Kerberos 101

¿Quién soy?

ReD

- Defensor de la privacidad
- Entusiasta de la tecnología
- Especialista en seguridad
- Cofundador de M4H
- Cofundador de Hacklabs
- Formador cuando me dejan

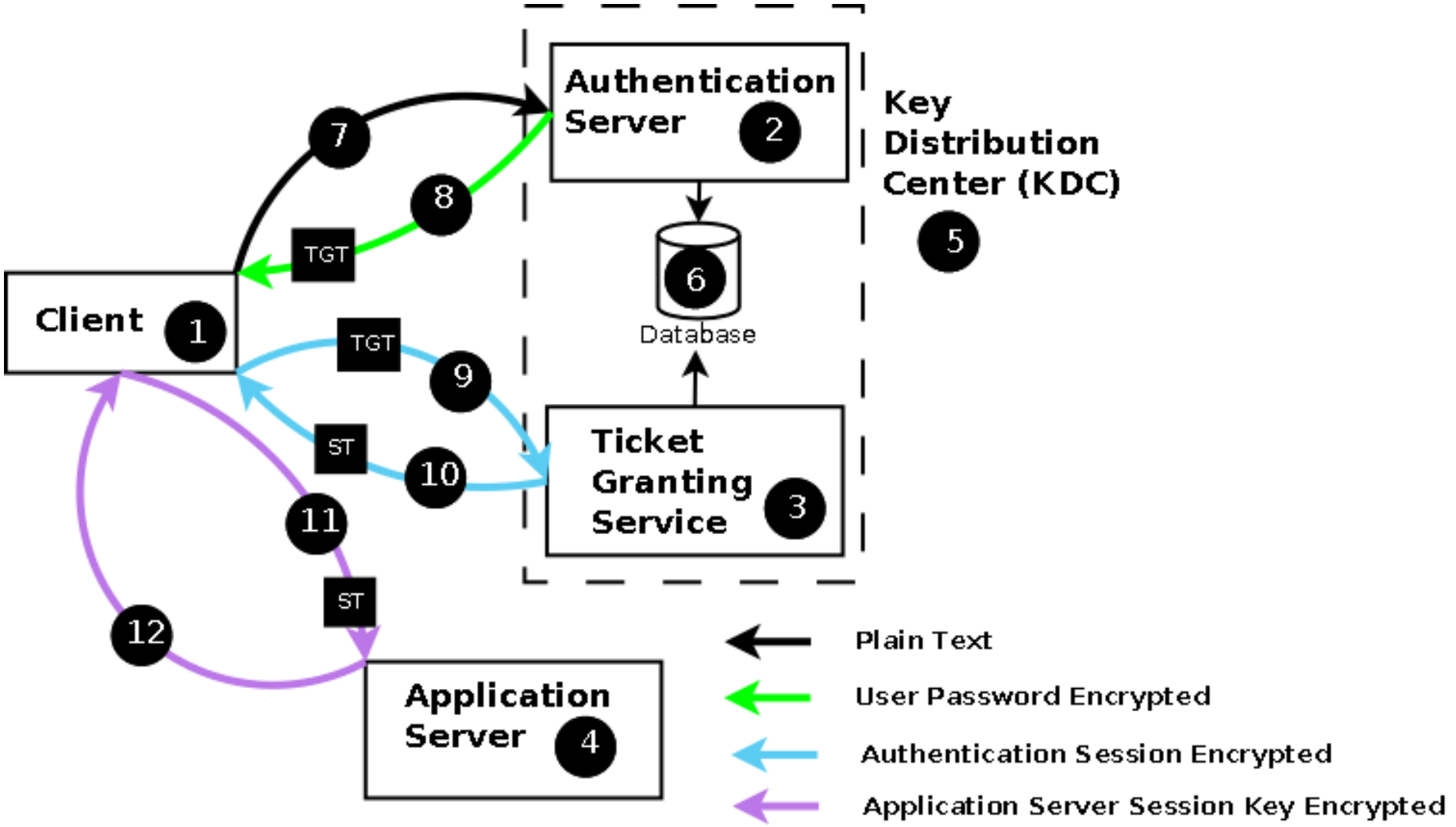
Kerberos

- Protocolo autenticación de red
- Creado por MIT
- Permite autenticación mutua
- Evita eavesdropping y ataques de Replay
- Key simetrica con un tercero de confianza

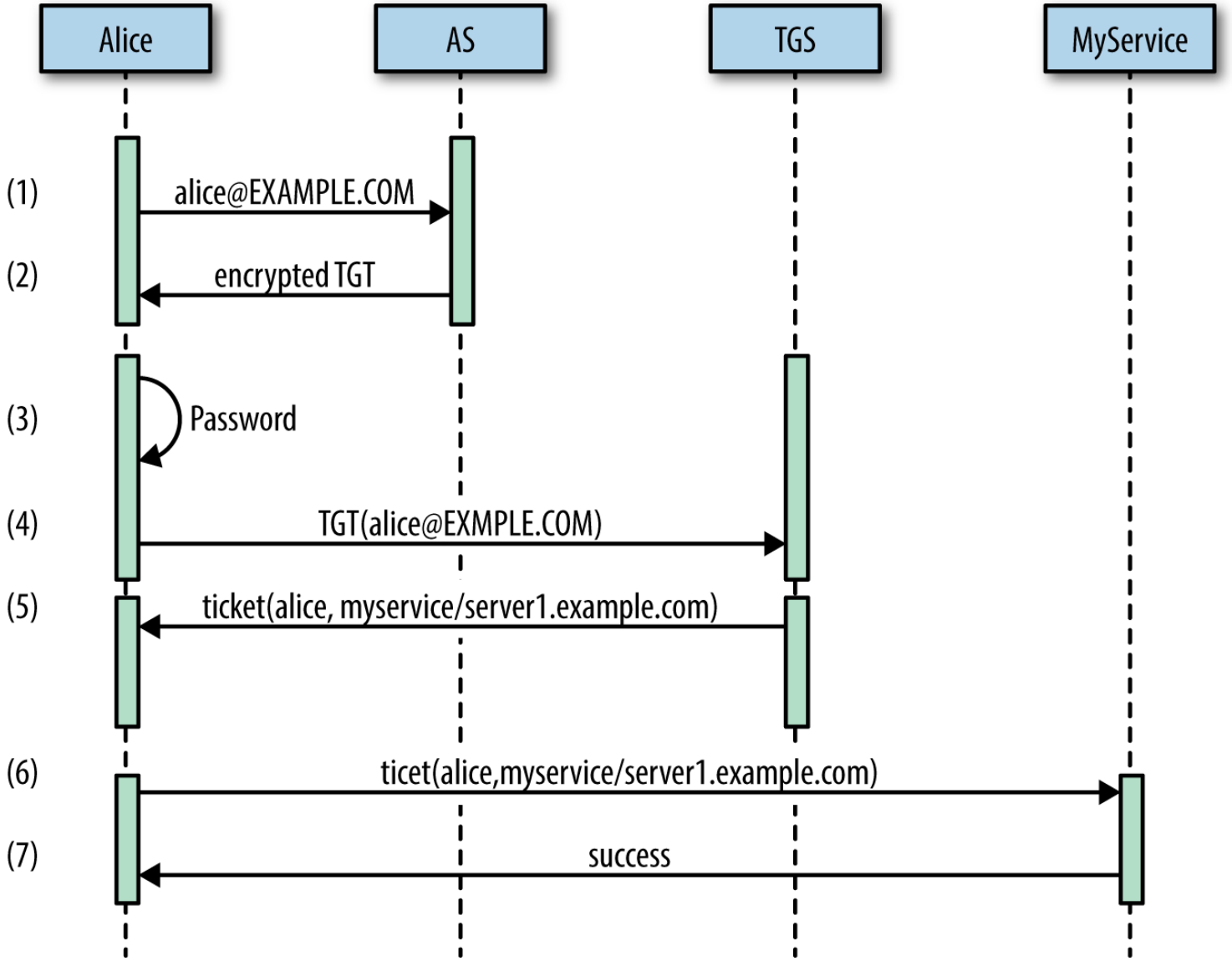
Conceptos

- **Realm**
- **Principal**
  - Usuario: usuario@REALM
  - Maquina: fqdn@REALM
  - Servicio: servicio/fqdn@REALM
- **Ticket**
- **KDC (Key Distribution Center)**
- **Kerberos Server**
- **Keytab**

Flujo


Authentication Server
2
Key Distribution Center (KDC)
5
7
8
TGT
Client
1
6
Database
TGT
9
ST
10
Ticket Granting Service
3
11
ST
12
Application Server
4
Plain Text
User Password Encrypted
Authentication Session Encrypted
Application Server Session Key Encrypted

Flujo


Alice
AS
TGS
MyService
(1)
alice@EXAMPLE.COM
(2)
encrypted TGT
(3)
Password
(4)
TGT(alice@EXMPLE.COM)
(5)
ticket(alice, myservice/server1.example.com)
(6)
ticet(alice,myservice/server1.example.com)
(7)
success

Necesidades

- **NTP**
- **BBDD (como LDAP)**
- **Paquetes servidor kerberos 5**
- **Configurar /etc/krb5.conf y /etc/kdc.conf**

Configuración krb5.conf

<<fichero de configuración>>

Configuración kdc.conf

<<fichero de configuración>>

Comandos de configuración

- **kadmin.local**
- **add_principal <usuario>**
- **ktadd -k [[FQDN]].keytab host/[[FQDN]]**
- **klist**

Comandos de configuración

- **kvno**
- **delprinc -force <principal>**
- **Kdestroy**
- **Ktutil**

Rol de administración

/etc/krb5kdc/kadm5.acl

<<<contenido>>>

SASL/GSSAPI

- **apt install libsasl2-modules-gssapi-mit**
  - Para poder realizar consultas SASL/GSSAPI

¿Preguntas?

Gracias!!

red@nosoloaulas.com