

migrate:

start: pwd  
end: sso, PQ



client



IdP  
@  
client realm

user @ domain

DNSSEC, DANE, TLS

~ Domain Registrar

⇒ easy

any  
protocol

BYOID

⇒  
Realm Crossover

it's  
me



foreign  
server

really?

Diameter?

# Bring Your Own Identity

<u>Mech</u>	<u>Start/pw?</u>	<u>End/ssu/PQ?</u>	<u>Integr. Proto</u>	<u>Xover</u>
SAML	Heavy	Possible ✓	✓ HTTP + SASL + ...	PKI
Kerberos	Infra	✓	✓ GSSAPI	KXOVER
SASL	✓ ← free choice → ✓		✓	SXOVER

→ SASL wins

↳ except on HTTP

Mechs for Realm Crossover

# HTTP - SASL



C2s = token

[S2s = serverstate]

realm  
mech



S2c = token

S2s = serverstate

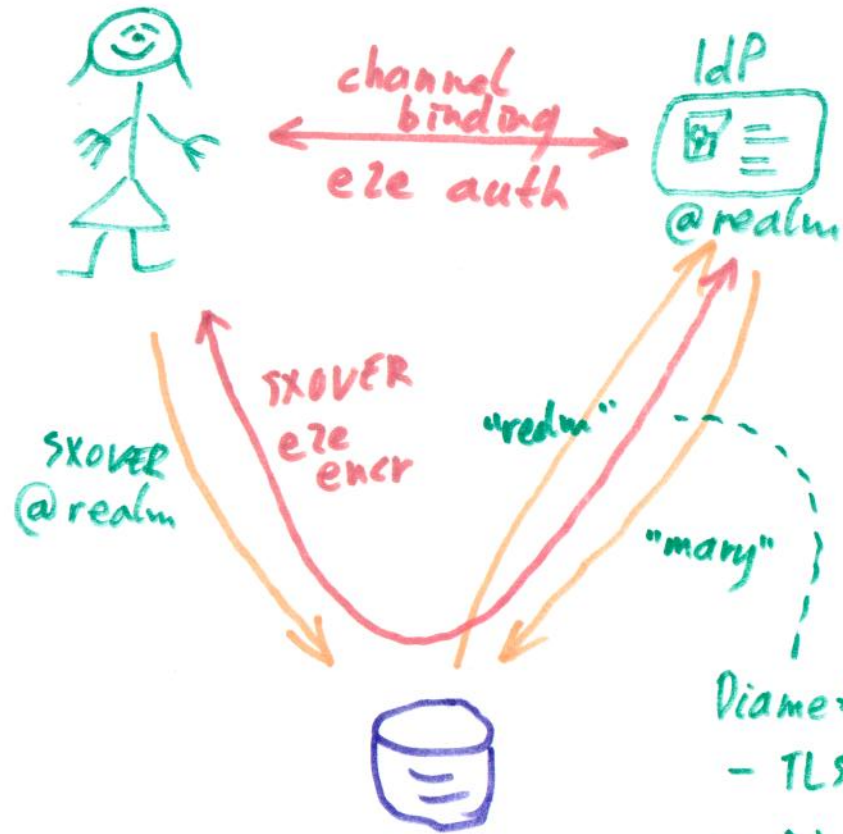
realm  
mechlist

200!



S2s = serverstate  
↳ cached from  
200 OK

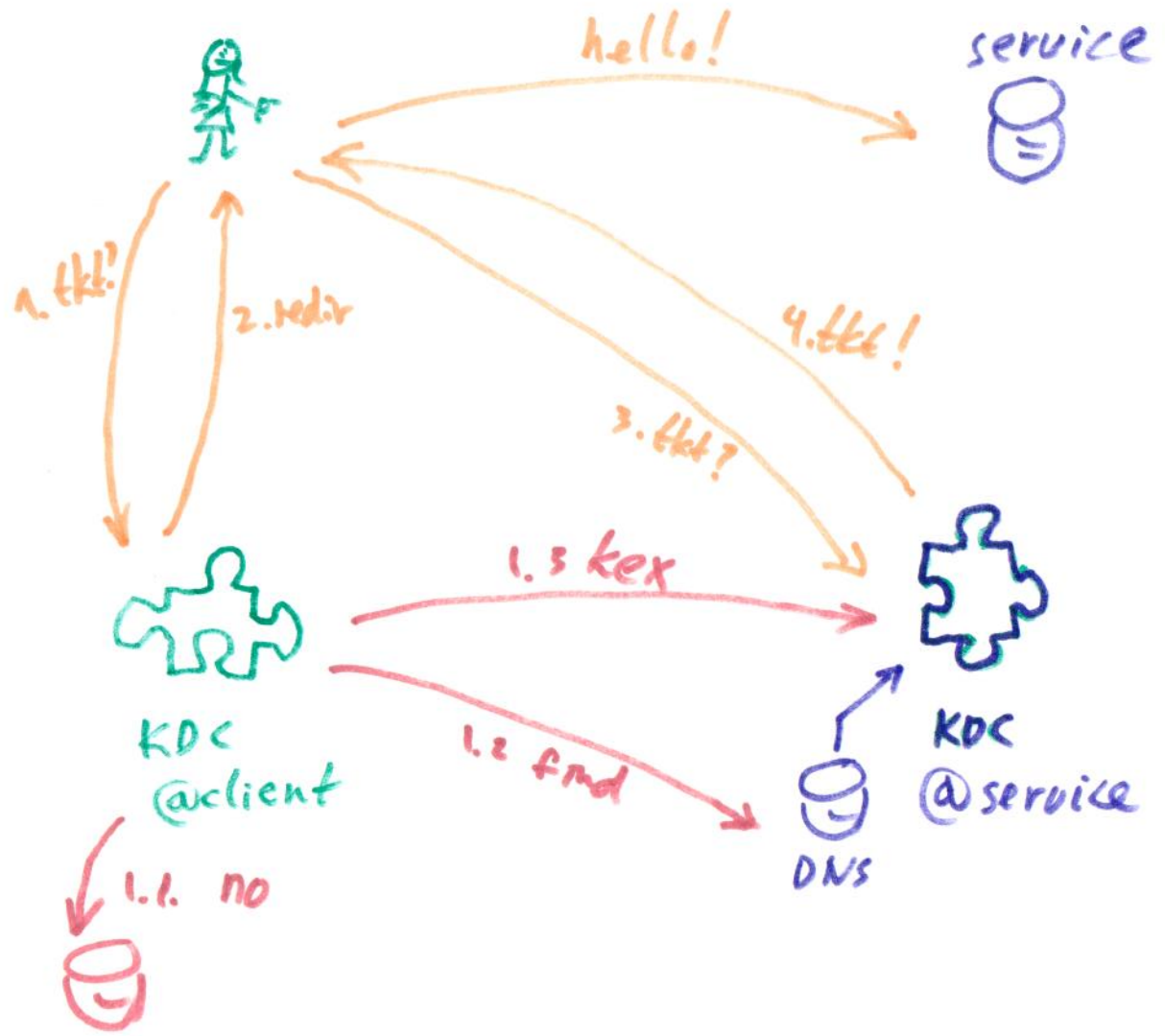
# SXOVER (SASL crossover)



Diameter:

- TLS (mutual)
- DNSSEC, DANE

# KXOVER (Kerberos Crossover)



- std clients
- KDC extension
- impromptu KEX
- DNSSEC, DANE, TLS
- Quantum Crypto!!