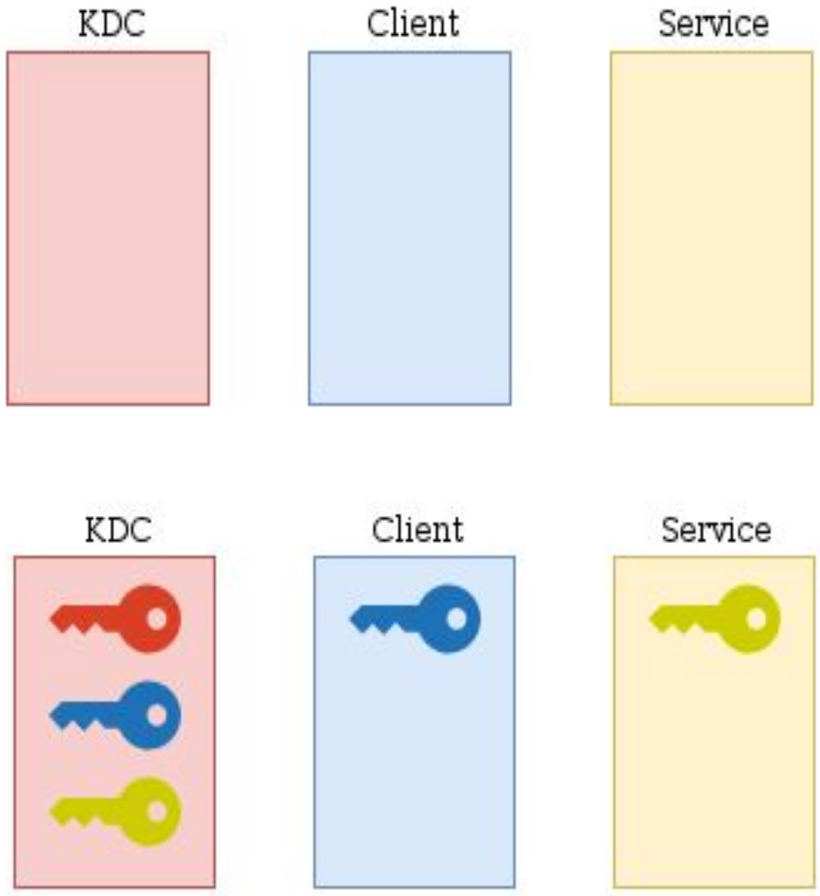
THE BRIDGE

CYBER SECURITY

Movimientos Laterales Kerberos

Windows: Kerberos

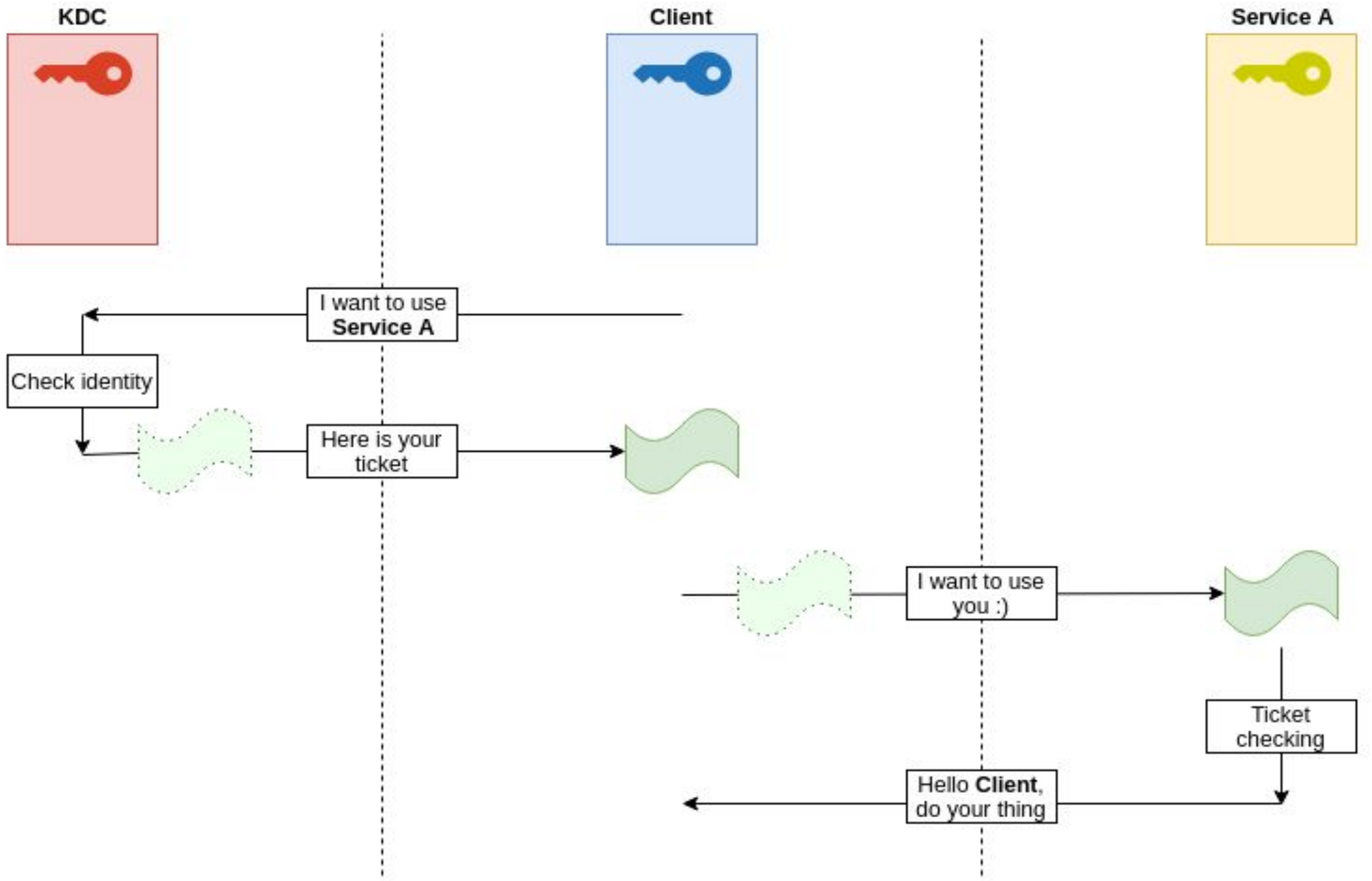


Se necesitan 3 entidades para llevar a cabo la autenticación:

- Un cliente
- Un servicio
- Un KDC (Key Distribution Center) -> El DC en dominio

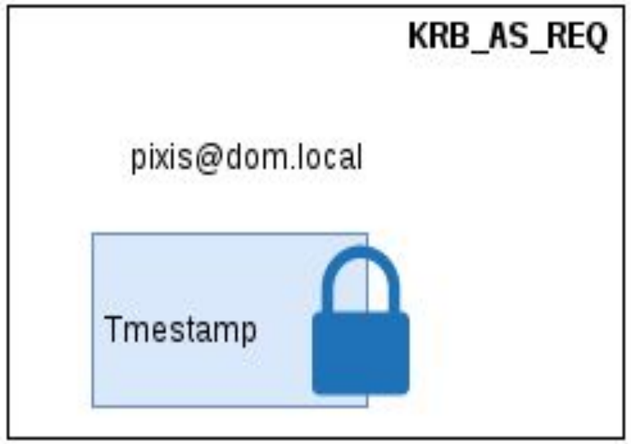
https://en.hackndo.com/kerberos/

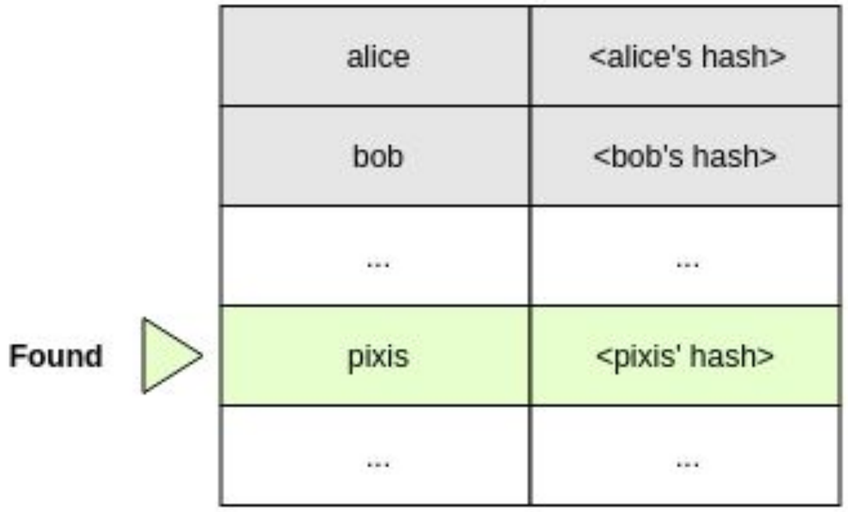
Windows: Kerberos



https://en.hackndo.com/kerberos/

Windows: Kerberos KRB_AS_REQ (User)

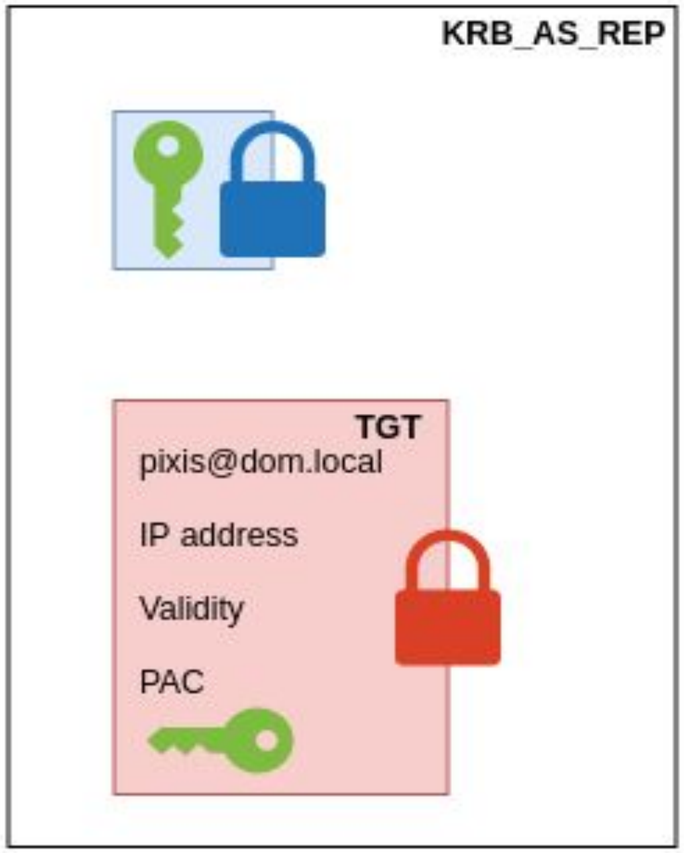




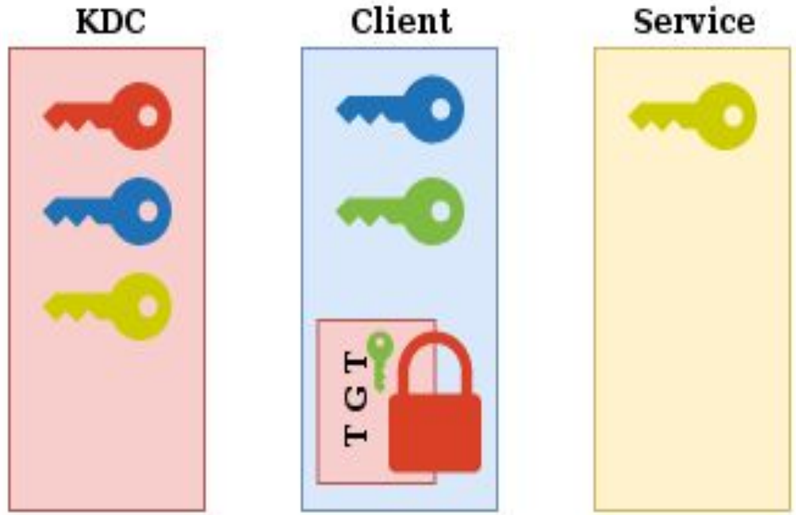
Session Key

https://en.hackndo.com/kerberos/

Windows: Kerberos KRB_AS_REP (Server)



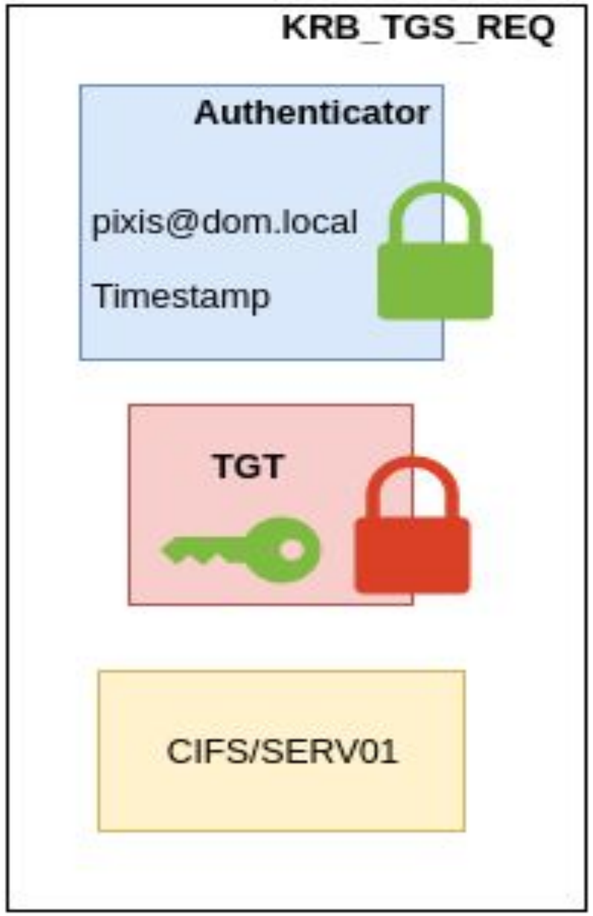
PAC (Privilege Attribute Certificate):
Información específica del usuario SID y grupos a los que pertenece.

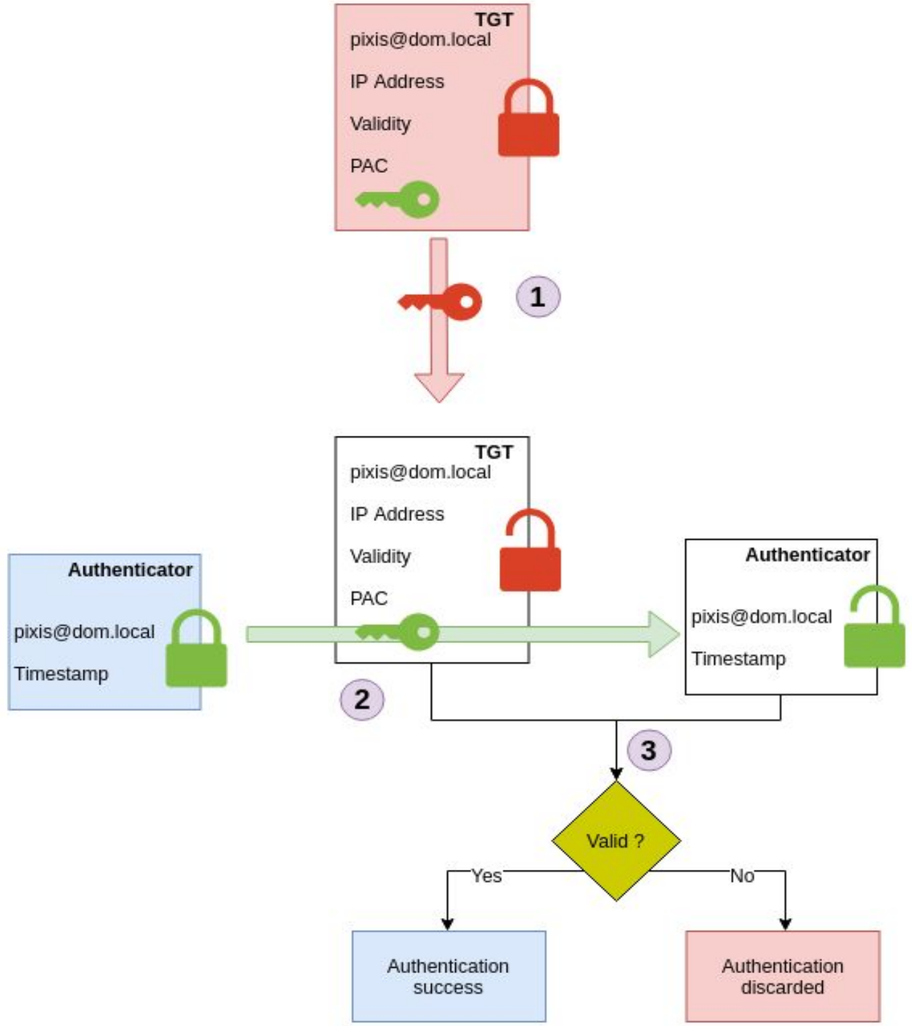


Krbtgt user

https://en.hackndo.com/kerberos/

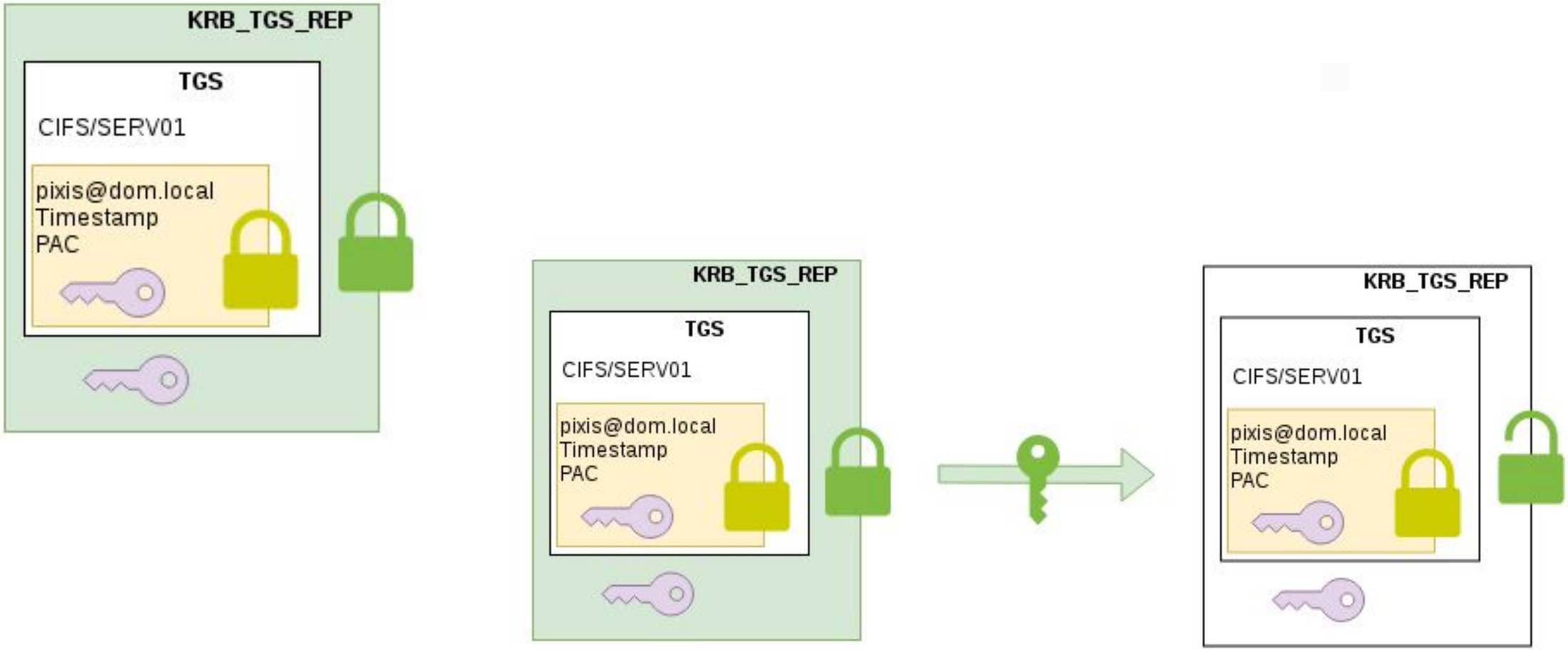
Windows: Kerberos KRB_TGS_REQ(Server)





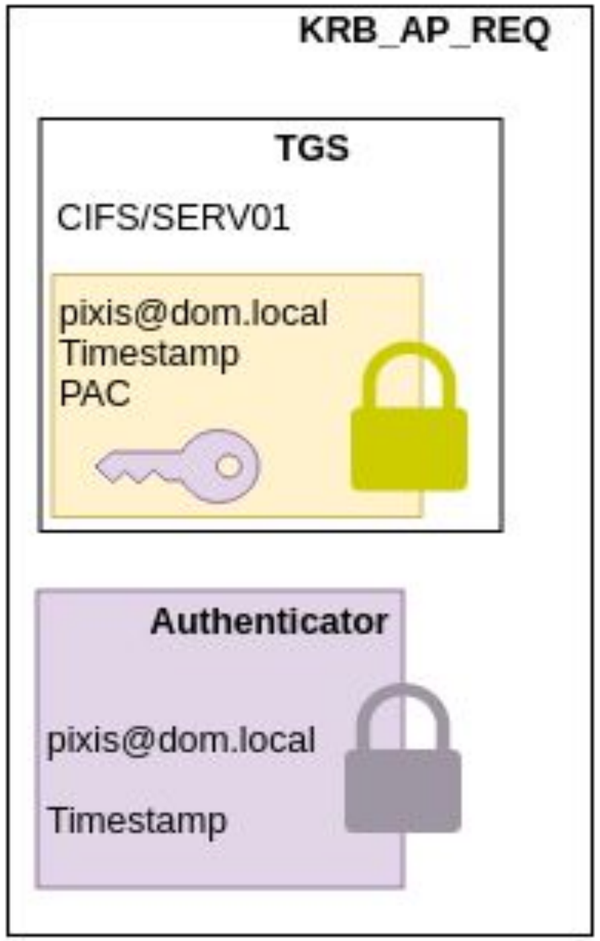
https://en.hackndo.com/kerberos/

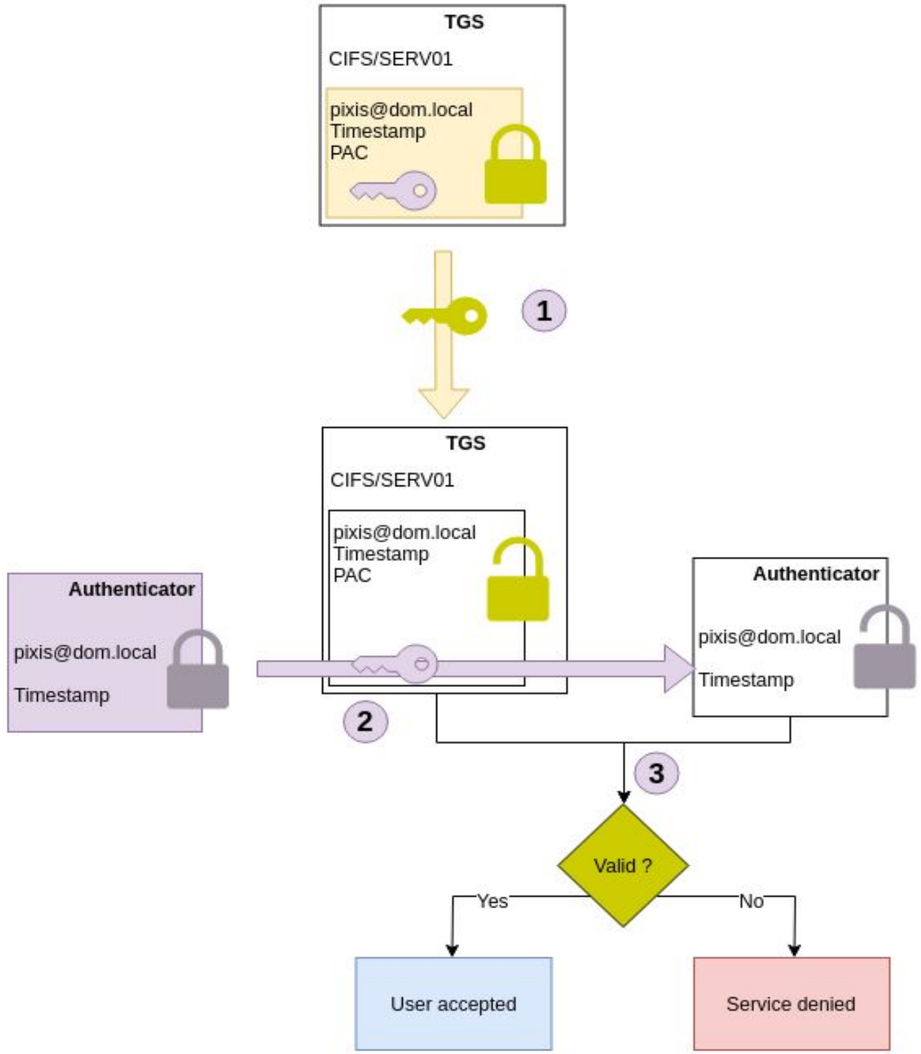
Windows: Kerberos KRB_TGS_REP(Server)



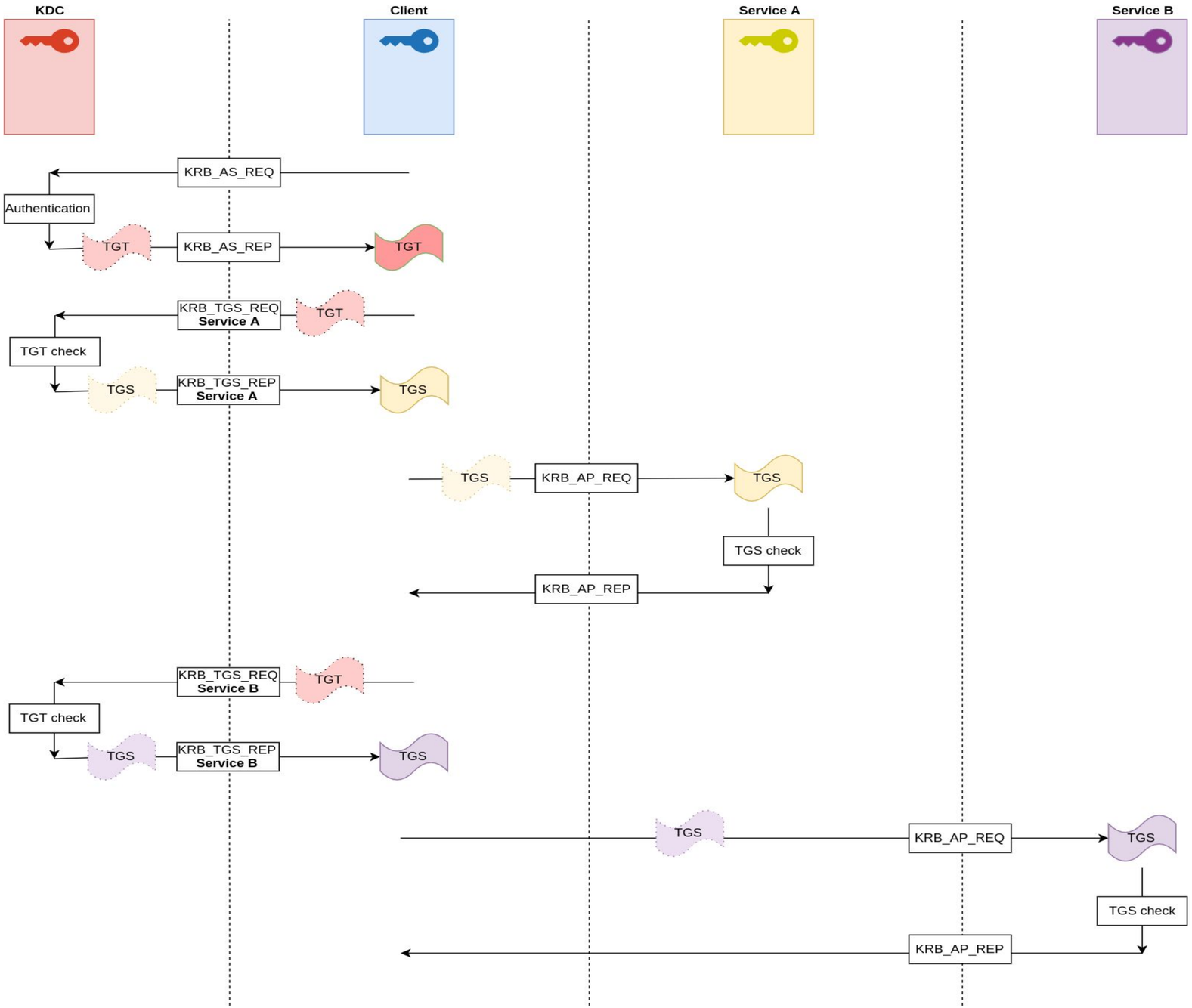
https://en.hackndo.com/kerberos/

Windows: Kerberos KRB_TGS_REP(Server)

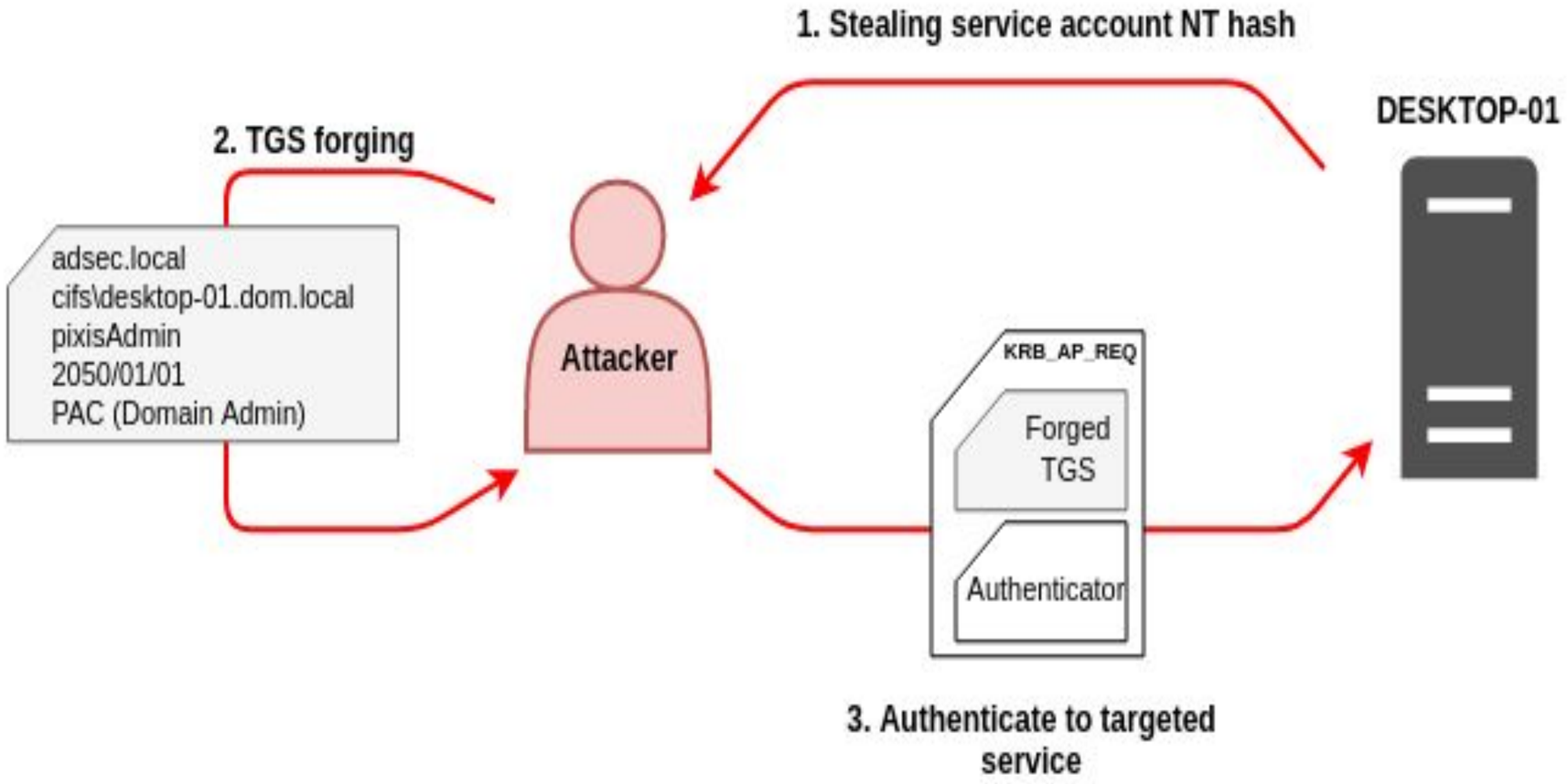




https://en.hackndo.com/kerberos/

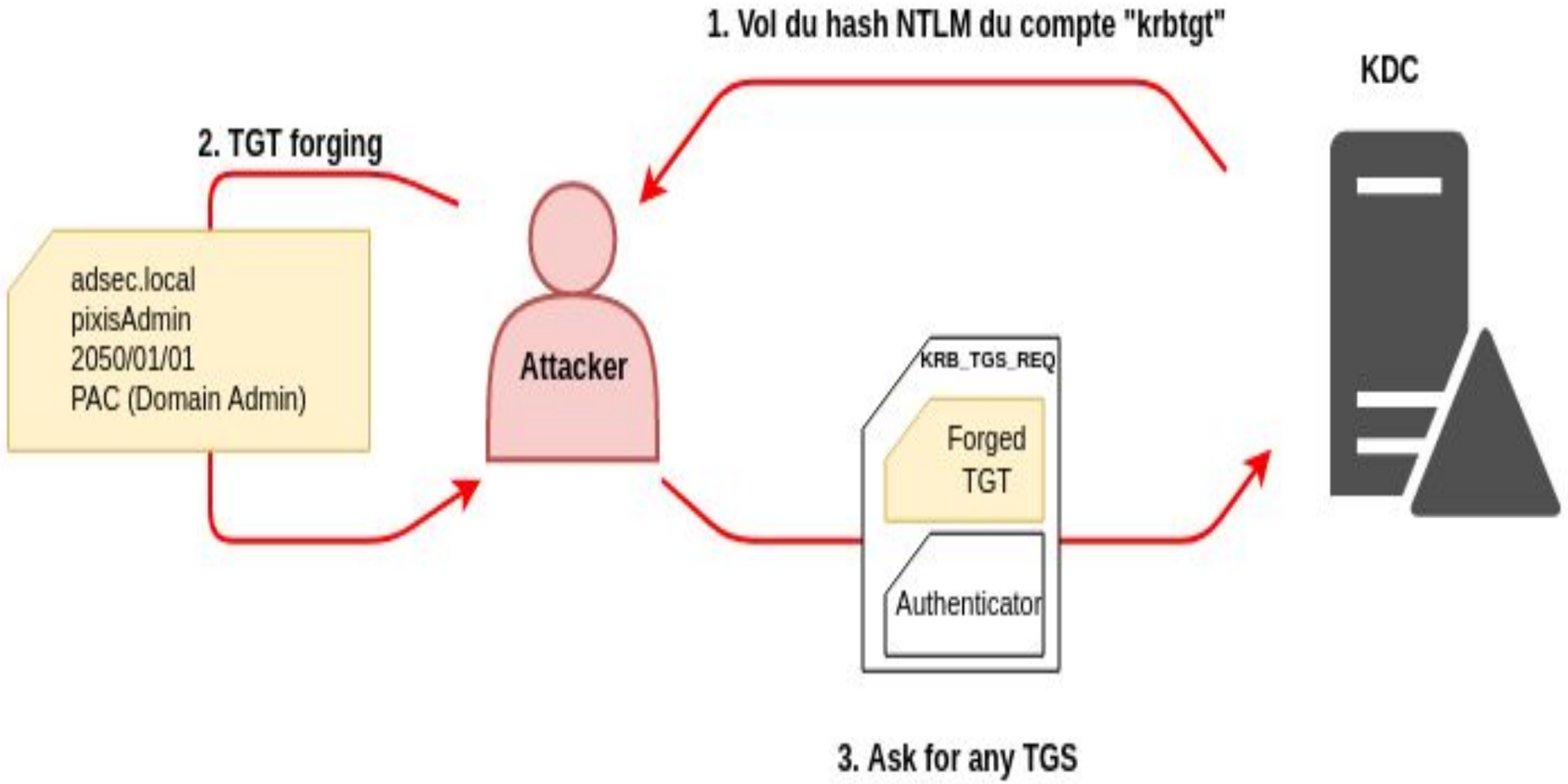

KDC
Client
Service A
Service B
KRB_AS_REQ
Authentication
TGT
KRB_AS_REP
TGT
KRB_TGS_REQ
Service A
TGT
TGT check
TGS
KRB_TGS_REP
Service A
TGS
TGS
KRB_AP_REQ
TGS
TGS check
KRB_AP_REP
KRB_TGS_REQ
Service B
TGT
TGT check
TGS
KRB_TGS_REP
Service B
TGS
TGS
KRB_AP_REQ
TGS
TGS check
KRB_AP_REP

Windows: Silver Ticket



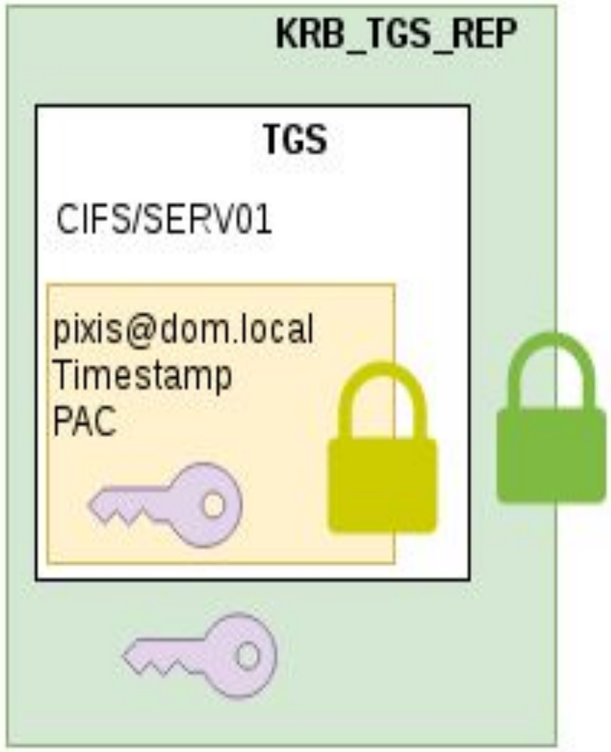
https://en.hackndo.com/kerberos/

Windows: Golden Ticket



https://en.hackndo.com/kerberos/

Windows: Kerberoasting



- Podemos solicitar TGS’s para autenticarnos en los servicios.
- El TGS está cifrado con el secreto (hash) del servicio.
- Posibles ataques de fuerza bruta (diccionario).

https://en.hackndo.com/kerberos/


THE
BRIDGE