Internet Security Days 2017 -- Security by Design

IAM mit Need-To-Know? Ja!

Æ-DIR -- paranoide Benutzerverwaltung mit OpenLDAP

Zur Person

- Michael Ströder <michael@stroeder.com>, Freiberufler
- Schwerpunkte
  - X.509-basierte PKI, angewandte Verschlüsselung, dig. Signatur
  - Verzeichnisdienste (LDAP etc.), Identity & Access Management
  - Single Sign-On, Zwei-Faktor Authentifizierung
- Open Source / Freie Software
  - Æ-DIR, OATH-LDAP
  - web2ldap, python-ldap

Agenda

- Æ-DIR
  - Ziele
  - Architektur
  - Datenmodell
- Anwendungsbeispiel SSH Proxy
- 2-Faktor-Authentifizierung mit OATH-LDAP
  - Architektur OTP-Validierung via LDAP
  - Sicheres Enrollment von yubikey-Tokens

Ziele

- Prinzipien
  - Need-to-know
  - Least Privilege
  - Separation of Duties
- Delegierte Administration überschaubarer Bereiche
- Aussagekräftiger Audit Trail
- Basis für Compliance-Checks

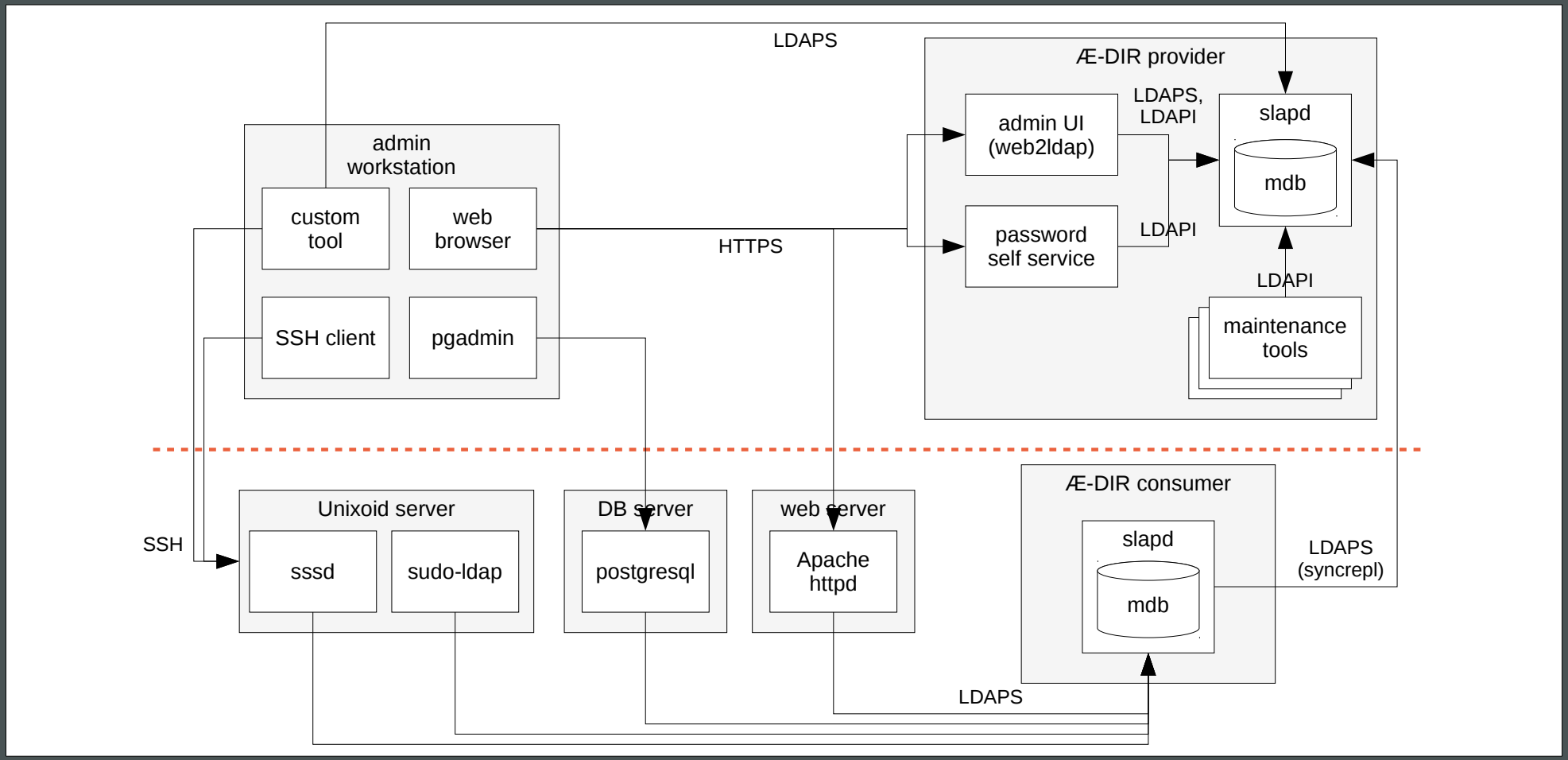
Paradigmen (1)

- Explizit ist besser als implizit
- Keine sichere Autorisierung ohne sichere Authentifizierung
- Keine anonymen Zugriffe
- Individuelle Authentifizierung
- Keine allmächtige Stellvertreterrollen
- Rechtevergabe immer basierend auf Gruppenzugehörigkeit

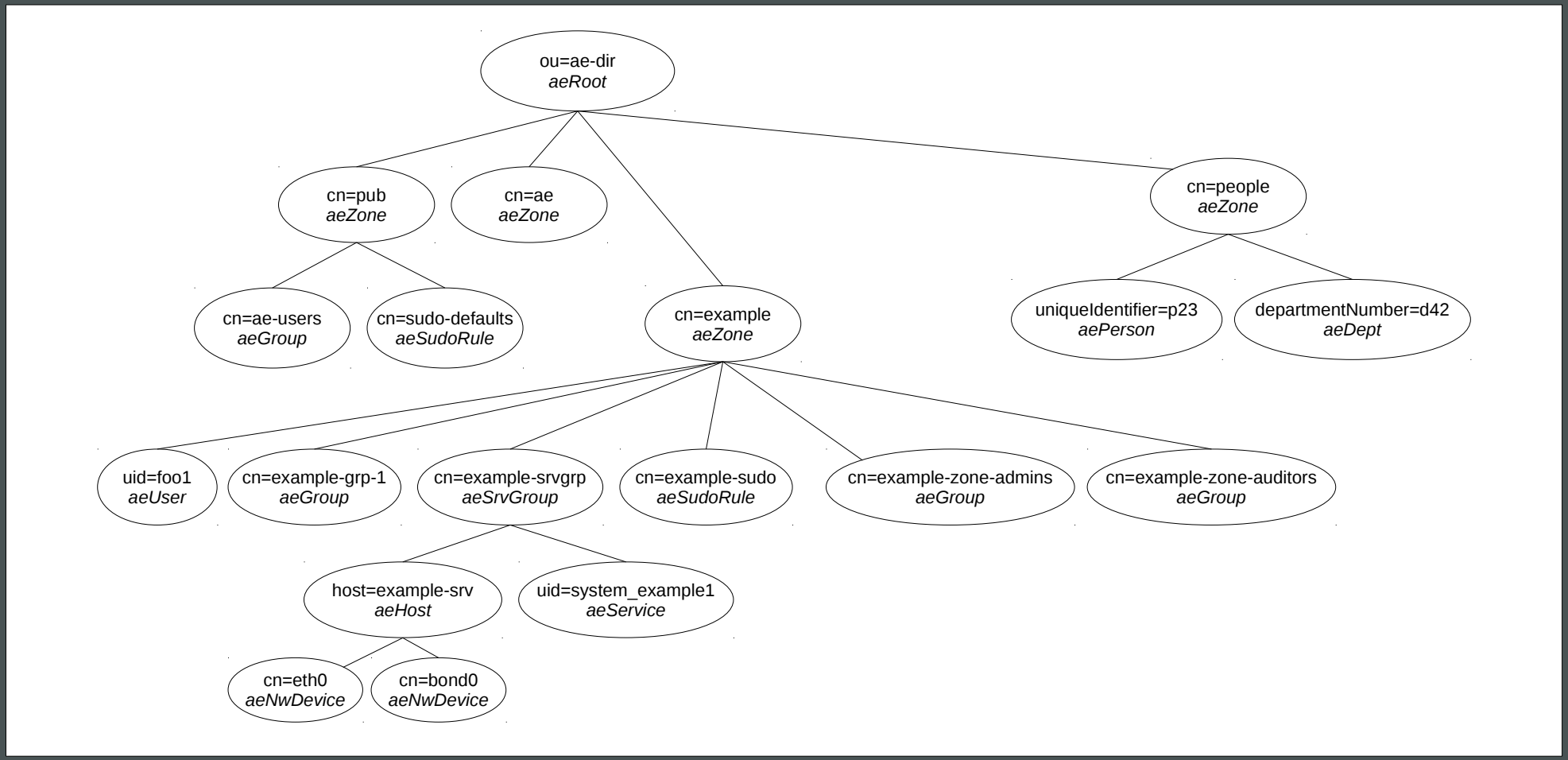
Paradigmen (2)

- Keine hierarchische Struktur erforderlich
- Eine Person ist kein Benutzer
- Rollentrennung mit mehreren Benutzern je Person
- Persistente IDs (keine Wiederverwendung)
- Nur verschlüsselter Netzwerkverkehr (TLS und SSH)
- Wohldefinierte Semantik und Syntax aller Objekte und ihrer Attribute (besser keine Daten als schlechte Daten)

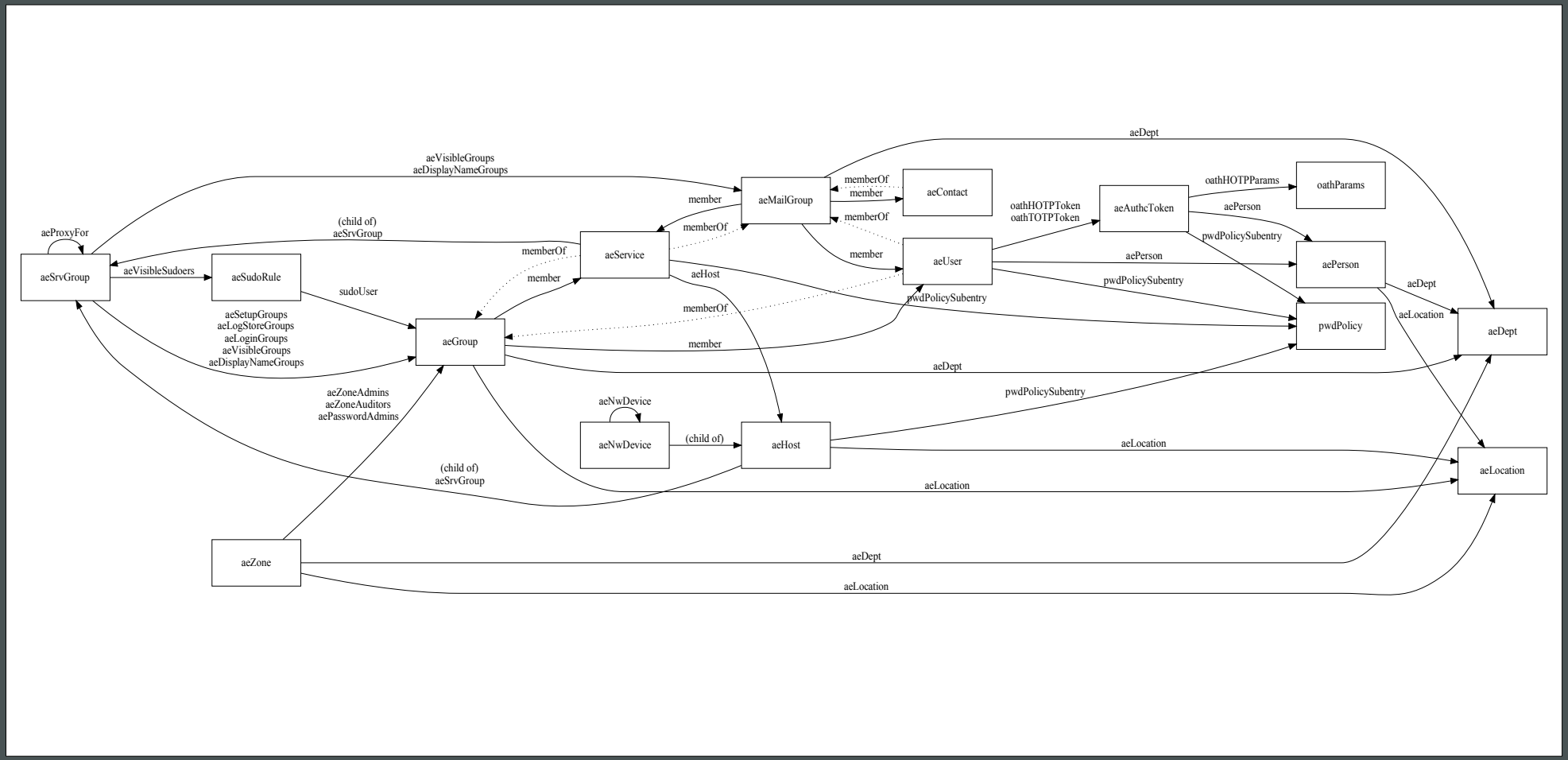
2-stufige Architektur



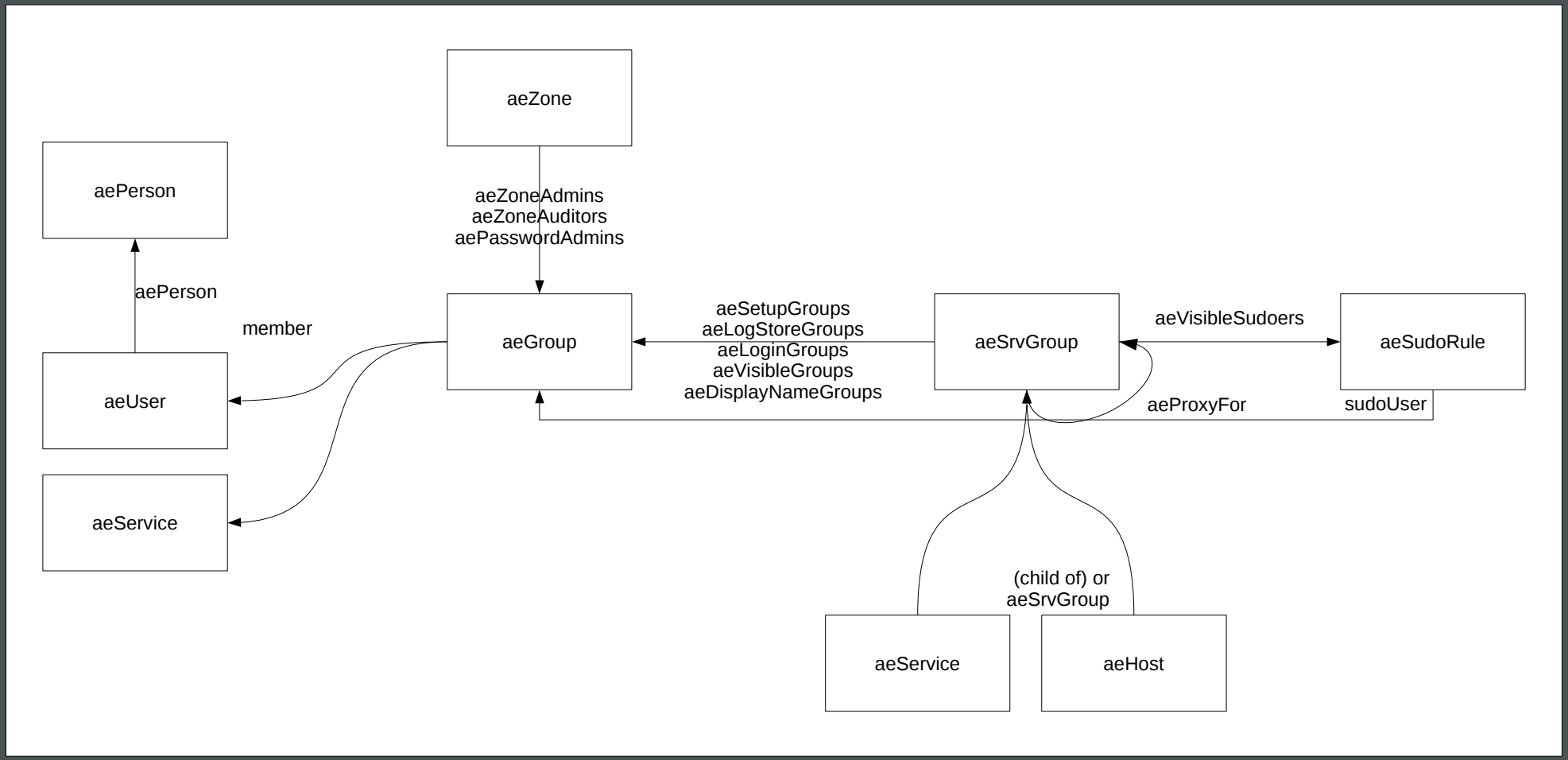
2-stufige Architektur



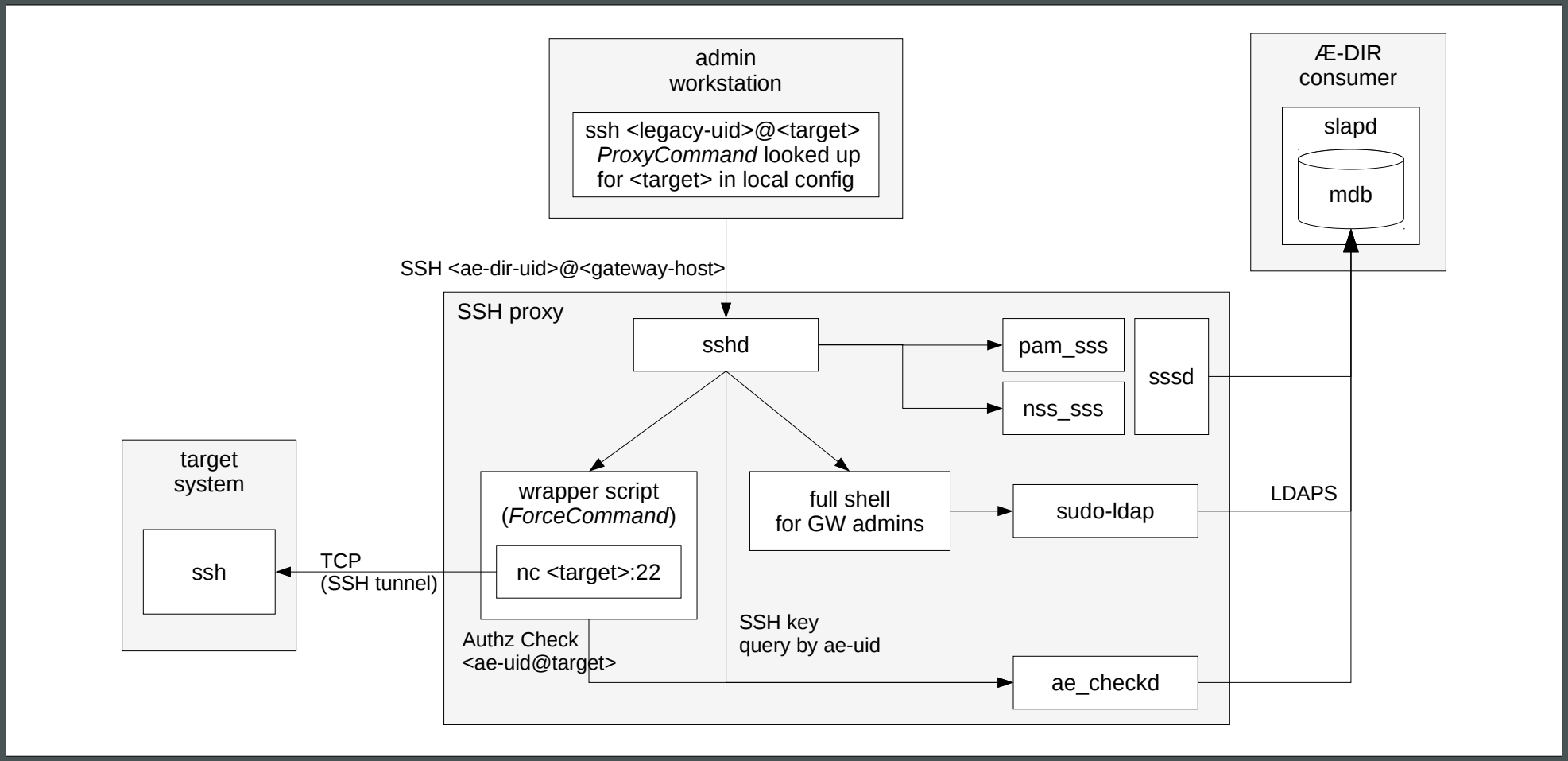
Entitäten (EER vollständig)



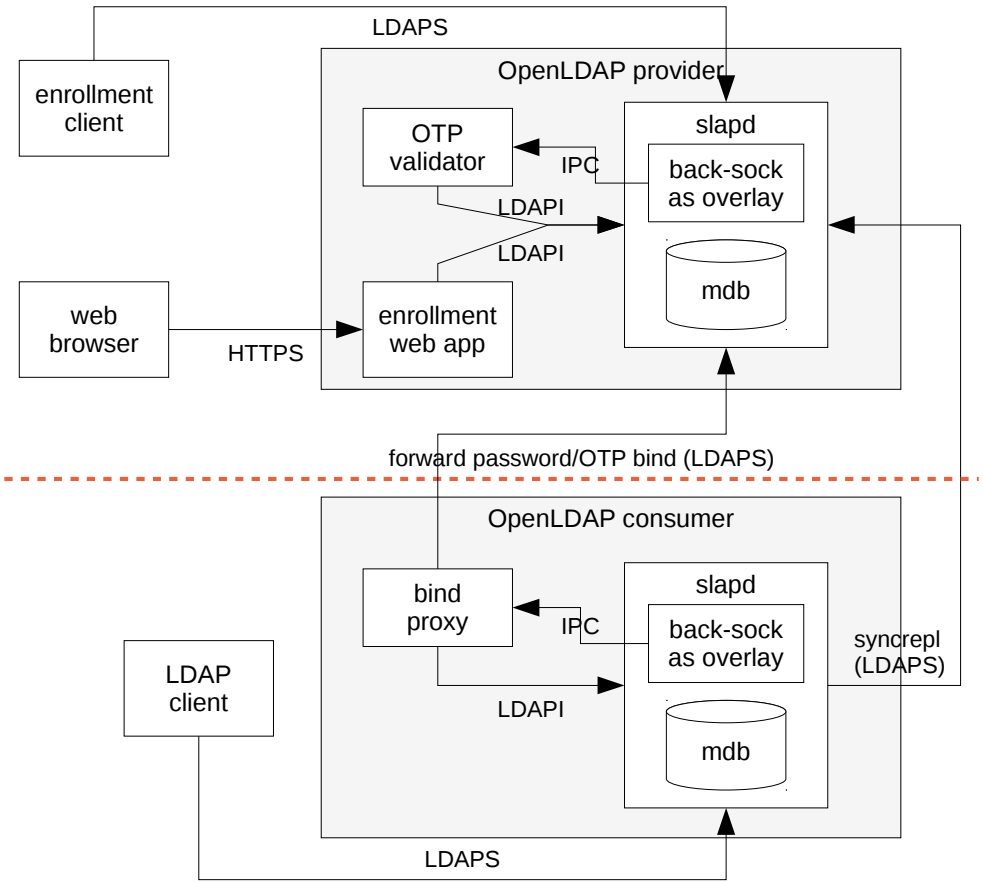
Berechtigungsbeziehungen (EER Authz)



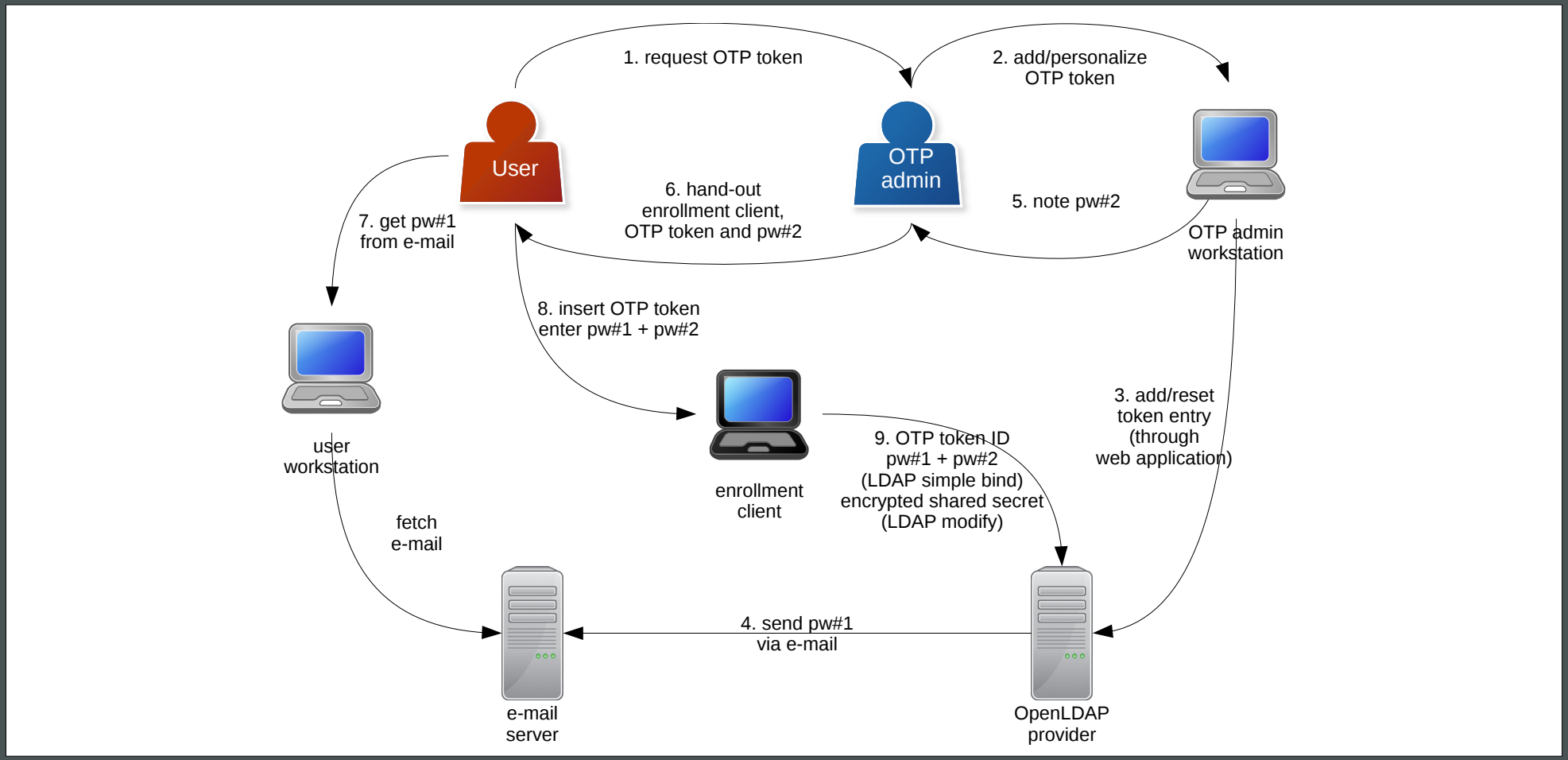
SSH Proxy mit Autorisierung



OATH-LDAP -- 2-stufige Architektur



OATH-LDAP -- Enrollment



Fazit

- Security by Design ist möglich
- Ja, ist auch anstrengend
- Benutzer brauchen Starthilfe und schlüssige Erklärungen
- Rückhalt durch Führungskräfte sehr hilfreich (Budget!)
- Ursprüngliche Sicherheitsversprechen nicht brechen
  => vor Änderungen immer gründlich nachdenken
- https://ae-dir.com -- https://oath-ldap.stroeder.com

Ausblick

- Weitere Ideen reichlich vorhanden
- Engere Integration
  - DevOps (ansible, puppet, o.ä.)
  - X.509 PKI für Server-Zertifikate, SSH Key Signing
  - WebSSO-Integration
  - Netzwerk Access Control
  - Deployment-Infrastruktur (PXE, TFTP-Boot, DHCP, Sys-DNS)
- Dokumentvorlagen für Compliance-Standards

:-/

? … !