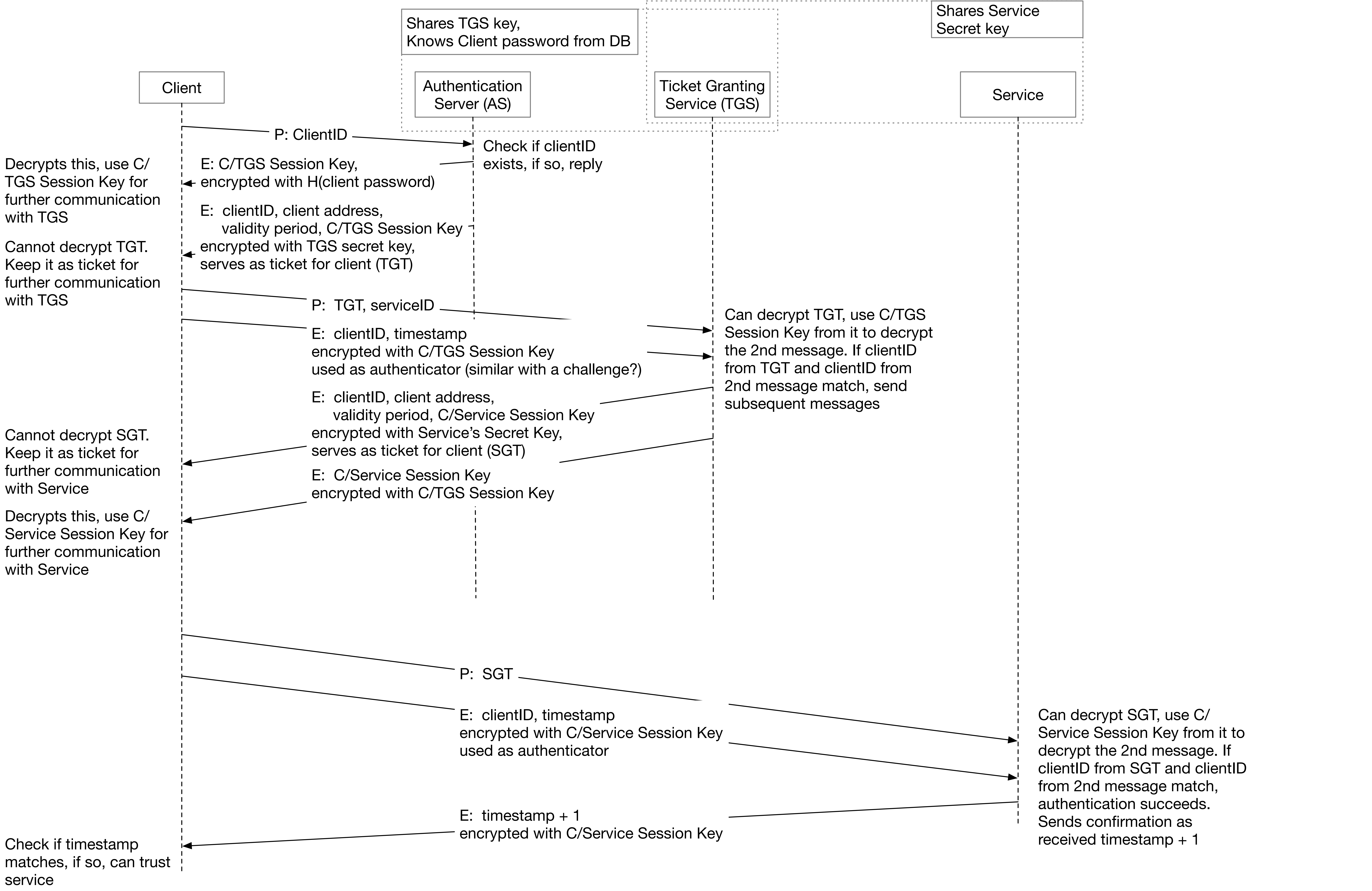

Shares TGS key,
Knows Client password from DB

Shares Service
Secret key

Client

Authentication
Server (AS)

Ticket Granting
Service (TGS)

Service

P: ClientID

Check if clientID
exists, if so, reply

E: C/TGS Session Key,
encrypted with H(client password)

Decrypts this, use C/TGS Session Key for further communication with TGS

E: clientID, client address,
validity period, C/TGS Session Key
encrypted with TGS secret key,
serves as ticket for client (TGT)

Cannot decrypt TGT. Keep it as ticket for further communication with TGS

P: TGT, serviceID

E: clientID, timestamp
encrypted with C/TGS Session Key
used as authenticator (similar with a challenge?)

Can decrypt TGT, use C/TGS Session Key from it to decrypt the 2nd message. If clientID from TGT and clientID from 2nd message match, send subsequent messages

E: clientID, client address,
validity period, C/Service Session Key
encrypted with Service's Secret Key,
serves as ticket for client (SGT)

Cannot decrypt SGT. Keep it as ticket for further communication with Service

E: C/Service Session Key
encrypted with C/TGS Session Key

Decrypts this, use C/Service Session Key for further communication with Service

P: SGT

E: clientID, timestamp
encrypted with C/Service Session Key
used as authenticator

Can decrypt SGT, use C/Service Session Key from it to decrypt the 2nd message. If clientID from SGT and clientID from 2nd message match, authentication succeeds. Sends confirmation as received timestamp + 1

E: timestamp + 1
encrypted with C/Service Session Key

Check if timestamp matches, if so, can trust service

A priori:
- Client password in TGS database (trust established offline); thus can be purely symmetric

Pros:
- Long-lived keys (client password, TGS Secret Key, Service Secret Key) are never transmitted on the network
- Granular Keys (session keys), least shared knowledge between parties
- Both-ways authentication, after the process client should be able to trust service and vice versa

Against spoofing / replaying:
- TGT and SGT contains (encrypted and only server can tell) client address. So even if spoofed replayed (say, TGT + authenticator), response won't get to the party replaying