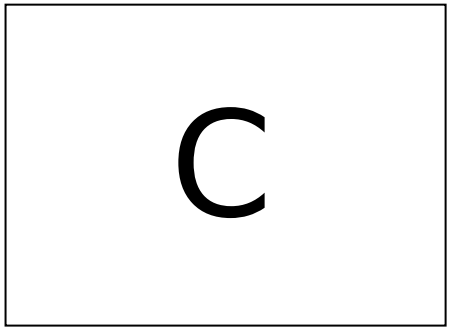
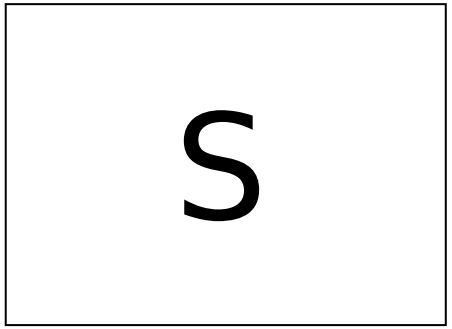

C


S

C

S

Clau pública S

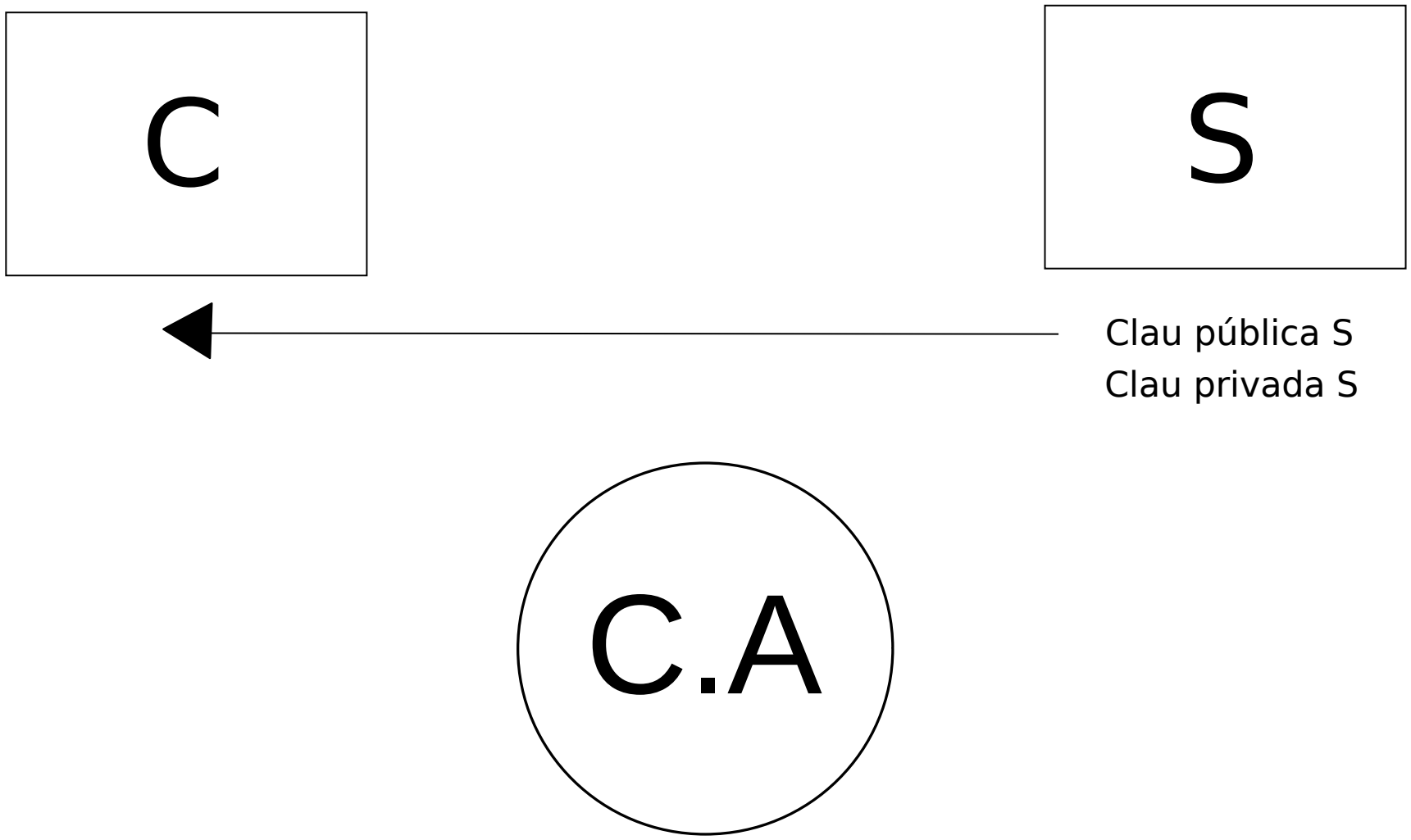
Clau privada S

Es generen amb eines com OpenSSL (o altres)

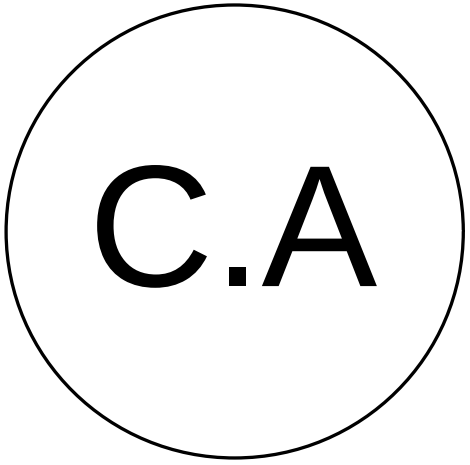
Es descarrega automàticament en la primera connexió feta via TLS

El client xifra el seu missatge amb la clau pública del servidor, qui serà, per tant, l'únic que el podrà desxifrar, perquè és l'únic que té la clau privada

Però ¿com pot tenir el client la garantia que aquesta clau pública sigui realment del servidor en qüestió i no d'un impostor?

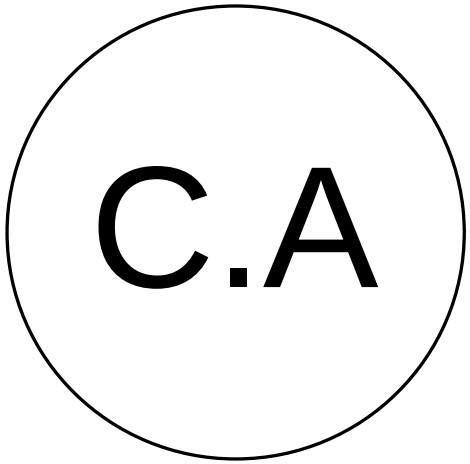

C
S
Clau pública S
Clau privada S
C.A
Clau pública C.A
Clau privada C.A

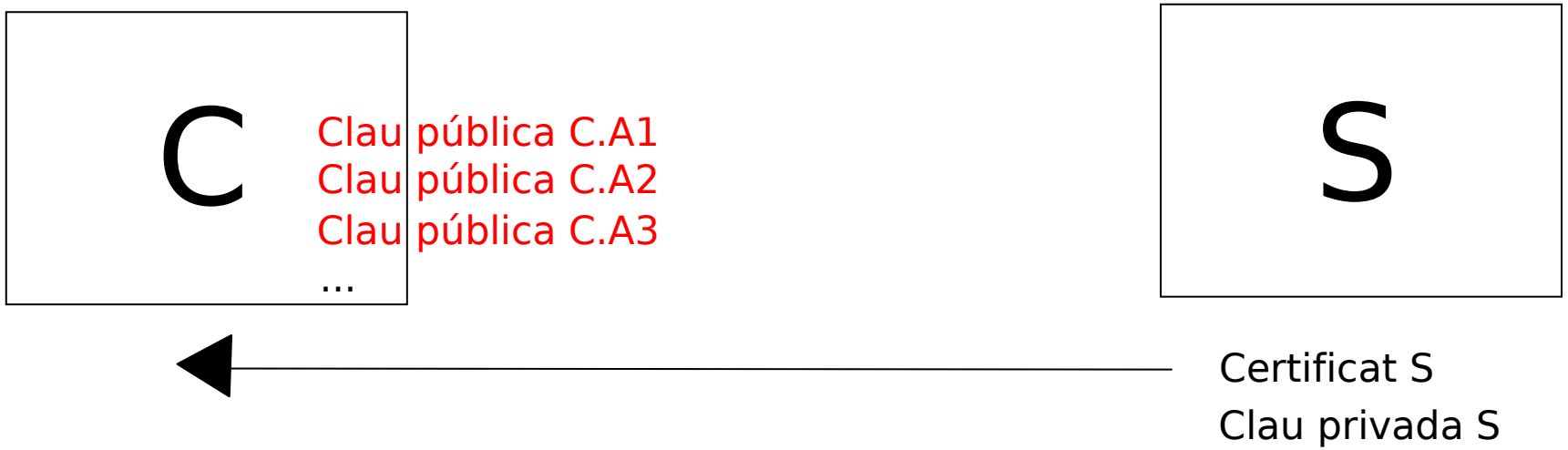
La C.A garanteix ("certifica") que la clau pública del servidor és realment d'ell en signar-la amb la seva pròpia clau privada (que només té ella)



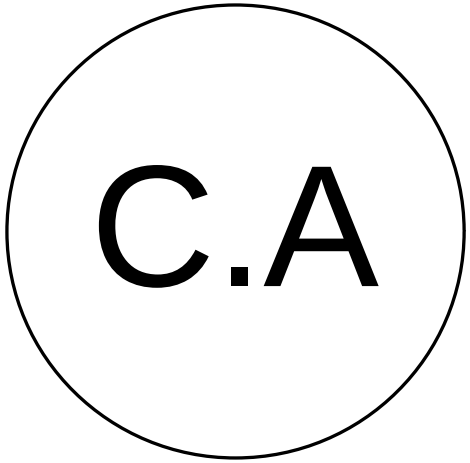
El resultat (simplificant: la clau pública del servidor signada per la clau privada de la C.A) és el que se'n diu "certificat" del servidor

Però, ¿per què el client hauria de confiar en el que hagi signat ("certificat") una C.A externa?



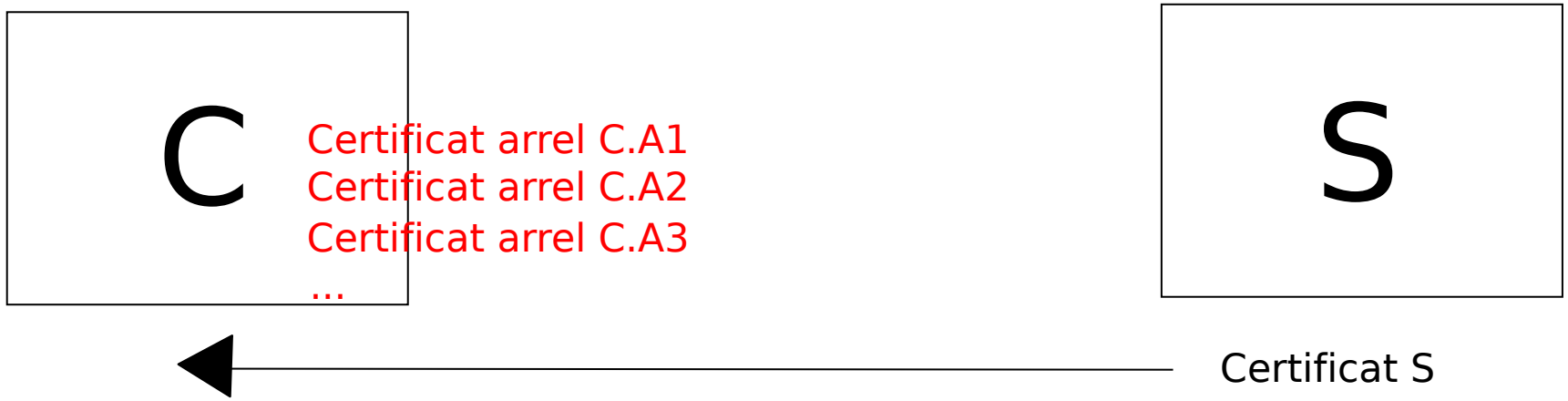


Perquè porta de sèrie ja incorporades al sistema un conjunt de claus públiques de C.As de confiança per poder verificar la seva signatura

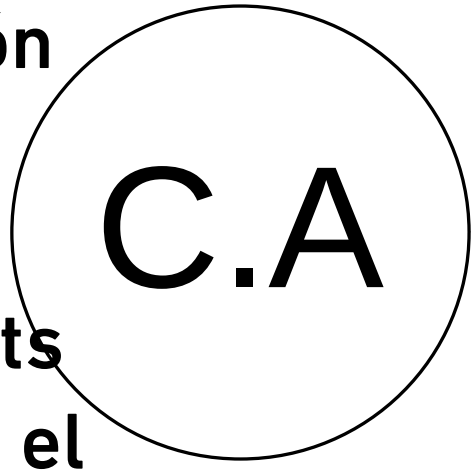


Clau pública C.A

Clau privada C.A

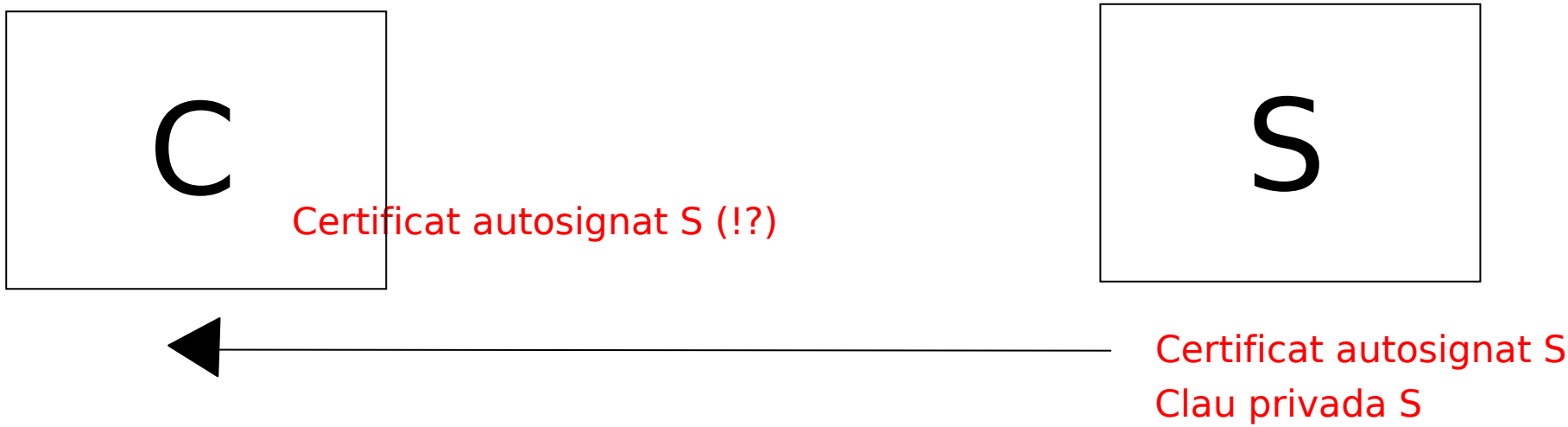


Bé, tècnicament no són claus públiques de C.As sinó són aquestes signades per la clau privada de la pròpia C.A (és a dir, són certificats "autosignats", tot i que en el cas concret de ser-ne de C.As es diuen certificats "arrel")



Clau pública C.A

Clau privada C.A



Els certificats de servidor "autosignats" per la seva pròpia clau privada poden ser una alternativa a l'ús de C.As però tenen el problema que el client, per tal d'acceptar-los i establir una conversa amb el servidor, ha d'haver incorporat prèviament el certificat "arrel" corresponent, que en aquest cas coincideix amb el propi certificat autosignat (problema de l'ou i la gallina)