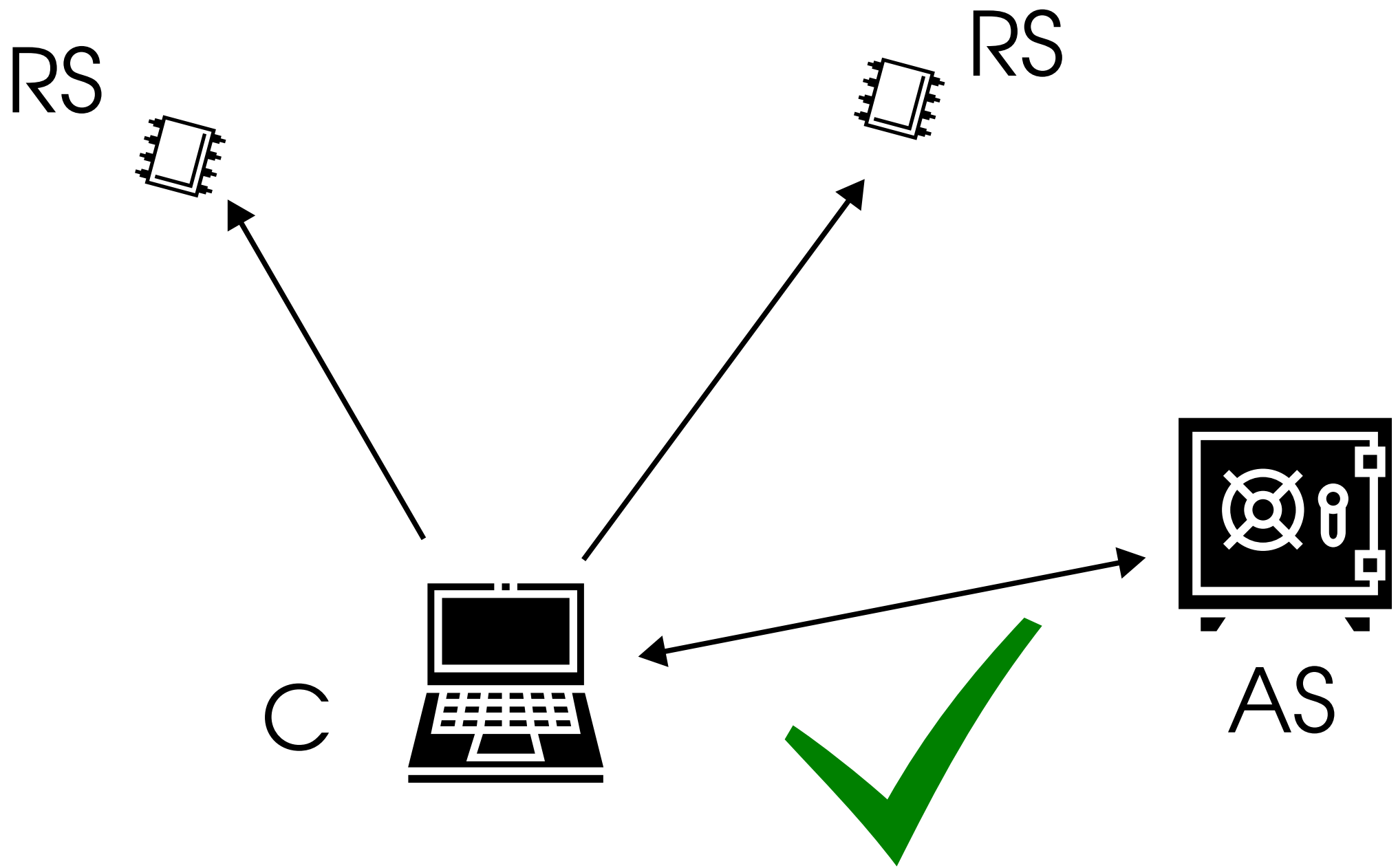
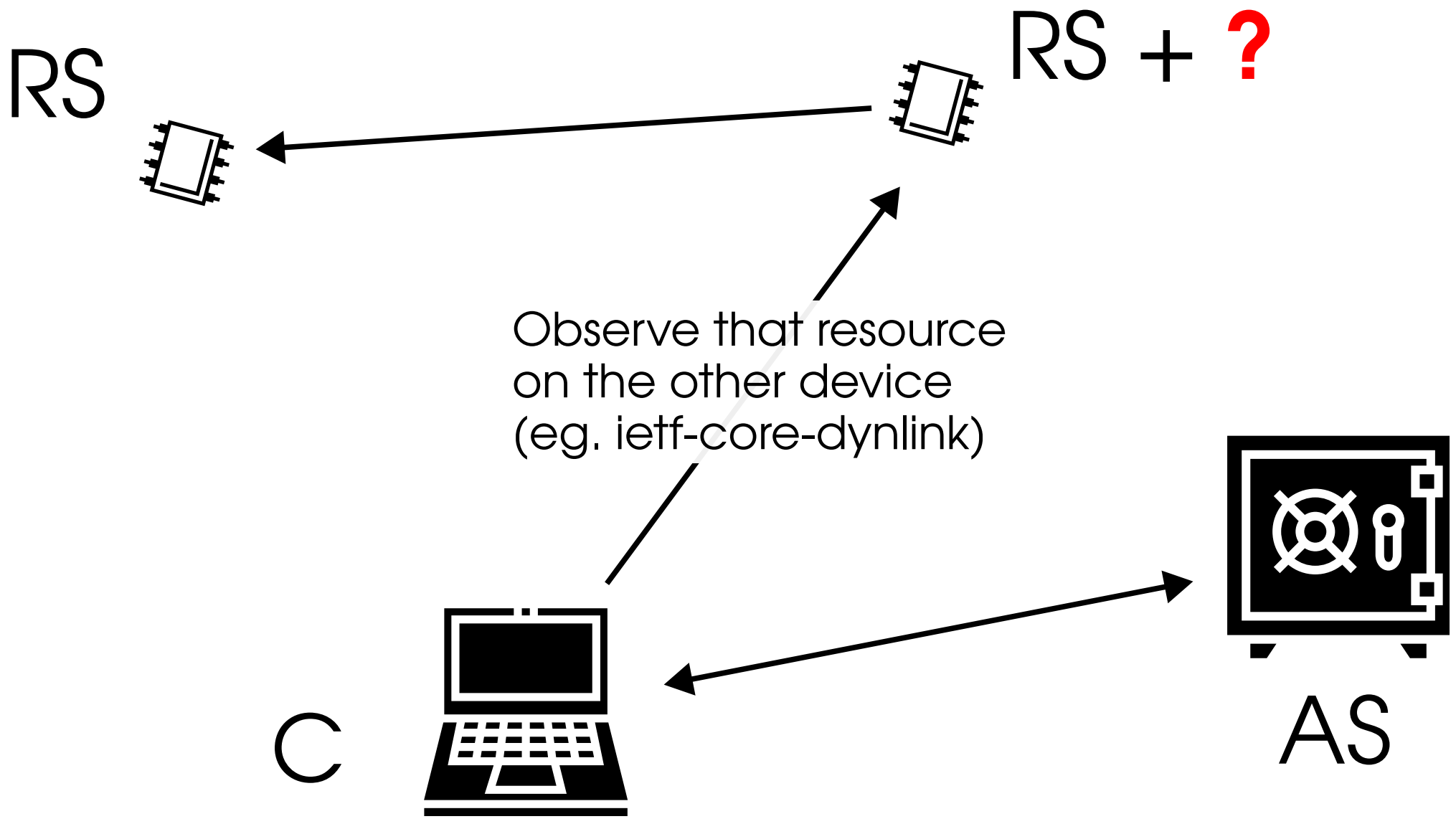
Machine-to-machine setup in ACE

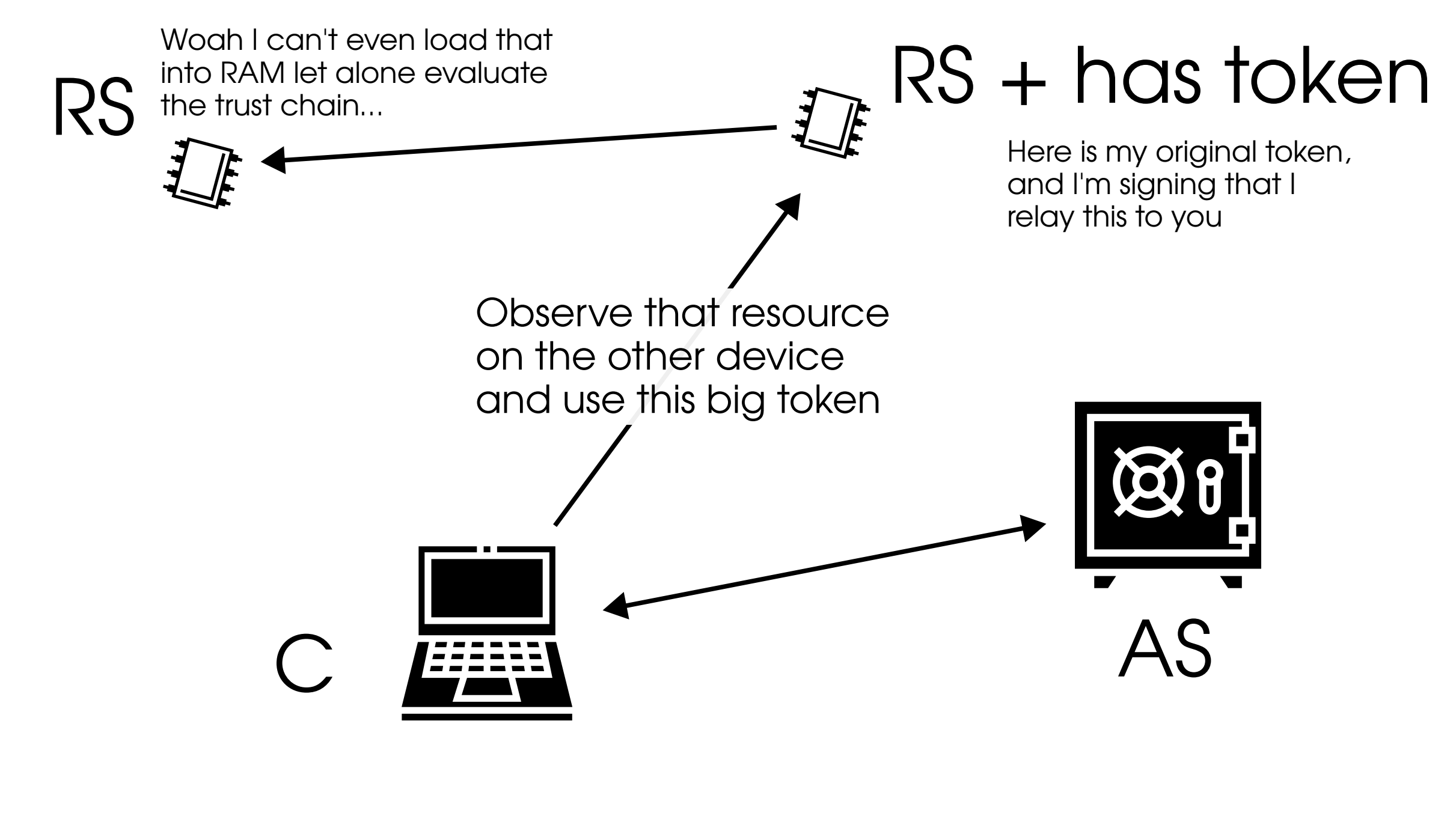
or: “Components we are missing for RIOT-rs”

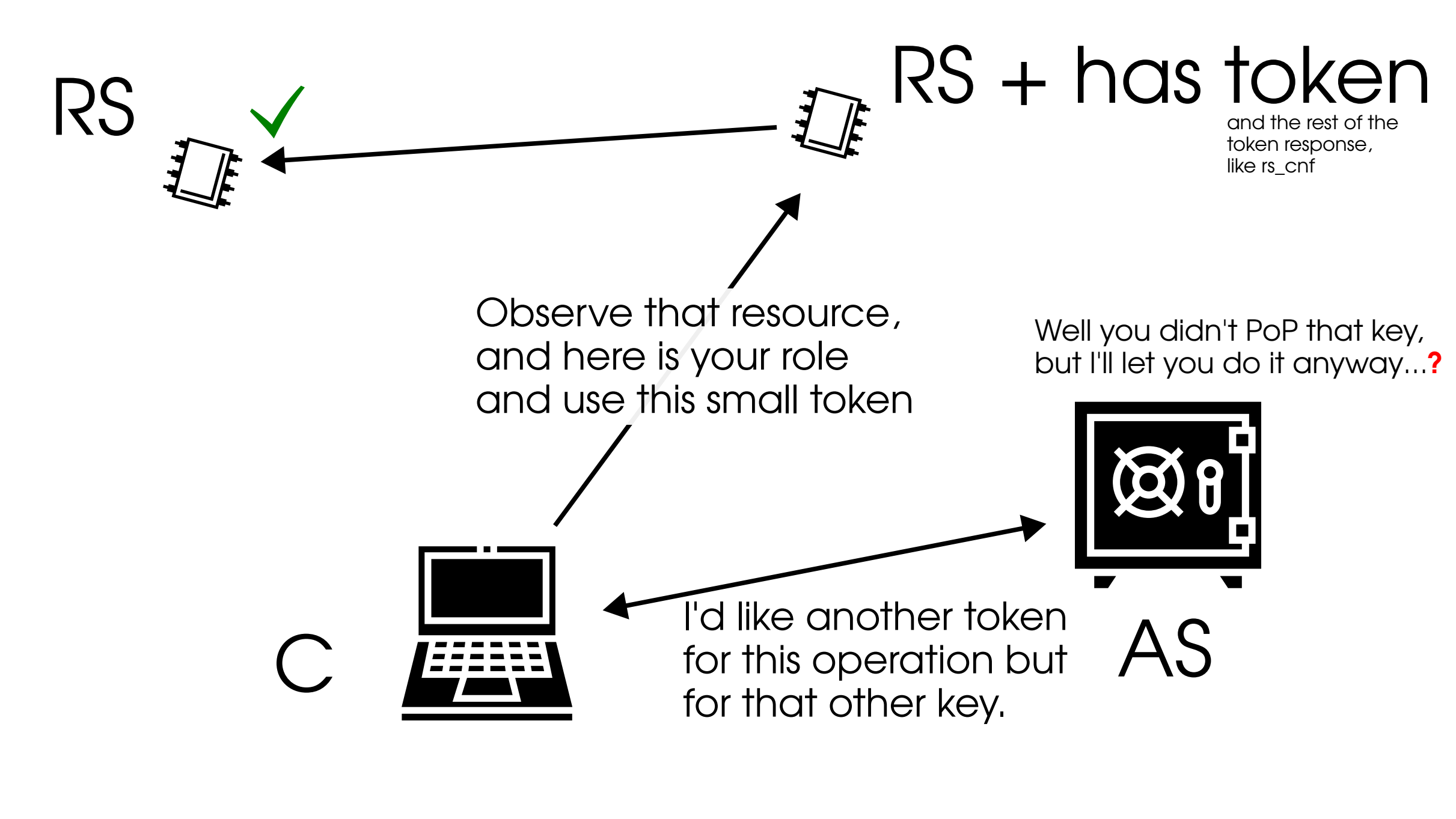
Christian Amsüss

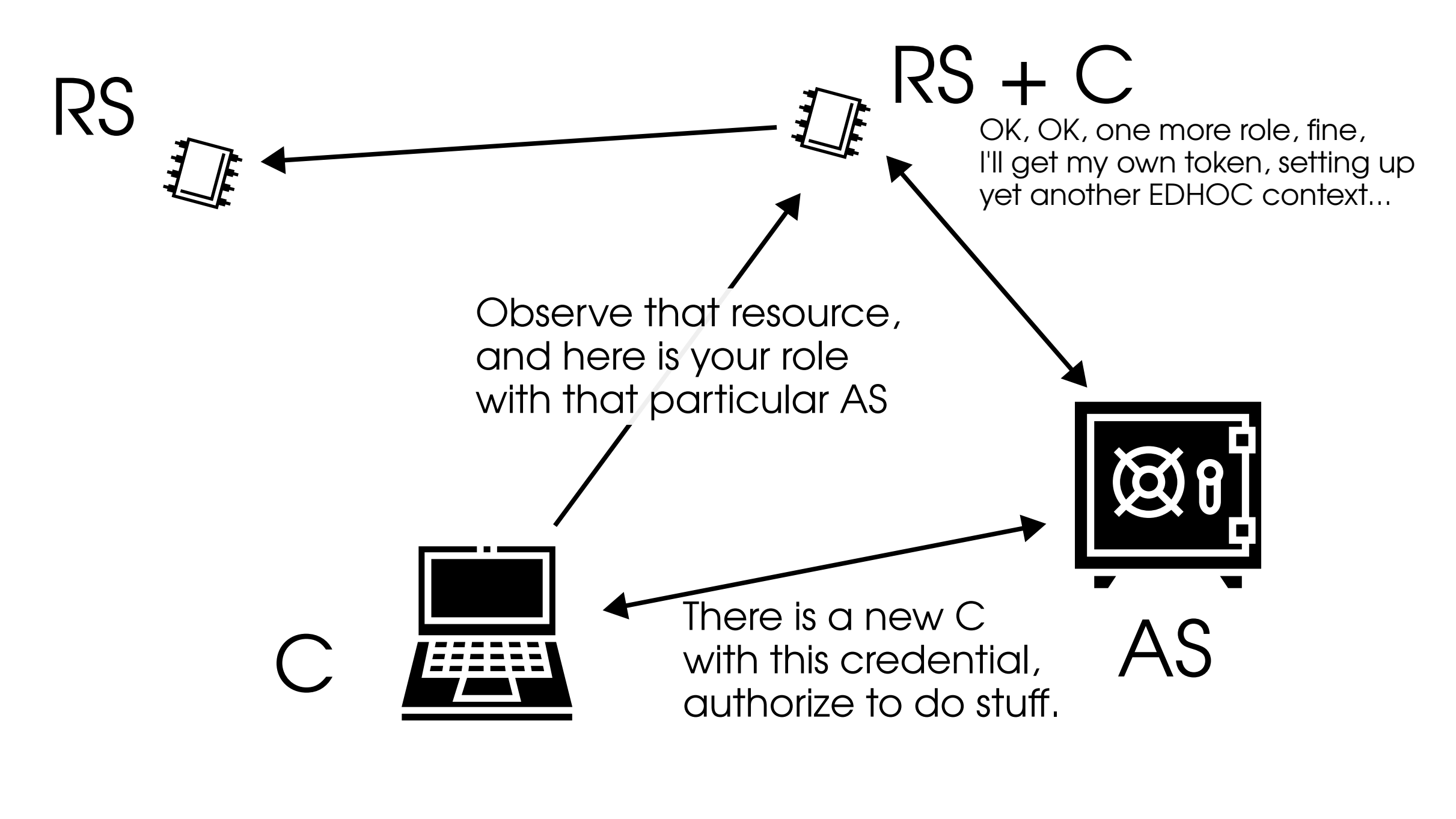
Images from Lorc and Delapouite
https://game-icons.net/1x1/lorc/microchip.html
https://game-icons.net/1x1/delapouite/laptop.html
https://game-icons.net/1x1/delapouite/strongbox.html
https://game-icons.net/1x1/delapouite/check-mark.html

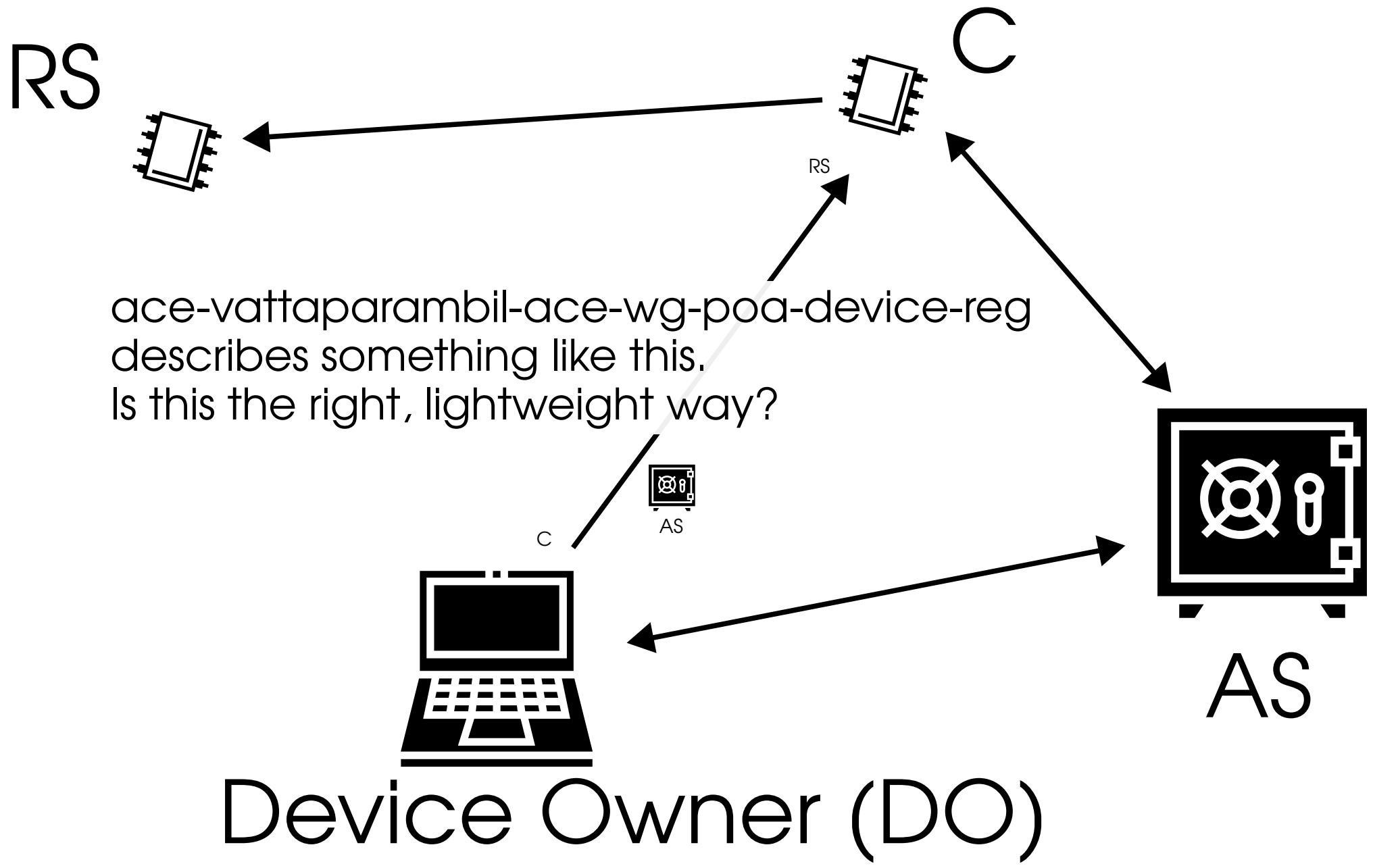

RS
RS
C
AS

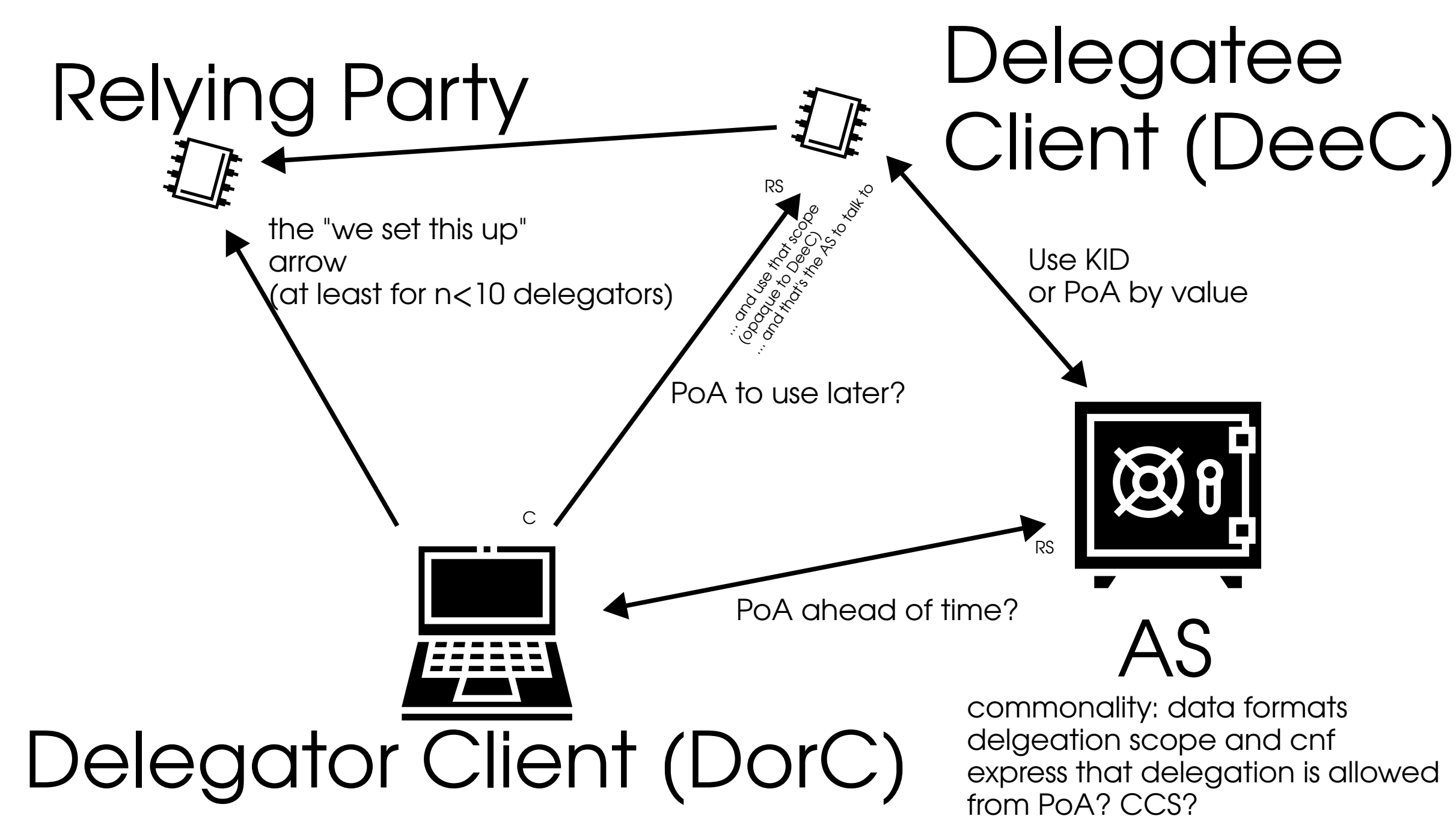

RS
RS + ?
Observe that resource
on the other device
(eg. ietf-core-dynlink)
C
AS


RS
Woah I can't even load that into RAM let alone evaluate the trust chain...
RS + has token
Here is my original token, and I'm signing that I relay this to you
Observe that resource on the other device and use this big token
C
AS


RS
RS + has token
and the rest of the token response, like rs_cnf
Observe that resource, and here is your role and use this small token
Well you didn't PoP that key, but I'll let you do it anyway...?
C
I'd like another token for this operation but for that other key.
AS


RS
RS + C
OK, OK, one more role, fine,
I'll get my own token, setting up
yet another EDHOC context...
Observe that resource,
and here is your role
with that particular AS
C
There is a new C
with this credential,
authorize to do stuff.
AS


RS
C
RS
ace-vattaparambil-ace-wg-poa-device-reg
describes something like this.
Is this the right, lightweight way?
AS
C
AS
Device Owner (DO)


Relying Party
Delegatee
Client (DeeC)
RS
... and use that scope
(opaque to DeeC)
... and that's the AS to talk to
the "we set this up"
arrow
(at least for n<10 delegators)
Use KID
or PoA by value
PoA to use later?
C
RS
PoA ahead of time?
AS
commonality: data formats
delgeation scope and cnf
express that delegation is allowed
from PoA? CCS?
Delegator Client (DorC)