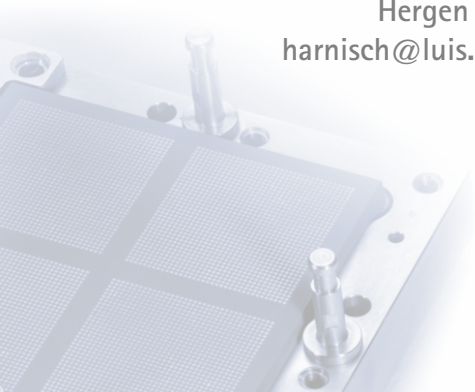


Identitätsmanagement

Kundentagung

Hergen Harnisch

harnisch@luis.uni-hannover.de



Was ist IdM?

Verwaltung personenbezogener Accounts & Berechtigungen:

- Automatisierung und Prozesse,
Anlegen und Löschen von Accounts & Rollen
- Mitarbeiter & Studierende, nur begrenzt Externe
- teilweise Organisations- und Personendaten
- Ziel: Automatisierung und Erhöhung der Sicherheit

LUH

Fokus auf zentrale Systeme mit Grobberechtigungen

2008 Einführung für Studierende

2017 Erweiterung auf Mitarbeiter

IT-Dienste & Passwörter

Nicht nur ein Account und ein Passwort!

- Nutzer bestellt einzelne Dienste aus Liste
- grundsätzlich je Dienst ein Passwort
- Dienst kann aber auch ein SSO-System sein (z.B. PCs, Webseiten)

Singe-Account- / Single-Passwörter-Systeme wären problematisch:

- unterschiedlicher Schutzbedarf
- Passwortspeicherung für einzelne Dienste
- Nutzung von unterschiedlichen Geräten aus
- Sperrung bei Missbrauch einzelner Dienste
- ... und das in Zeiten von BYOD, Identitätsdiebstahl & Key-Loggern

Roll-Out Mitarbeiter

Stand Roll-Out:

- Roll-Out für alle OEs und Großteil der Mitarbeiter abgeschlossen
- spezielle Nutzergruppen noch in Klärung mit Dez.2
- neue Mitarbeiter derzeit noch „händisch“

Leider erst später (wg. EPV):

- einige Nutzergruppen erst später möglich
- vernünftige Rollen (z.B. OE-bezogen)
- daher unzureichend für viele dezentrale Systeme

Angebundene Systeme

- WLAN/VPN
- Cloud-Dienste
- Netzwerk-Shares (beginnend mit IdM-Home)
- PC-Login für Pools (derzeit Linux, Windows in Planung)
- Webseiten über WebSSO (auch SAP-SLcM),
auch Dienste der DFN-AAI & Edugain

In Planung:

- persönliche Mail-Konten (auch Exchange)
- zentrale Webseiten, vorallem Stud.IP

Einordnung in LUH

Was ist mit BIAS?

- BIAS zunehmend durch IdM ersetzt für persönliche Accounts; Migration nach Diensten, LUIS fordert ggf. zum Wechsel auf
- BIAS aber noch für Funktions-Accounts, OE-bezogene Zugänge; langfristig aber auch Lösung über IdM

Was ist mit Gästen?

- längerfristige kommen ins IdM (über Meldung an Dez.2)
- kurzfristige über Gästetickets etc.
- derzeit noch Ausnahmen/Sonderfälle über BIAS

Dezentrale Systeme?

- kommen später, nicht immer sinnvoll

Ausblick

Derzeit stehen IdM-interne Arbeiten an:

- Vereinfachung bei Neueinstellung
- Konsolidierung
- Studierendenkarte
- Betrachtungen für EPV in SAP:

Auch weitere Zielsysteme:

- Mail, Stud.IP, zentrale Webdienste (s.o.)
- dezentrale Webanwendungen über WebSSO möglich
- grundsätzlich immer Beratung & indiv. Absprache nötig

vgl. <https://www.luis.uni-hannover.de/idm-admin.html>