Das Kerberos-Protokoll

Eine Zusammenfassung des Beitrags
zu den
Chemnitzer Linuxtagen 2012

Von Mathias Feiler
(Kommunikations-, Informations- und Medienzentrum der Universität Hohenheim)

Begriffe

- Authentifizierung
  - Ist er der, für den er sich ausgibt?
- Autorisierung
  - Darf er mit dem Ding tun, was er tun will?
- Realm
  - Das Reich eines Kerberos-Servers
- Prinzipal
  - Eine Identität in einem Kerberos-Realm (oft ein Mensch)
- Key (oder Schlüssel)
  - Parameter der (De-) Chiffrierung (Ver- und Entschlüsselung)
- Ticket (oder gelegentlich auch Tocken)
  - Eine im Serverkey verschlüsselte Datenstrucktur
  - Zeitlich eng begrenzter Ausweis (Vergl. Fahrschein)

Kerberos allgemein

- Zentrales 'Trusted Third Party' Authentisierungssystem
  - Alle, Klienten und Server müssen dem Kerberos bekannt sein
- Symmetrische Verschlüsselung
- Jedes Prinzipal hat ein gemeinsames Geheimnis (Key) mit dem Kerberosserver
  - Wird aus Passwort hergestellt
- Die Zeit ist für Kerberos sehr wichtig
  - Typische Zeitfenster: +/- 2 bis 5 Minuten
    - Wenn Kerberos permanent verweigert : Uhr überprüfen.

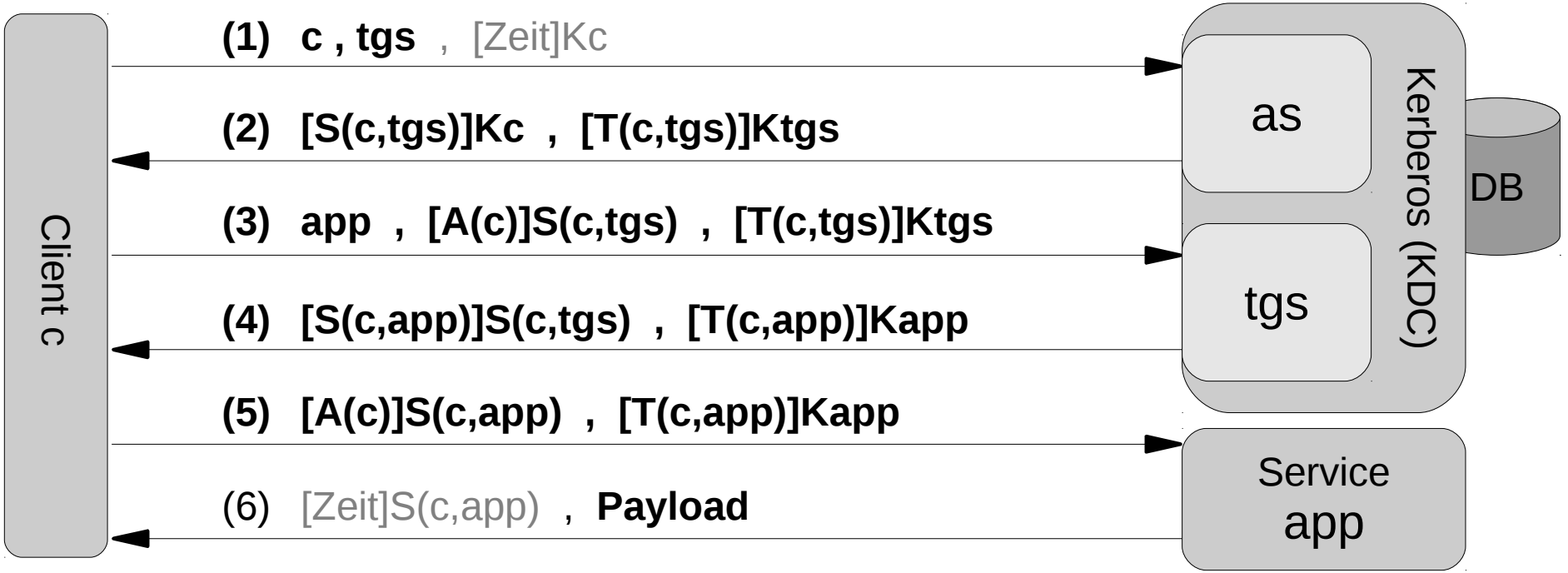
Kerberos Authentifizierung

- Das richtige Passwort führt zu einem TGT.
- Gegen das “Ticket Granting Ticket” (TGT) bekommt der Klient Tickets für beliebige Dienste/Server.
  - Bietet echtes „single sign on“
- Erst wenn ein Dienst erfolgreich beansprucht wurdeist die Authentisierung als 'bestanden' zu bezeichnen.
- 'preauthentication' und 'mutual authentication' sind optional
- Kann über mehrere Realms verkettet werden

Notation

c	Client (Prinzipal)
as	Authentication Service
tgs	Ticket Granting Service
d,app	Anbieter eines 3. Service, Dienstes oder Applikation, z.B. Notenabfrage
A(x)	Authenticator von x = x,Zeit
S(x,y)	Sessionkey für die geheime Kommunikation von x und y
T(x,y)	Ticket von x für y = x,y,S(x,y),Zeit,Lebensdauer,...
Kx	Privater Key von x
[ ]	Verschlüsselt
[ ]Kx	Verschlüsselt mit dem privaten Key von x
[ ]S(c,tgs)	Verschlüsselt mit dem Sessionkey von c und tgs

Kerberos Authentifizierungsablauf



Schritt (1) und (2) sind nur ein mal pro Sitzung notwendig.
Schritt (3) bis (6) können beliebig oft für verschiedene Dienste wiederholt werden.

Erklärung

(1) KRB_AS_REQ

Ggf. Preauthentication : Zeit , verschlüselt im privaten Key von c ↔ Passwort

(2) KRB_AS_REP

Bringt TGT und den passenden Sessionkey, verschl. im Key von c ↔ Passwort

(3) KRB_TGS_REQ

Anfrage auf Ticket für app , gegen TGT und Authenticator = (Zeit verschlüsselt im Sessionkey)

(4) KRB_TGS_REP

Tichet und Sessionkey für app versch. In Sessionkey aus dem TGT

(5) KRB_AP_REQ

Anfrage auf Service gegen Ticket und Authenticator =(Zeit verschlüsselt im 2. Sessionkey, dem für app)

(6) KRB_AP_REP

Ggf. Zeit verschlüsselt zurück, Dienstleitsung , ggf gesichert oder verschlüsselt.