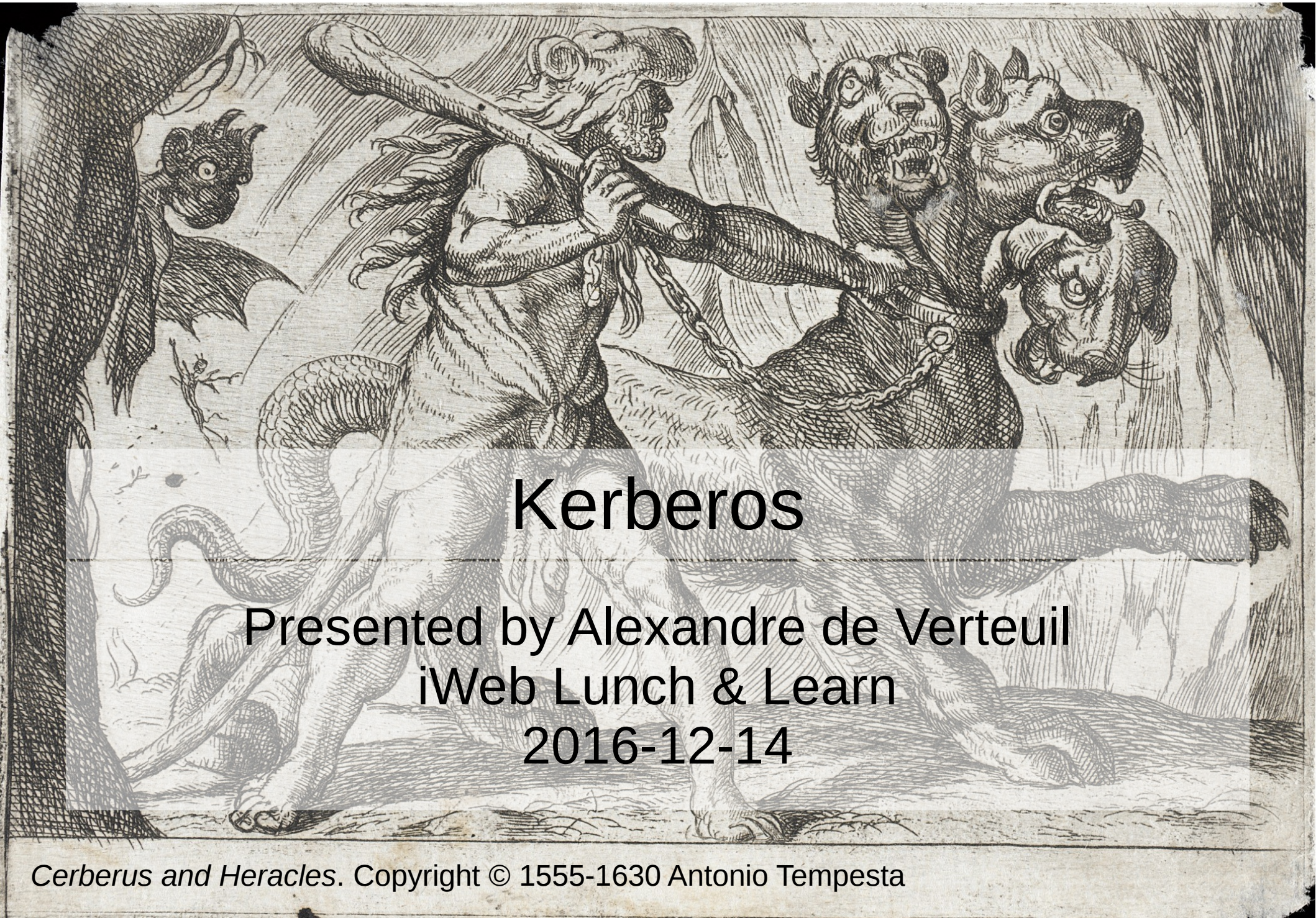


Kerberos

Presented by Alexandre de Verteuil
iWeb Lunch & Learn
2016-12-14

Cerberus and Heracles. Copyright © 1555-1630 Antonio Tempesta

Copying

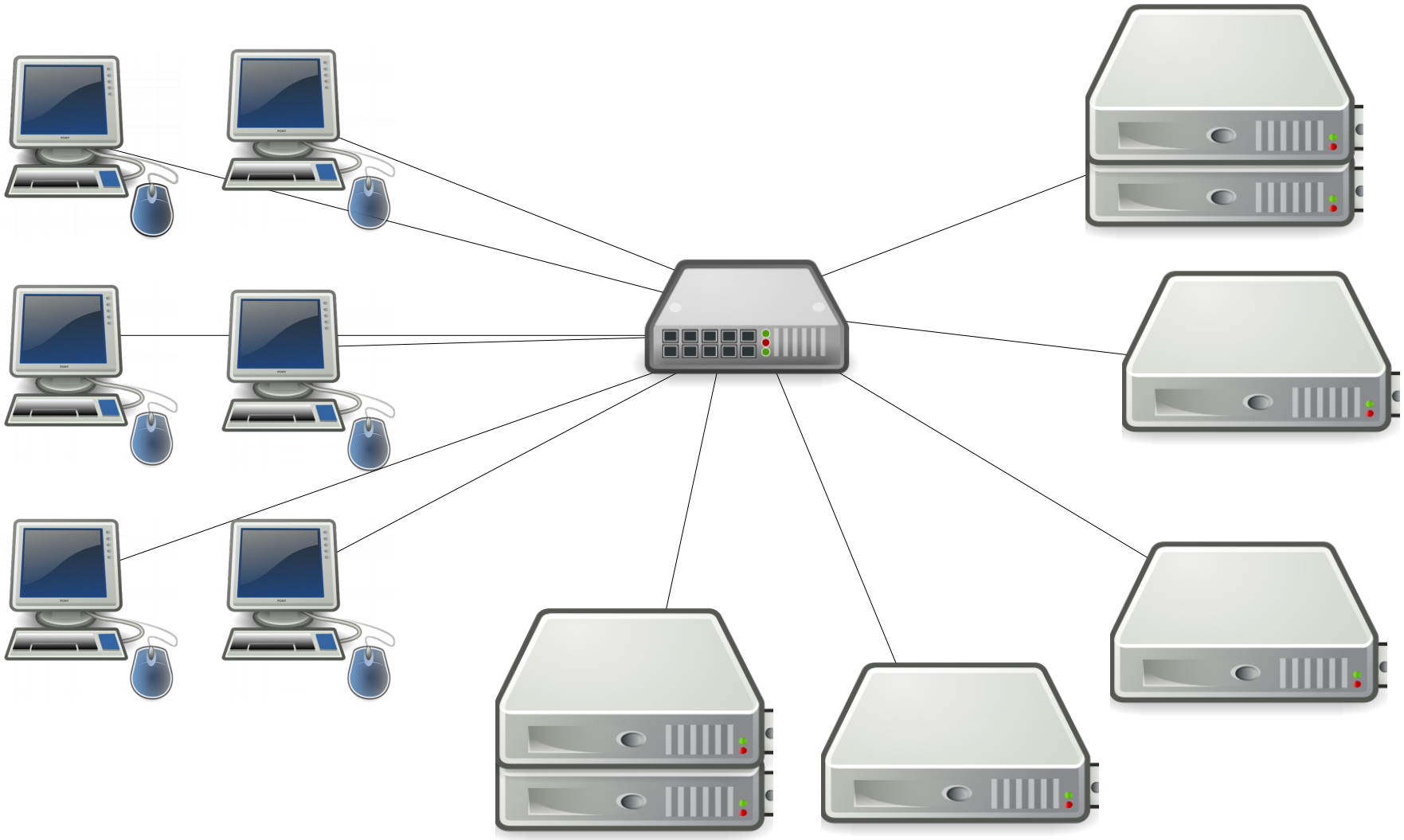
Creative Commons License

References

- **Designing an Authentication System: a Dialogue in Four Scenes**
  https://web.mit.edu/kerberos/dialogue.html
- RFC 4120 - The Kerberos Network Authentication Service (V5)
  https://tools.ietf.org/html/rfc4120
- MIT 6.858: Computer Systems Security,
  Fall 2014 Lecture 13: Kerberos
  https://www.youtube.com/watch?v=bcWxLl8x33c
- Kerberos FAQ, v2.0
  http://www.faqs.org/faqs/kerberos-faq/general/

Mainframe and terminals

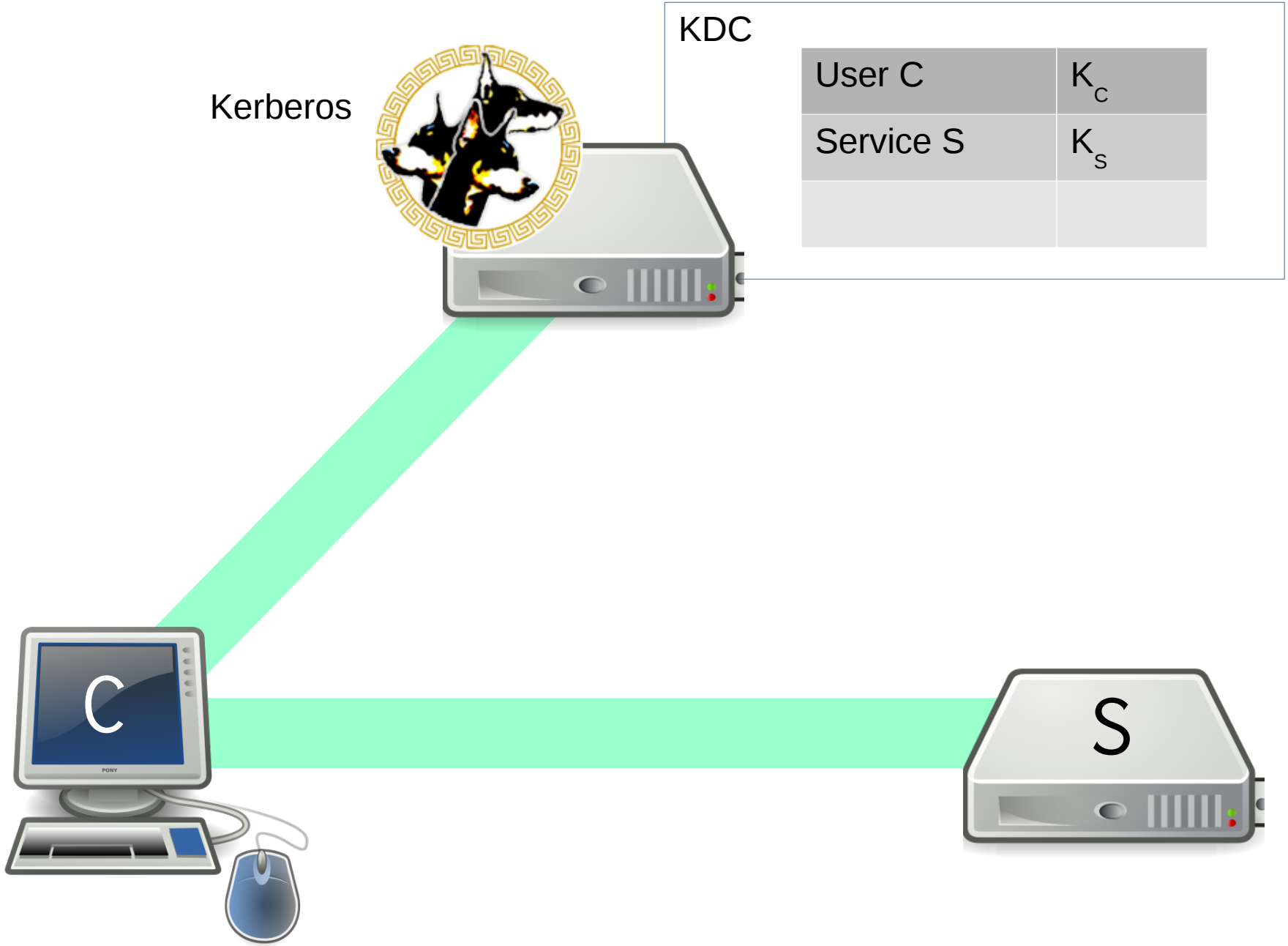
Servers and client workstations



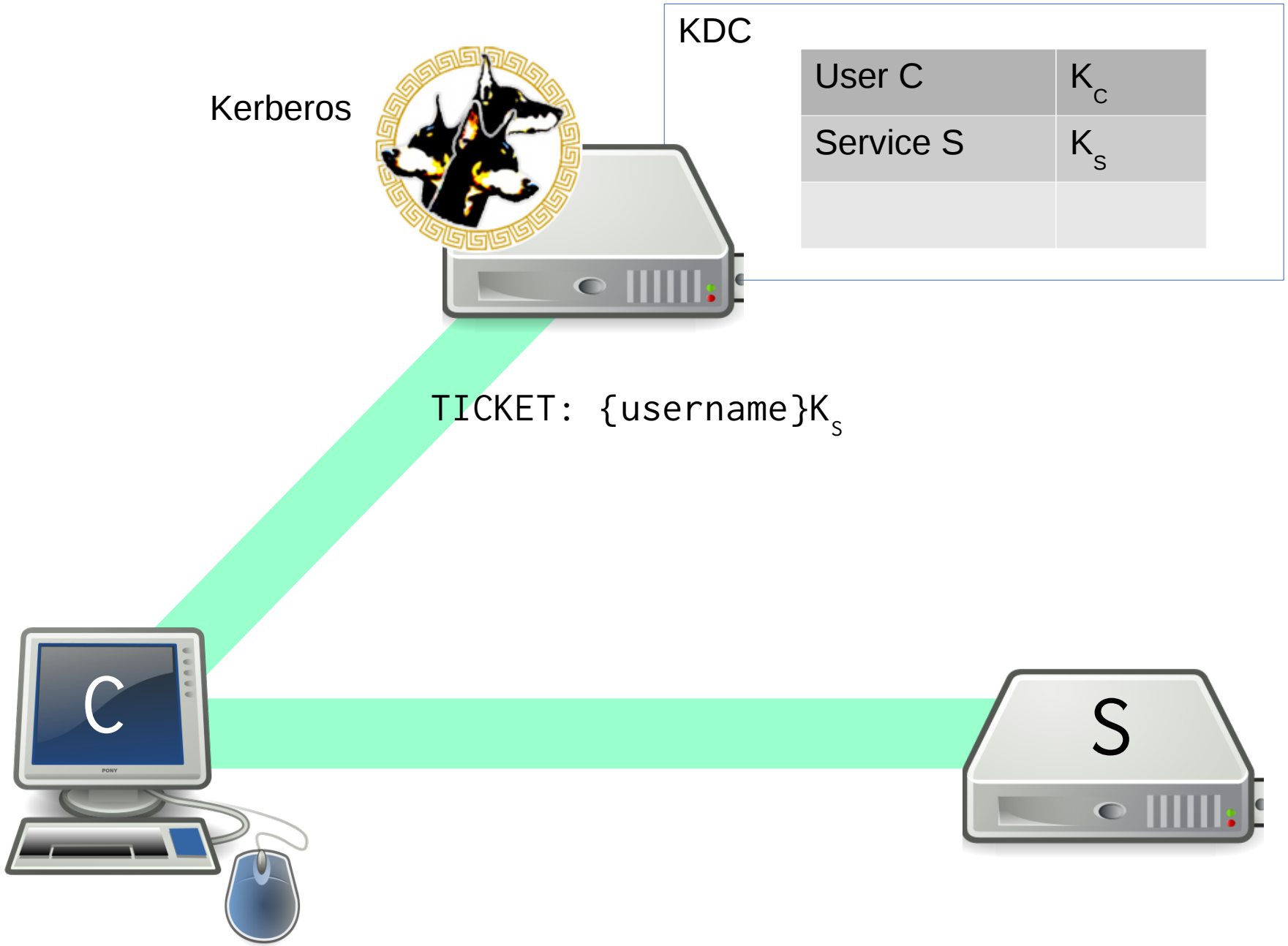
Design requirements, part 1

- The physical security of all hosts is not assumed
- Packets travelling along the network can be read, modified and inserted at will
- Machines that provide services must be able to confirm the identities of people who request services

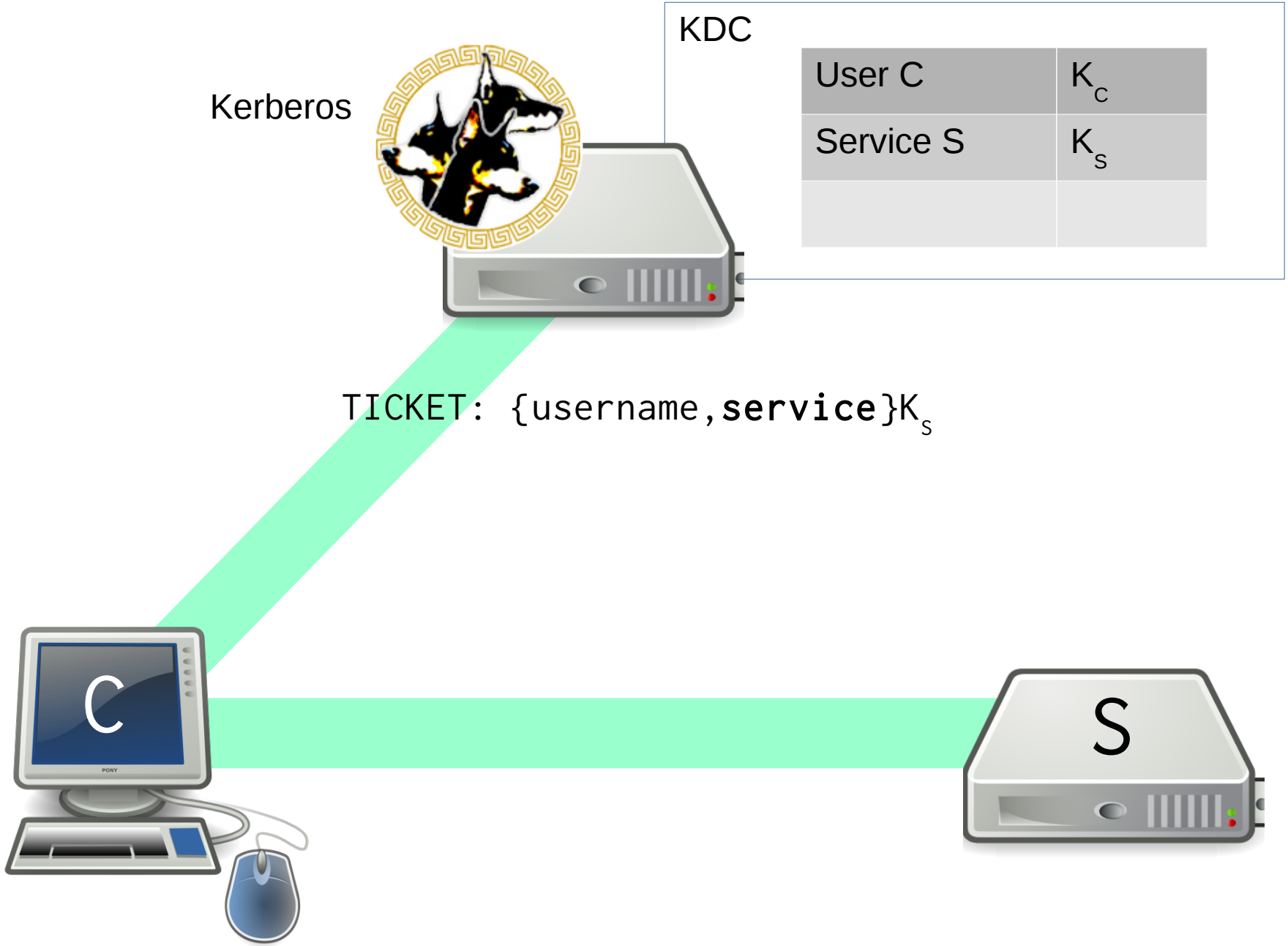
Authentication Service



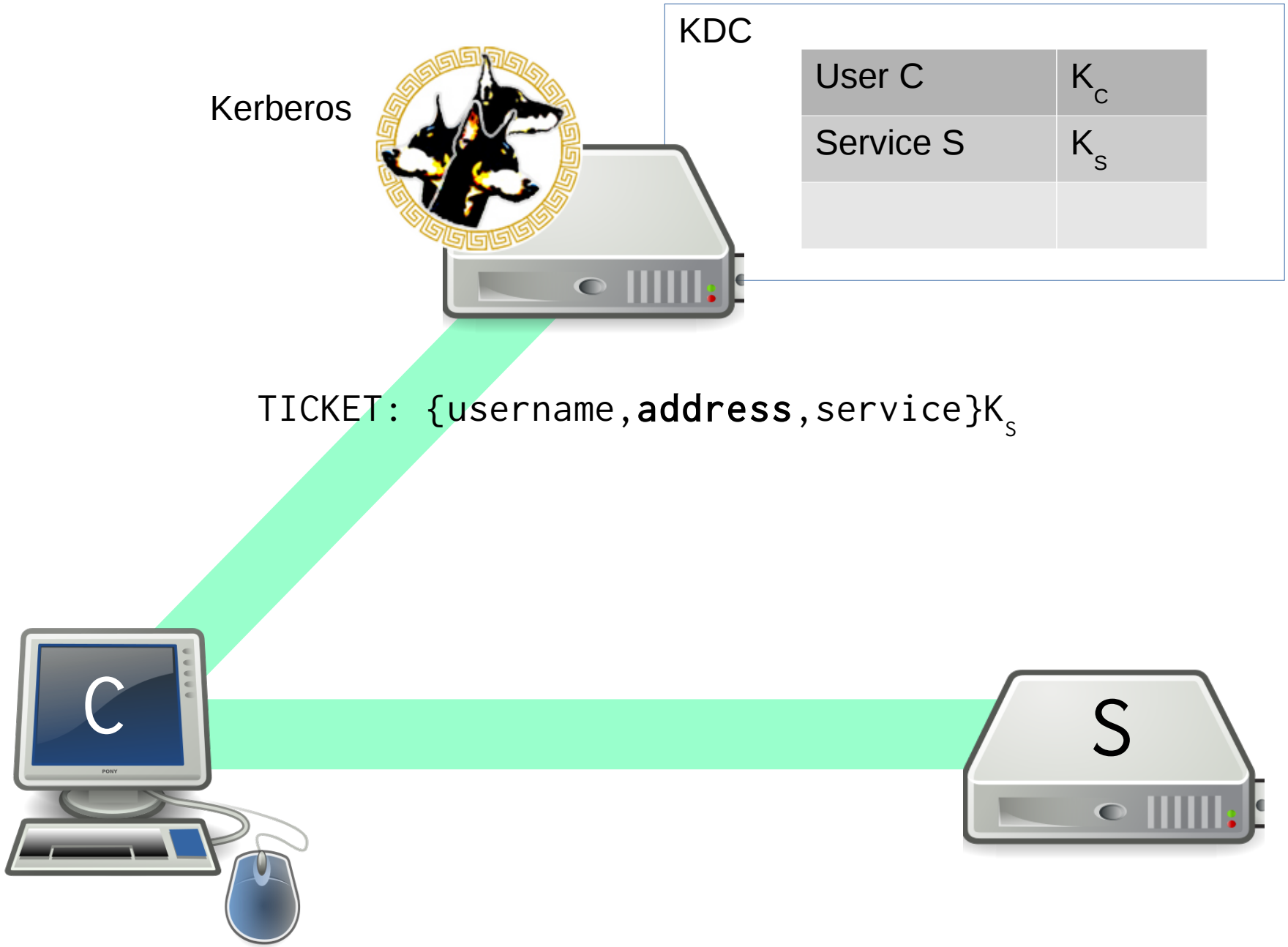
Service Ticket



Service Ticket



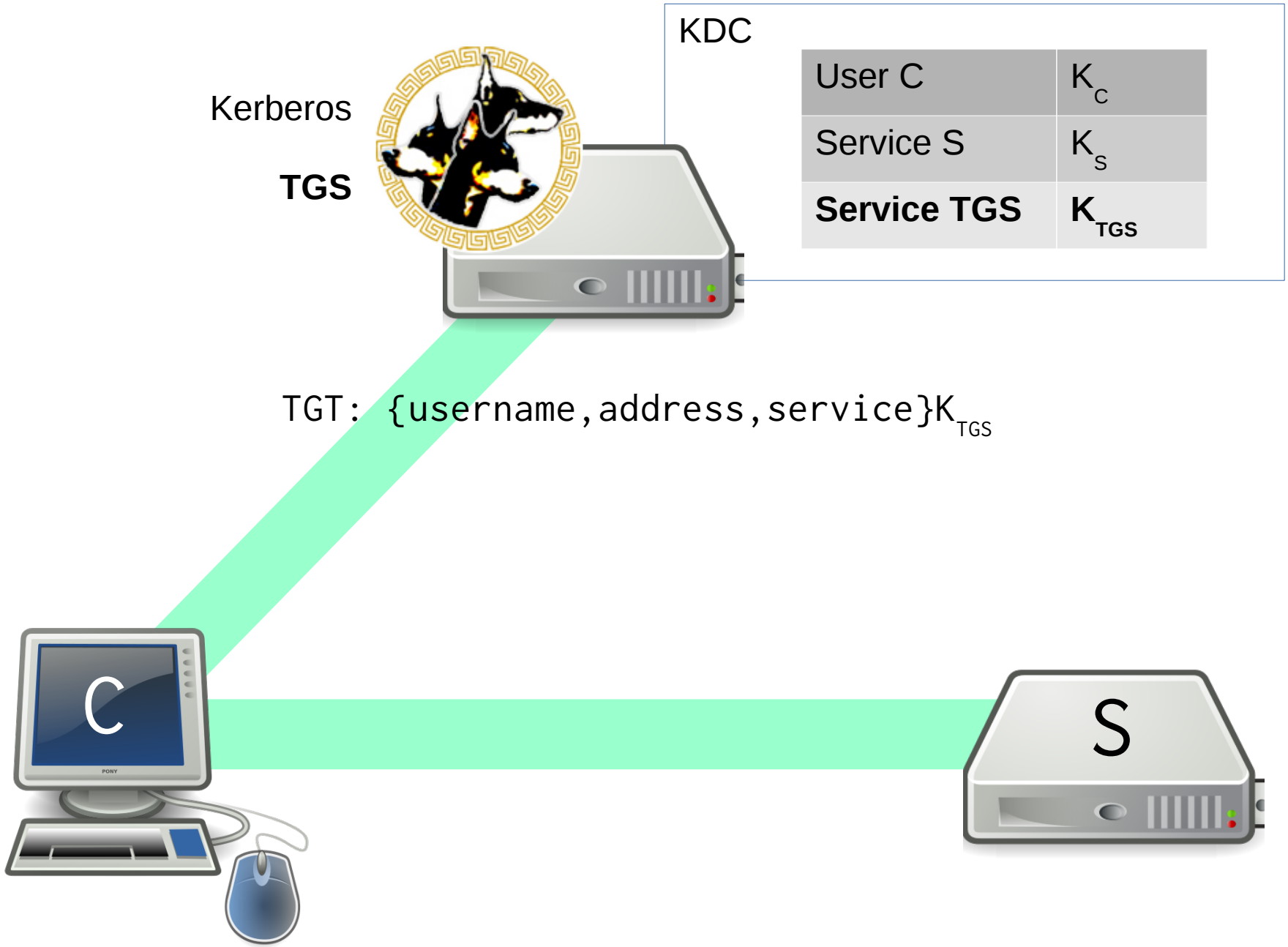
Service Ticket



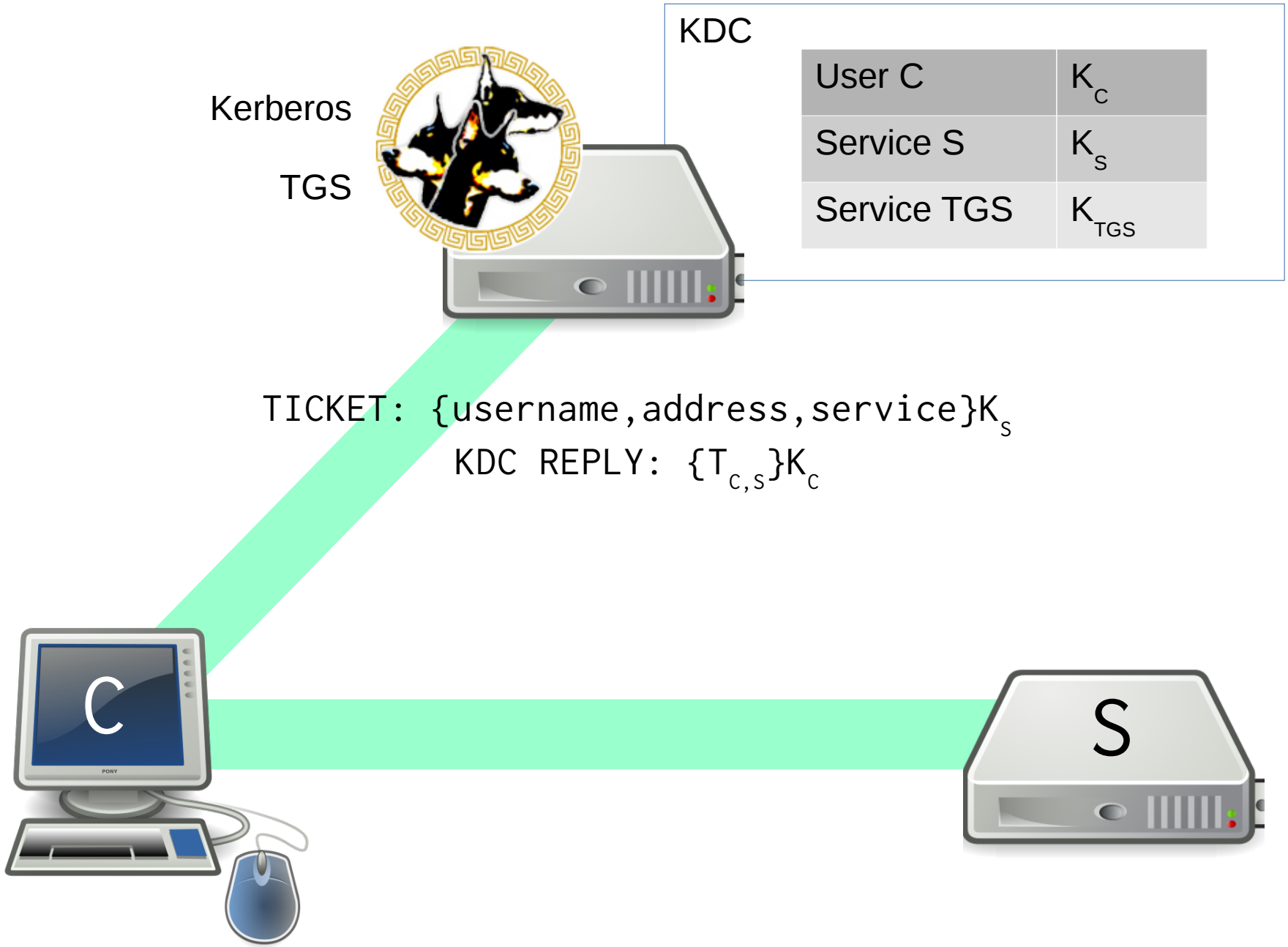
Design requirements, part 2

- Users only have to enter their password once, at the beginning of the session
- Password should not be sent in cleartext

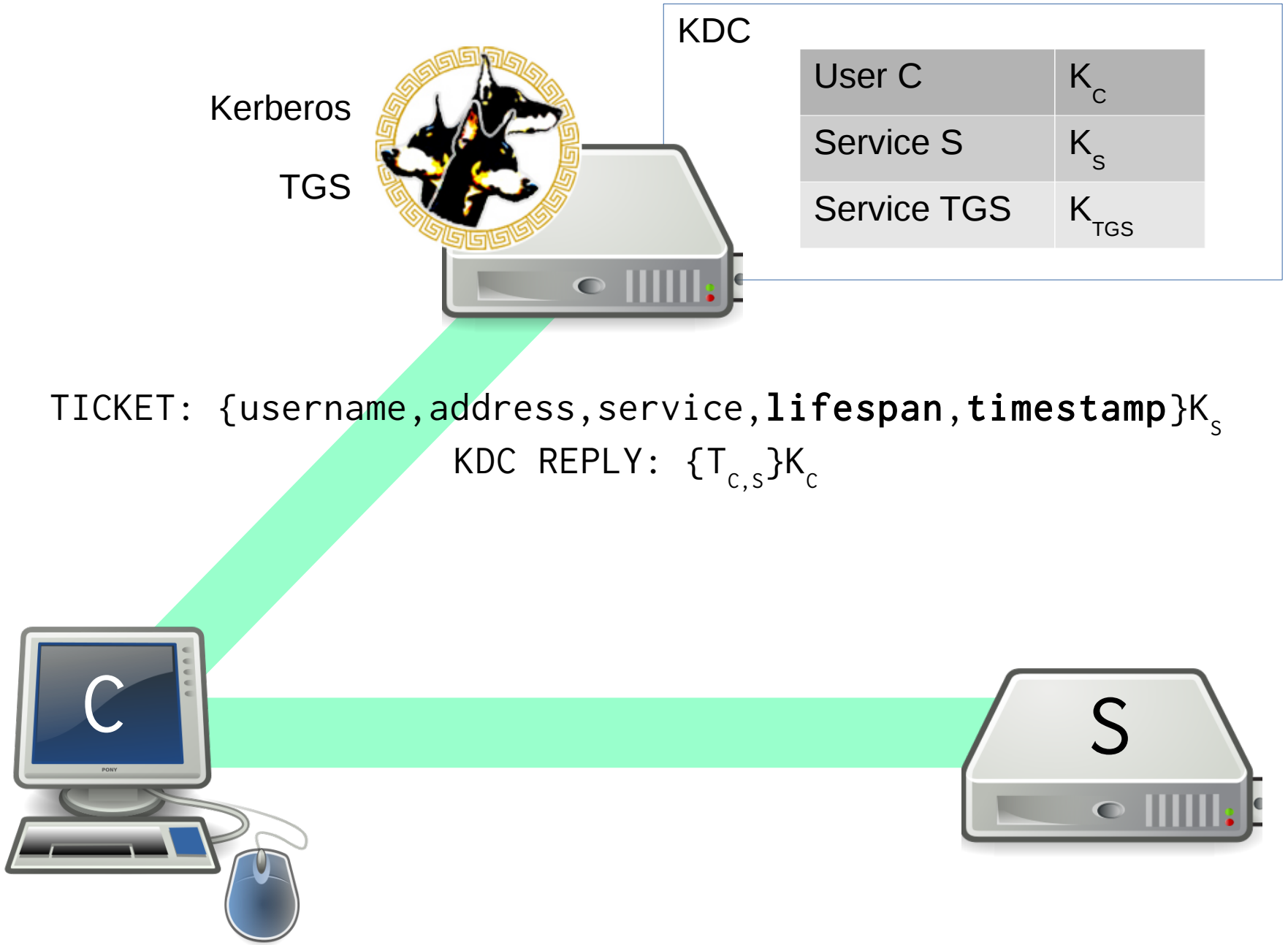
Ticket Granting Service



KDC Reply


KDC
Kerberos
TGS
User C
K_C
Service S
K_S
Service TGS
K_{TGS}
TICKET: {username,address,service}K_S
KDC REPLY: {$T_{C,S}$}K_C
C
S

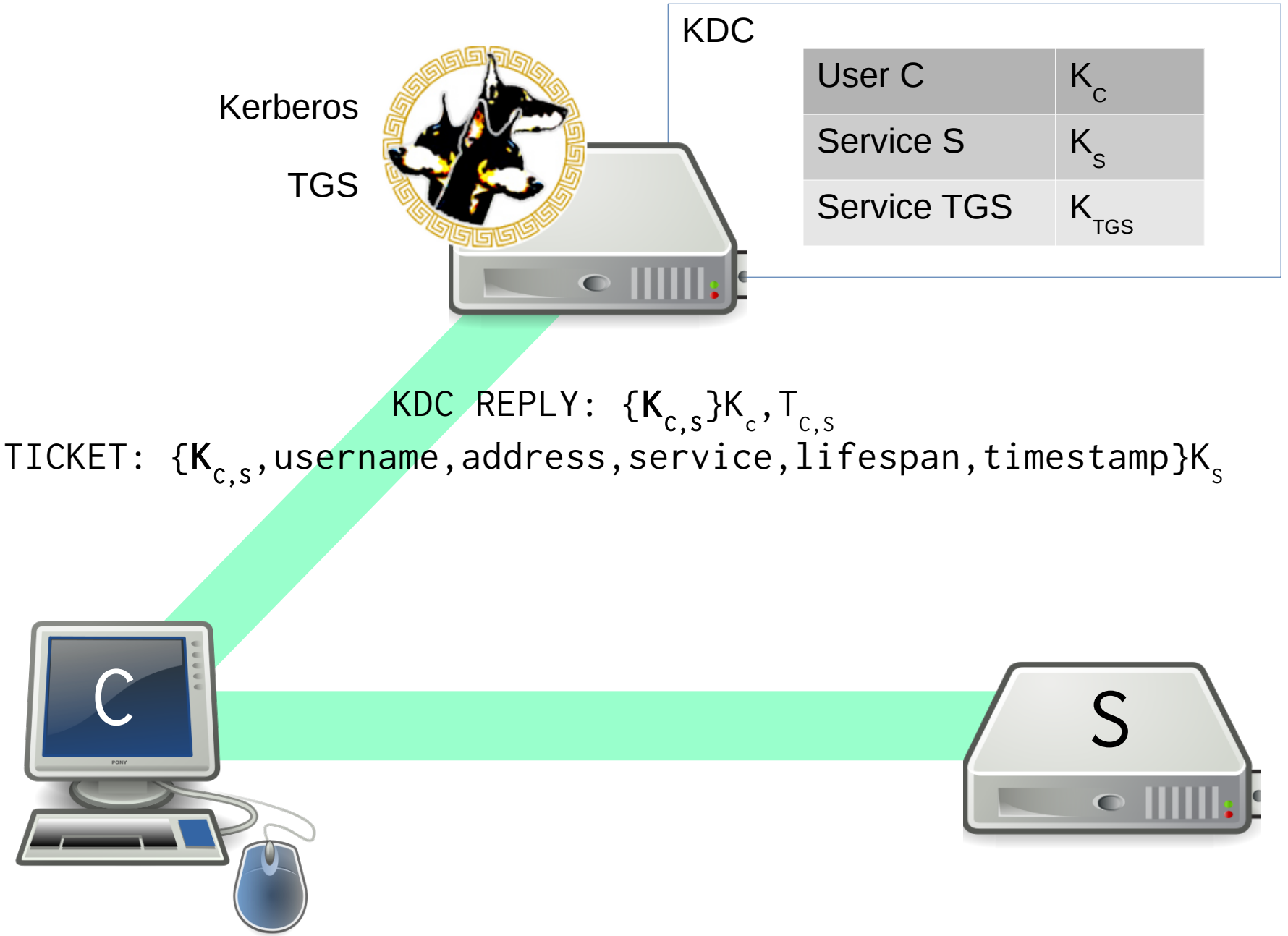
Ticket Lifetime



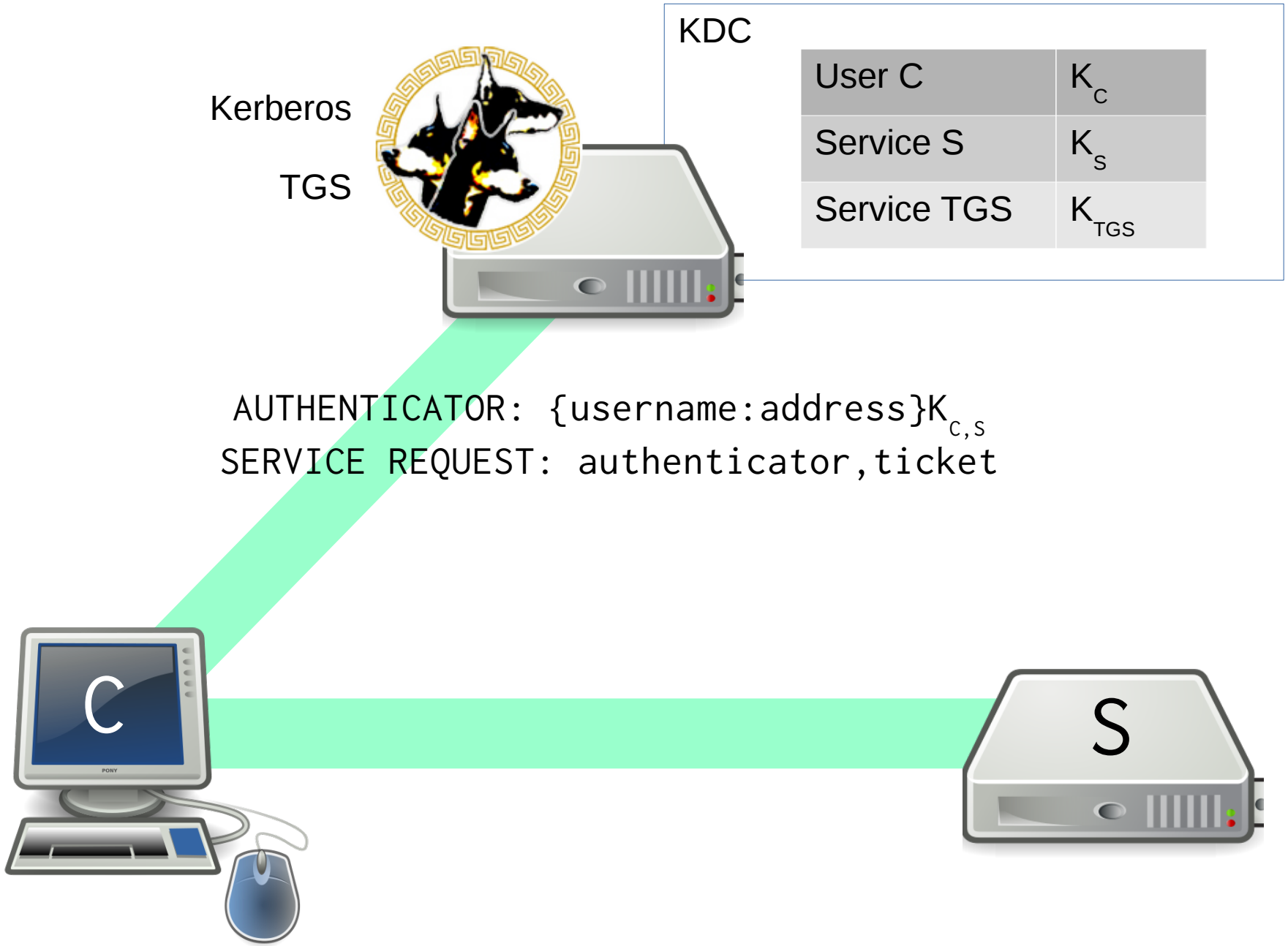
Design requirements, part 3

- A network service must be able to prove that the person using a ticket is the same person to whom that ticket was issued

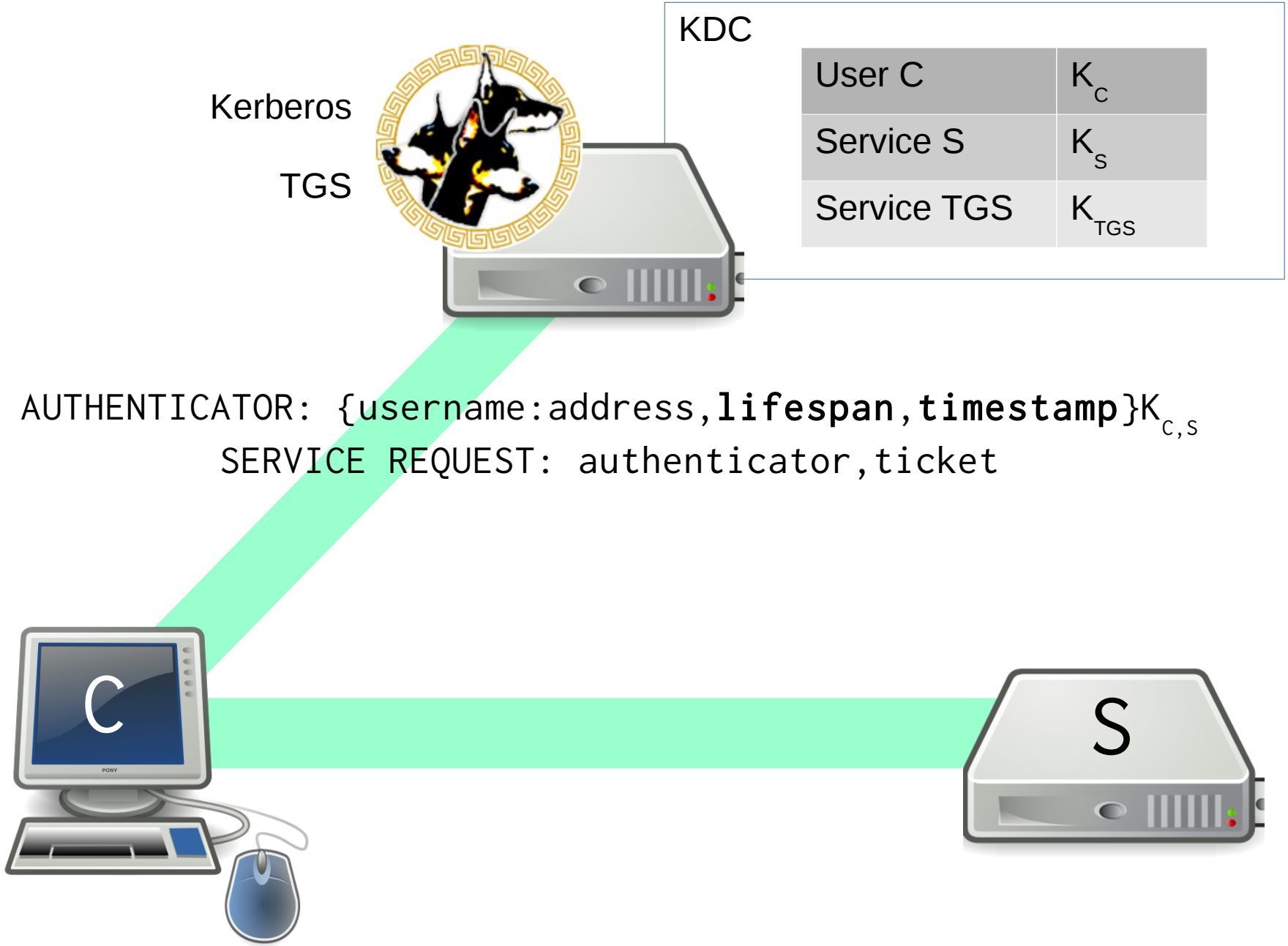
Session Key


KDC
User C
K_C
Service S
K_S
Service TGS
K_{TGS}
Kerberos
TGS
KDC REPLY: $\{K_{c,s}\}K_c, T_{C,S}$
TICKET: $\{K_{c,s}, username, address, service, lifespan, timestamp\}K_S$
C
S

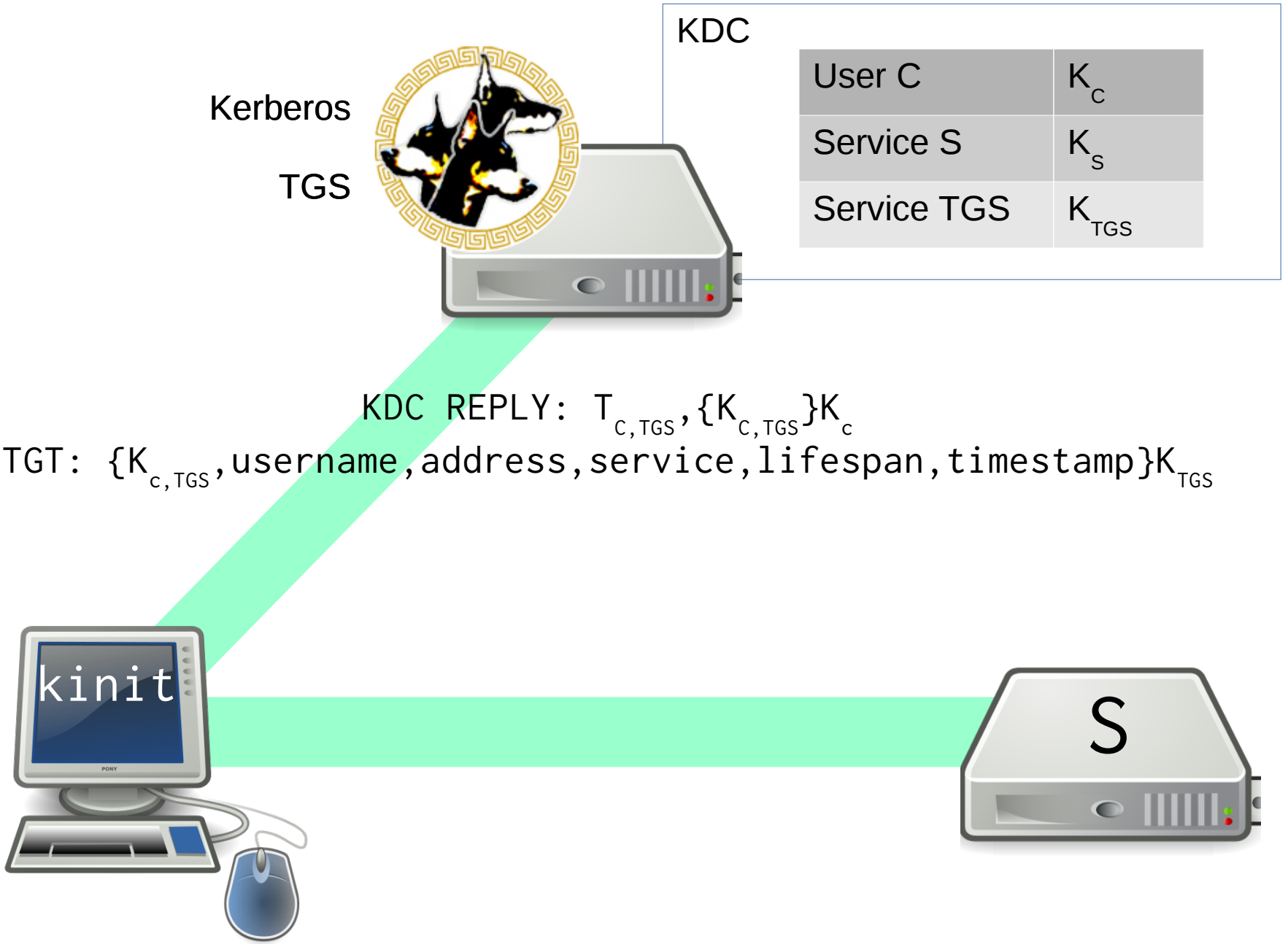
Authenticator



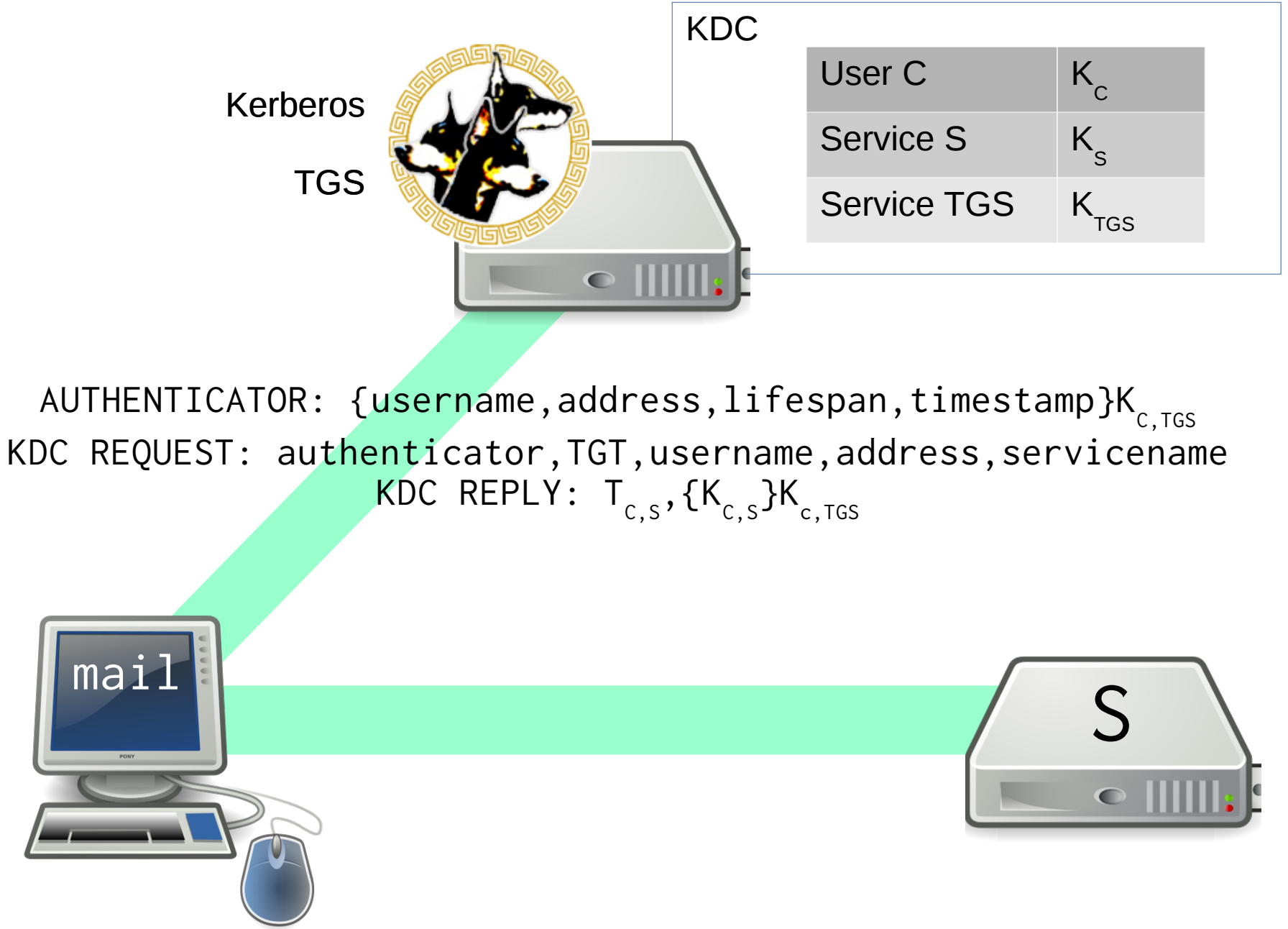
Authenticator, non-reusable



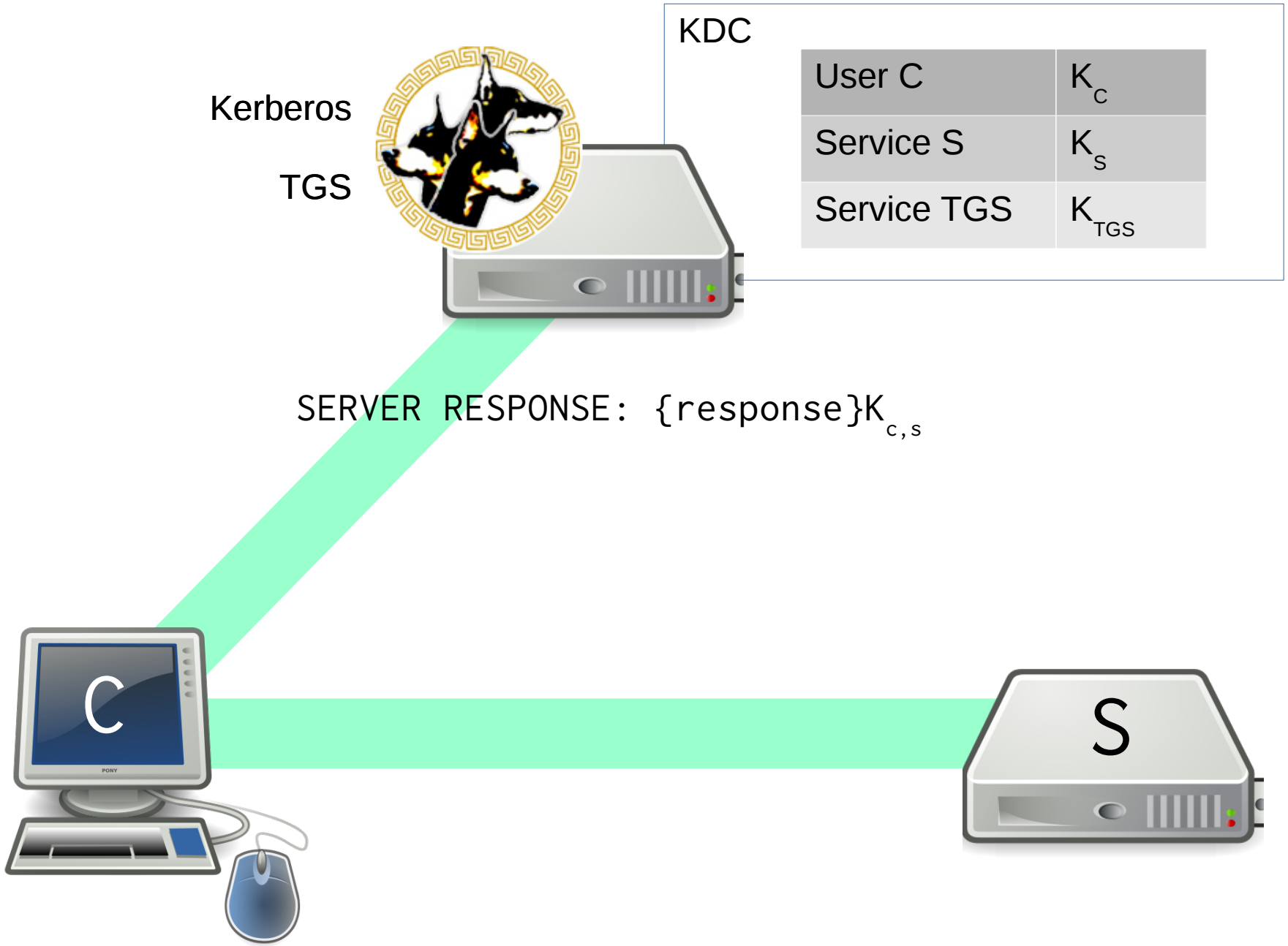
Initial login



Mail program



Mutual authentication



It’s just an introduction!

- Cross-realm trust, transitivity
- Changes in Kerberos 5
- sssd, FreeIPA, Samba 4, GSSAPI
- Credentials caching
- Kerberos browser integration