REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

Kerberos

Systemausbildung − Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten

14.07.2021 – Florian Klemenz

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

Definition

`88/tcp,88/udp`

Bezeugen der Echtheit einer Entität
(Benutzer/Dienste/Rechner/...)

Kerberos ist ein Netzwerkprotokoll zur sicheren Authentifizierung von Teilnehmern in einem ungesicherten Netzwerk auf sicheren Rechnern.

Benutzer oder Dienste
im Netzwerk

Feindliche Übernahme des
Rechners ist zu vermeiden ;)

Verschlüsselte Kommunikation
in Internet, WLAN und LAN

Inhalt

- Geschichte
- Grundlagen
  - Symmetrisches Needham-Schroeder-Protokoll
  - Umsetzung in der Praxis
- Kerberos
  - Ablauf des Verbindungsaufbaus zu Diensten
  - Erweiterung auf SingleSignOn (SSO)
- Umsetzung am “RRZE”
- Schwachstellen, Vorteile und Grenzen

Geschichte – Teil 1

- Teil des Projekts “Athena” (1983-1991) am MIT
  → Kerberos als Sicherheitssystem
- Ab ca. 1988 als Version 4 außerhalb des MIT
- 1993 als Version 5 erstmals spezifiziert im RFC 1510
- 2005 abgelöst durch RFC 4120 für Kerberos V5

  “to clarify aspects of the protocol and its intended use that require more detailed or clearer explanation”

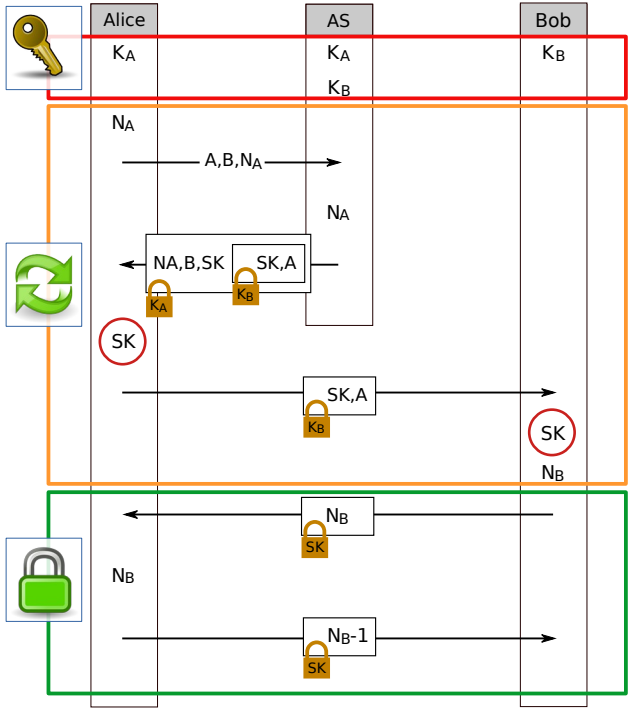
Aufbau einer Campus-weiten verteilten Rechnerumgebung

Geschichte – Teil 2

- Öffentliche Spezifikation in den RFCs ermöglicht weitere Implementierungen
- Standardprotokoll für die Authentifizierung ab Windows-2000
- weitere Implementierung ist “Heimdal”
- “MIT-Kerberos” im Linux-Umfeld am häufigsten im Einsatz

Symmetrisches Needham-Schroeder-Protokoll

- Protokoll für sicheren Datenaustausch: Authentifizierung der Teilnehmer + verschlüsselte Übertragung
- Zentrales Element: **AuthenticationService (AS)** Kommunikationsteilnehmer verfügen über gemeinsame Schlüssel (**pre-shared secrets**) mit der TrustedThirdParty (→ AS)
- Authentifizierung und Austausch eines **SessionKey** (**SK**) durch Nachweis, dass A→K_A und B→K_B besitzt

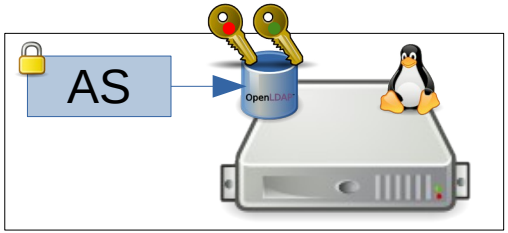


Von Michael F. Schönitzer - Eigenes Werk, CC-BY 4.0, https://commons.wikimedia.org/w/index.php?curid=55390446

AS → Key Distribution Center

- MIT-Kerberos Implementierung hat als zentrales Element das **Key Distribution Center (KDC)**
- Der KDC hält die Schlüssel aller Teilnehmer in einer Datenbank (hier ein LDAP)
- Der Authentication Service (AS) ist Teil des KDC und hat damit auch Zugriff auf alle Schlüssel

Key Distribution Center (KDC)



linuxkdc

Teilnehmer → Principals

- sind eine **authentifizierbare Entitäten** und können sich auf einzelne **Benutzer**, **Computer**, **Dienste**, Prozesse oder Threads beziehen
- müssen **identifiziert und authentifiziert** werden, bevor ihnen Rechte und Privilegien zugewiesen werden können.
- sind durch eine zugehörige **Kennung (Security Identifier)** identifiziert

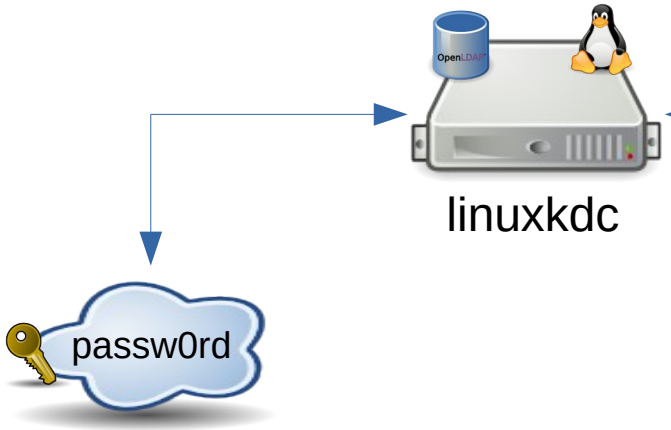
Users/Clients

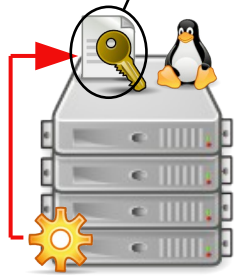
Server/Services

Teilnehmer/Kommunikationspartner

Quelle: https://de.wikipedia.org/wiki/Prinzipal_(Computersicherheit)

Pre-Shared Secrets





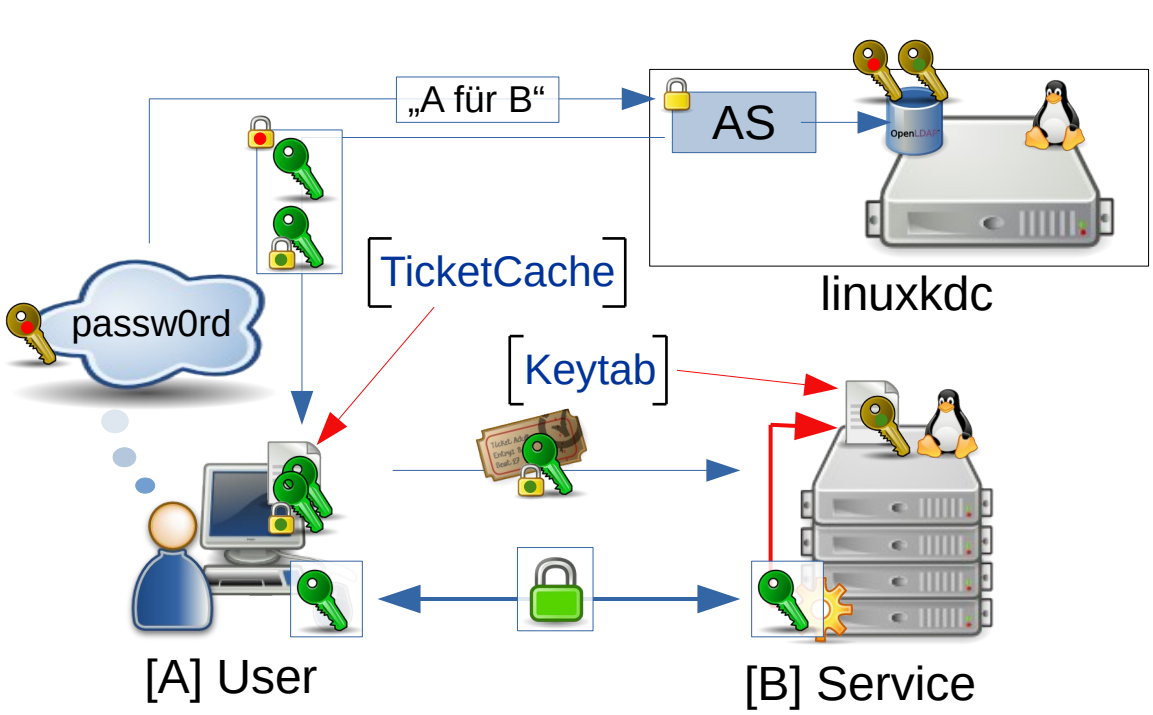
Keytab – Enthält einen Export ausgewählter kryptographischer Schlüssel aus dem KDC

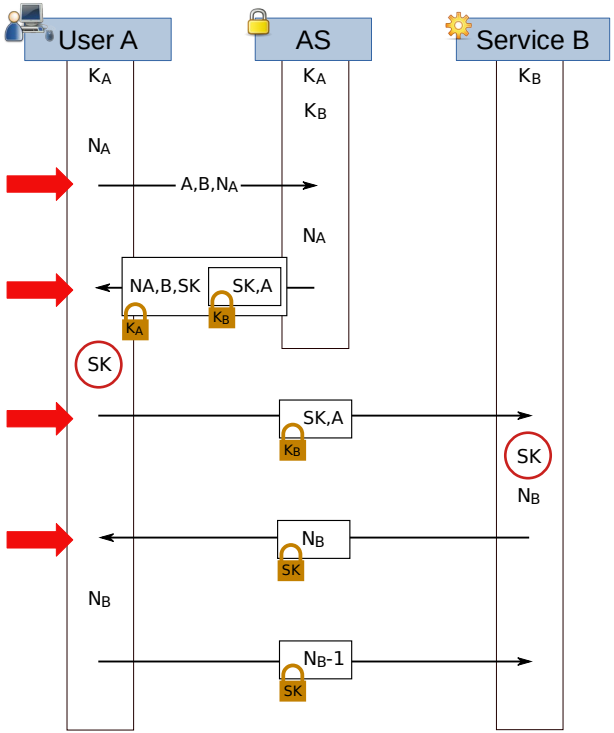
Keytabs

- Container für verschiedene kryptografische Schlüssel
- verschiedene Hash-Algorithmen vorgeneriert
- KVNO → Key Version Number
  Wird inkrementiert, wenn ein neuer Schlüssel ausgestellt wird
  (z.B. bei einer Passwortänderung)

```
root@linux-proxy[ ~ ]# klist -kte
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------
   2 11/09/2017 10:24:49 host/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (aes256-cts-hmac-sha1-96)
   2 11/09/2017 10:24:49 host/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (aes128-cts-hmac-sha1-96)
   2 11/09/2017 10:24:49 host/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (des3-cbc-sha1)
   2 11/09/2017 10:24:49 host/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (arcfour-hmac)
   2 11/09/2017 10:24:49 nfs/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (aes256-cts-hmac-sha1-96)
   2 11/09/2017 10:24:49 nfs/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (aes128-cts-hmac-sha1-96)
   2 11/09/2017 10:24:49 nfs/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (des3-cbc-sha1)
   2 11/09/2017 10:24:49 nfs/linux-proxy.rrze.uni-erlangen.de@LINUX.FAU.DE (arcfour-hmac)
```

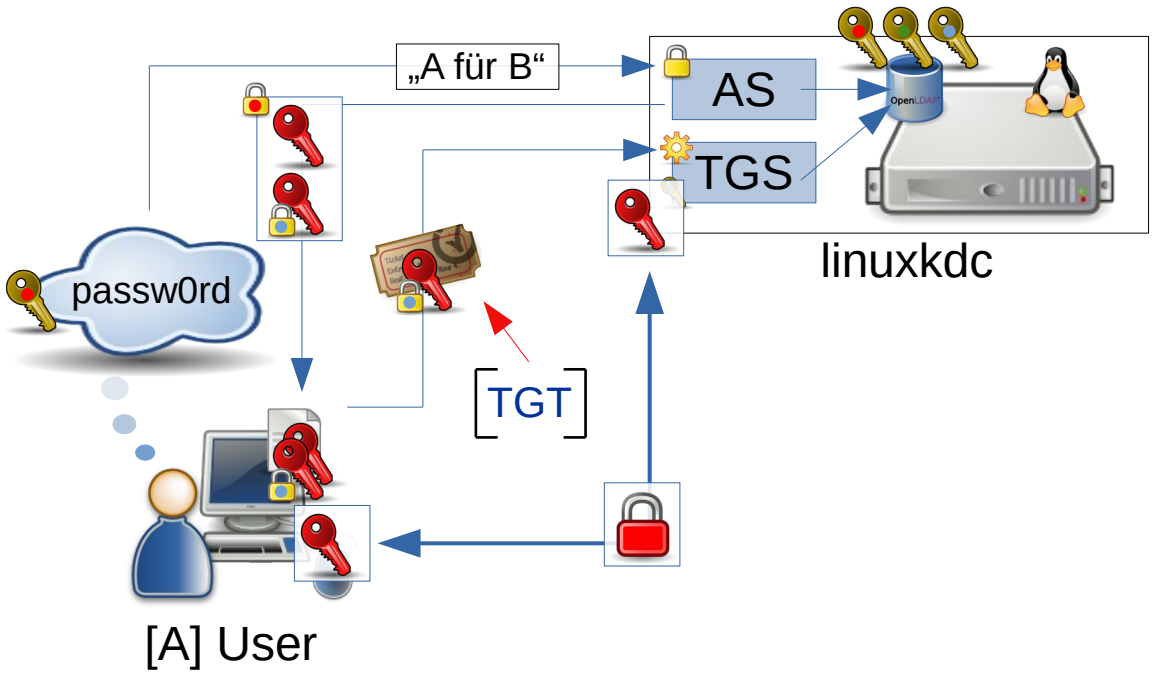
Verbindungsaufbau zu einem Dienst

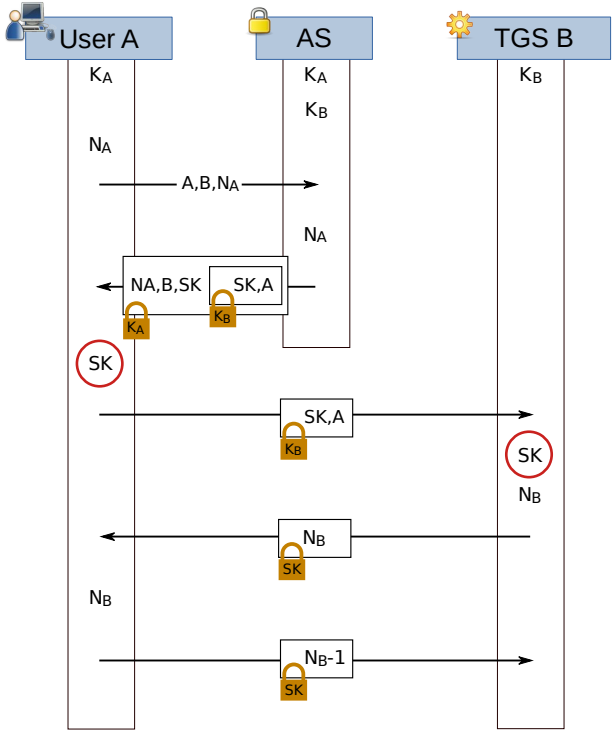




= SessionKey = Pre-Shared Secret

Erweiterung auf SingleSignOn (SSO) – Teil 1

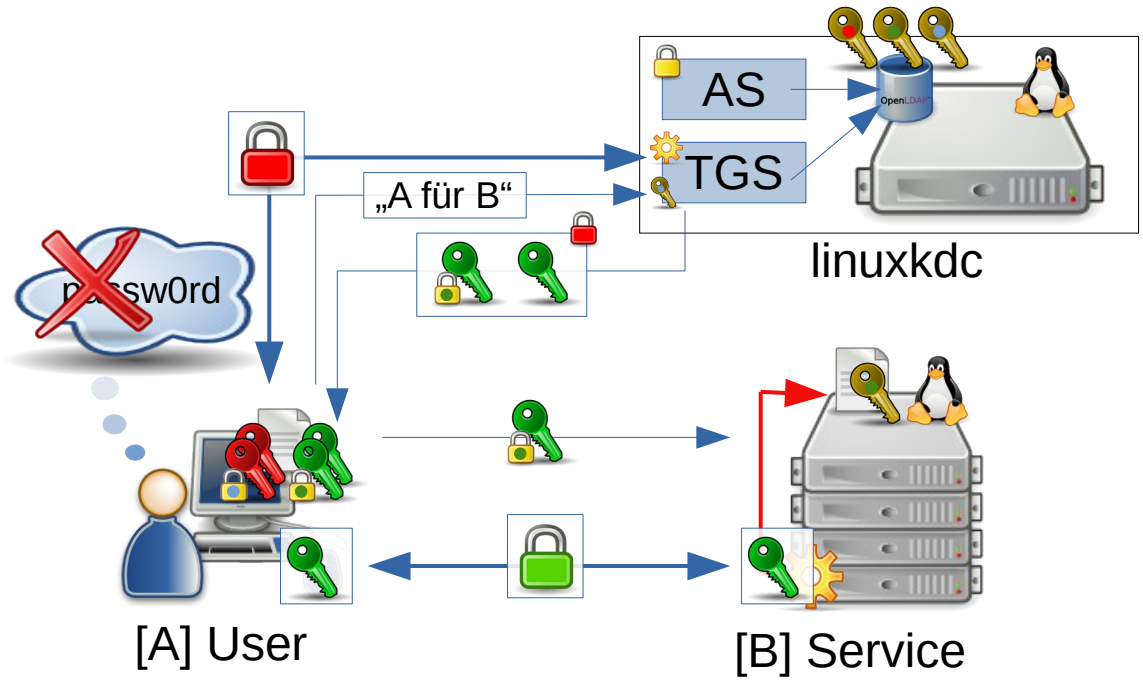


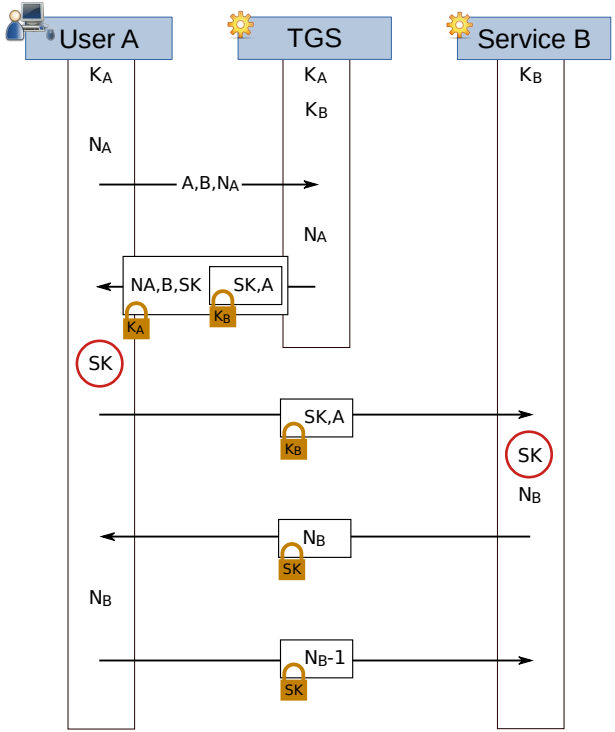


= SessionKey/TGT

= Pre-Shared Secret

Erweiterung auf SingleSignOn (SSO) – Teil 2





= TGT (SK) = Service (SK) = Pre-Shared Secret

TicketCache / ServiceTickets / TGT für Clients

TGT

ServiceTicket

TicketCache

unverschlüsselter SessionKey

verschlüsselter SessionKey
(mit Schlüssel des Zieles)

```
unrz[redacted]@[redacted] [ ~ ]$ klist
Ticket cache: FILE:/tmp/krb5cc_12186
Default principal: [redacted]@LINUX.FAU.DE

Valid starting       Expires              Service principal
15.07.2020 12:43:13  15.07.2020 22:43:13  krbtgt/LINUX.FAU.DE@LINUX.FAU.DE
15.07.2020 12:43:23  15.07.2020 22:43:13  host/dialog.rrze.uni-erlangen.de@LINUX.FAU.DE
```

Schwachstellen

- **Keytabs** mit Pre-Shared Secrets:
  Dienste können “übernommen” werden
  → z.B. Man-in-the-middle Attacke
  - Gegenmaßnahmen: Zugriffsschutz auf den Systemen

- **TicketCaches** mit TGTs/ServiceTickets:
  Anmeldung mit Identität des Benutzers
  - Gegenmaßnahmen:
    Zugriffsschutz auf den Systemen + Begrenzung der Gültigkeit

Aufbau am RRZE

- IdMS
  Identity Management System

„Benutzerverwaltung“

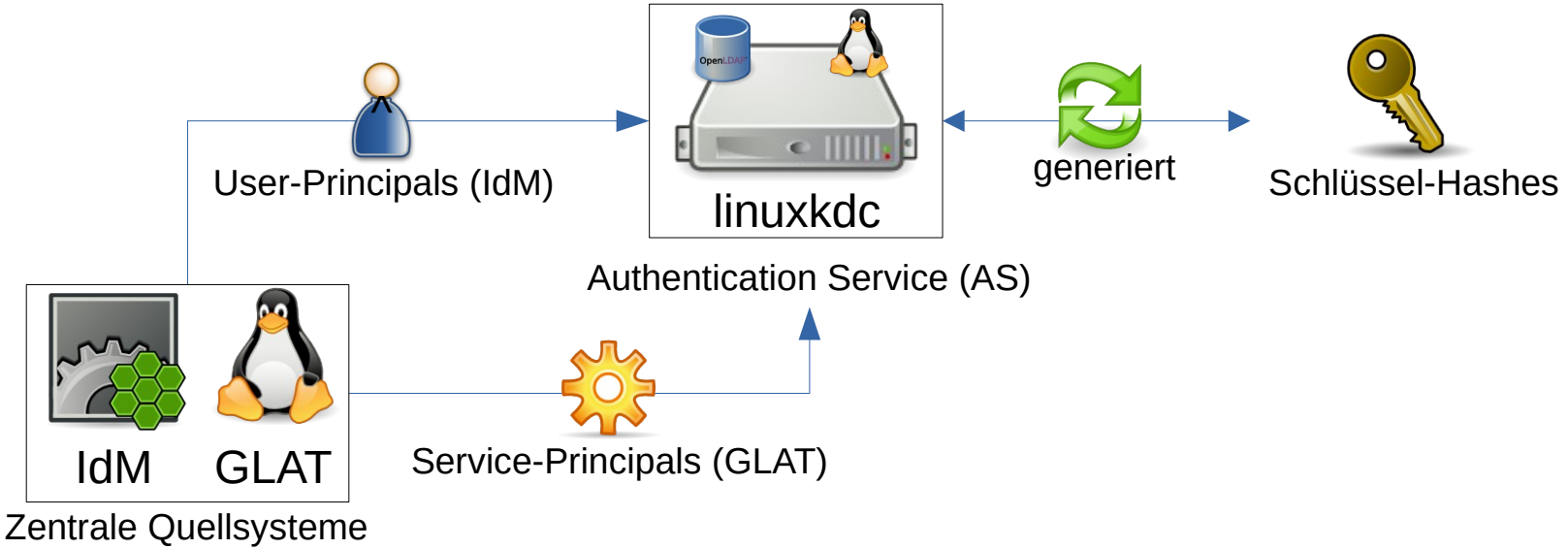
- GLAT
  Grand Linux Administration Toolkit

„Rechnerverwaltung“

- linuxkdc
  Key Distribution Center (KDC) und Authentication Service (AS) für den Realm “LINUX.FAU.DE”

„Kerberos-Server“

Anlage/Provisionierung von Principals



Principal	geheimer Schlüssel
[IdM-Kennung]@LINUX.FAU.DE	Passwort (IdM)
host/dialog.rrze.uni-erlangen.de@LINUX.FAU.DE	Passwort (Zufall)

Daten eines Principals auf dem KDC

```
root@linuxkdc-master:~# kadmin.local
Authenticating as principal root/admin@LINUX.FAU.DE with password.
kadmin.local:  getprinc [redacted]
Principal: [redacted]@LINUX.FAU.DE
Expiration date: [never]
Last password change: Tue Nov 21 17:13:52 CET 2017
Password expiration date: [none]
Maximum ticket life: 1 day 00:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Tue Nov 21 17:13:52 CET 2017 (kadmind@LINUX.FAU.DE)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 4
Key: vno 64, aes256-cts-hmac-sha1-96
Key: vno 64, aes128-cts-hmac-sha1-96
Key: vno 64, des3-cbc-sha1
Key: vno 64, arcfour-hmac
MKey: vno 1
Attributes:
Policy: [none]
```

Name/Identifier

Ticketlaufzeit

Schlüssel-Hashes (generiert aus dem Passwort)

Realms und Cross-Realm Trusts

- Windows/Mac am RRZE nutzen Windows Active-Directory (AD) Infrastruktur → Realm: **FAUAD.FAU.DE**
- Bidirektionaler Trust mit **LINUX.FAU.DE** Realm

Vorteile

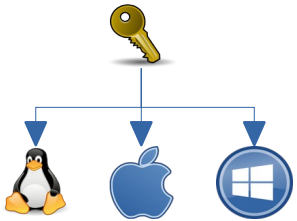
- Ermöglicht echtes “Single Sign On” (nicht nur Web)

Ticket Granting Tickets (TGT)

- Ermöglicht verschlüsselte Kommunikation (z.B. genutzt von NFSv4)

Session Keys (SK)

- Funktioniert auch über OS und Domain-Grenzen hinweg



Cross-Realm Trusts

Grenzen: Authentication vs. Authorization

- Kerberos liefert nur **Authentifizierung**
  (und kann LDAP in diesem Punkt ersetzen)
- **Authorisierung** muss anders gelöst werden!
- Viele Systeme nutzen gruppenbasierte Authorisierung eines bestehenden Verzeichnisdienstes
- Deshalb zusätzliche LDAP-Anbindung meistens sinnvoll

Mehr Infos
→ https://www.anleitungen.rrze.fau.de

RRZE-Veranstaltungskalender und Mailinglisten

- Kalender abonnieren oder bookmarken
  - www.rrze.fau.de/veranstaltungen/veranstaltungskalender/

- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet.
  - Auch diese Liste kann man abonnieren: https://lists.fau.de/mailman/listinfo/rrze-aktuelles

Vielen Dank für Ihre Aufmerksamkeit!

Regionales Rechenzentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
www.rrze.fau.de