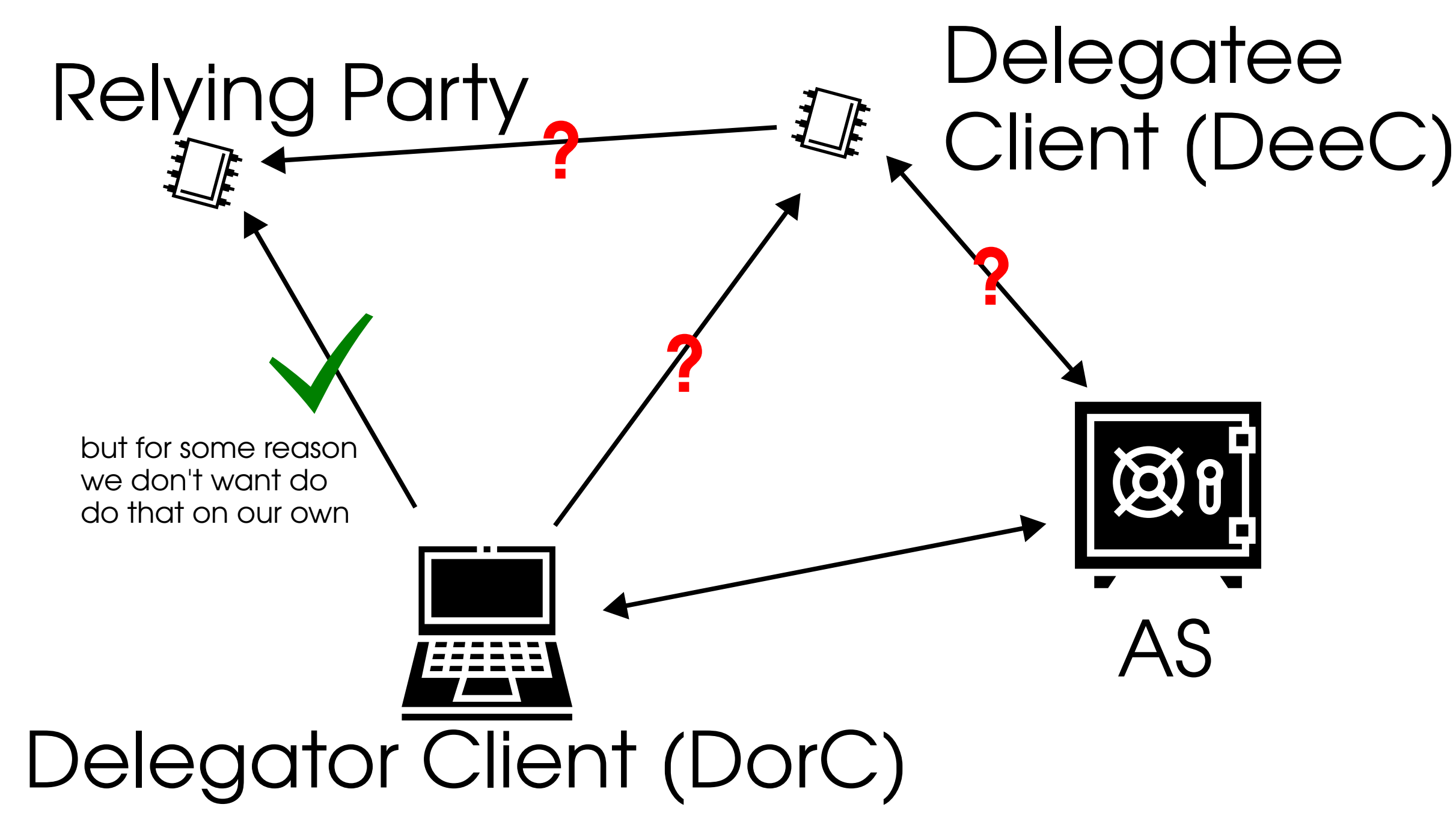
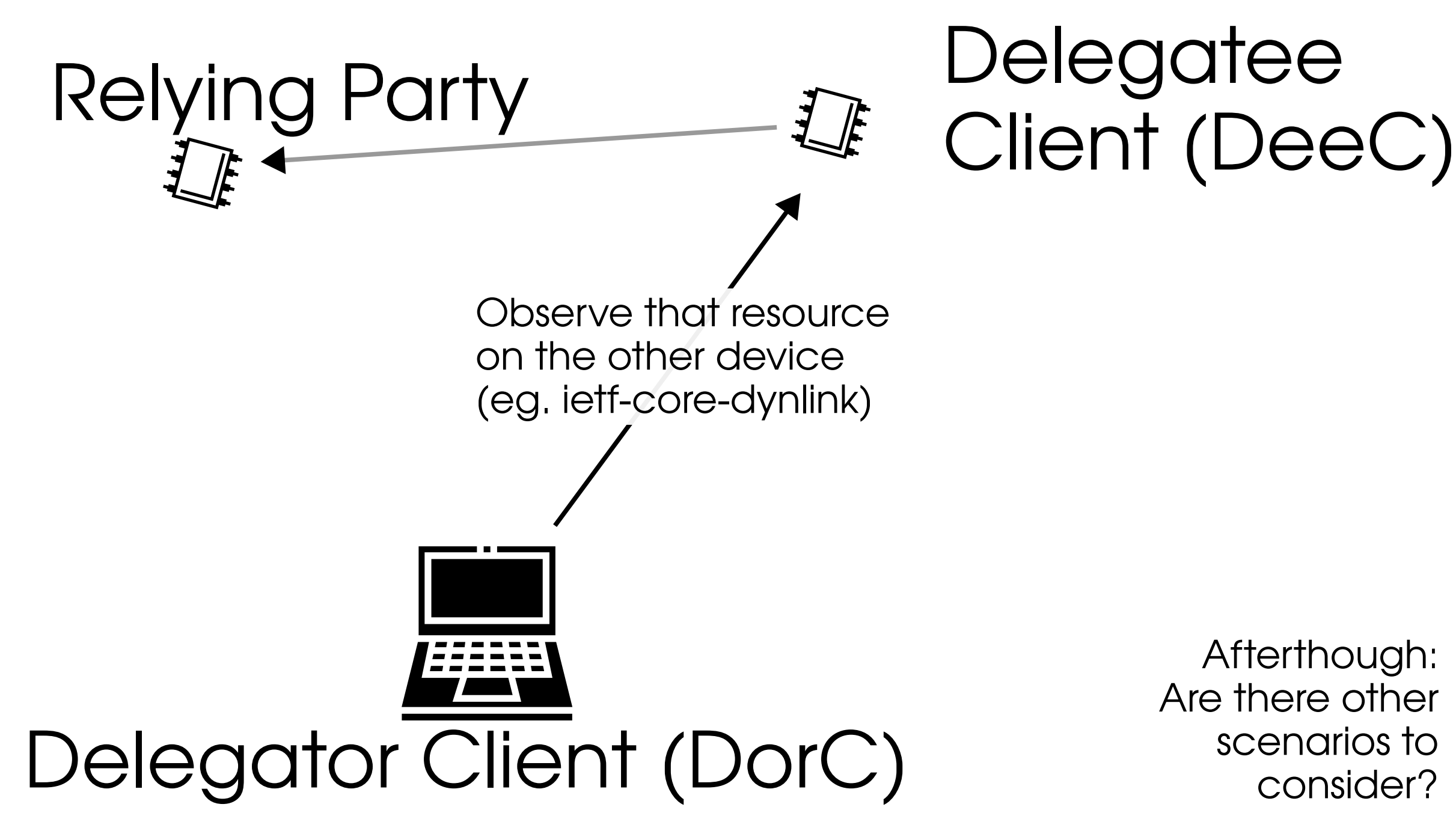
Machine-to-machine setup in ACE

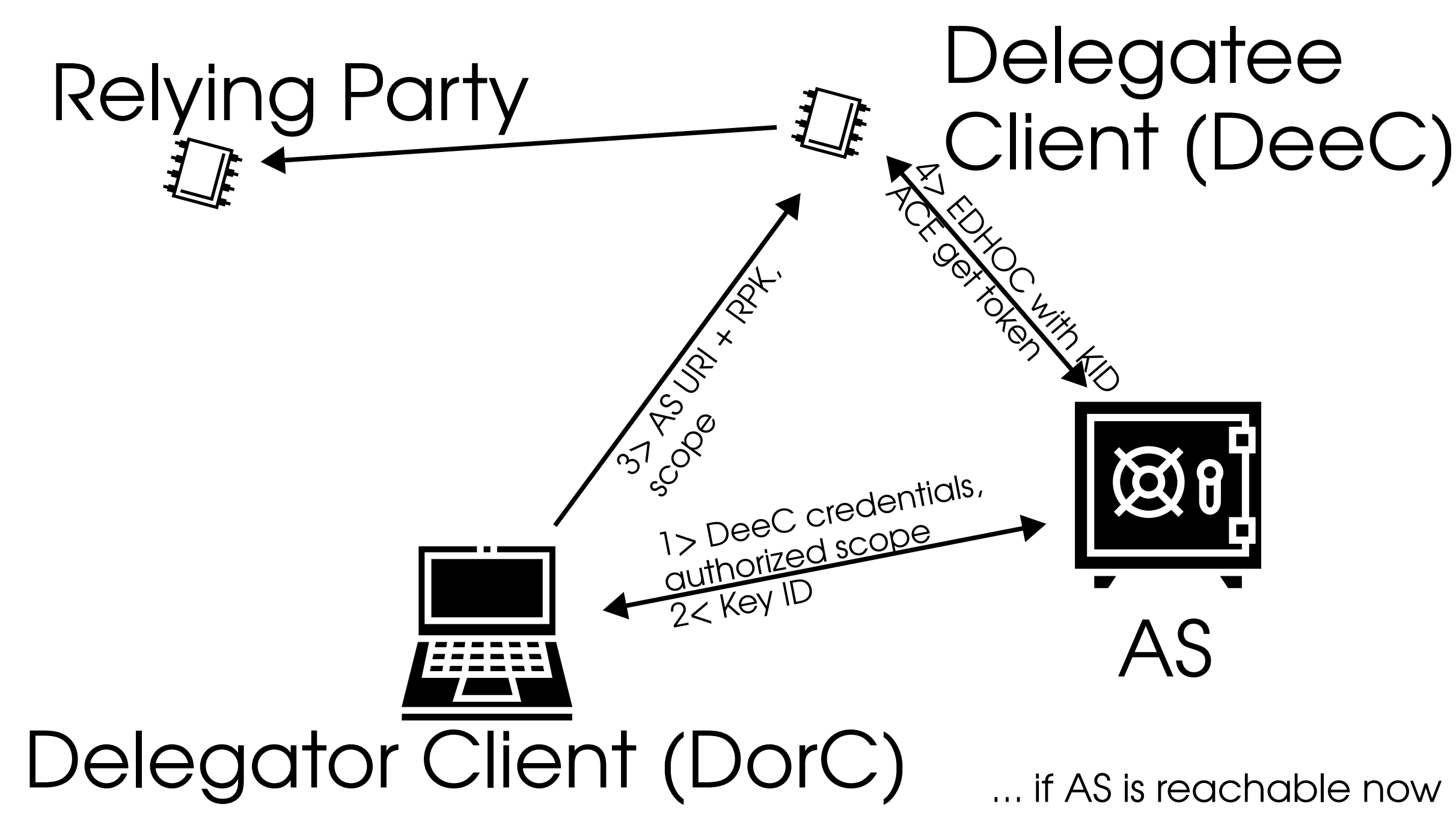
or: “Components we are missing for RIOT-rs”

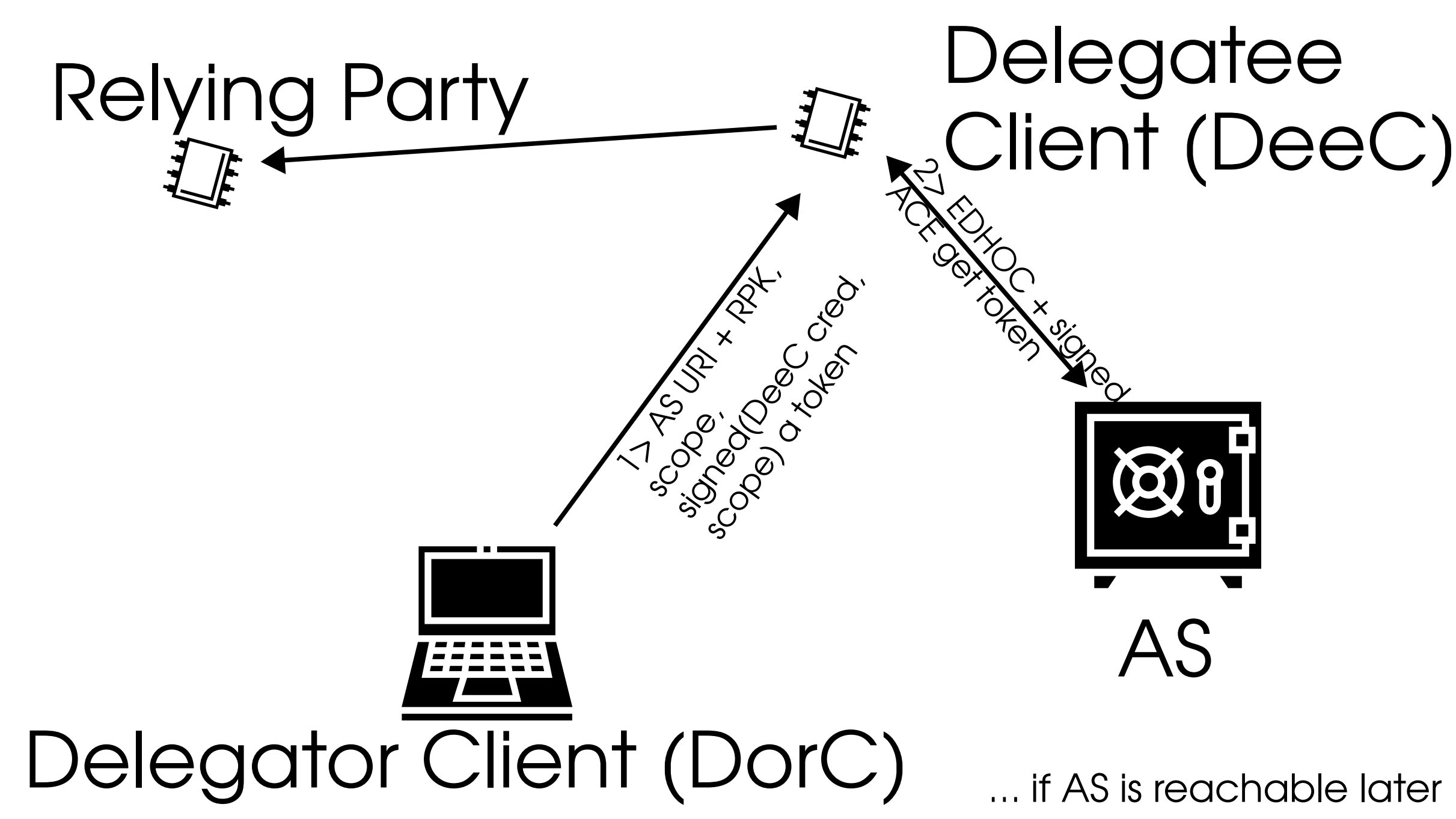
Christian Amsüss

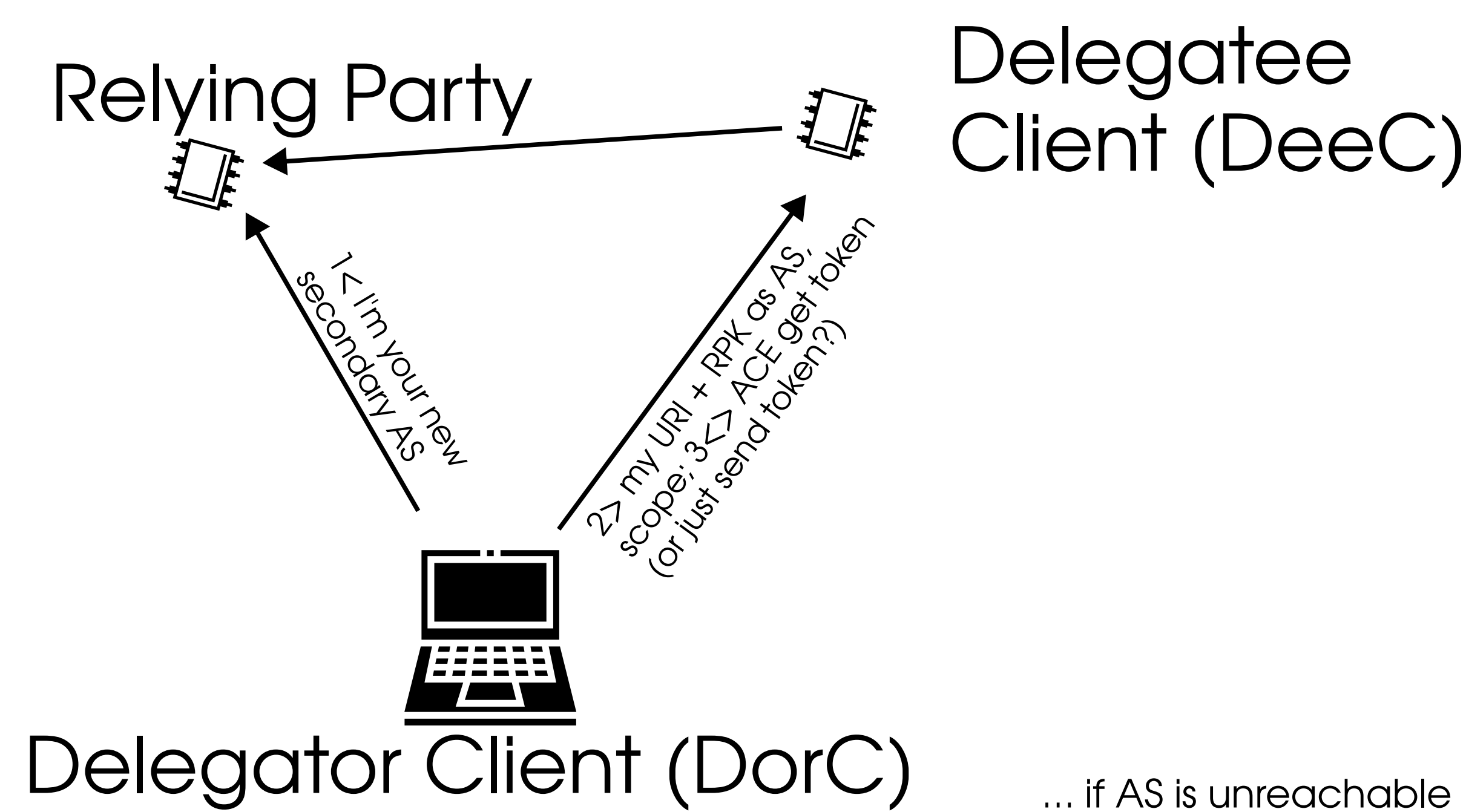
Images from Lorc and Delapouite
https://game-icons.net/1x1/lorc/microchip.html
https://game-icons.net/1x1/delapouite/laptop.html
https://game-icons.net/1x1/delapouite/strongbox.html
https://game-icons.net/1x1/delapouite/check-mark.html


Relying Party
Delegatee
Client (DeeC)
?
?
?
but for some reason
we don't want do
do that on our own
AS
Delegator Client (DorC)


Relying Party
Delegatee
Client (DeeC)
Observe that resource
on the other device
(eg. ietf-core-dynlink)
Delegator Client (DorC)
Afterthough:
Are there other
scenarios to
consider?


Relying Party
Delegatee Client (DeeC)
4> EDHOC with KID
ACE get token
3> AS URI + RPK, scope
1> DeeC credentials, authorized scope
2< Key ID
AS
Delegator Client (DorC)
... if AS is reachable now


Relying Party
Delegatee
Client (DeeC)
1> AS URI + RPK,
scope,
signed(DeeC cred,
scope) a token
2> EDHOC + signed
ACE get token
AS
Delegator Client (DorC)
... if AS is reachable later



... if AS is unreachable