

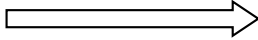
A (Alice)

is trusting CA 2

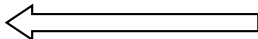
B (Bob)

CA 1

- (1) Request for identity  
and random number n



- (2) Certificate of B and  
number n crypted with  
the private key of B



### Certificate of B

Identity of B

Public Key of B

Identity of CA 1

Signature of CA 1

The number n which was  
crypted by B can be decrypted  
with the public key of B.

Hence, the identity of B is  
valid, if CA 1 can be trusted.

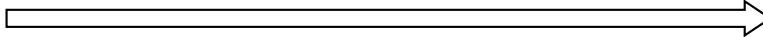
Problem: CA 1 is unknown  
Solution: Check certificate  
of CA 1

The number n which was  
crypted by CA 1 can be decryp-  
ted with the public key of CA 1

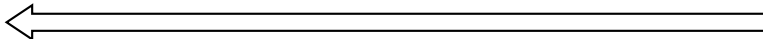
Hence, the identity of CA 1 is  
valid, if CA 2 can be trusted.

CA 2 is pre-configured to be  
trusted. From this it follows  
that the identity of B is valid.

- (3) Request for identity  
and random number n



- (4) Certificate of CA 1 and  
number n crypted with  
the private key of CA 1



### Certificate of CA 1

Identity of CA 1

Public Key of CA 1

Identity of CA 2

Signature of CA 2