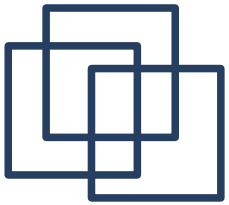
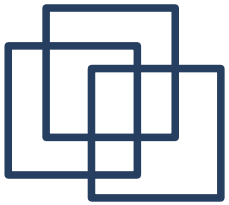


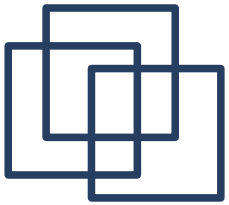
Kerberos V5 mit Debian

Mike Wiesner
mike@agile-entwicklung.de



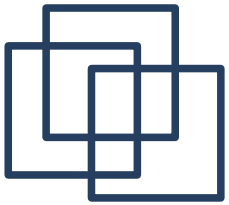
Agenda

- Einführung
- Implementierungen
- Installation
- Kerberized Services
- Windows Integration

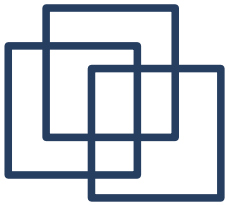


Über mich

- Softwareentwickler bei der Firma GABO
- Projekte: Linux Firewalls, Integrationslösungen, Webportale, ...
- aktives Mitglied bei SelfLinux

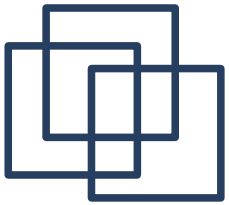


- Einführung
  - Was ist Kerberos
  - Funktionsweise
  - Vor-/Nachteile
- Implementierungen
- Installation
- Kerberized Services
- Windows Integration



Was ist Kerberos?

- Kerberos...
  - ... ist ein verteilter Authentifizierungsdienst
  - ... ist konzipiert für offene und unsichere Netze
  - ... ermöglicht Single-Sign-On
  - ... ist Plattform und Systemunabhängig
  - ... verwendet symmetrische Verschlüsselung
  - ... ist in RFC 1510 beschrieben

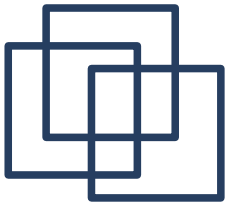


Principals & Realms

- Kerberos Principals bestehen aus:

  `component[/component]...@REALM`

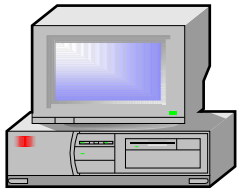
  z.B.: `mike/admin@agile-entwicklung.de`
- Die erste component gibt den Benutzernamen an
- Die zweite (optionale) component die „Rolle“
- Der Realm gibt die Auth. Domäne an.



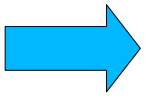
KDC

- KDC = Key Distribution Center
- Besteht aus:
  - Principal Database
    - Speichert Principals und Keys
  - Authentication Server (AS)
    - Erstellt das Ticket Granting Ticket (TGT)
  - Ticket Granting Server (TGS)
    - Erstellt Service Tickets für ein TGT

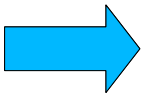
Authentication Server

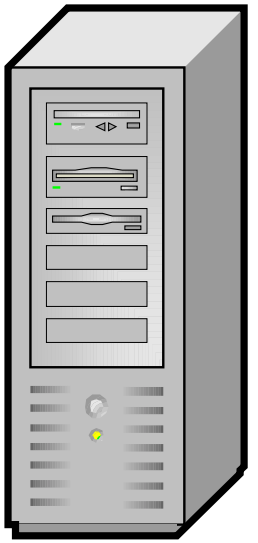


Client

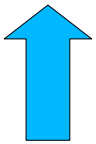


Client Principal
Client timestamp
krbgt principal name
Requested lifetime



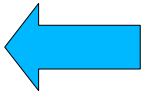


Authentication Server



Users's copy of AS session key
krbtgt principal name
Ticket lifetime

User's key 

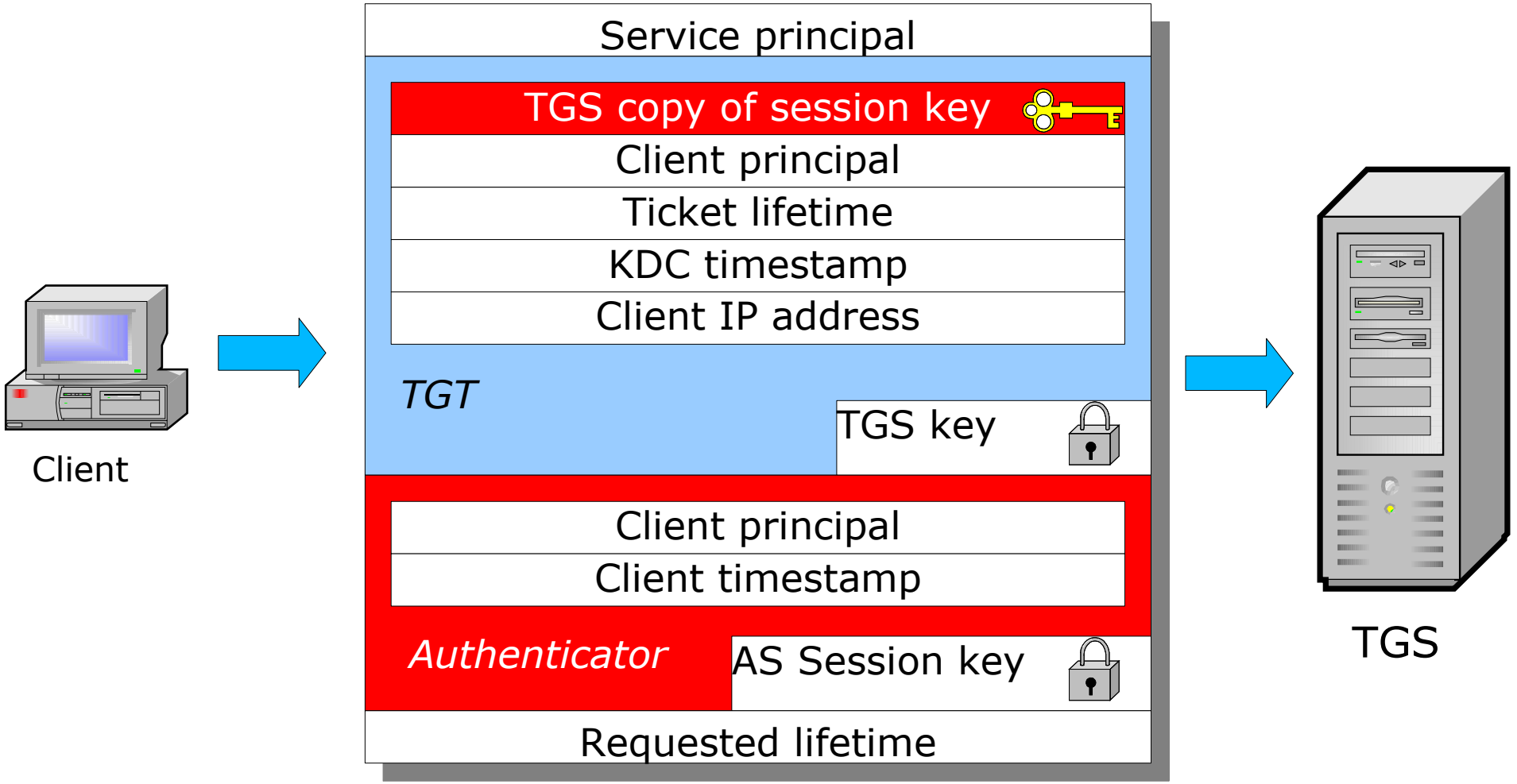


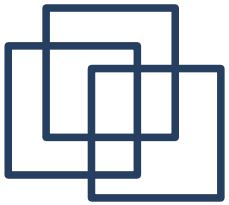
TGS copy of AS session key
Client principal
Ticket lifetime
KDC timestamp
Client IP address

TGT

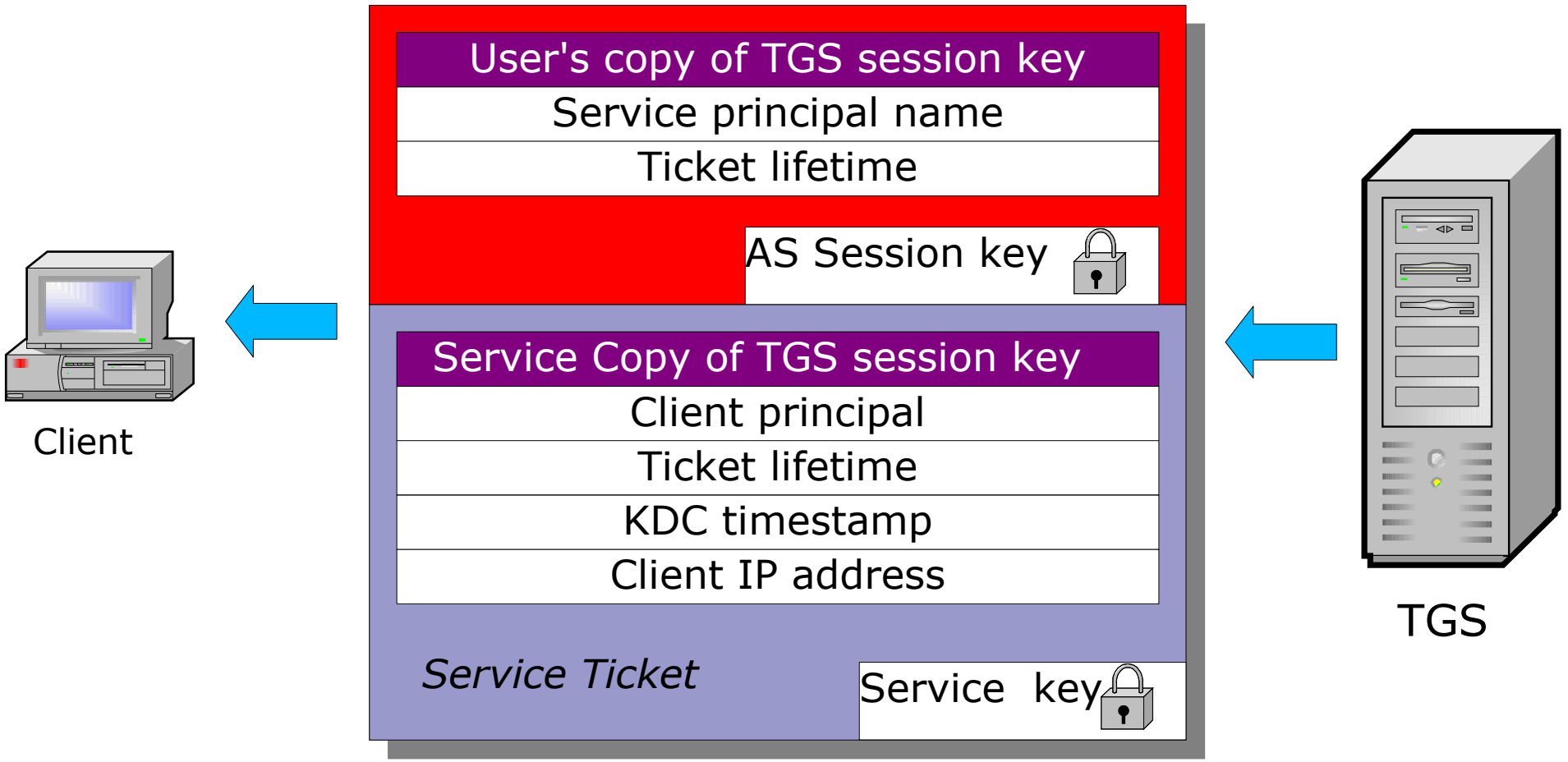
TGS key 

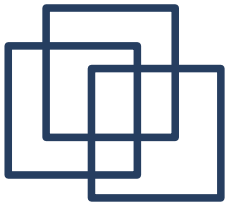
Ticket Granting Server



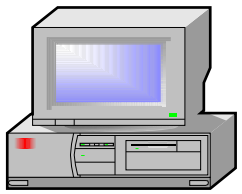


Ticket Granting Server

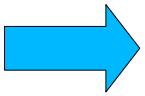




Service



Client



Service Specific Information

Service Copy of TGS session key

Client principal

Ticket lifetime

KDC timestamp

Client IP address

Service Ticket

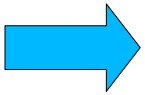
Service key

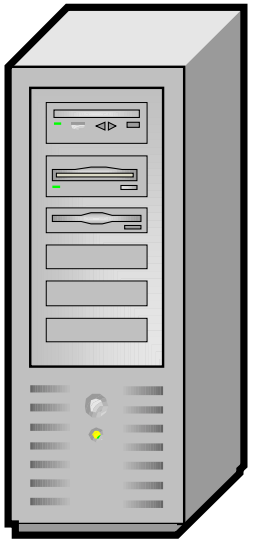
Client principal

Client timestamp

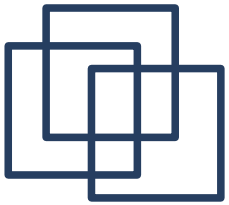
Authenticator

TGS Session key



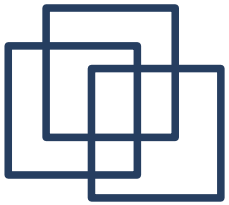


Service



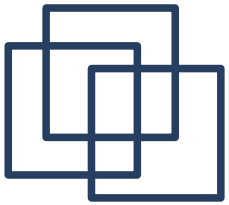
Vorteile von Kerberos

- Sichere, gegenseitige Authentifizierung aller Beteiligten
- Keine Verbindung zwischen KDC und Services nötig
- Geringe Belastung des KDCs
- Authorisierung wird dem Service überlassen
- Plattform und Systemunabhängig



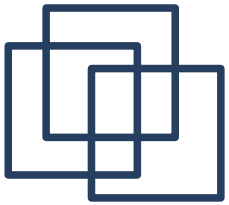
Nachteile von Kerberos

- Keys müssen zu den Services verteilt werden
- Uhrzeiten müssen synchronisiert sein (ntpdate, rdate)
- Nicht ohne weiteres mit Firewalls einsetzbar (NAT)
- Mangelnde Unterstützung bei den Clients (derzeit)

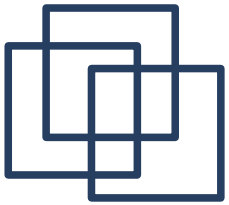


weitere Protokolle

- Generic Security Services API (GSSAPI):
  - generisches Interface zur Unterstützung von „strong Authentication“ , wie z.B. Kerberos
  - wird oft von Services verwendet um Kerberos zu unterstützen
- Security Support Provider Interface (SSPI):
  - Microsoft Pendandt zu GSSAPI

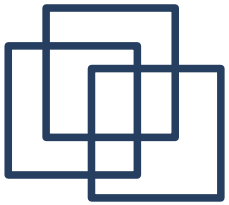


- Einführung
- Implementierungen
- Installation
- Kerberized Services
- Windows Integration



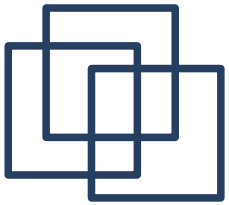
MIT

- Referenzimplemetierung
- Weit verbreitet
- Wird in den USA entwickelt
- Unterstützt seit 1.3 unter anderem RC4 und AES zur Verschlüsselung.
- Wird von vielen Anwendungen unterstützt.



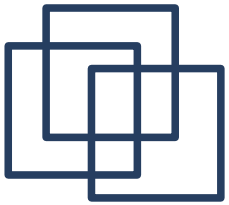
Heimdal

- Neuere Implementierung
- Wird außerhalb der USA entwickelt
- Bessere Master/Slave Synchronisierung
- Unterstützung von (3)DES, AES und RC4
- Kerberos API und GSSAPI unterscheiden sich jedoch von den MIT APIs

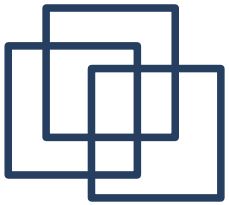


Microsoft

- Neueste Implementierung
- Unterstützt nur Kerberos 5
- Unterstützt nur RC4 und DES, kein 3DES
- Unix Clients mit Windows KDC funktioniert
- Windows Clients mit Unix KDC funktioniert nicht ohne weiteres
- Kein GSSAPI (dafür SSPI)

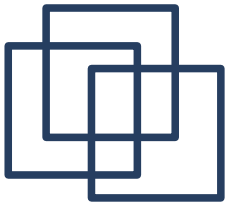


- Einführung
- Implementierungen
- Installation auf einem Debian System
  - KDC einrichten
  - Client einrichten
- Kerberized Services
- Windows Integration



Beispiel

- Betriebssystem: Debian 3.1 (sarge)
- Implementierung: MIT
- Service: ssh
- 3 Rechner: kdc, client, server
- 1 Domain: agile-entwicklung.de
- 1 Realm: AGILE-ENTWICKLUNG.DE
- 2 Benutzer: root, mike



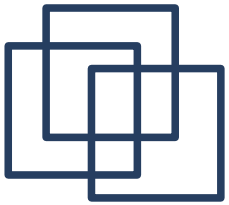
KDC einrichten

- KDC installieren:

```
apt-get install krb5-kdc krb5-admin-server
```

- Anlegen des Realms „`AGILE-ENTWICKLUNG.DE`“ in `/etc/krb5.conf`
- Konfigurieren des Realms in `/etc/krb5kdc/kdc.conf`
- Realm erzeugen:

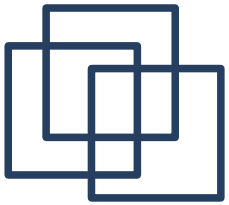
```
kdb5_util create -s
```



KDC einrichten (2)

- Admin Benutzer anlegen und testen:

```
kdc# kadmin.local
kadmin.local: addprinc mike/admin
kadmin.local: listprincs
kadmin.local: exit

kdc# /etc/init.d/krb5-kdc start

kdc# kinit mike/admin
kdc# klist
```



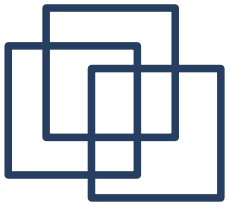
KDC einrichten (3)

- Admin Benutzer Rechte zuweisen:

```
kdc# vi /etc/krb5kdc/kadm5.acl
mike/admin@AGILE-ENTWICKLUNG.de  *
```

- Keytab mit Kadmin Principals erzeugen

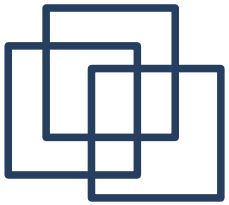
```
kdc# kadmin.local
kadminl.local: ktadd -k
  /etc/krb5kdc/kadm5.keytab kadmin/admin
  kadmin/changepw
```



KDC einrichten (4)

- Benutzer anlegen und testen:

```
kdc# /etc/init.d/krb5-kdc restart
kdc# kadmin
kadmin: addprinc mike
kadmin: addprinc root
kadmin: exit
kdc# kdestroy
kdc# kinit mike
```



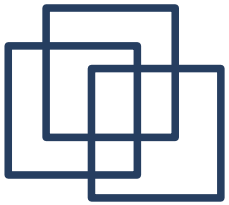
Client einrichten

- Kerberos Clients installieren:

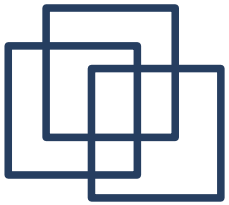
```
client# apt-get install krb5-user krb5-client
```

- Test

```
client# kinit mike/admin
client# kadmin
```



- Einführung
- Implementierungen
- Installation auf einem Debian System
- Kerberized Services
  - Keytabs
  - Login
  - SSH
- Windows Integration

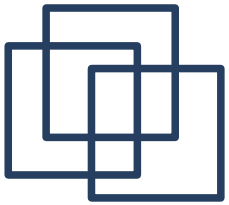


Keytabs

- Service Keys werden in Keytabs (i.d.R. /etc/krb5.keytab) gespeichert.

- Principal anlegen und Key exportieren:

```
client# kadmin
kadmin: addprinc host/client.agile-
  entwicklung.de
kadmin: ktadd host/client.agile-entwicklung.de
```



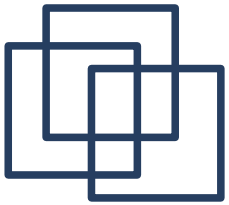
Login

- lokalen Benutzer anlegen

```
client# adduser --disabled-password mike
```

- PAM Modul installieren

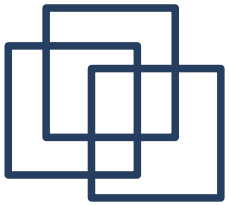
```
client# apt-get install libpam-krb5
```



Login (2)

- PAM einrichten

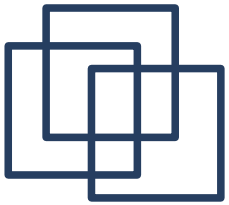
```
client# vi /etc/pam.d/common-auth
auth    sufficient    pam_krb5.so forwardable
auth    required      pam_unix.so nullok_secure
client# vi /etc/pam.d/common-password
password    sufficient    pam_krb5.so use_authtok
password    sufficient    pam_unix.so ...

client# vi /etc/login.defs
CLOSE_SESSIONS yes
```



Login (3)

- Testen

```
client# login mike
Password for mike@AGILE-ENTWICKLUNG.DE: xxx
mike@client$ klist
mike@client$ exit
```



SSH

- Kerberized SSH installieren

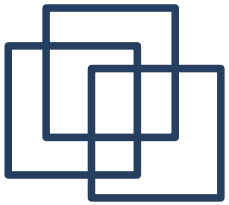
```
server# apt-get install ssh-krb5 krb5-user
```

- Principal anlegen und Key exportieren

```
server# kinit mike/admin

server# kadmin

kadmin: addprinc host/server.agile-
  entwicklung.de

kadmin: ktadd host/server.agile-entwicklung.de
```

- Benutzer anlegen

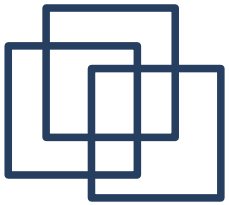
```
server# adduser --disabled-password mike
```



SSH (2)

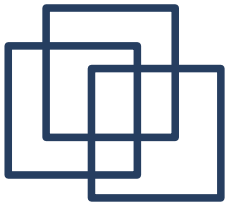
- Testen

```
client# login mike
mike@client$ ssh server
mike@server$ klist
mike@server$ exit
mike@client$ klist
```

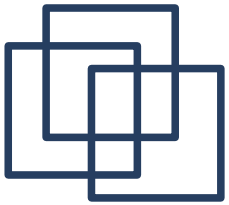


Weitere Services

- Cyrus IMAP
- OpenLDAP
- Putty
- Reflection X
- Eudora
- Apple Mail.app
- ...

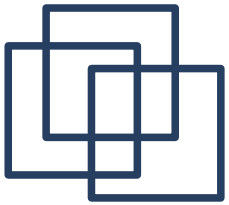


- Einführung
- Implementierungen
- Installation auf einem Debian System
- Kerberized Services
- Windows Integration
  - als Samba Server
  - als Kerberos Client/Service



Samba Server

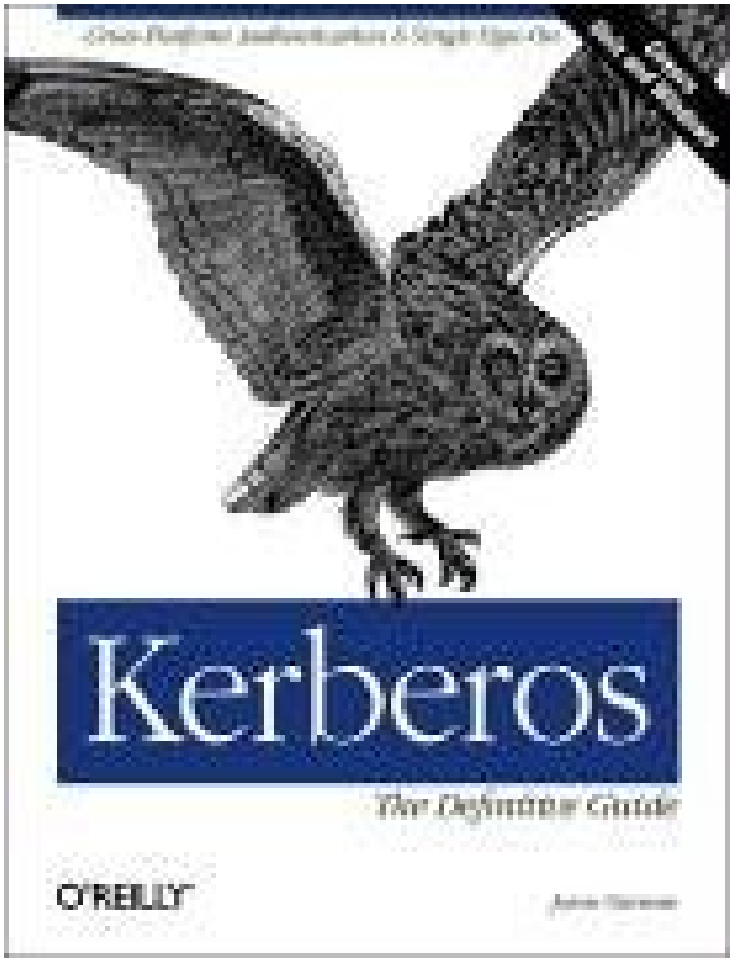
- Samba mit Kerberos Support installieren
- Kerberos mit Windows Domänen Controller als KDC konfigurieren
- Samba auf Kerberos Authentifizierung umstellen
- Domäne beitreten (net join)



Kerberos Client/Service

- Kerberos mit Windows Domänen Controller als KDC konfigurieren
- Linux Host Principal als „Benutzer“ in der Domäne anlegen
- Principal Key mit „ktpass“ in eine keytab exportieren
- keytab auf den Linux Host kopieren bzw. Importieren.

Buchempfehlung



Kerberos, The Definitiv Guide

Jason Garmen

ISBN: 0596004036