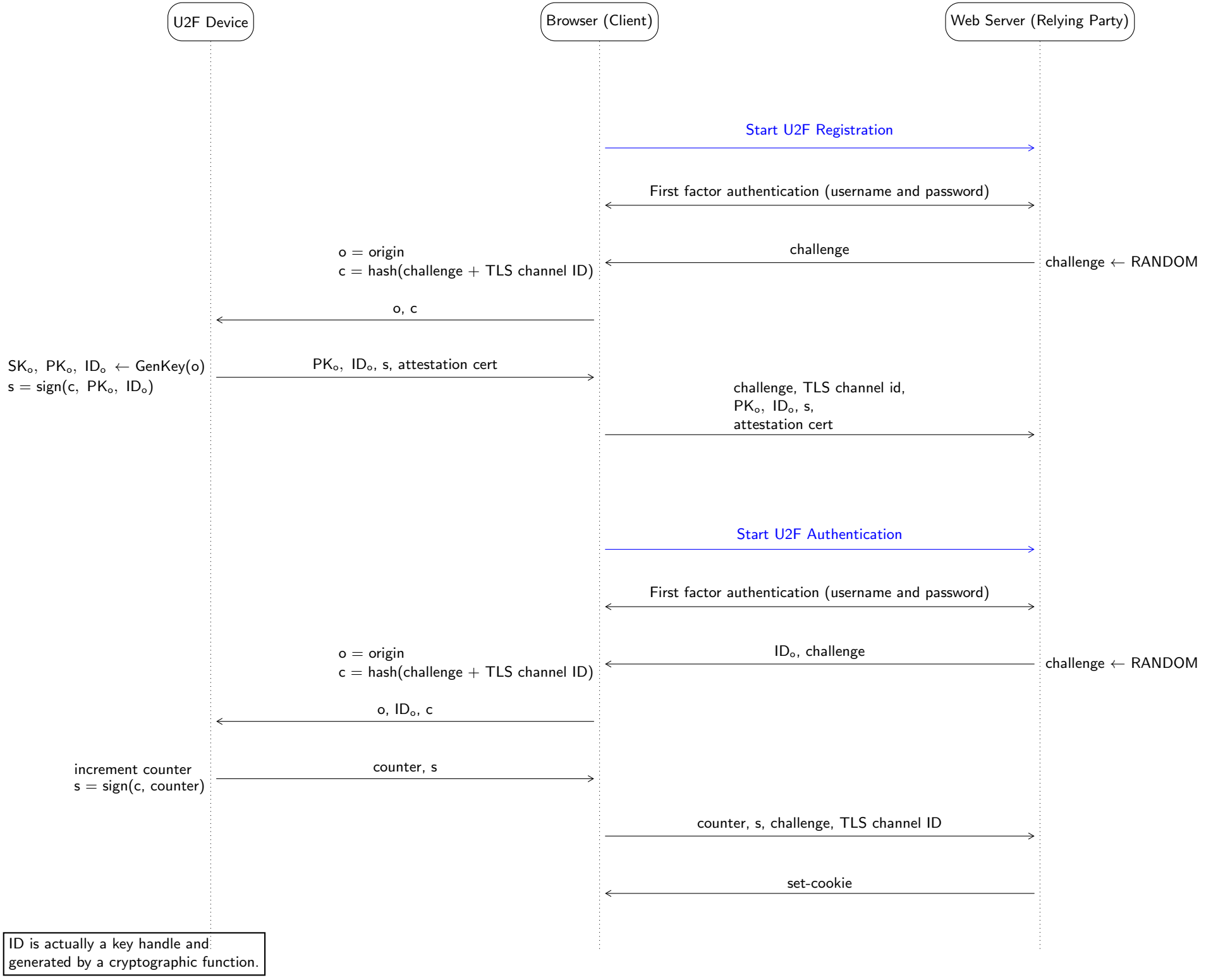
U2F Device
Browser (Client)
Web Server (Relying Party)
Start U2F Registration
First factor authentication (username and password)
o = origin
c = hash(challenge + TLS channel ID)
challenge
challenge ← RANDOM
o, c
SK_o, PK_o, ID_o ← GenKey(o)
s = sign(c, PK_o, ID_o)
PK_o, ID_o, s, attestation cert
challenge, TLS channel id,
PK_o, ID_o, s,
attestation cert
Start U2F Authentication
First factor authentication (username and password)
o = origin
c = hash(challenge + TLS channel ID)
ID_o, challenge
challenge ← RANDOM
o, ID_o, c
increment counter
s = sign(c, counter)
counter, s
counter, s, challenge, TLS channel ID
set-cookie
ID is actually a key handle and
generated by a cryptographic function.