Kerberos

"On the Internet, no one knows you're a dog."

Özgür Yazılım Günleri – 2012
Eray Aslan
eras@gentoo.org

Gündem:

- Kısa tarihçe
- Kimlik Doğrulama Prensipleri
- Kerberos Protokolü
- Protokolün İşleyişi
- Sonuç

Kerberos

Güvenlik ihtiyacı:

- Authentication – Kimlik Doğrulama
  - Kim onay istiyor?
- Authorization – Yetkilendirme
  - Yetkisi var mı?
- Audit – Denetleme
  - Yapılanların kontrolü

Kerberos

Authentication – Kimlik Doğrulama

- Ne biliyorsun?
- Neye sahipsin?
- Nesin?

Daha kuvvetli

Kerberos

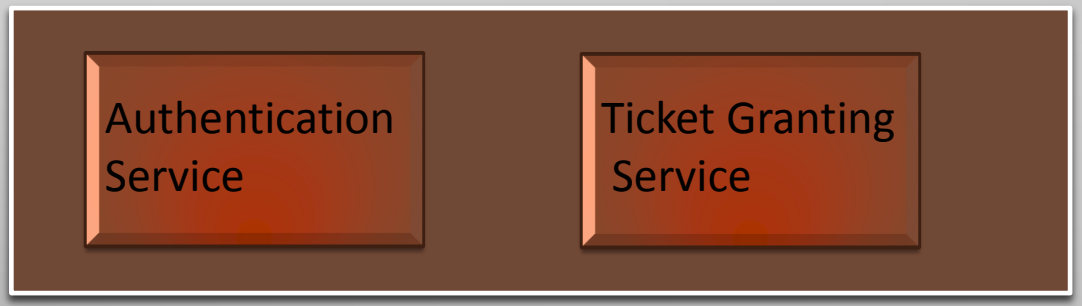
- Network üzerinden kimlik doğrulama protokolü
- Karşılıklı doğrulama (mutual authentication)
- 88/udp, 749/tcp …
- MIT tarafından geliştirildi (Project Athena)
- V5: RFC1510 - 1993 ve RFC4120 - 2005
- Ortak anahtar tabanlı (shared secret key)
- Güvenilen hakem (Trusted Third Party – TTP)
  - Bütün kullanıcı ve servis şifreleri
- SSO (single sign on)
- MIT, Heimdal, MS Windows, Shishi
- *BSD, *nix, OSX, Solaris, AIX, …

Kerberos

Aktörler:

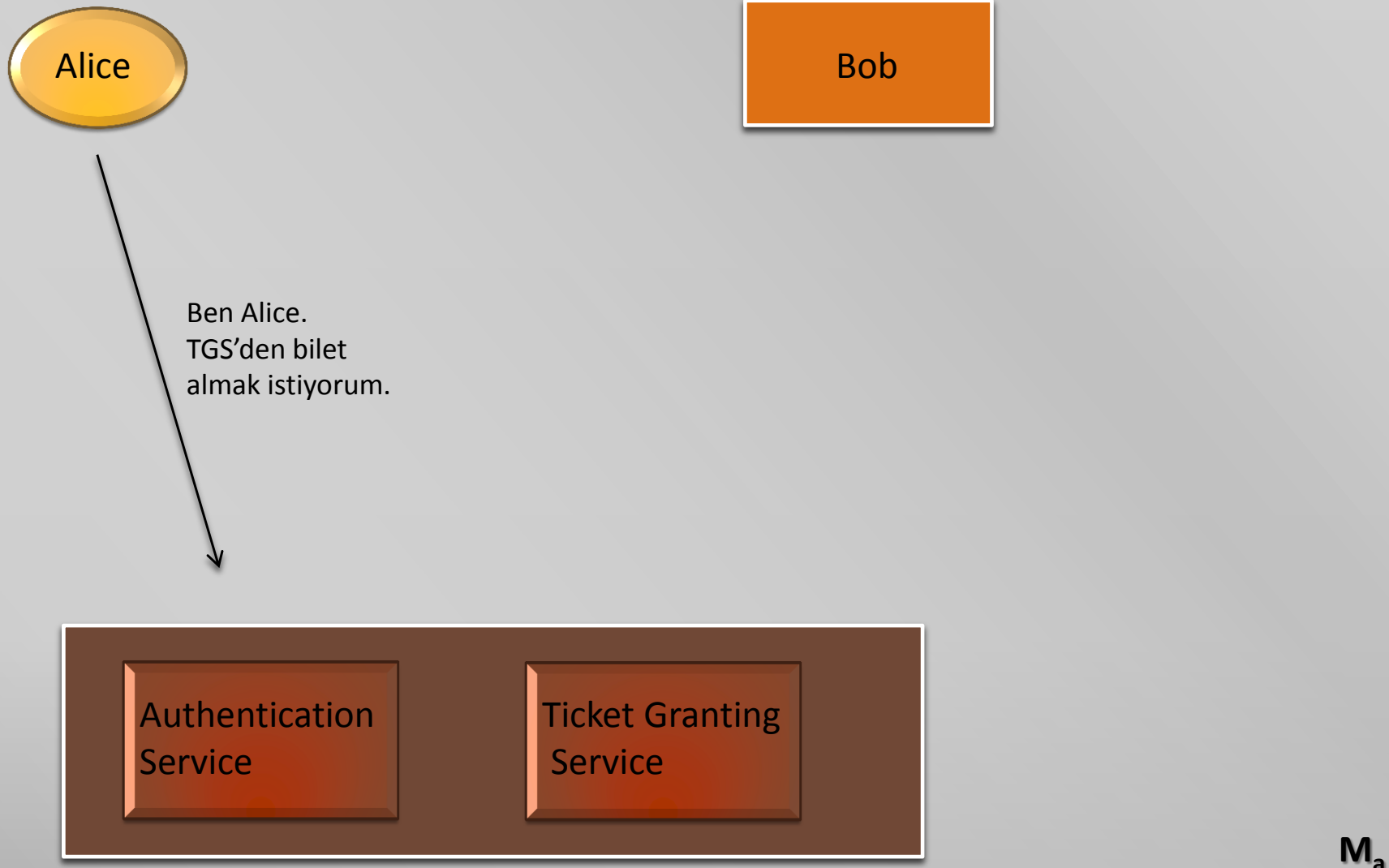
Desktop

Sunucu



Kerberos Sunucusu (KDC)

Kerberos


Alice
Bob
Ben Alice.
TGS'den bilet
almak istiyorum.
Authentication
Service
Ticket Granting
Service

M_a

Kerberos

Alice

Bob

Peki. Bu kutuyu şifren ile kilitledim. Açabilirsen TGS'yi kullanabilirsin.

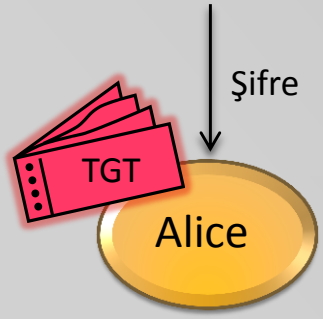
Authentication Service

Ticket Granting Service

S_a

M_b

Kerberos

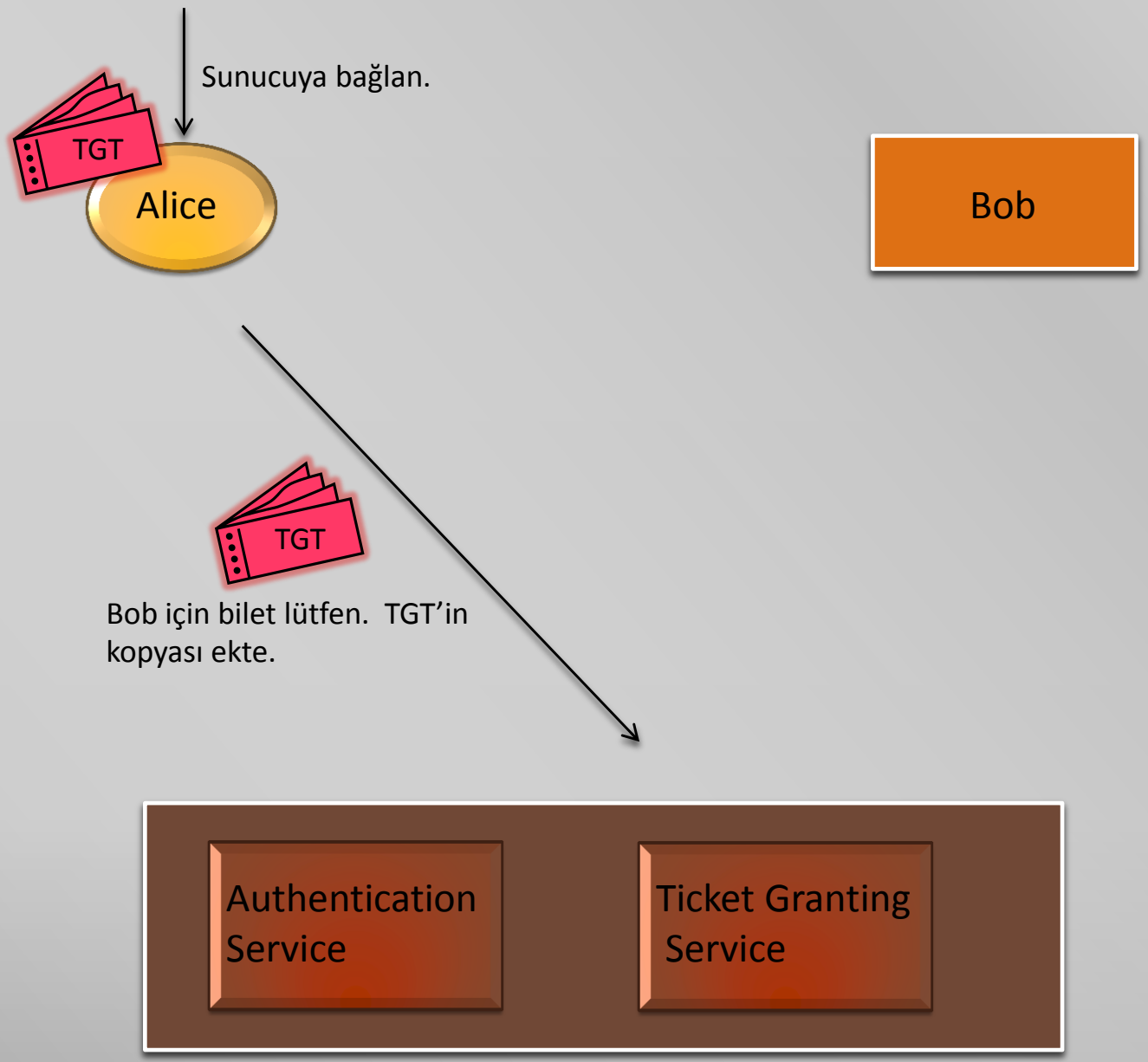


Bob

Authentication Service

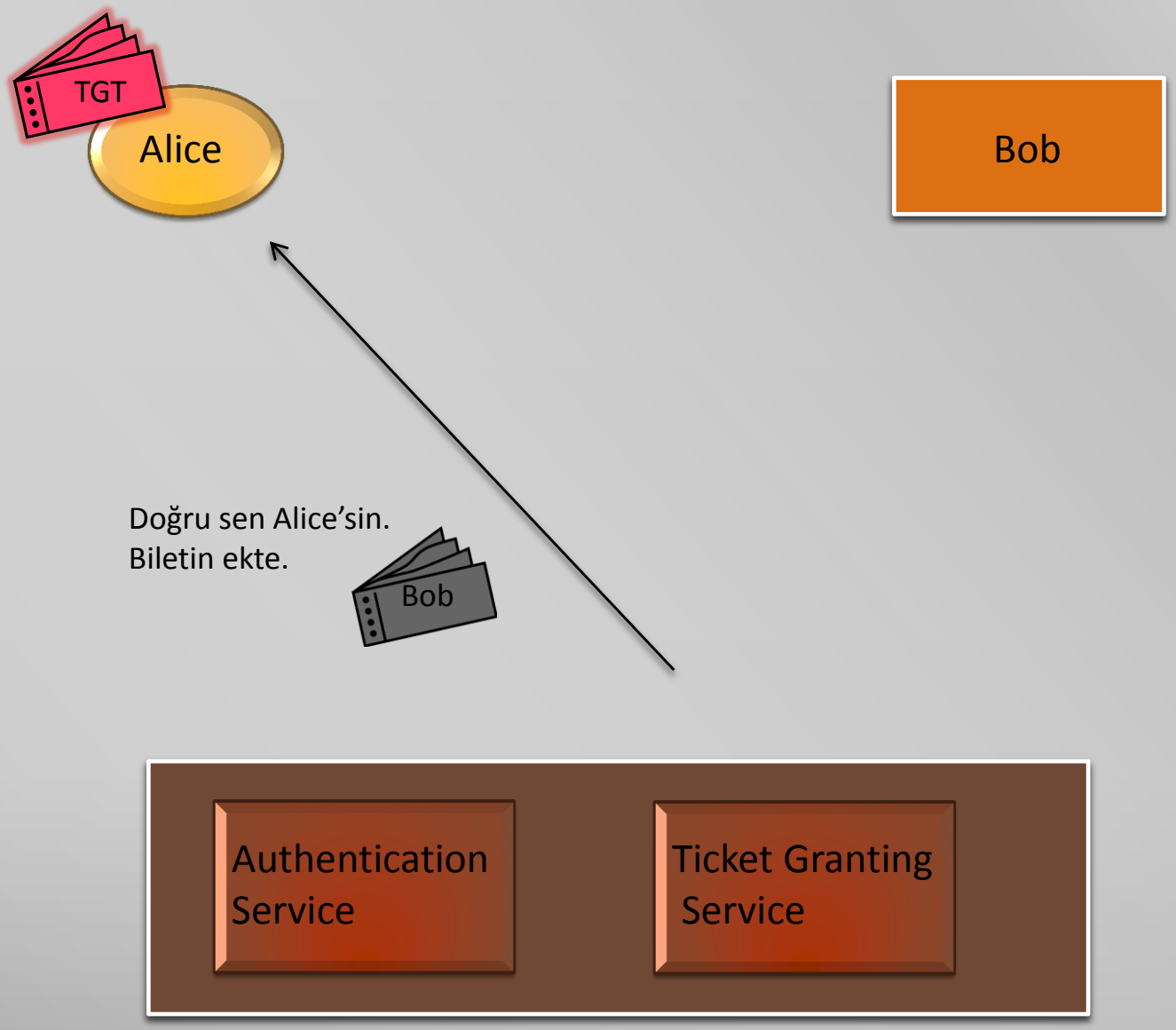
Ticket Granting Service

Kerberos


Sunucuya bağlan.
TGT
Alice
Bob
TGT
Bob için bilet lütfen. TGT'in kopyası ekte.
Authentication Service
Ticket Granting Service

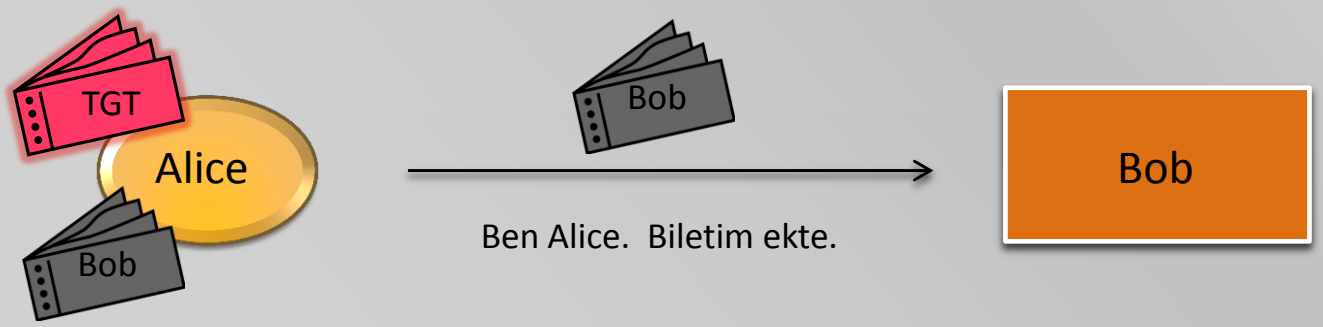
M_c

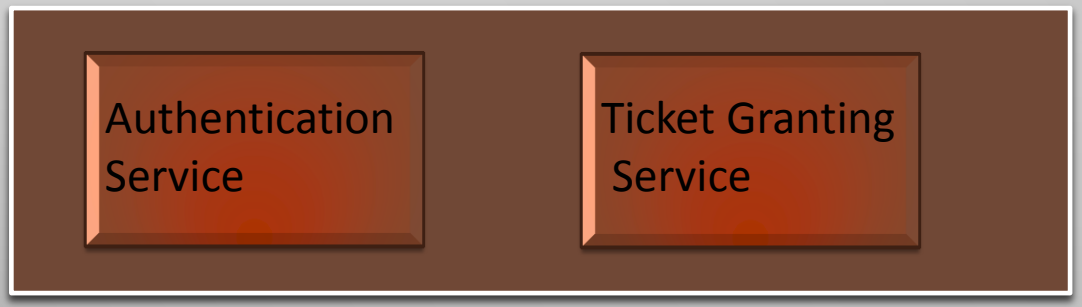
Kerberos


TGT
Alice
Bob
Doğru sen Alice'sin.
Biletin ekte.
Bob
Authentication Service
Ticket Granting Service

M_d

Kerberos

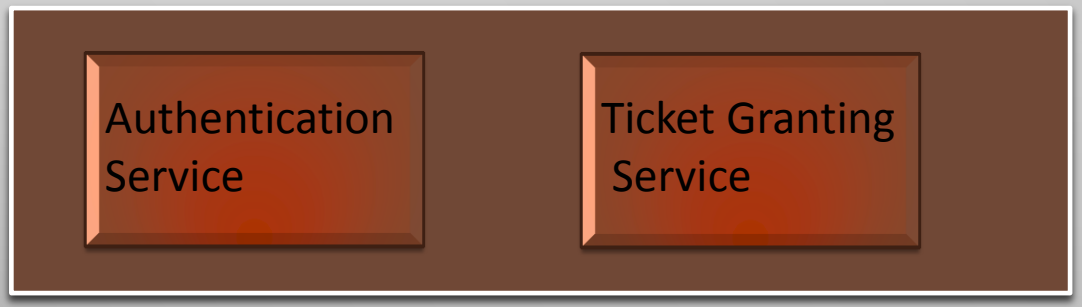

TGT
Alice
Bob
Bob
Ben Alice. Biletim ekte.
Bob


Authentication Service
Ticket Granting Service

M_e

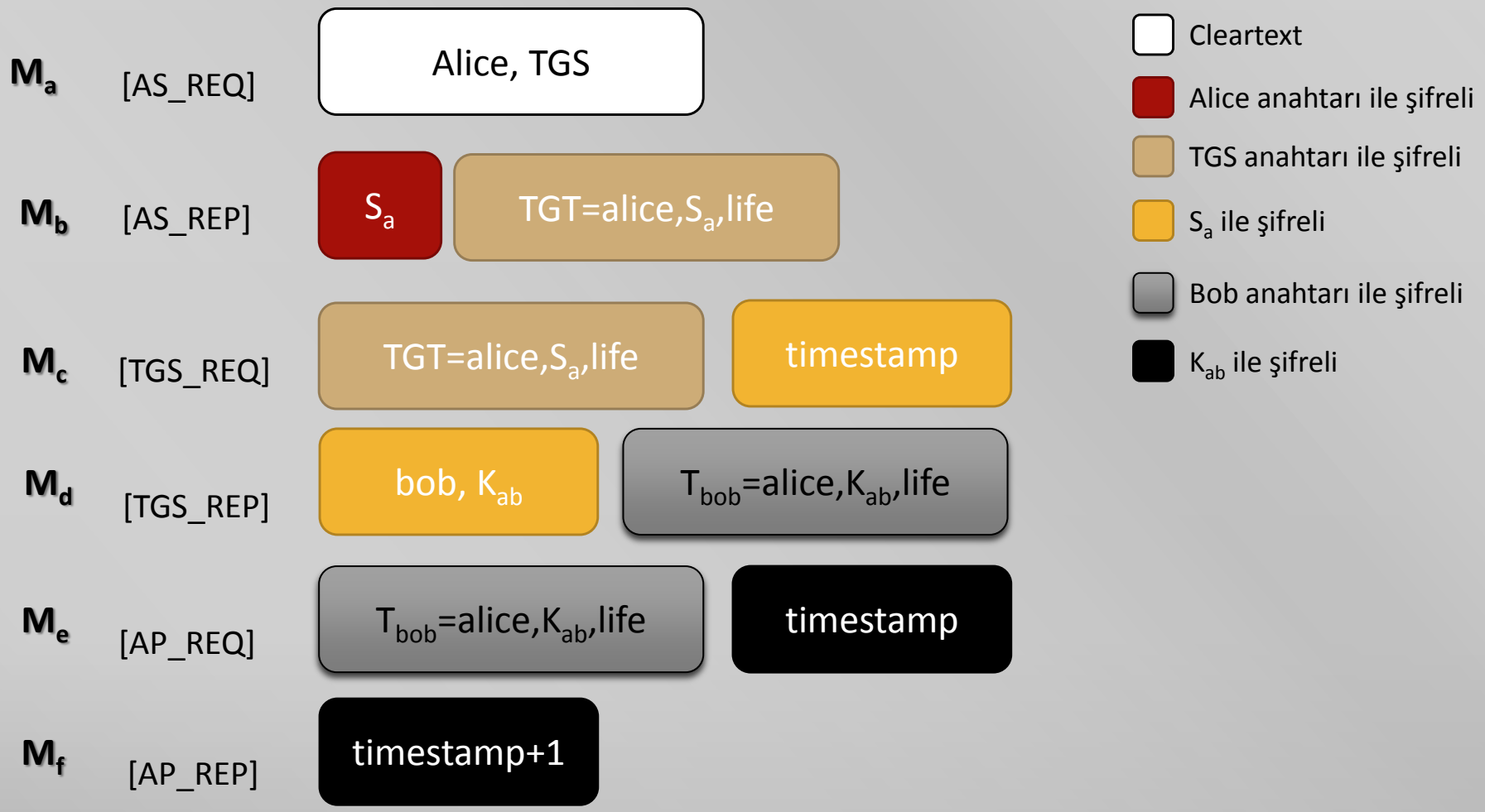
Kerberos


TGT
Alice
Bob
Bob+1
OK. Ben de Bob.
Bob


Authentication Service
Ticket Granting Service

M_f

Kerberos

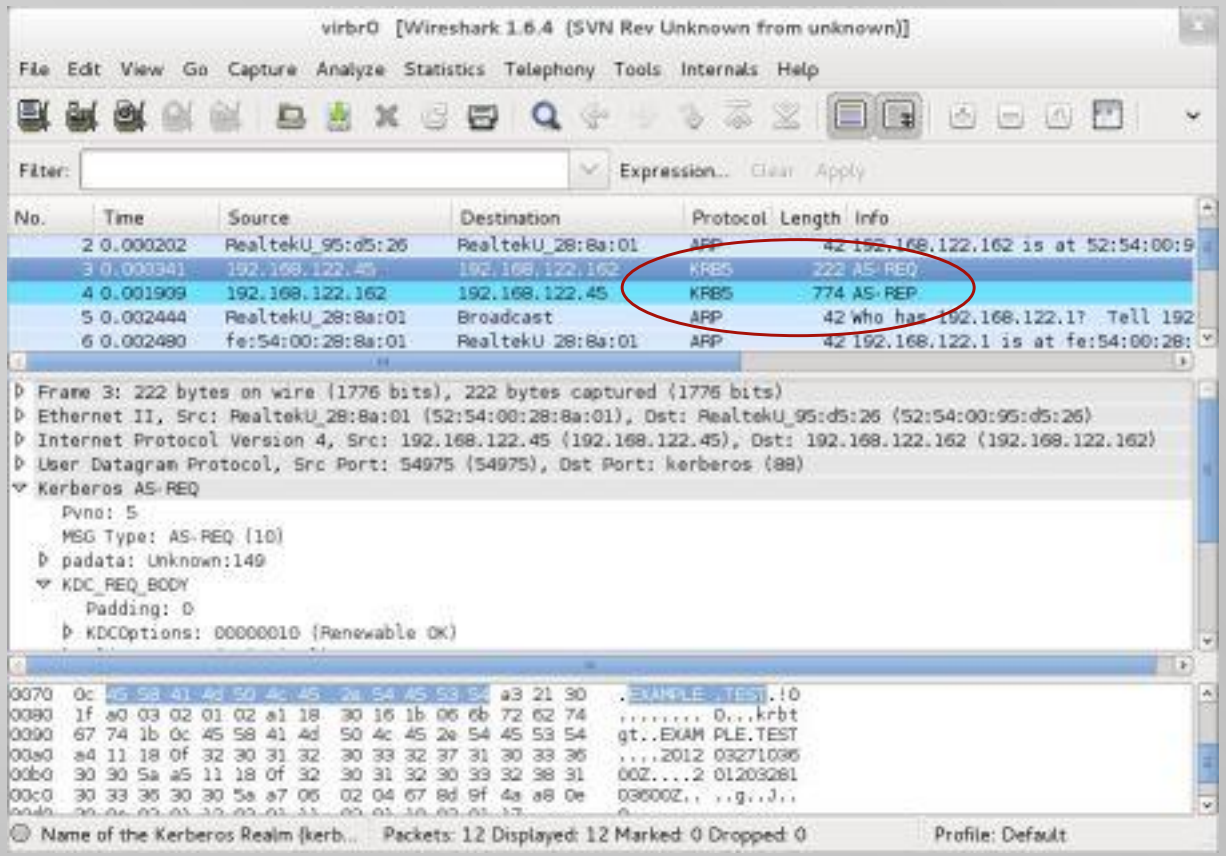

M_a [AS_REQ]
Alice, TGS
M_b [AS_REP]
S_a
TGT=alice,S_a,life
M_c [TGS_REQ]
TGT=alice,S_a,life
timestamp
M_d [TGS_REP]
bob, K_{ab}
T_{bob}=alice,K_{ab},life
M_e [AP_REQ]
T_{bob}=alice,K_{ab},life
timestamp
M_f [AP_REP]
timestamp+1
Cleartext
Alice anahtarı ile şifreli
TGS anahtarı ile şifreli
S_a ile şifreli
Bob anahtarı ile şifreli
K_{ab} ile şifreli

Kerberos

- Alice kimlik doğrulaması yaptı. Ama erişime izni olup olmadığına Bob karar verecek.
- TGT'lerin son kullanma tarihi var
- Güvensiz network
- Güvenli bilgisayar
- Güvenli zaman servisi
- Preauth, FAST, PKINIT
- Single Point of Failure
  - Slave KDC’ler
  - Bütün şifreler tek yerde
- Admin protokolleri farklı

Kerberos

- Pratikte?



- Sonuç:
  - Karışık sistemlerde:
    - Windows, *nix, Solaris vs
  - Ölçeklenebilir
  - Geniş Destek
  - Karmaşık

Sorular?