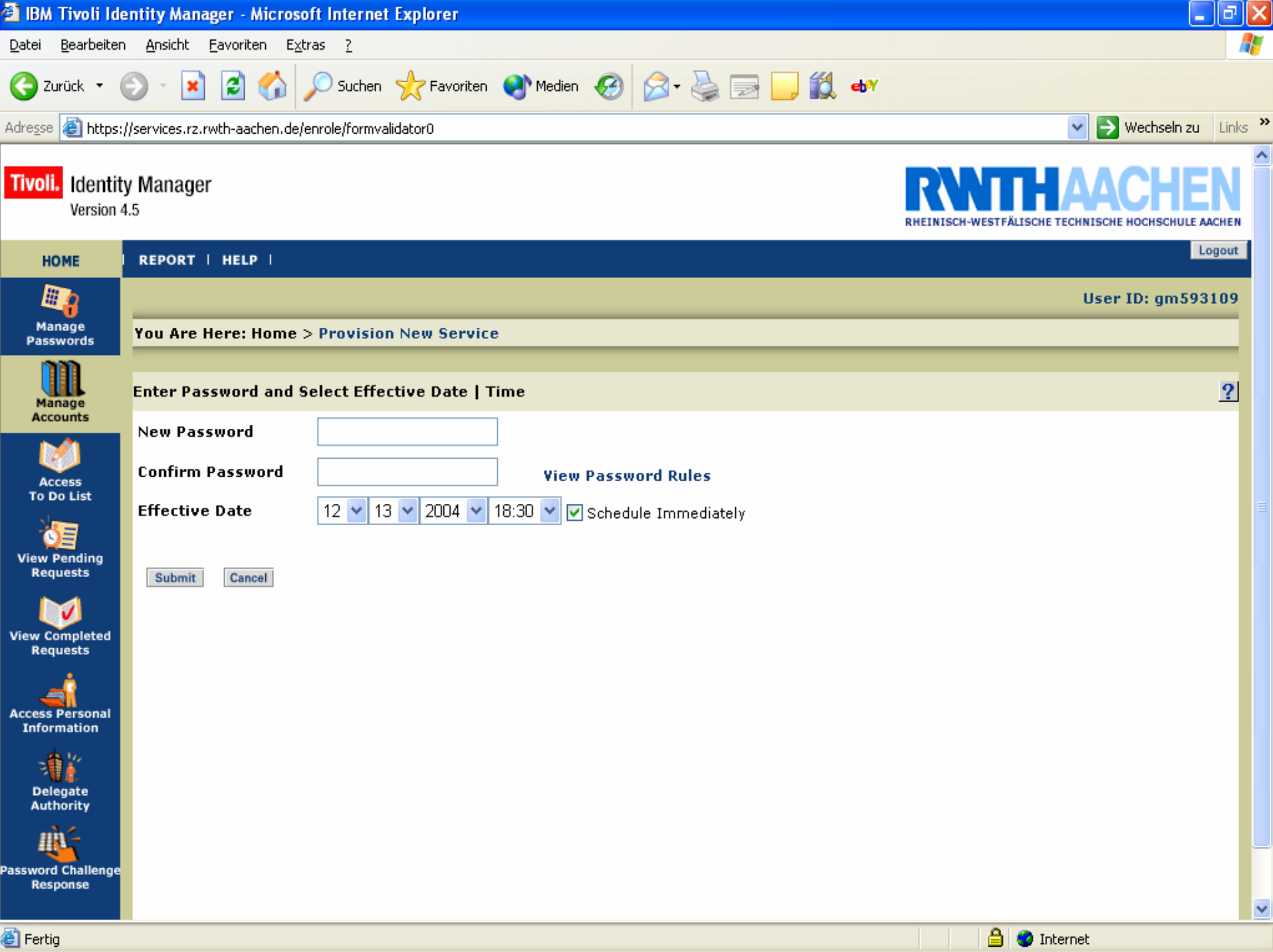
Internet

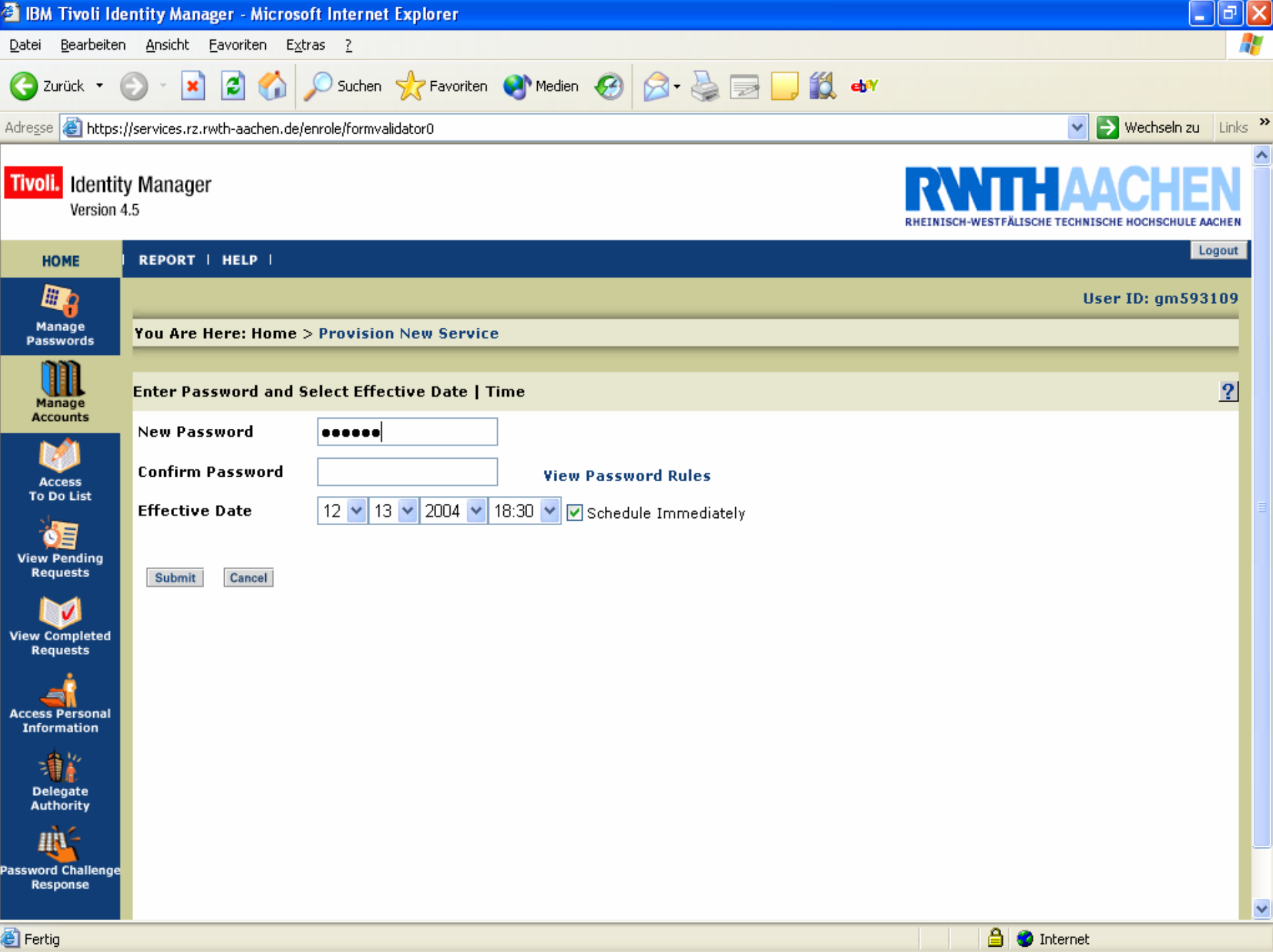

IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/account_list
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME REPORT | HELP |
Logout
User ID: gm593109
You Are Here: Home > Account Management
Manage Passwords
Manage Accounts
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
Provision | De-Provision | Modify | Suspend | Restore Accounts
User ID
Service Name
Status
gm593109 VPN/MoPS/Dialup Active
gm593109 Webspace-privat (www-users) Active
gm593109 RWTH Mailservice Active
gm593109 CAMPUS Office Active
gm593109 ITIM Service Active
GM593109 Tivoli Storage Manager - Archiv Active
New Suspend Restore De-Provision Change Password Refresh
Fertig
Internet

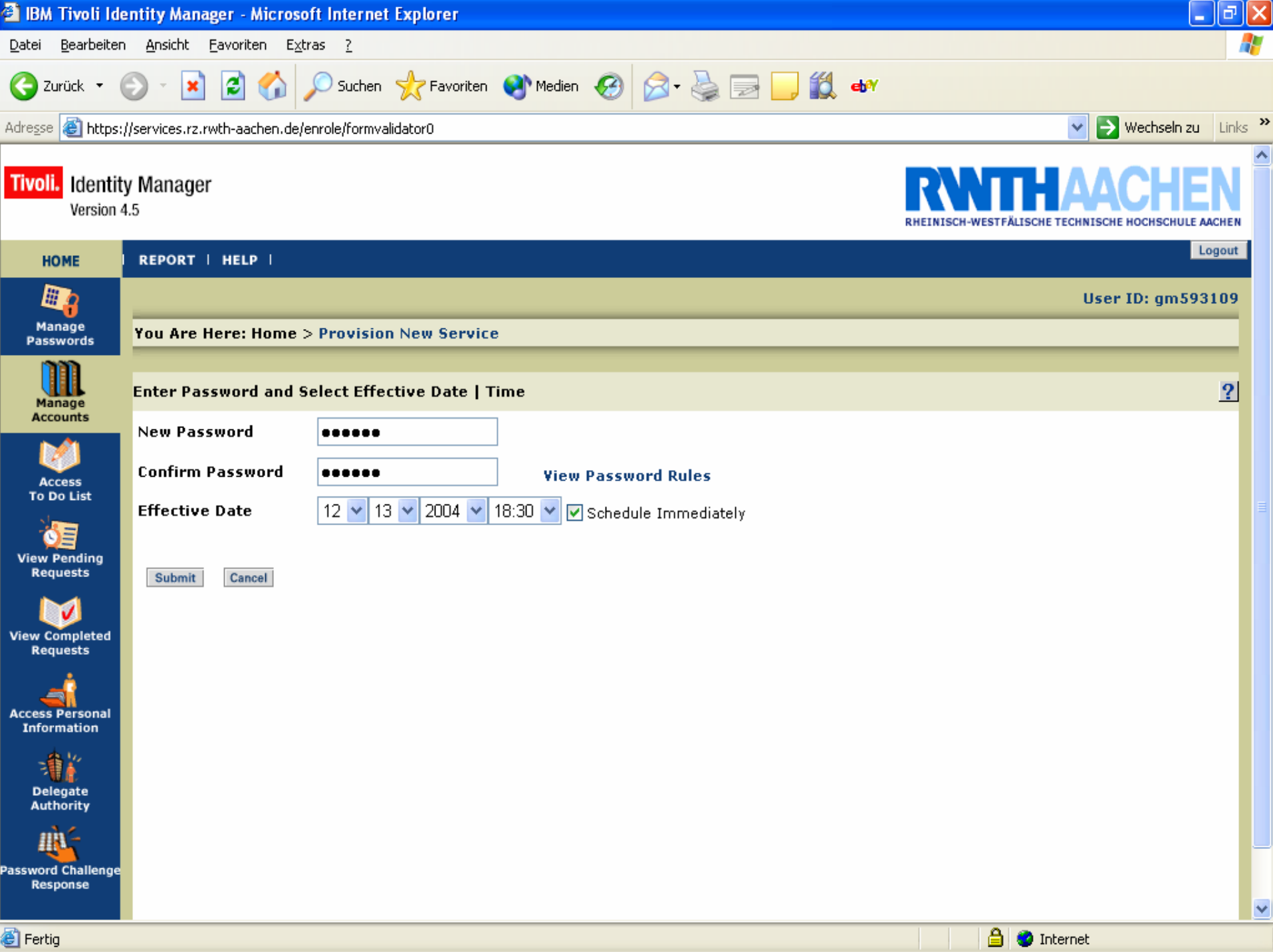

IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/account_provision
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Provision Service
Select a Service
Service Name
MSDNAA
RZ CIP-Pool
Tivoli Storage Manager - Archiv
Webspace-privat (www-users)
Continue
Cancel
Fertig
Internet

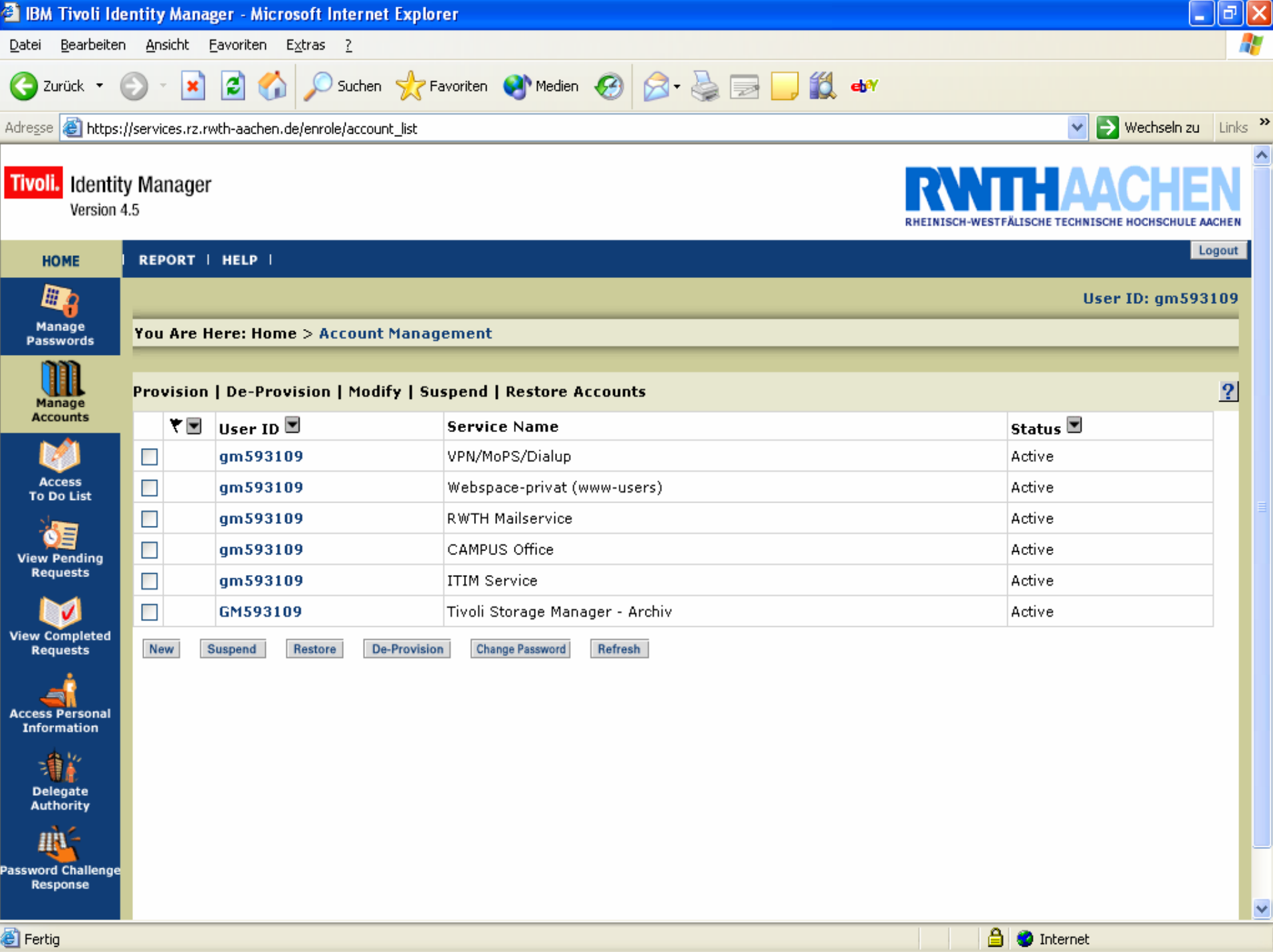

IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/account_provision
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Provision Service
Select a Service
Service Name
MSDNAA
RZ CIP-Pool
Tivoli Storage Manager - Archiv
Webspace-privat (www-users)
Continue
Cancel
Internet

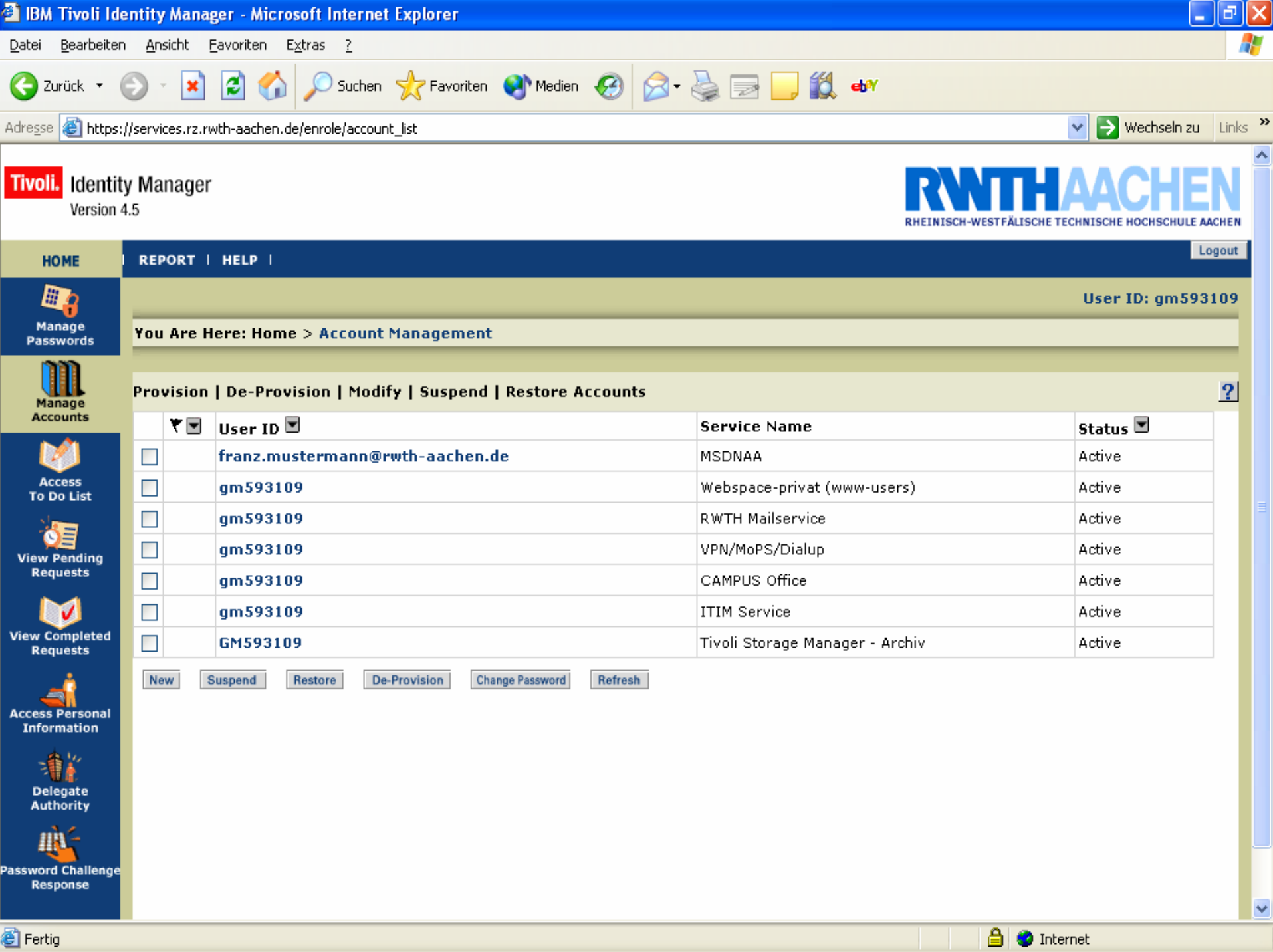

IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/account_form_manager
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Provision a new service
Add | Modify Account
User Id franz.mustermann@rwth-aachen.de
Submit Reset Cancel
Fertig
Internet

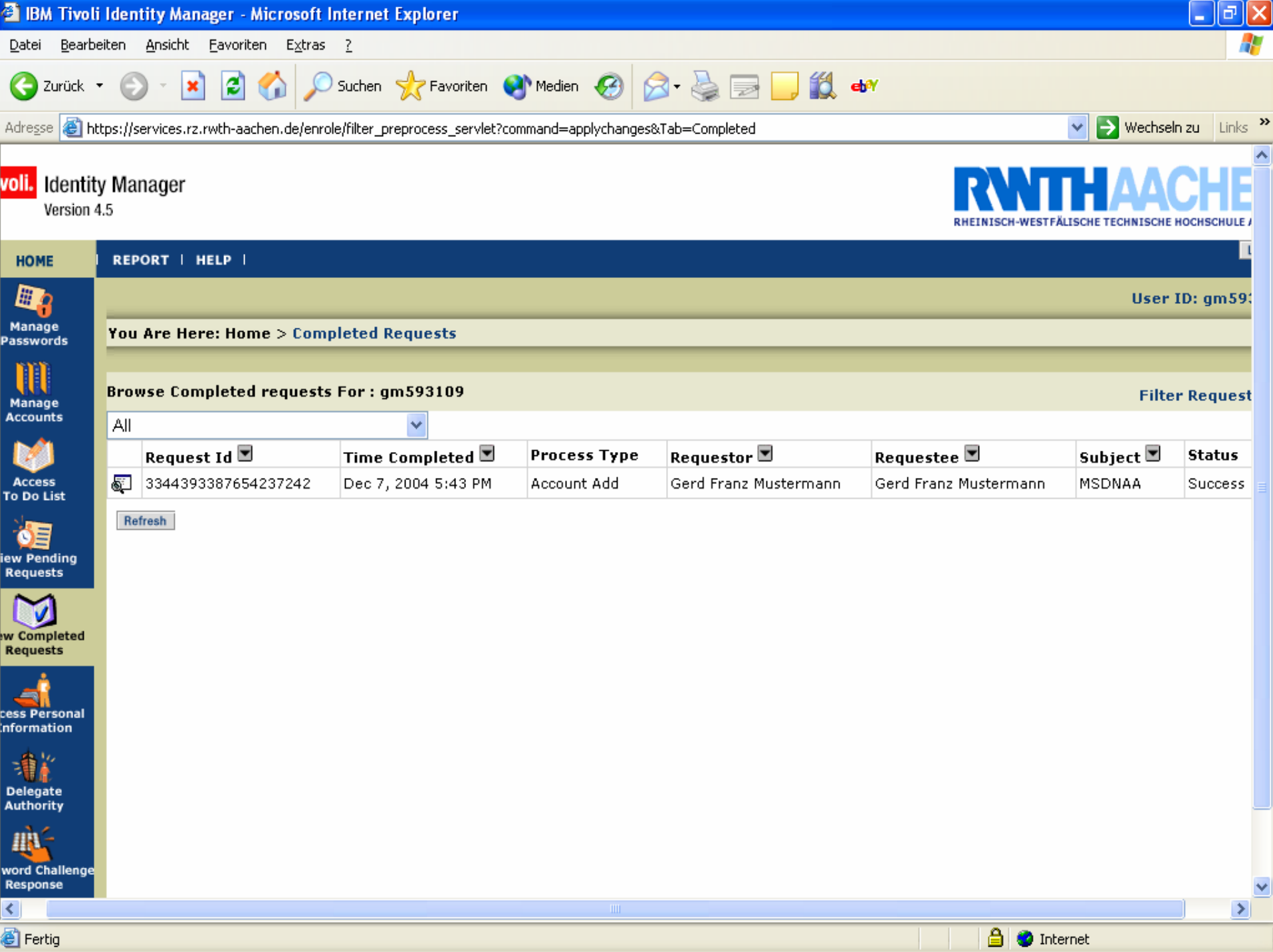

IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/formvalidator0
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Provision New Service
Enter Password and Select Effective Date | Time
New Password
Confirm Password
View Password Rules
Effective Date
12 13 2004 18:30
Schedule Immediately
Submit
Cancel
Fertig
Internet

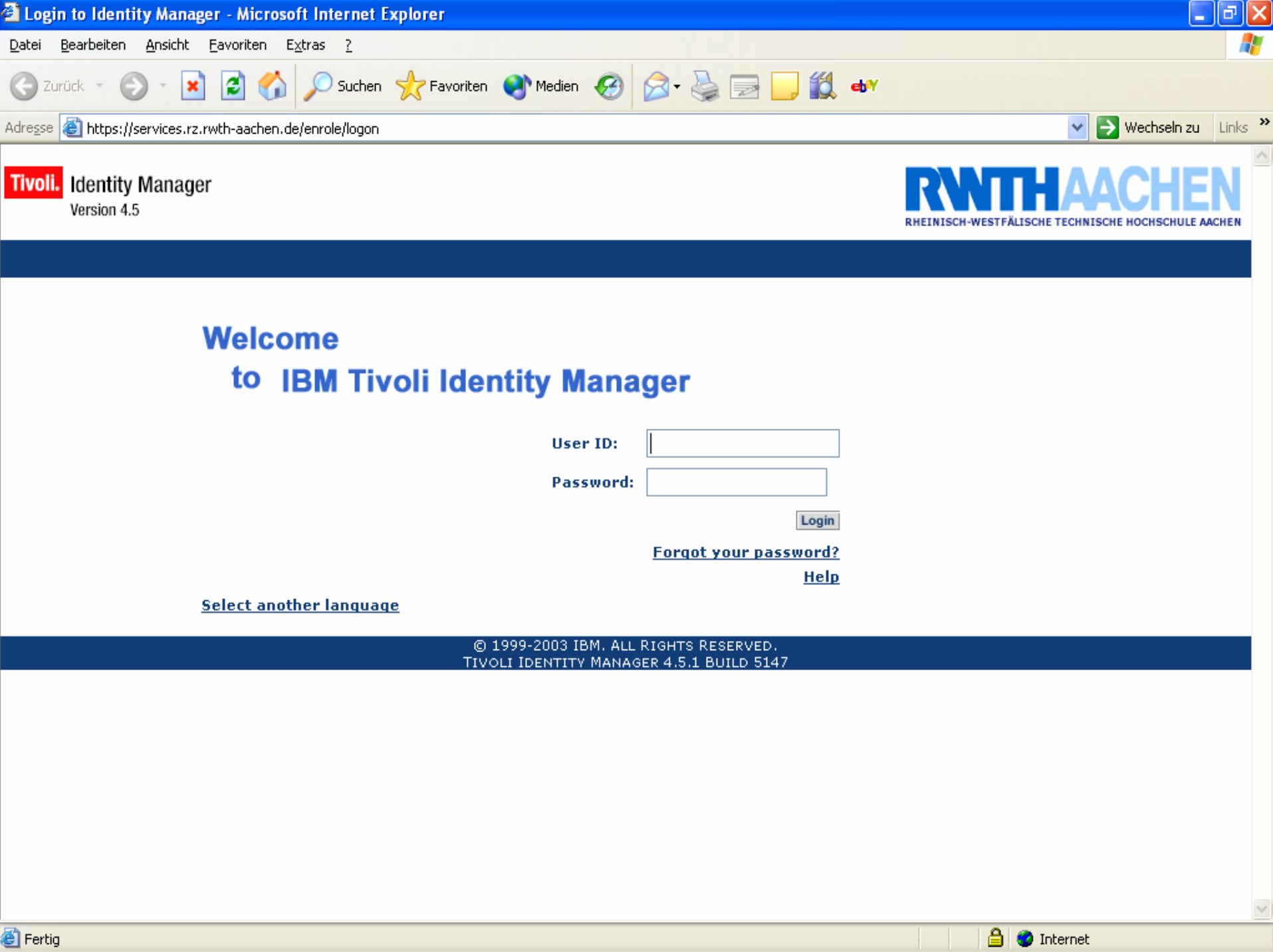

IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/formvalidator0
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Provision New Service
Enter Password and Select Effective Date | Time
New Password
Confirm Password
View Password Rules
Effective Date
12 13 2004 18:30
Schedule Immediately
Submit
Cancel
Fertig
Internet


IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/formvalidator0
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Provision New Service
Enter Password and Select Effective Date | Time
New Password
Confirm Password
View Password Rules
Effective Date
12 13 2004 18:30
Schedule Immediately
Submit
Cancel
Fertig
Internet


IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/account_list
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Account Management
Provision | De-Provision | Modify | Suspend | Restore Accounts
User ID
Service Name
Status
gm593109 VPN/MoPS/Dialup Active
gm593109 Webspace-privat (www-users) Active
gm593109 RWTH Mailservice Active
gm593109 CAMPUS Office Active
gm593109 ITIM Service Active
GM593109 Tivoli Storage Manager - Archiv Active
New
Suspend
Restore
De-Provision
Change Password
Refresh
Fertig
Internet


IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/account_list
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
HOME
REPORT | HELP |
Logout
Manage Passwords
Manage Accounts
Access To Do List
View Pending Requests
View Completed Requests
Access Personal Information
Delegate Authority
Password Challenge Response
User ID: gm593109
You Are Here: Home > Account Management
Provision | De-Provision | Modify | Suspend | Restore Accounts
User ID
Service Name
Status
franz.mustermann@rwth-aachen.de MSDNAA Active
gm593109 Webspace-privat (www-users) Active
gm593109 RWTH Mailservice Active
gm593109 VPN/MoPS/Dialup Active
gm593109 CAMPUS Office Active
gm593109 ITIM Service Active
GM593109 Tivoli Storage Manager - Archiv Active
New
Suspend
Restore
De-Provision
Change Password
Refresh
Fertig
Internet


IBM Tivoli Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/filter_preprocess_servlet?command=applychanges&Tab=Completed
Wechseln zu Links
Identity Manager
Version 4.5
RWTH AACHE
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE
HOME
REPORT | HELP |
User ID: gm59
You Are Here: Home > Completed Requests
Manage Passwords
Manage Accounts
Access To Do List
iew Pending Requests
w Completed Requests
cess Personal nformation
Delegate Authority
word Challenge Response
Browse Completed requests For : gm593109
Filter Request
All
Request Id
Time Completed
Process Type
Requestor
Requestee
Subject
Status
334439338765423724 2
Dec 7, 2004 5:43 PM
Account Add
Gerd Franz Mustermann
Gerd Franz Mustermann
MSDNAA
Success
Refresh
Fertig
Internet


Login to Identity Manager - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse https://services.rz.rwth-aachen.de/enrole/logon
Wechseln zu Links
Tivoli. Identity Manager
Version 4.5
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN
Welcome
to IBM Tivoli Identity Manager
User ID:
Password:
Login
Forgot your password?
Help
Select another language
© 1999-2003 IBM. ALL RIGHTS RESERVED.
TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147
Fertig
Internet

2.3 Erfahrungen

1. **Einführung**
   - Ausgangslage, Ziele, Architektur
2. **Erfahrungen: Identitätsmanagement des RZ**
   - Überblick, Freischaltprozess für Studierende
   - Quellsysteme: Anbindung der „HR-Feeds“
   - Zielsysteme: Provisionierung neuer Dienste
   - Wandel, Aufwände, Fazit
3. **Ausblick: RWTH-Identitätsmanagement**
   - Was fehlt noch für die RWTH?
   - .. und über die RWTH hinaus.
4. **Zusammenfassung**

Arbeit und Prozesse ändern sich

- **RZ-Mitarbeiter**
  - Abgabe von Verantwortung für Provisionierung. Konzentration auf Qualität des Dienste
  - Keine Standardanfragen von Kunden
- **Kunden (Studierende und Mitarbeiter)**
  - Standardvorgänge können Online (24x7) erfolgen.
  - Kein Durchfragen zu den für den Dienst zuständigen Mitarbeitern
  - Leichter Zugang zu Hilfe für die meisten Fragen (11 Std./5 Tage)
- **Helpdesk-Personal**
  - Vermittler zwischen technischem Personal und „Laien“.
  - Know How: Prozesse, Virenschutz und Beseitigung, Emailkonfiguration, WLAN/VPN

Kosten

- 2 kleine Server
- Softwarekosten (NRW-Landeslizenz für IBM/Tivoli)
- Ca. 8 Personentage Serviceleistung für die Pilotinstallation
- Bislang 1 volle Stelle für 12 Monate
- Im Mittel eine weitere Stelle wechselnd je nach Projektfortschritt
- Beteiligung der Diensterbringer in der Migrationsphase
- → Erheblicher Aufwand für ein mittleres Uni-RZ

Konsequenz

- **Es geht nicht „nebenher“**
- **Es geht nicht ohne erheblichen eigenen Einsatz**
  - Knowhow-Aufbau
  - Internes Wissen ist nicht beim Dienstleister
- **CIO mit Weisungsbefugnis für die beteiligten Stellen oder externer Dienstleister/Moderator ist unabdingbar**

3. RWTH-Identitätsmanagement

1. **Einführung**
   - Ausgangslage, Ziele, Architektur
2. **Erfahrungen: Identitätsmanagement des RZ**
   - Überblick, Freischaltprozess für Studierende
   - Quellsysteme: Anbindung der „HR-Feeds“
   - Zielsysteme: Provisionierung neuer Dienste
   - Wandel, Aufwände, Fazit
3. **Ausblick: RWTH-Identitätsmanagement**
   - Was fehlt noch für die RWTH?
   - .. und über die RWTH hinaus.
4. **Zusammenfassung**

3. RWTH Identity Management

- **Projektgruppe**
  - RZ zusammen mit der Verwaltung (Federführung)
  - Einbeziehung eines externen Projektpartners
  - In engem Kontakt mit anderen NRW-Hochschulen
- **Projektziele**
  - Identity Management für die RWTH
  - „lifelong“ RWTH Kundennummer

HR-Feeds auf der TODO-Liste

Aktuell: Identifizierung der Mitarbeiter

- **Aktuell: Realisierung der Prozesse für Mitarbeiter**
- **Anschließend:**
  - Gäste, Gastwissenschaftler (=nicht SVA Mitarbeiter)
  - Alumni (neue und existierende)
  - Stadtnutzer der Bibliothek
  - Klinikmitarbeiter? (SAP)
  - ?

Was fehlt …

- **Saubere Prozesse erfordern saubere Ausgangsdaten**
  - Studierende:
    - Abgleich mit HIS/SOS
    - Regelmäßige Information über Abgänge
  - Mitarbeiterdaten:
    - nur aus HIS/SVA, nur geringer Umfang
    - Regelmäßige Information über Abgänge
  - Gäste:
    - individuelle Anmeldung über die Hochschuleinrichtungen
    - Keine Kenntnis über Abgänge
- **Zuständigkeit für mehrfache Gruppenzugehörigkeit?**

Jenseits der RWTH

- **ITIM organisiert Identitäten in Containern**
- **RWTH Studierende und Mitarbeiter in einem Container**
  - Es fehlt die klare Trennung
  - Zuordnung zu FB oft willkürlich, nicht eindeutig
- **Aufnahme von Angehörigen anderer Hochschulen in jeweils eigene Container**
  - Dezentrale Pflege der Daten
  - Zentrales provisionieren, auch von Diensten außerhalb der RWTH

Zusammenfassung und Ausblick

- **ITIM ist seit 7/04 im Produktionsbetrieb**
  - >40.000 Identitäten, >125.000 Accounts
  - 11 provisionierte Dienste
- **erheblicher Investitionsaufwand, 1 Jahr Vorlauf**
- **zentralisierte Benutzerverwaltung/Help-Desk reduziert Aufwände bei den Diensten deutlich**
  - Manche Dienste werden erst dadurch realisierbar
- **beschleunigt neue Dienste einzuführen (MSDN-AA)**
- **Ausweitung auf hochschulweites Identitätsmanagement läuft**
  - Kooperation mit NRW-Hochschulen

Vielen Dank für Ihre Aufmerksamkeit !