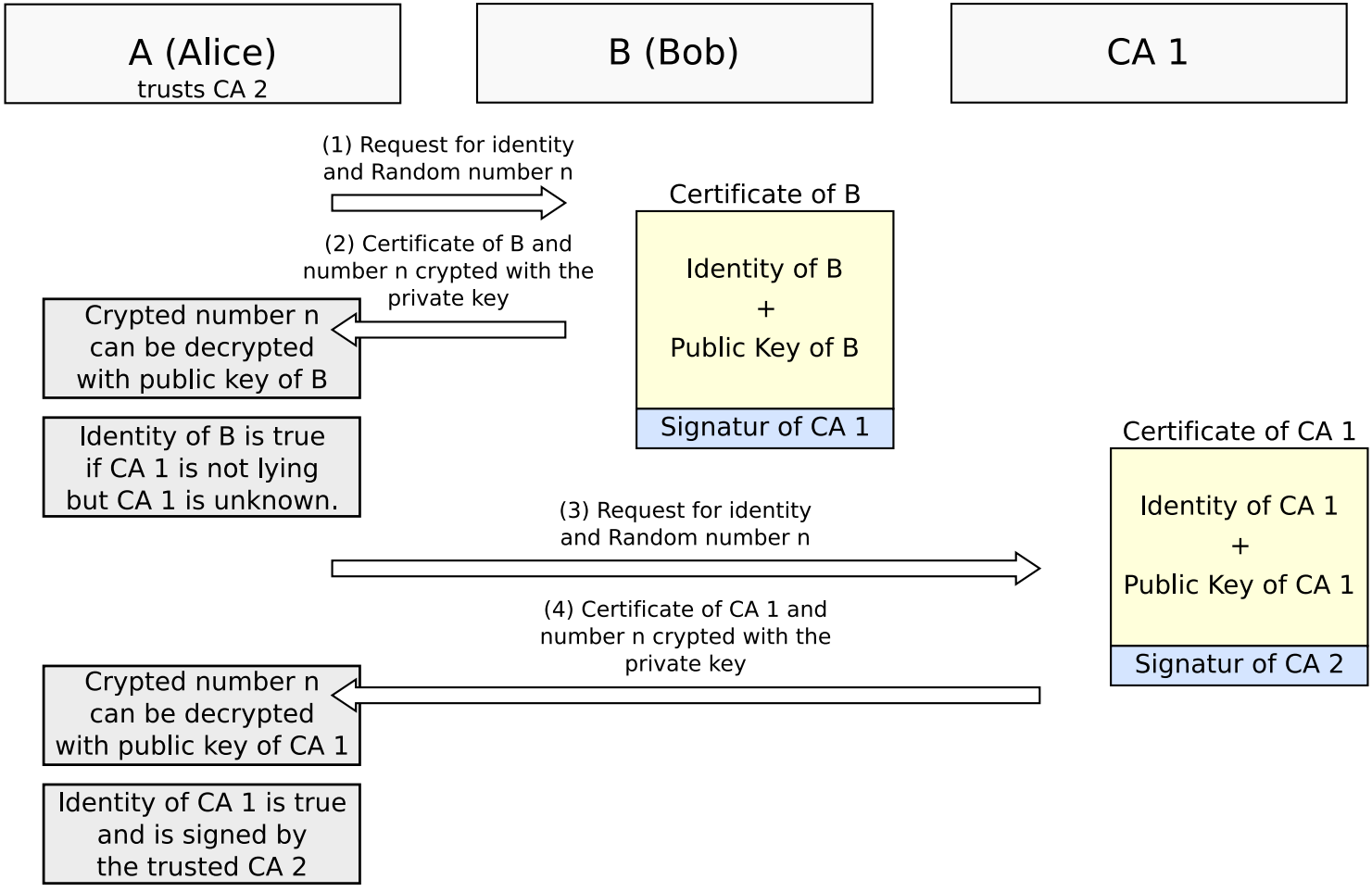
A (Alice)
trusts CA 2
B (Bob)
CA 1
(1) Request for identity
and Random number n
Certificate of B
(2) Certificate of B and
number n crypted with the
private key
Identity of B
+
Public Key of B
Signatur of CA 1
Crypted number n
can be decrypted
with public key of B
Identity of B is true
if CA 1 is not lying
but CA 1 is unknown.
Certificate of CA 1
(3) Request for identity
and Random number n
Identity of CA 1
+
Public Key of CA 1
Signatur of CA 2
(4) Certificate of CA 1 and
number n crypted with the
private key
Crypted number n
can be decrypted
with public key of CA 1
Identity of CA 1 is true
and is signed by
the trusted CA 2