nethz - Authentication and Authorization at ETH Zurich

"nethz" is the central user management system of the ETH Zürich. It regulates the access to the following IT user services of the ETH: the ETH network via VPN, wireless lan or modem, email, central file storage located on the NAS server and to computers in the student computer rooms.

A growing number of ETH electronic services require the "nethz password" and check access authorization in the nethz data base. The authentication data is provided on an LDAP server (Unix) as well as on the Active Directory (Windows), use of which is also made available to ETH organisational units. The latter benefit from an integrated nethz account management and are spared the necessity of their own domain controllers as well as the development of a great amount of specific know-how.

The ETH user administration nethz is integrated in the Swiss universities authentication and authorizing infrastructure federation (AAI) Switch.

Specifications
• high availability due to redundantly laid out systems
• encrypted password filing system
• automatic allocation of account data and default services to ETH members, at entry or enrolment, respectively
• automatic expiration of access to services, after leaving the ETH or deregistering, respectively
• defining of personal passwords and administration of allocated services by web application
• administration of passwords and services by entitled persons using the web application
• accounts for guests, courses, congresses with a definable start and expiration date

Default Services
• nethz: general authentication for web applications
• Mailbox: email-/calendar service, Active Directory account
• NAS/DFS: access the ETH network using a commercial internet provider, wireless access points or docking stations at the ETH.
• VPN: software distribution system for employees and students

Authentication Systems
• AAI -- Authentication/authorization of web page applications with Shibboleth. We operate a so called home organization (Identity Provider) on the basis of Shibboleth and the LDAP infrastructure described below.
• ldaps -- Authentication/authorization with LDAP, recommended for Web applications. The nethz service password is used. System: openLDAP on Solaris. Connection possible with SSL and registered web server IP number only.
nethz - Authentication and Authorization at ETH Zurich

- **Active Directory** -- Authentication/authorization against a Windows 2003 domain. For special applications with increased security requirement. The mailbox service password is used.
- **Radius** -- Authentication/authorization using radius protocol against a radius server (radiusator), which consults the nethz data base.
  Radius is used for the following network access services: VPN, Dialup, iPass.

_Update: Zurich, 20 Dezember 2016_