IAM - Authentifizierung und Autorisierung an der ETH

«IAM» bezeichnet die zentrale Authentifizierungs- und Autorisierungs-Infrastruktur der ETH, welche den Zugriff zu den Informatik-Basis-Dienstleistungen der ETH regelt: Zugang zum ETH-Netzwerk via VPN, Wireless-LAN, Netzanschluss, E-Mail, zentraler Speicherplatz auf dem NAS, Zugang zu den Computern in den öffentlichen Computerräumen für Studierende usw.

Die Authentifizierungs- und Autorisierungsdaten werden auf dem zentralen IAM-System «DirX» verwaltet. Dieses steuert die Directories openLDAP, Active Directory sowie RADIUS, deren Nutzung auch ETH-Organisationseinheiten angeboten wird.

Die ETH-Benutzerverwaltung **IAM** ist integriert in die schweizweite, föderative Authentifizierungs- und Autorisierungs-Infrastruktur (AAI) von Switch.

Wichtige Merkmale

- hohe Verfügbarkeit durch redundant ausgelegte Systeme
- verschlüsselte Ablage der Passwörter
- automatische Zuteilung von Kontoinformationen und Default-Services an ETH-Angehörige beim Eintritt resp. Immatrikulation
- automatischer Ablauf der Zugangsberechtigungen von ETH-Angehörigen nach dem Austritt resp. Exmatrikulation
- Setzen von eigenen Passwörtern über eine Web-Applikation mit Reset-Self-Service
- Administration von Passwörtern und Services durch berechtigte Personen über eine Web-Applikation
- Konten für Gäste, Kurse, Kongresse mit definierbarem Start- und Ablaufdatum
- Selbstregistrierung für Tagesgäste

Default Services

- allg. Authentifizierung für Applikationen
- Mailbox: Mail- / Kalenderservice, Active Directory Account
- WLAN_VPN: Zugriff zum ETH-Netzwerk über fremde Internet-Provider, Wireless Access Points resp. Docking-Plätze an der ETH.

Authentifizierungs-Systeme

- **AAI** -- Authentifizierung/Autorisierung von Webseiten/-Anwendungen mit Shibboleth. Wir betreiben eine so genannte Home-Organisation (Identity Provider) auf der Basis von Sibboleth und der nachfolgend beschriebenen LDAP-Infrastruktur.
- **ldaps** -- Authentifizierung/Autorisierung über LDAP, Verbindung nur über SSL **und** freigeschaltete IP-Nummer des Webservers möglich.
- **Active Directory** -- Authentifizierung/Autorisierung an einer Windows Domäne.

- **RADIUS** -- Authentifizierung/Autorisierung über das RADIUS-Protokoll an einem RADIUS-Server (Radiator).
  RADIUS wird für die Netzwerk-Zugangsservices VPN und iPass verwendet.

Update: Zürich, 18. April 2019
Autor: Giorgio Broggi, Informatikdienste