

OpenVMS Kerberos

ACME, LDAP, X.500

Authenticatie in een OpenVMS
omgeving

Agenda

- Inleiding
- OpenVMS authenticatie en authorisatie
- Traditioneel (username/password-based)
- ACME, Kerberos, LDAP, X.500
- Kerberos principes
- Inpassing kerberos in OpenVMS
- Tips en hints
- vragen

Inleiding

- **Wie**
 - Ton van der Zwet
- **Waarom**
 - Onderzoek (inpas)mogelijkheden
- **Hoe**
 - Labomgeving obv personal-alpha

OpenVMS authenticatie en autorisatie

- Authenticatie

- Wie ben “ik”

- Local: (sysuaf)
username/password
 - remote (proxy): (idem + netproxy)
nodename/username (password)
 - Batch: (idem + local trust)
Autorisatie bij submit
 - Netwerk daemon: (idem + local trust)
protocol/networkstack

- Autorisatie

- Wat mag “ik”

- Priv's (sysuaf)
 - Quota's (sysuaf)
 - Rights (sysuaf/rightslist)

Authenticatie

- Authenticatie?
 - Wie is u??
 - Zekerheid?
 - Blauwe ogen...
 - Username/password (index & sleutel)
 - Vertrouwde bron

ACME, Kerberos, LDAP, X.500

- ACME
 - Authentication Credential Management Extension
- Kerberos
 - Strong network authentication protocol
- LDAP
 - Lightweight Directory Access Protocol
- X.500
 - Protocollen tbv gebruik directory services
- HP OpenVMS Enterprise Directory
 - HP implementatie X.500

ACME

- ACME
 - Authentication Credential Management Extension
 - Een “ander” login-pad
 - Meerdere authenticatiemethoden mogelijk
 - Traditioneel (~loginout.exe)
 - Microsoft LAN Manager authentication
 - LDAP (active directory, enterprise directory)
 - Kerberos
 - Nieuw (biometrisch, RFID, ...(zelf te bouwen...))

Kerberos



- Sterk netwerk authenticatie protocol
- Client/server applicaties
- Secret-key cryptografie
- Massachusetts Institute of Technology.
- <http://www.kerberos.org/>

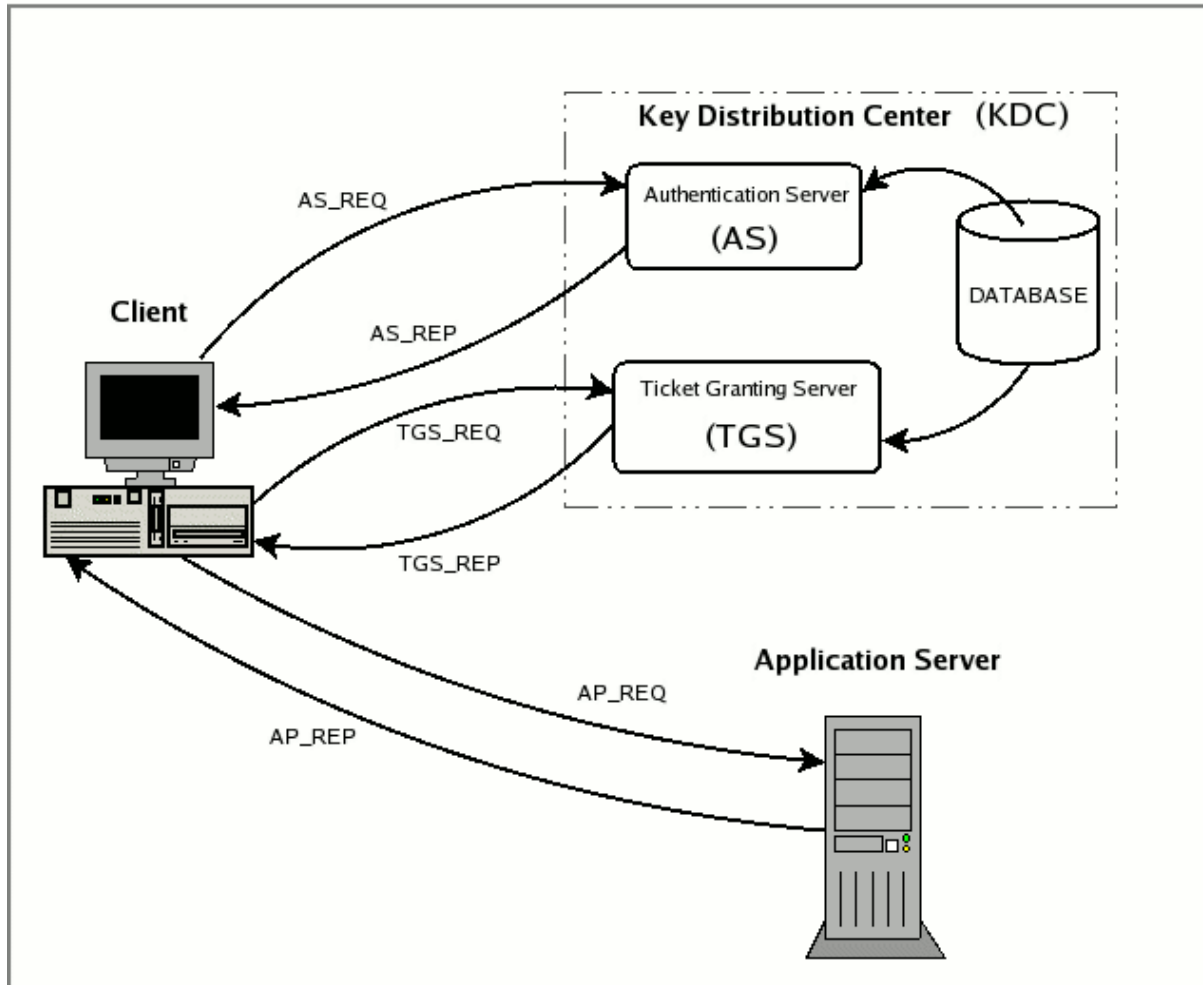
LDAP, X.500, Enterprise directory

- LDAP
 - Netwerkprotocol (versie LDAPv3)
 - Benadering directoryservices (bv. MSAD)
- X.500
 - (heavy-weight) directory service (ITU-T-standaard)
- HP OpenVMS Enterprise Directory
 - X.500 met LDAPv3 (TCP/IP) toegang

Kerberos ICM ACME

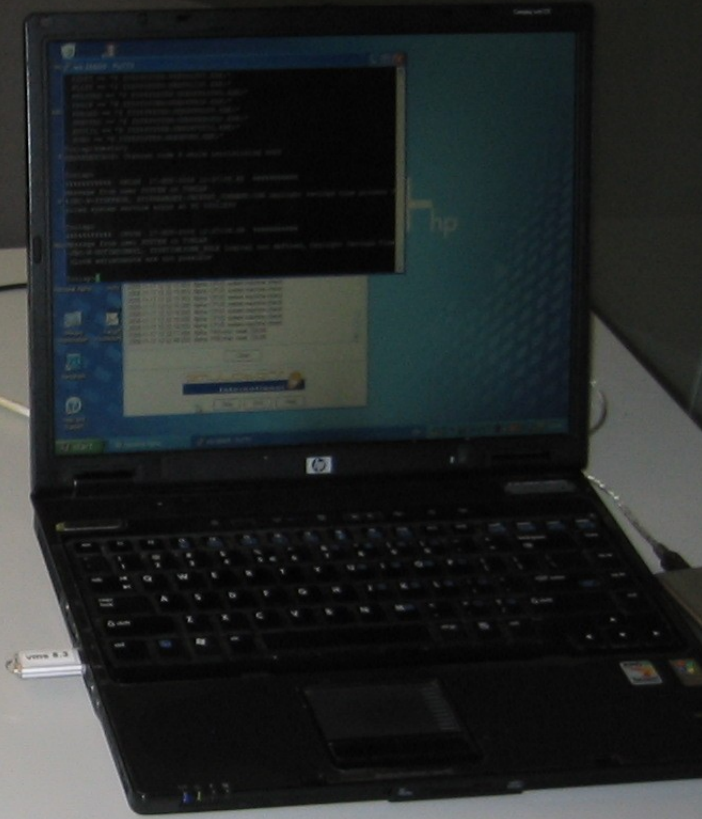
- Kerberos op OpenVMS gebruikers zijn verplicht om meerdere login stappen uit te voeren: één keer om in te loggen op OpenVMS zelf en één keer (kinit) om de Kerberos credentials te krijgen. De ACME agent haalt de Kerberos credentials automatisch op.

Working Kerberos



Inpassing kerberos in OpenVMS

- Foto van lab-omgeving
- Opzet/inrichting LAB
- Uitgevoerde testen
- Conclusies
- Status / nog uit te voeren





Tips en hints

- Zorg voor een juiste UTC-tijd!
 - Zomertijd-wintertijd
- Eerst TCP/IP op orde brengen
 - Gebruik fully qualified names
- Werk de administratie in de juiste volgorde bij
- Mutatie? → Kdestroy!
- Case-sensitive.....
- Namen binnen een REALM moeten uniek zijn...
- Test het ontwerp in een “LAB”

Vragen?

Conventions used for diagrams


 Message between host and KDC
(over network)

 User interaction

 Internal use (locally)


 Container encrypted
with the associated key

 Unencrypted container

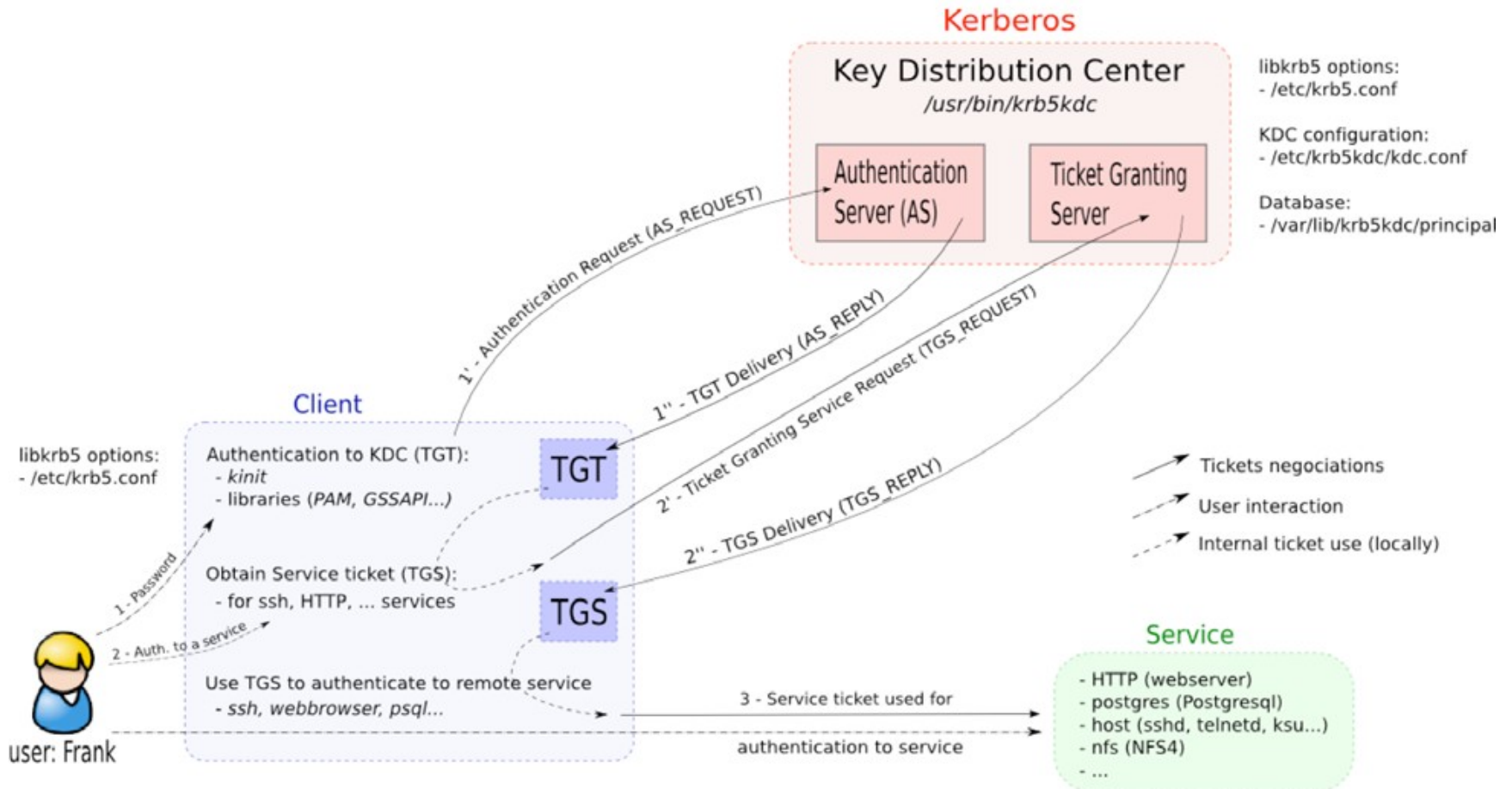
 Client's long term key

 krbtgt principal's key (KDC)

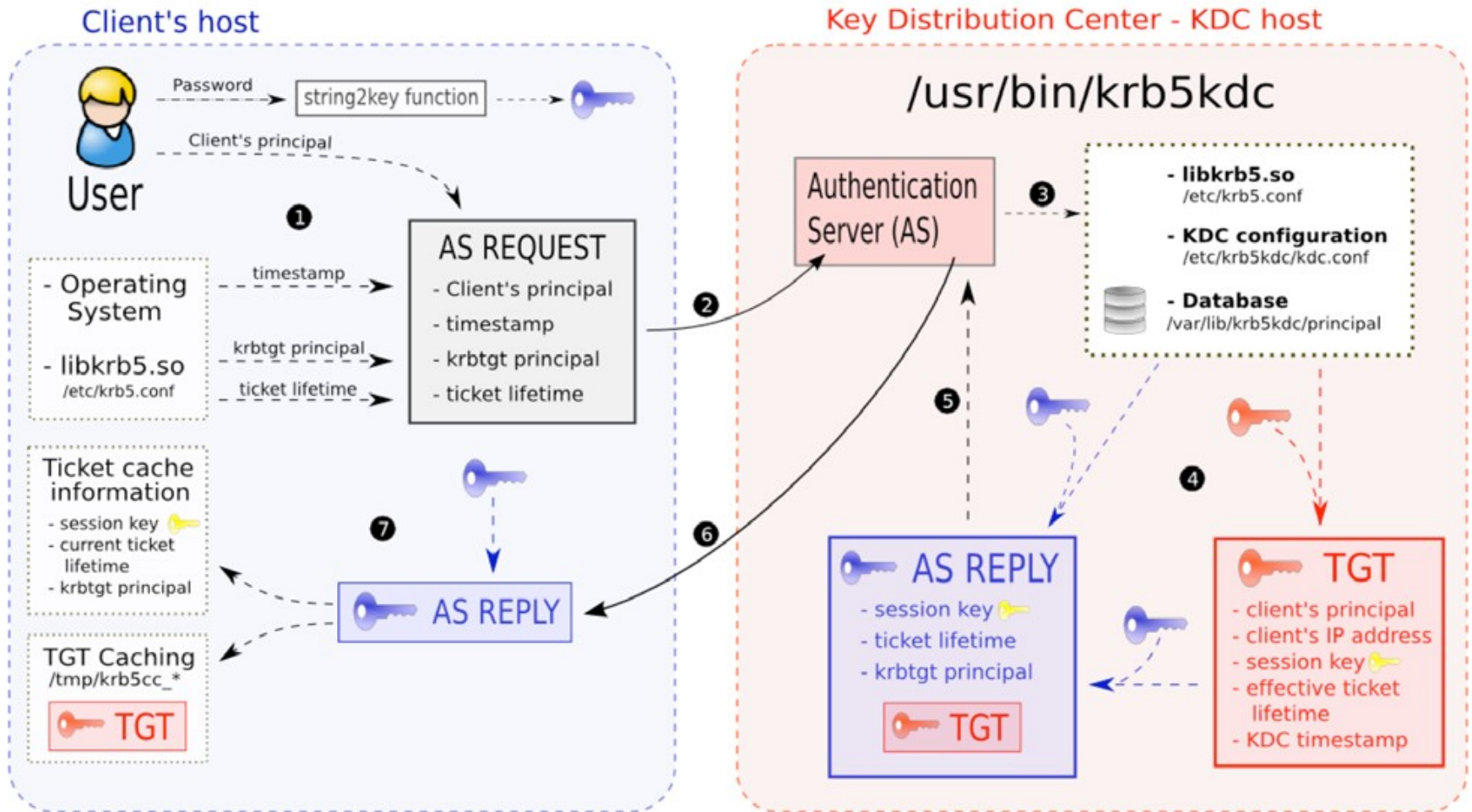
 Service's long term key

 Session keys (short term)

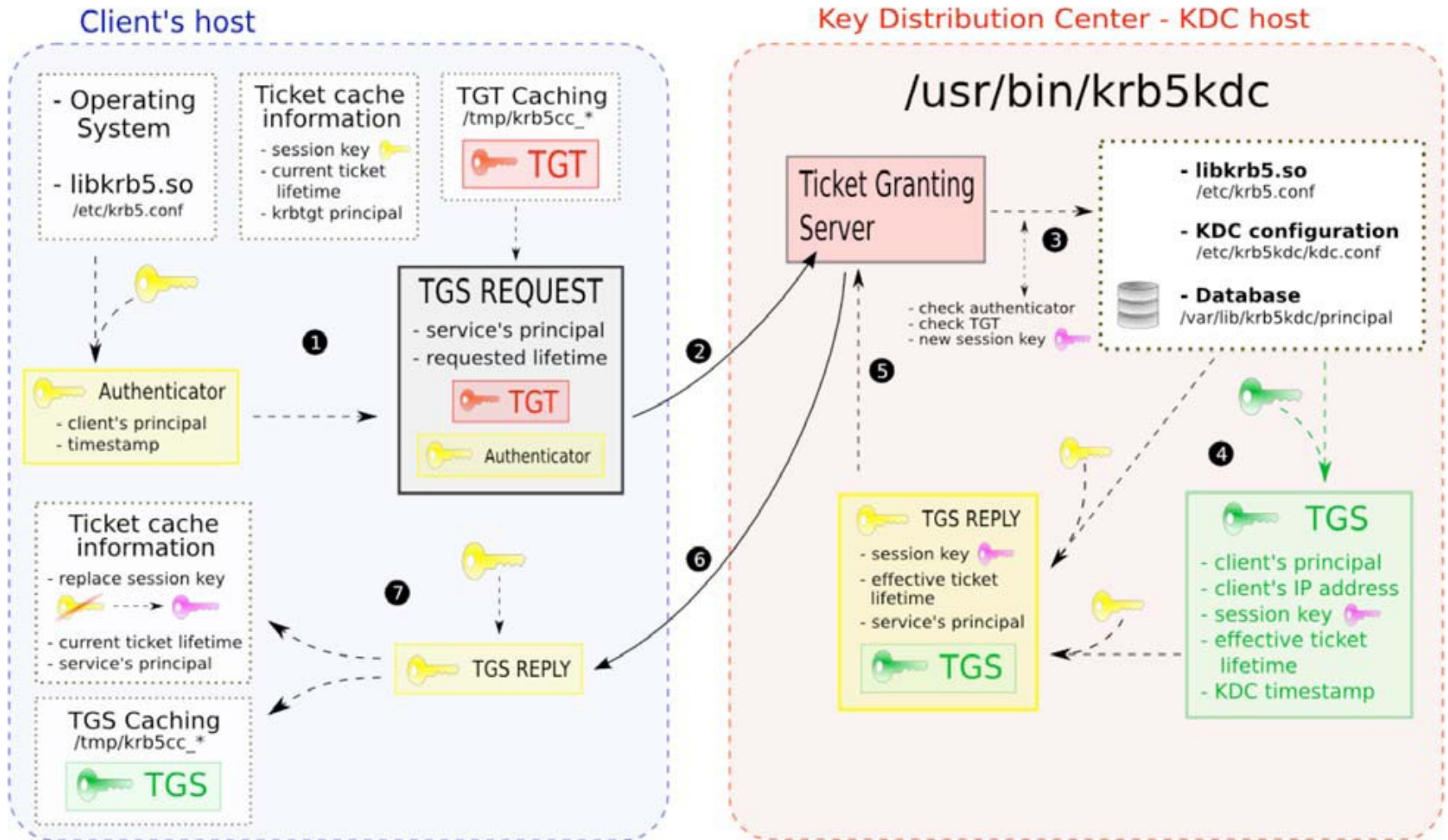
KerberosV5 Tickets Negotiation mechanism

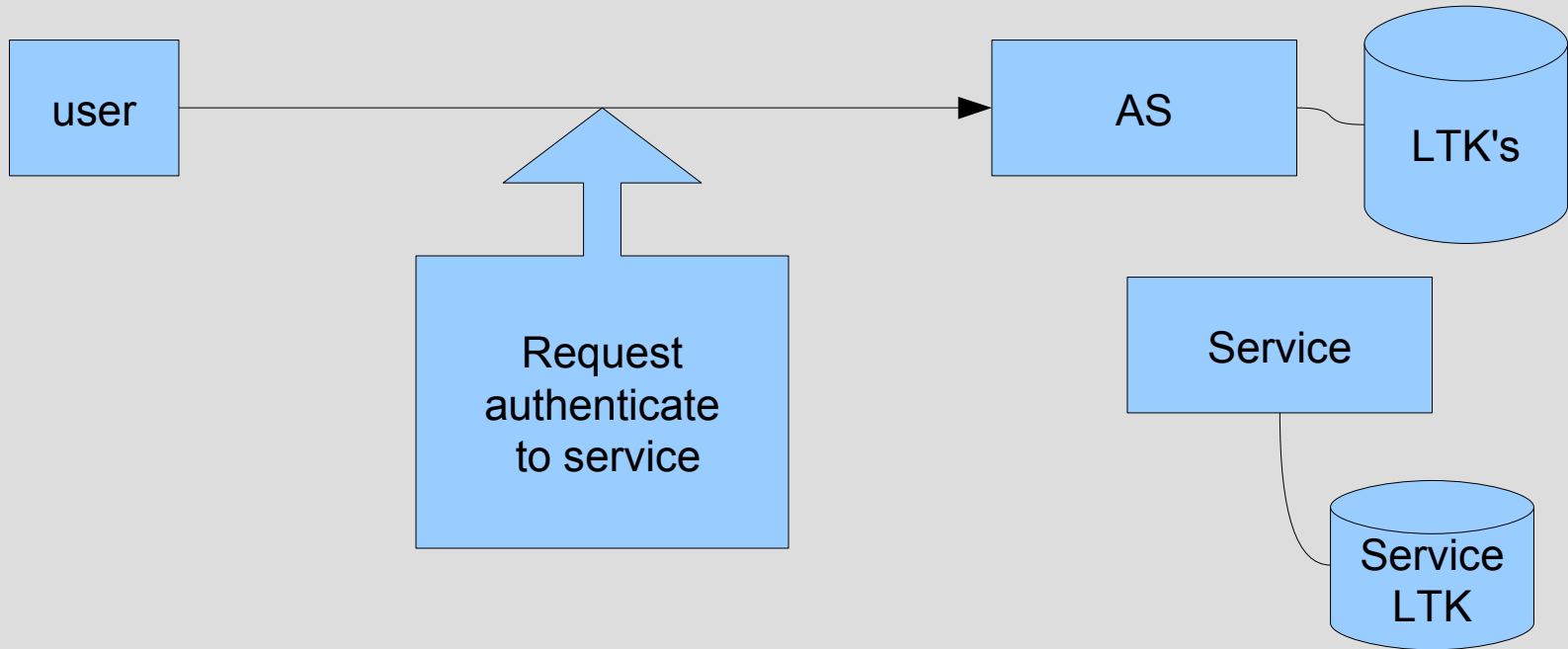


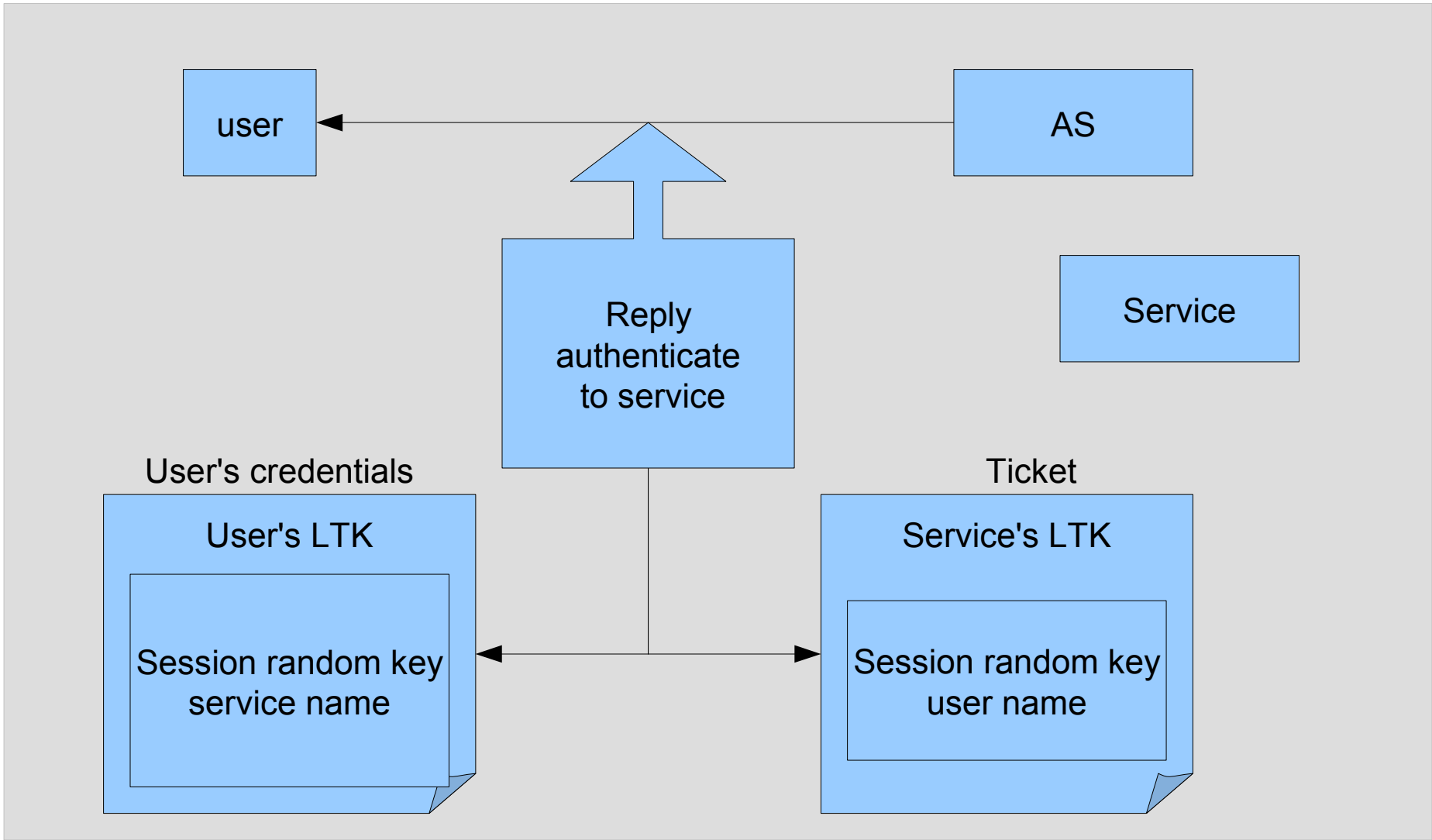
KerberosV5 Authentication Service - TGT delivery

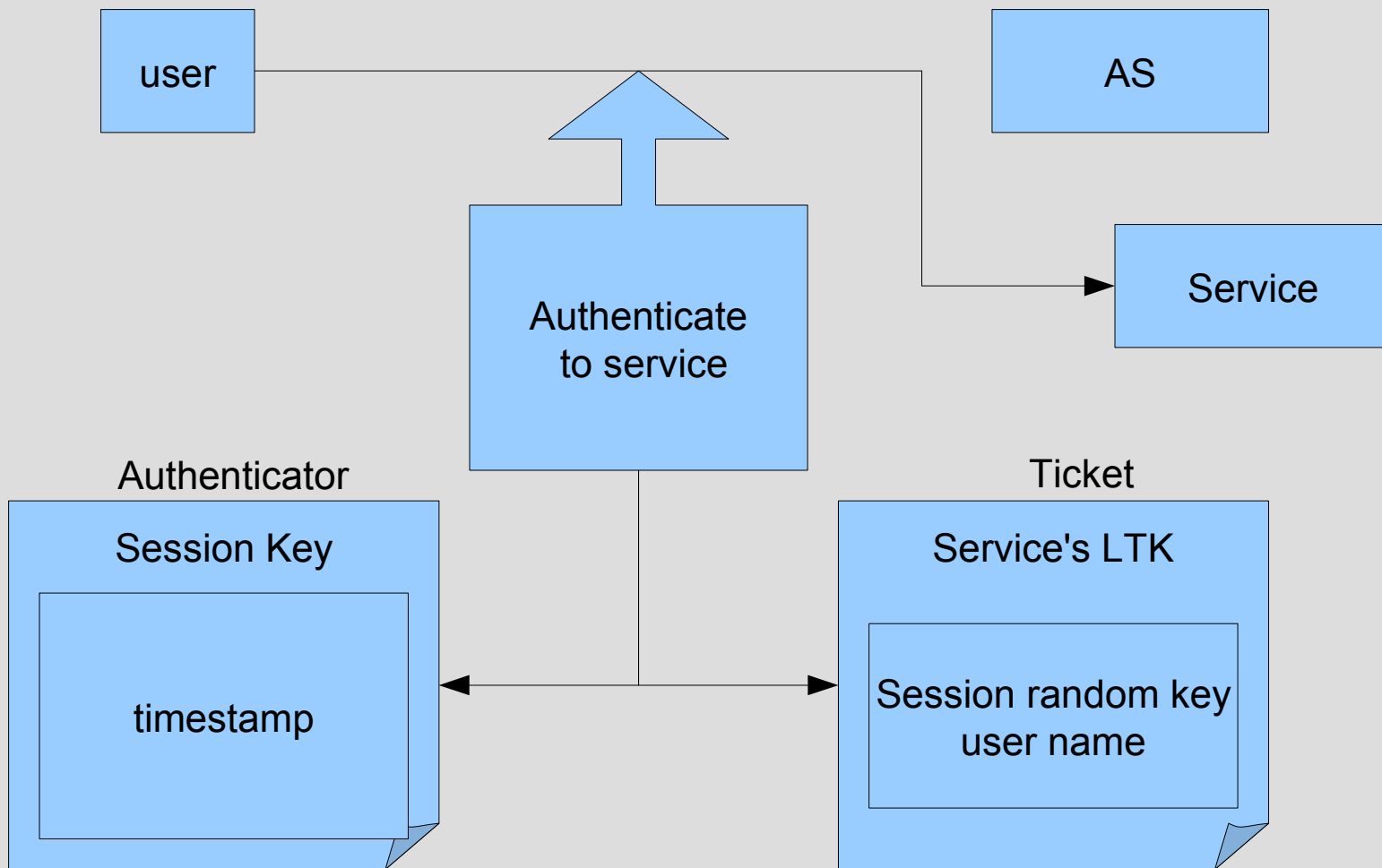


KerberosV5 Ticket Granting Service - TGS delivery









OpenVMS Kerberos

ACME, LDAP, X.500

Authenticatie in een OpenVMS omgeving

1

Positionering presentatie:

- geen (pre-) sales, geen bit-niveau uitwerking
- wel overzicht 'traditionele' authenticatie versus 'nieuwe' authenticatie
- korte verklaring verschil authenticatie versus autorisatie
- nadruk op werkwijze, gebruikerservaring

Agenda

- Inleiding
- OpenVMS authenticatie en autorisatie
- Traditioneel (username/password-based)
- ACME, Kerberos, LDAP, X.500
- Kerberos principes
- Inpassing kerberos in OpenVMS
- Tips en hints
- vragen

2

Er is ruimte voor vragen, (kleine) discussies, mogelijk een korte demo

Bedoeling is een overzicht te geven en de animo voor een sig-bijeenkomst te polsen, waar dan gericht en diepgaander authenticatie kan worden uitgewerkt.

Inleiding

- Wie
 - Ton van der Zwet
- Waarom
 - Onderzoek (inpas)mogelijkheden
- Hoe
 - Labomgeving obv personal-alpha

3

Ton van der Zwet, (ton.vanderzwet@oooovms.dyndns.org) sinds versie 1.x met VMS bezig en lang lid van OpenVMS gebruikersverenigingen (DECUS, ...)

Deze presentatie is ontstaan omdat ik geïnteresseerd geraakt ben in de nieuwe mogelijkheden die beschikbaar kwamen met de komst van ACME, Kerberos en LDAP op OpenVMS. Als gebruiker van LINUX, OpenSource en met name OpenOffice zijn mijn interesses al langer breder dan de VMS-only producten. In deze open wereld zijn VMS-only toepassingen nauwelijks bekend, maar de OpenSource functioneel “gelijkwaardige” producten des te meer. Het gebruiken van de kwaliteiten van OpenVMS in deze wereld is voor mij een uitdaging.

Het uitzoeken van de mogelijkheden van OpenVMS in een complexe client/server omgeving vereist een aantal (OpenVMS) servers. Deze hebben we heel snel en flexibel kunnen realiseren door een aantal laptop's te voorzien van een ALPHA emulator (Personal Alpha). Deze methode is ook voor een hobbyist, eventueel met de hulp van een aantal mede-hobbyisten, zonder hoge kosten te realiseren.

Bij mijn werkgever is er al langer een wens om tot een single-signon werkwijze te komen. Deze is echter gebaseerd op een windows/AD/E-dir omgeving. Hoe past OpenVMS in dit plaatje...

Mijn dank gaat uit naar Fekko Stubbe en Martin Borgman voor hulp bij het realiseren van dit onderzoek. Zonder hun inhoudelijke bijdragen en feedback zou deze presentatie niet tot stand gekomen zijn.

OpenVMS authenticatie en autorisatie

- Authenticatie
 - Wie ben “ik”
 - Local: (sysuaf)
username/password
 - remote (proxy): (idem + netproxy)
nodename/username (password)
 - Batch: (idem + local trust)
Authorisatie bij submit
 - Netwerk daemon: (idem + local trust)
protocol/networkstack
- Authorisatie
 - Wat mag “ik”
 - Priv's (sysuaf)
 - Quota's (sysuaf)
 - Rights (sysuaf/rightslist)

4

De sysuaf vormt de basis voor de lokale authenticatie en autorisatie database. Voor het authenticatie gebruik wordt de index (username) - sleutel (password) combinatie vergeleken met de authenticatie aanvraag. Username komt functioneel overeen met de public-key; het password met de (shared) secret key. Dit is een long term key. (longterm kan zijn 1-malig tot oneindig zijn, afhankelijk van de beveiligings-strategie)

Zijstap: ALF (automatic login facility) met sysalf als database werkt op basis van poortnaam (device), een userproces wordt gestart zodra er een bijvoorbeeld een return wordt ingegeven op deze poort. Bijvoorkeur te gebruiken daar waar slechts één applicatie gebruikt wordt, bijvoorbeeld point of sales terminals.

Decnet proxy database heeft de vorm van “nodename”::”remote user” mapped naar “lokale user”. Velden in deze database mogen wildcards zijn! Wordt niet aanbevolen voor interactief gebruik!

Batch: het submitten van een batchjob kan alleen vanuit een geauthenticeerd proces met de juiste autorisatie. De job-gegevens worden opgeslagen in de beveiligde queue-database. Een eenmaal gesubmitte job is in principe vwb authenticatie niet meer te wijzigen .

Voor een TCP/IP daemon wordt door een listener op een vastgesteld poortnummer geluisterd. Zodra daar een volgens het protocol geldige activiteit plaatsvind, wordt er lokaal een activiteit uitgevoerd (bijvoorbeeld telnet: start een nieuwe telnet sessie onder het account van de nieuwe gebruiker)

Authorisatie: wat zijn de resources die het proces mag benaderen/gebruiken/verwijderen. Bijvoorbeeld CPU-time, memory, devices, files --> “objecten”

Authenticatie

- Authenticatie?
 - Wie is u??
 - Zekerheid?
 - Blauwe ogen...
 - Username/password (index & sleutel)
 - Vertrouwde bron

5

Authenticatie betreft het zekerstellen van de identiteit van de aanvrager. De manier waarop dit veelal gebeurt is gebaseerd op het vertrouwen van één of meerdere kenmerken/attributen van de aanvrager. De traditionele attributen van de aanvrager zijn een unieke username en het bijbehorende password. Deze combinatie is ook vastgelegd in de authenticatie/authorisatie databases van de server. De username is te vergelijken met een public key en wordt gebruikt als index in de databases. Nadelen van deze methode zijn onder andere een beperkte lange termijn veiligheid omdat bij elke authenticatie dezelfde combinatie moet worden gebruikt. (kans op onderschepping, maatregelen: korte password lifetime, encrypted verbindingen)

Nieuwe technieken maken het gebruik van andere attributen mogelijk: bijvoorbeeld biometrische authenticatie

Een andere oplossingsrichting is de encryptie van de communicatie in combinatie met wederzijdse authenticatie voordat er geautoriseerd kan worden. Deze methodiek wordt gebruikt door kerberos: Lokaal eenmalige authenticatie dmv de traditionele methode, daarna wordt er door het gebruik van een uniek eenmalig ticket met beperkte levensduur (TGT) per service een andere unieke eenmalige authenticatiekey aangemaakt. Ook voor de kerberos omgeving geldt dat er een trustrelatie tussen de authenticator (ook AS, of KDC genoemd) en de serviceleveranciers en clients moet bestaan. In de volgende dias wordt aangegeven hoe kerberos dit realiseert.

ACME, Kerberos, LDAP, X.500

- ACME
 - Authentication Credential Management Extension
- Kerberos
 - Strong network authentication protocol
- LDAP
 - Lightweight Directory Access Protocol
- X.500
 - Protocollen tbv gebruik directory services
- HP OpenVMS Enterprise Directory
 - HP implementatie X.500

6

Het ACME mechanisme is de, door HP gedocumenteerde en beschikbaar gestelde interface voor de authenticatie van “gebruikers”.

Kerberos is een beveiligd, uitgaande van een onveilig (inter)netwerk, authenticatieprotocol. Het protocol is bedoeld voor client-server omgevingen, met ruime interpretatie van clients en servers (services).

LDAP, X.500 zijn gestandaardiseerde protocollen die het gebruik van directories (verzamelingen gegevens veelal gebruikt tbv authenticatie en autorisatie) beschrijven.

X.500 is gebaseerd op het OSI-model (7 laags-structuur), met de daarbij behorende zware, geformaliseerde protocol-beschrijvingen. Een X.500 implementatie vereiste behoorlijk veel ICT resources.

LDAP is een een afgeslankte implementatie van directory gebruiksprotocollen. LDAP vereist (veel) minder ICT resources.

HP OpenVMS Enterprise Directory is een X.500 implementatie met DECNET-V en TCP/IP (LDAP) koppelingen.

ACME

- ACME
 - Authentication Credential Management Extension
 - Een “ander” login-pad
 - Meerdere authenticatiemethoden mogelijk
 - Traditioneel (~loginout.exe)
 - Microsoft LAN Manager authentication
 - LDAP (active directory, enterprise directory)
 - Kerberos
 - Nieuw (biometrisch, RFID, ...(zelf te bouwen...))

7

Het ACME mechanisme is de, door HP gedocumenteerde en beschikbaar gestelde interface voor de authenticatie van “gebruikers”. Doordat dit mechanisme extendable is, kunnen er allerlei (toekomstige) authenticatiemethodieken op een OpenVMS systeem gebruikt gaan worden. Het vereist “alleen” een het schrijven van een nieuwe extensie/plug-in. Te denken valt aan bijvoorbeeld biometrische authenticatiemethoden (iris-scan, vingerafdruk, ...) of nieuwe technologieën (RFID,...)

Door HP zijn een aantal modules (extenties) geleverd (Traditioneel, MSLM, LDAP/MSAD, Kerberos)

Kerberos



- Sterk netwerk authenticatie protocol
- Client/server applicaties
- Secret-key cryptografie
- [Massachusetts Institute of Technology.](http://www.kerberos.org/)
- <http://www.kerberos.org/>

8

Kerberos is ontwikkeld om authenticatie te doen over niet veilige verbindingen. Deze presentatie gaat uit van een Kerberos 5 implementatie. Microsoft gebruikt Kerberos 5 in AD

Kerberos is ontwikkeld als een authenticatie machine voor project Athena van het MIT in 1983. Het is vrijgegeven als Open Source in 1987 en in 1993 is het een IETF standard geworden.

Links naar de websites:

Website van het MIT, waar veel info te vinden valt:

<http://web.mit.edu/kerberos/>

Website van het kerberos consortium:

<http://www.kerberos.org/>

Onder de tab software zijn whitepapers te vinden.

<http://www.kerberos.org/software/index.html>

LDAP, X.500, Enterprise directory

- LDAP
 - Netwerkprotocol (versie LDAPv3)
 - Benadering directoryservices (bv. MSAD)
- X.500
 - (heavy-weight) directory service (ITU-T-standaard)
- HP OpenVMS Enterprise Directory
 - X.500 met LDAPv3 (TCP/IP) toegang

9

LDAP is een [netwerkprotocol](#) dat beschrijft hoe gegevens uit [directoryservices](#) benaderd moeten worden over bijvoorbeeld [TCP/IP](#)

For LDAP V2:

- RFC 1777 Lightweight Directory Access Protocol
- RFC 1558 A String Representation of LDAP Search Filters
- RFC 1778 The String Representation of Standard Attribute Syntaxes

For LDAP V3:

- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- RFC 2253 Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
- RFC 2254 The String Representation of LDAP Search Filters
- RFC 2255 The LDAP URL Format
- RFC 2256 A Summary of the X.500 (96) User Schema for use with LDAP V3

MS AD is een Microsoft X.500 implementatie met Kerberos 5 voor authenticatie. AD registreert LDAP en Kerberos poorten in Dynamic DNS (Bind 8 en hoger)

X.500 is een [standaard](#) die de [protocollen](#) definieert voor [directoryservices](#) om te gebruiken voor het uitwisselen van informatie. X.500 is ontwikkeld door de [ITU-T](#) (toen nog CITT genaamd) in samenwerking met [ISO](#).

De opbouw van de X.500-standaard volgt het [OSI](#)-model

DUA – Directory User Agent

DSA – Directory System Agent

Directory Protocollen in X.500

DAP - Directory Access Protocol (DUA-DSA)

DSP - Directory System Protocol (DSA-DSA)

DISP - Directory Information Shadowing Protocol (DSA-DSA)

DOP - Directory Operational Binding Management Protocol (DSA-DSA)

(LDAP – Lightweight Directory Access Protocol)

HP Enterprise directory is een volledige X500 directory implementatie (ISO/OSI-model) waarbij in versie 5.4 de noodzaak om de net te gebruiken vervallen is. Met deze versie is ook een TCP/IP-only benadering met LDAP mogelijk

Kerberos ICM ACME

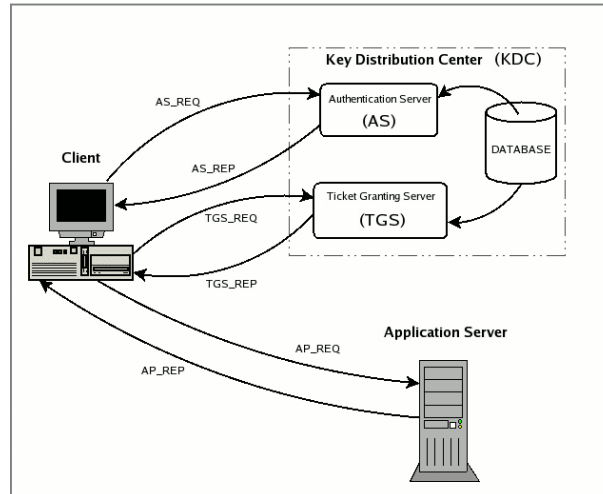
- Kerberos op OpenVMS gebruikers zijn verplicht om meerdere login stappen uit te voeren: één keer om in te loggen op OpenVMS zelf en één keer (kinit) om de Kerberos credentials te krijgen. De ACME agent haalt de Kerberos credentials automatisch op.

10

Deze opmerking komt uit de ACME kerberos documentatie. Op dit moment is de status van de Kerberos agent “nog niet op productie-kwaliteit”

De voordelen van de ACME-integratie zijn echter dat bijvoorbeeld de password synchronisatie over het hele REALM bij het inloggen via ACME/KERBEROS gebeurt. Wij zijn nog met onderzoek bezig naar de mogelijkheden en inpasbaarheid van KERBEROS in een ACME omgeving.

Werking Kerberos



11

Deze dia laat in grote stappen de werking van kerberos zien: Belangrijk is dat er altijd contact (tbv ticket, credentials) moet worden opgenomen met een KDC voordat er door een (application) server service verleend kan worden. Alle componenten (users, clients, hosts, services, kdc,...) moeten met hun LTK's opgenomen zijn in de "databases" (KDC alles, overigen alleen hun eigen keys).

Door encryptie, wederzijdse bekendheid (trust), single session (encryption) keys en tijdigheid als randvoorwaarde te gebruiken, is de betrouwbaarheid (positieve authenticatie) hoog. De strikte naleving van alle randvoorwaarden is echter cruciaal. Het niet invullen van een van de randvoorwaardes leidt tot afwijzing.

Voor meer detail zijn er dia's uit de whitepapers van het kerberos consortium toegevoegd. Tevens is er een stapsgewijze beschrijving van het authenticatie mechanisme (zonder tgt-schil) opgenomen.

Inpassing kerberos in OpenVMS

- Foto van lab-omgeving
- Opzet/inrichting LAB
- Uitgevoerde testen
- Conclusies
- Status / nog uit te voeren

12

Foto (of aanwijzen) van de lab-opstelling

Inrichting twee (drie) VMS 8.3 servers, 1 KDC, 1 (2) client

Ktelnet login client-(KDC)server en v.v., Ktelnet login client-client v.v.

Conclusies:

- tcp/ip (NTP, DNS, local host, ...) inrichting kritisch!
- Case-sensitive
- Timing handelingen kritisch
- Foutmeldingen cryptisch
- Inzicht werking is cruciaal

Nog uit te voeren:

- acme-koppeling
- AD/ldap/E-dir/HPED integratie testen (vereist uitbreiding LAB...)



Te zien zijn twee laptops verbonden via een simpele netwerk-switch, ieder met een personal alpha implementatie. Beide draaien onder OpenVMS 8.3 met kerberos 3.1. Door gebruik te maken van een USB-stick kan snel een extra machine (kopie stick) worden opgetuigd. De linker machine is ingericht als KDC. De rechter machine is een client (applicatie server). Een aantal test-users zijn opgevoerd, en kunnen dmv ktelnet (telnet/authen 'node' 2323) of ssh single sign-on op deze 'infrastructuur' werken. Ook ReflectionX is in de single sign-on mode te gebruiken.

Tips en hints

- Zorg voor een juiste UTC-tijd!
 - Zomertijd-wintertijd
- Eerst TCP/IP op orde brengen
 - Gebruik fully qualified names
- Werk de administratie in de juiste volgorde bij
- Mutatie? → Kdestroy!
- Case-sensitive.....
- Namen binnen een REALM moeten uniek zijn...
- Test het ontwerp in een "LAB"

14

Ook als de "tijd" (show time) op alle systemen goed staat, moet de UTC tijd (=TIJD MET DIFF) gelijk zijn. Gebruik zonodig de procedure sys\$startup:utc\$time_setup.com

```
STAR> sh log *time*
```

```
"SYS$LOCALTIME" = "SYS$SYSROOT:[SYS$ZONEINFO.SYSTEM.EUROPE]AMSTERDAM."  
"SYS$TIMEZONE_DAYLIGHT_SAVING" = "1"  
"SYS$TIMEZONE_DIFFERENTIAL" = "7200"  
"SYS$TIMEZONE_NAME" = "CEST"  
"SYS$TIMEZONE_RULE" = "CET-1CEST-2,M3.5.0/02,M10.4.0/03"
```

```
STAR> sh time
```

```
12-NOV-2008 10:12:54
```

```
STAR> sh log *time*
```

```
"SYS$LOCALTIME" = "SYS$SYSROOT:[SYS$ZONEINFO.SYSTEM.EUROPE]AMSTERDAM."  
"SYS$TIMEZONE_DAYLIGHT_SAVING" = "0"  
"SYS$TIMEZONE_DIFFERENTIAL" = "3600"  
"SYS$TIMEZONE_NAME" = "CET"  
"SYS$TIMEZONE_RULE" = "CET-1CEST-2,M3.5.0/02,M10.4.0/03"
```

```
STAR> sh time
```

```
12-NOV-2008 10:15:27
```

Breng eerst de netwerkadministratie op orde, let op eenduidig gebruik FQDN, case, alias, DNS, local host tabellen, ip-adressen ipv FQDN. Test alle netwerkfunctionaliteiten beide kanten op. Let op firewall instellingen.

Eerst de KDC dan de hosts (services) op de KDC, dan de hosts local keytab, dan de users

Als er een wijziging nodig is, synchroniseer alle locaties waar die info (credentials, keytab's). Omdat de credentials in een lokale cache worden opgeslagen en zolang de lifetime (bijvoorbeeld 8 uur) niet verlopen is door een KINIT niet vernieuwd worden is KINIT alleen NIET voldoende: gebruik eerst een KDESTROY, dan een KINIT.

De wereld buiten OpenVMS is CASE-sensitive, Kerberos is geen uitzondering.... Zorg voor eenduidigheid bij het opvoeren van gegevens.

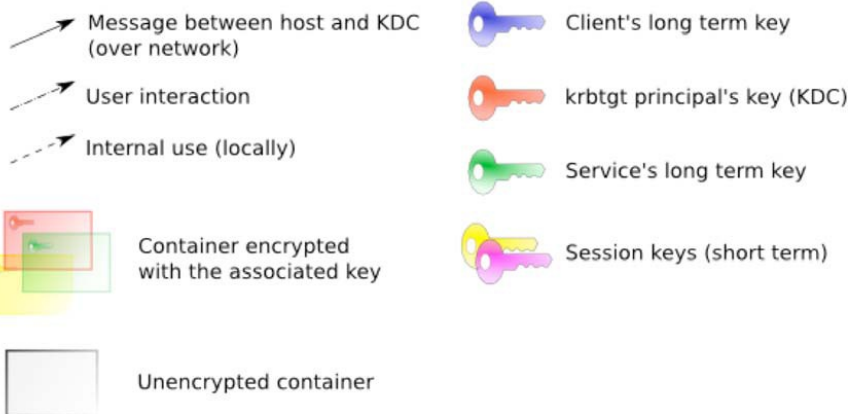
Namen binnen een REALM moeten uniek zijn, denk daarbij ook aan default-namen en functies... De username SYSTEM geeft in een Kerberos realm toegang tot alle servers op het lokale system-account.... Een apart password is daarbij niet meer nodig ;-)

Nadat een ontwerp gemaakt is, test de opzet op onverwachte effecten in een "LAB", Voer gefaseerd in: Tijdinstellingen en synchronisatie dmv NTP, Breng TCP/IP over het hele REALM in kaart en werk bij naar een ontwerp.

Vragen?

- Klik om overzicht toe te voegen

Conventions used for diagrams

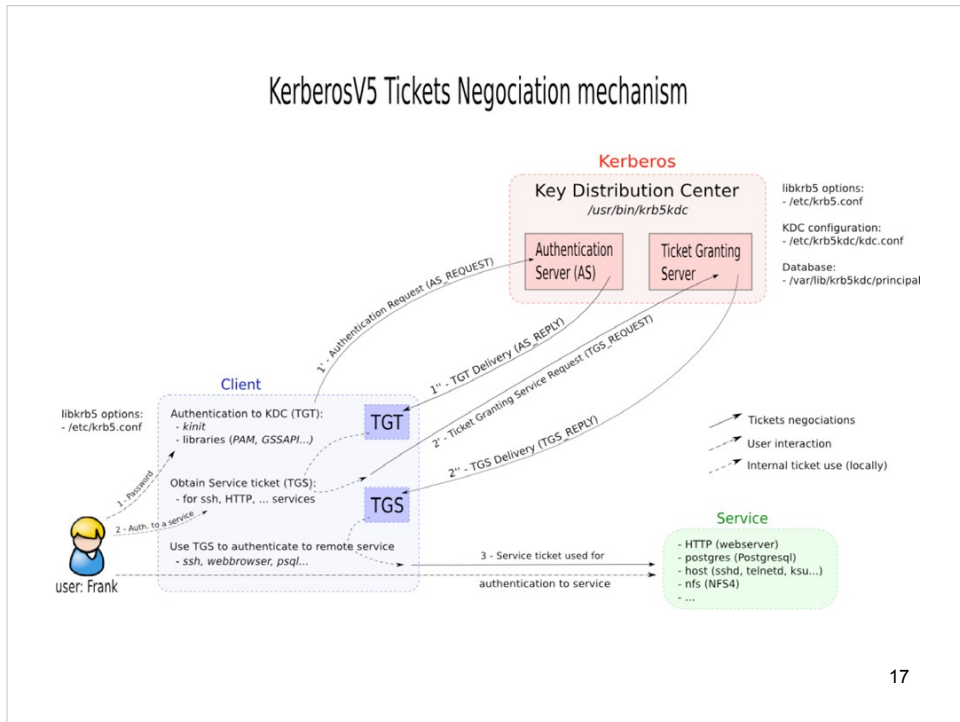


16

Deze dia komt uit “**The MIT Kerberos Administrator’s How-to Guide, draft 1.0**” van de site van het kerberos consortium.
<http://www.kerberos.org/software/adminkerberos.pdf>

Deze dia is nodig (legenda) om de volgende dias te kunnen lezen.

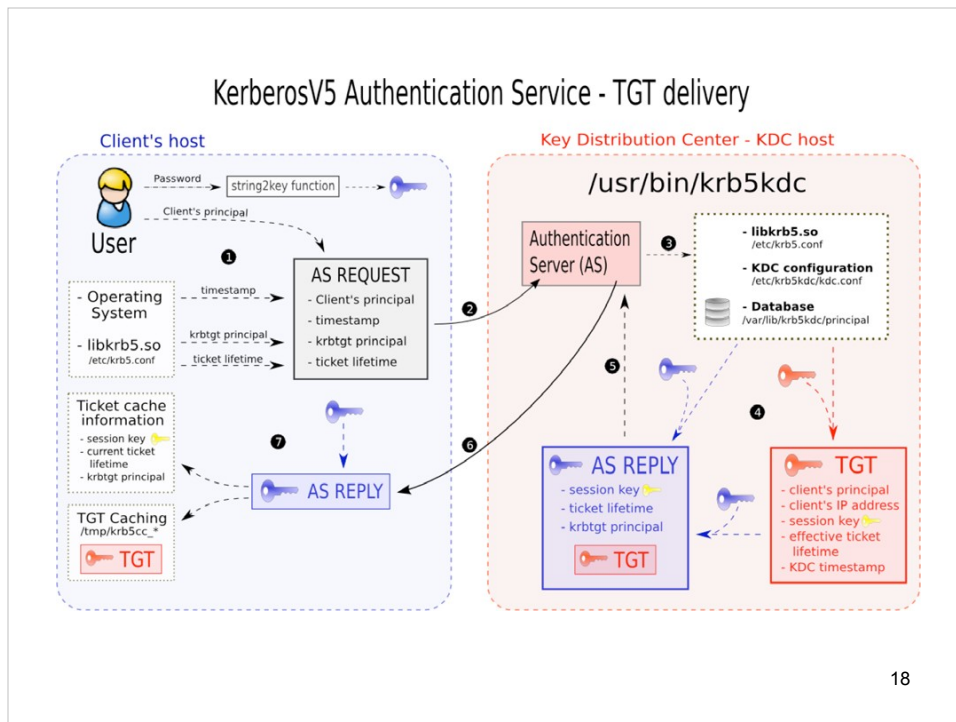
KerberosV5 Tickets Negotiation mechanism



17

Deze dia komt uit “**The MIT Kerberos Administrator’s How-to Guide, draft 1.0**” van de site van het kerberos consortium.
<http://www.kerberos.org/software/adminkerberos.pdf>

Deze dia is functioneel gelijk aan dia 11, maar is tijdens de presentatie moeilijker te lezen....

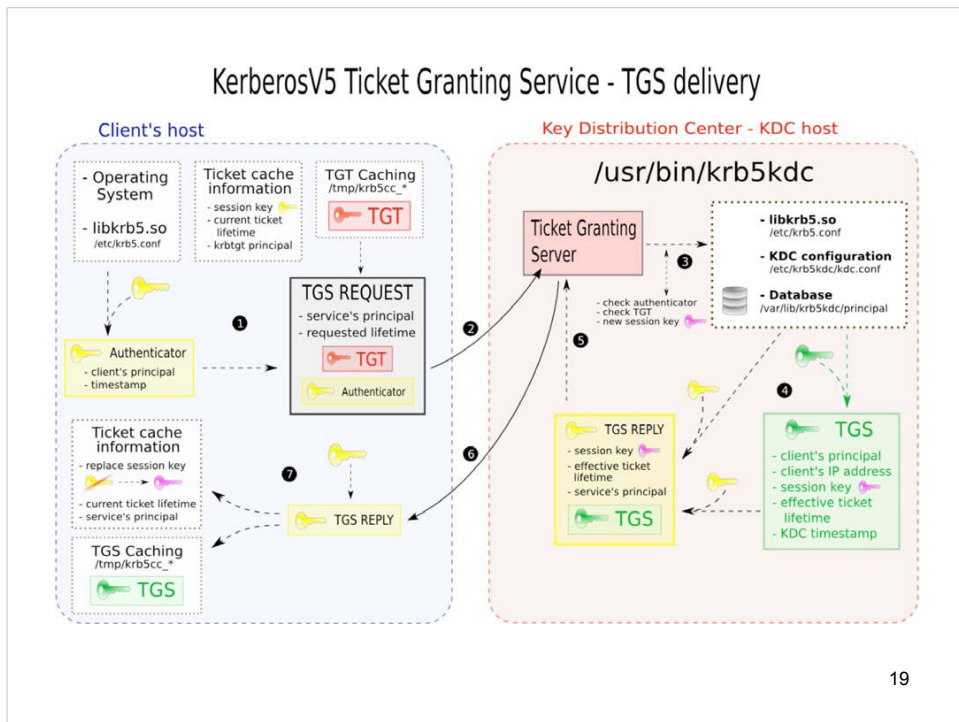


18

Deze dia komt uit “**The MIT Kerberos Administrator’s How-to Guide, draft 1.0**” van de site van het kerberos consortium.
<http://www.kerberos.org/software/adminkerberos.pdf>

Deze dia geeft in meer detail de eerste stap (het verkrijgen van het TGT) weer. Belangrijk is dat de user zijn wachtwoord:

- 1 slechts 1-maal nodig heeft (per TGT lifetime)
- 2 zijn wachtwoord nooit unencrypted tussen de clients-host en de KDC verstuurd wordt.

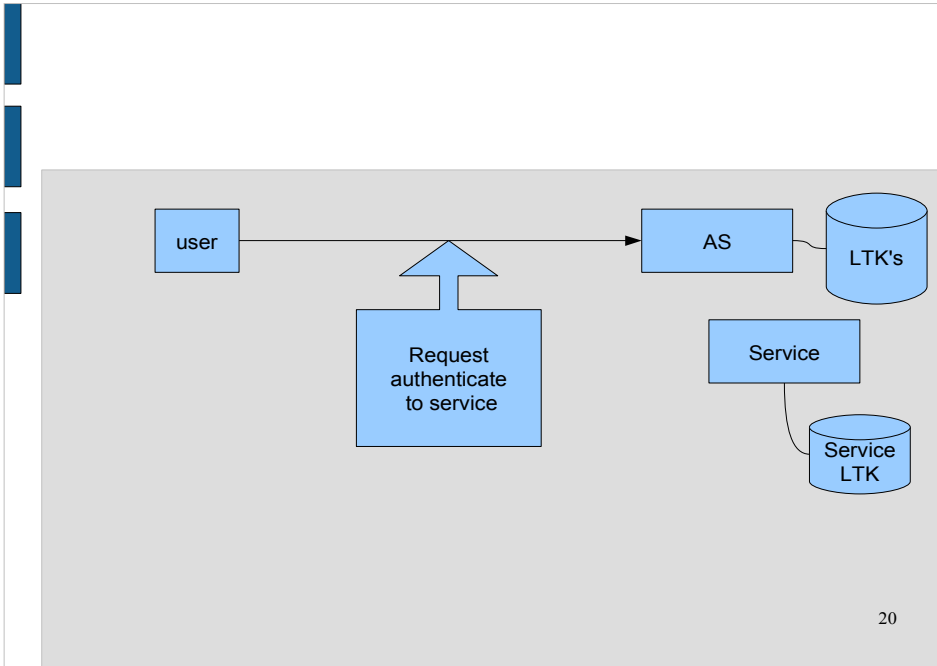


19

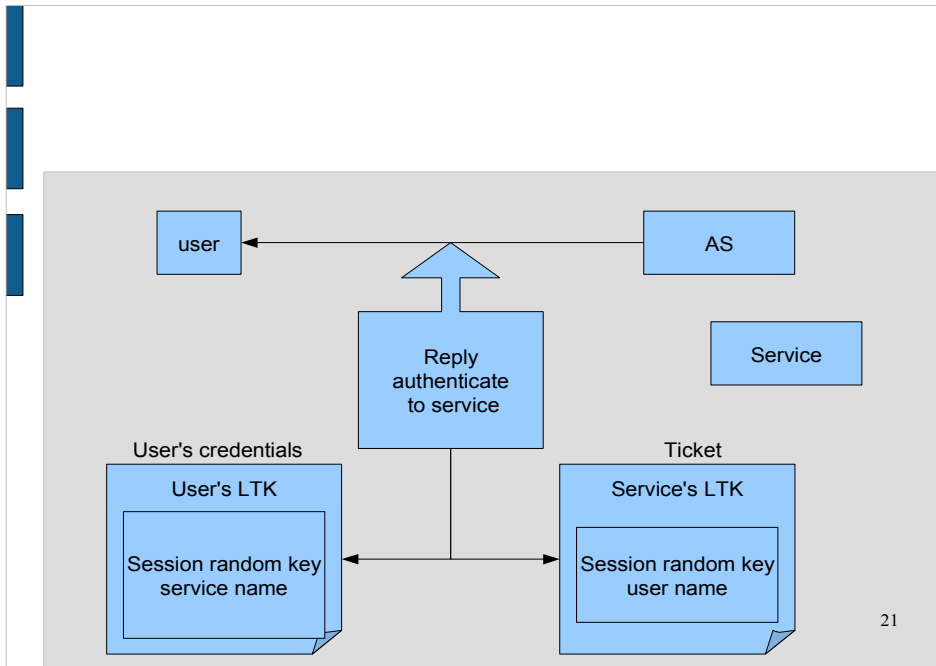
Deze dia komt uit “**The MIT Kerberos Administrator’s How-to Guide, draft 1.0**” van de site van het kerberos consortium.
<http://www.kerberos.org/software/adminkerberos.pdf>

Deze dia geeft in meer detail de tweede stap (het verkrijgen van het TGS) weer. Belangrijk is dat de sessionkey:

- 1 opgeslagen wordt in de ticket cache
- 2 'onder water' gewijzigd wordt (ticket lifetime)

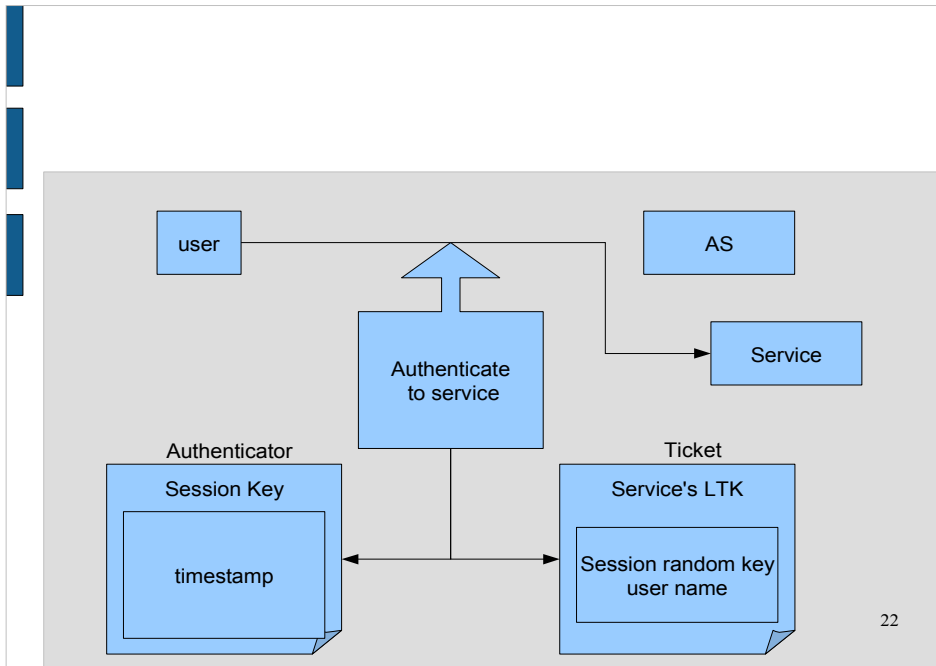


Simpele weergave van de eerste stap in de authenticatie tbv een service (geen tgt schil)



Antwoord van de AS bestaat uit twee pakketten:

- 1 user's credentials, encrypted met de user's LTK, met als inhoud de session random key en de service naam
- 2 service ticket, encrypted met de service's LTK, met als inhoud dezelfde session random key en de users name



De connectieaanvraag van de user naar de service bestaat (o.a.?) uit een tweetal pakketten:

- authenticator, deze bestaat (o.a.?) uit een timestamp encrypted met de session key

- service ticket, deze wordt ongewijzigd meegestuurd (zie vorige dia).

Door de met de service's LTK encrypted session key en username kan de service niet alleen de authenticator decrypten, maar tegelijkertijd impliciet de authenticiteit valideren van de aanvraag, immers de AS heeft beide geauthenticeerd en heeft beider LTK's gebruikt voor de encryptie.