EKCA

OpenSSH User Certs used as "Login Tickets"

Michael Ströder

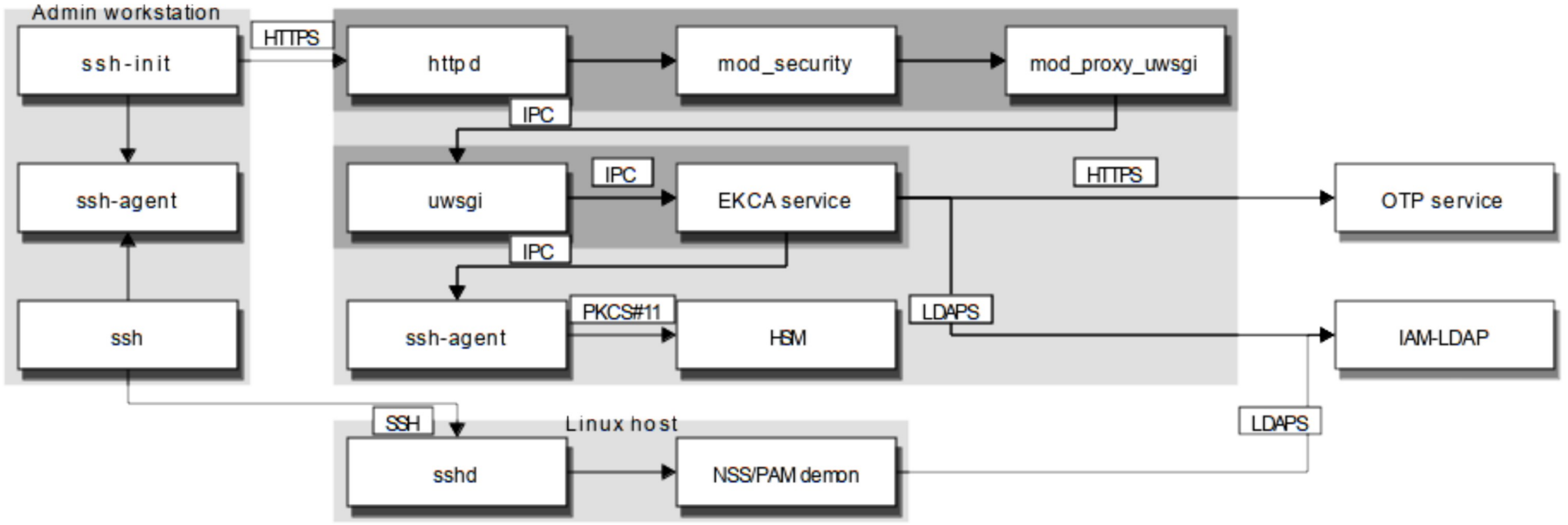
Why?

- Enforce key rotation
- No long-term private keys on disk
- Revocation of long-term keys does not work
- Hardware tokens are too slow
- Add multi-factor authc
- Avoid Kerberos ;-)
- => use temporary OpenSSH user certs (not X.509!)

EKCA

- Many existing implementations, but unclear support
- Implemented in Python 3
- Apache License 2.0
- Simple CLI client for Unixoids, MacOS & Windows 10
- Simple web service (WSGI)
- Using HSM via ssh-agent -S
- SSH cert options read from user's LDAP entry
- Password and OTP plugins (Python namespace packages)

Architecture



Demo
User Certificates