Authorization of AKE/enrolment

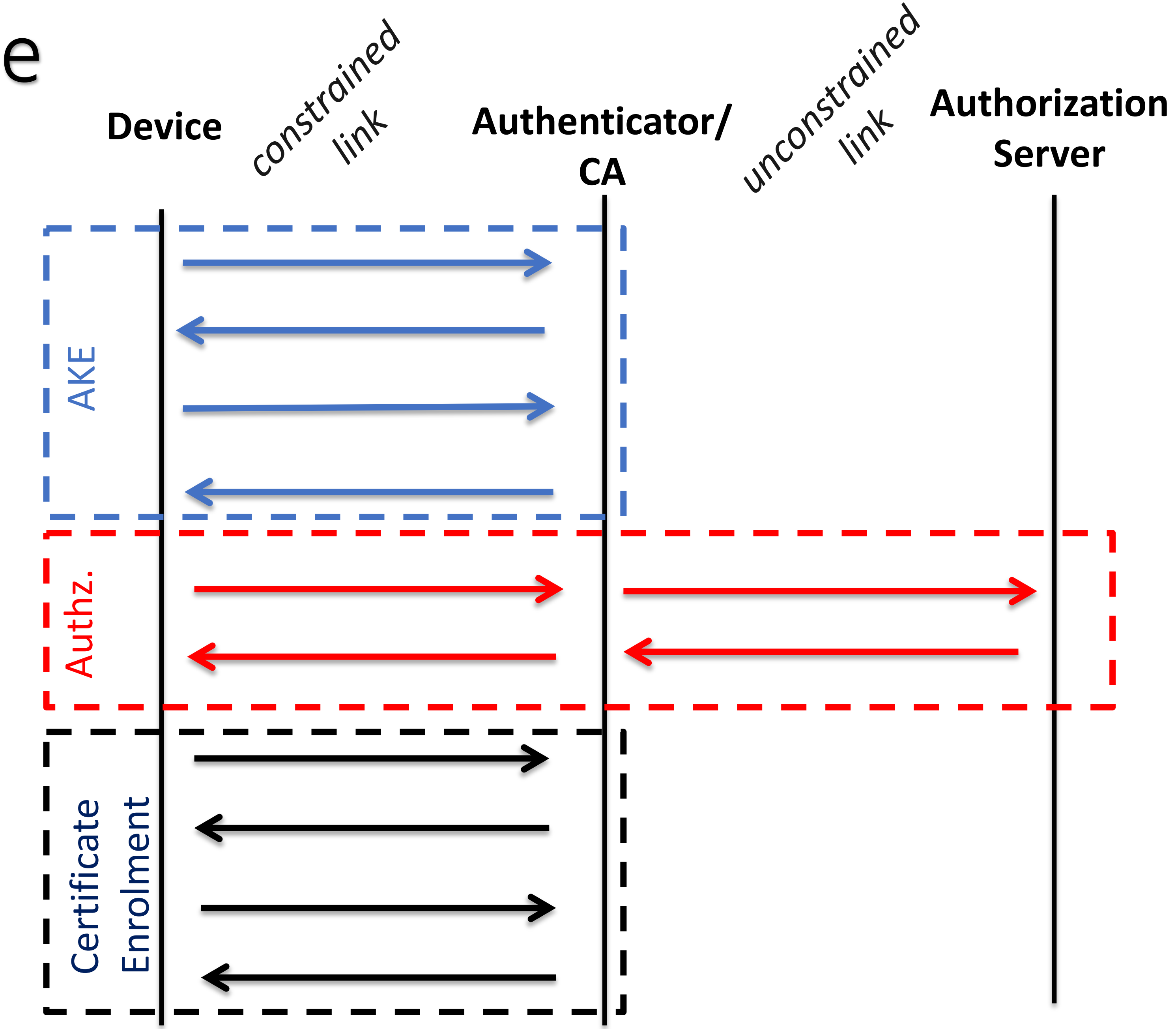
draft-selander-ace-ake-authz-02

Göran Selander, John Mattsson, Ericsson
Michael Richardson, SSW
Mališa Vučinić, INRIA
Aurelio Schellenbaum, ZHAW

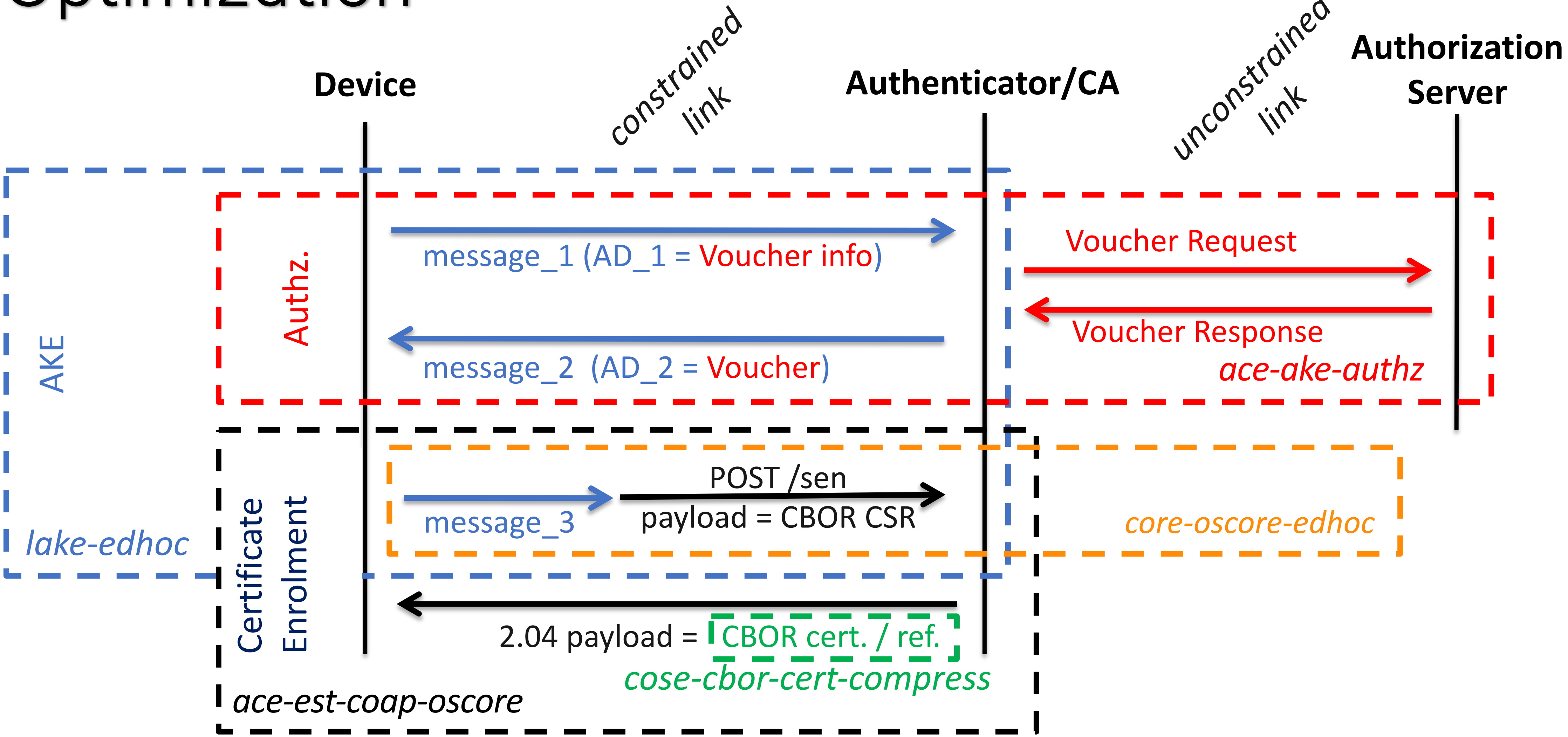
ACE, IETF 109, November 2020

Device join example

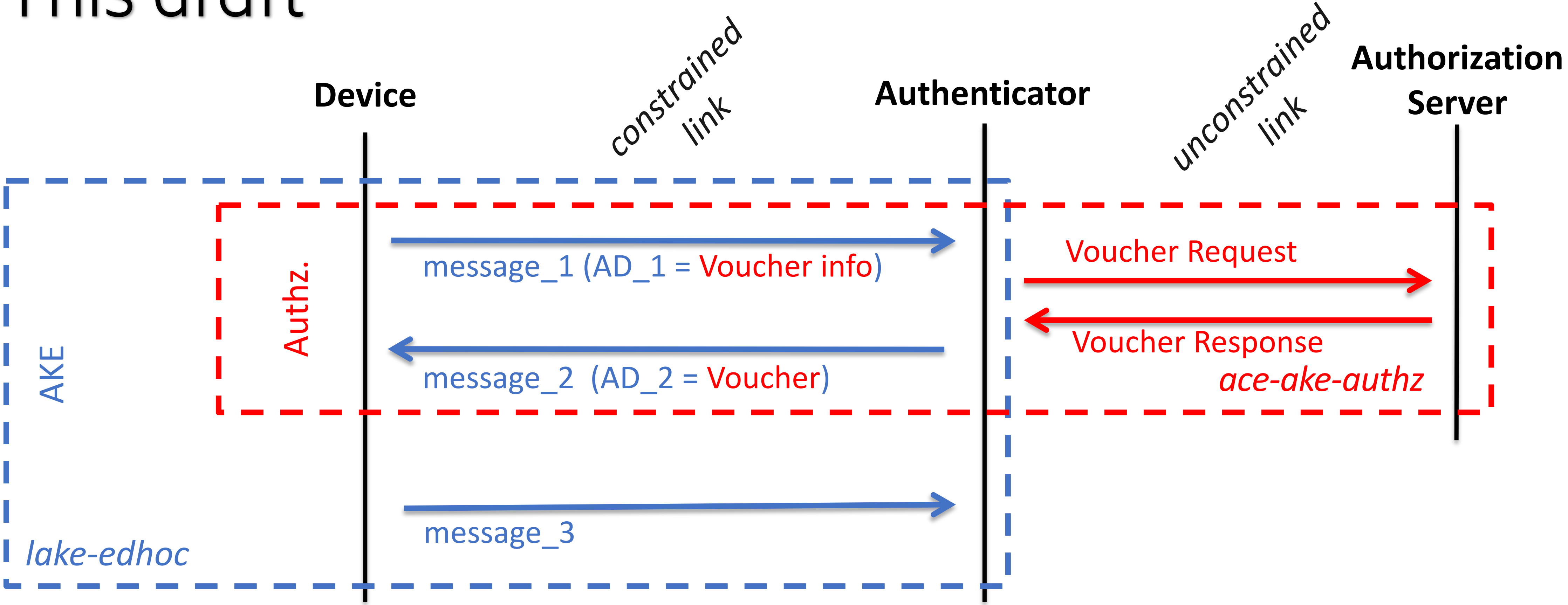
- Device joining network
  - Authenticate
  - Authorize
  - Enrol operational certificate
- Potential inefficiencies
  - Sequential processing
  - Same data in different phases
  - Data sent over constrained link which can be accessible over unconstrained link



Optimization



This draft



- Lightweight authentication and authorization
- Makes use of Auxiliary Data (AD) in EDHOC (draft-ietf-lake-edhoc)
- Reuse of data: Identifiers etc. sent in EDHOC also used for authorization
- Lower overhead: Transport credentials over unconstrained instead of constrained network

Protocol sketch

Assumptions

U ←→V

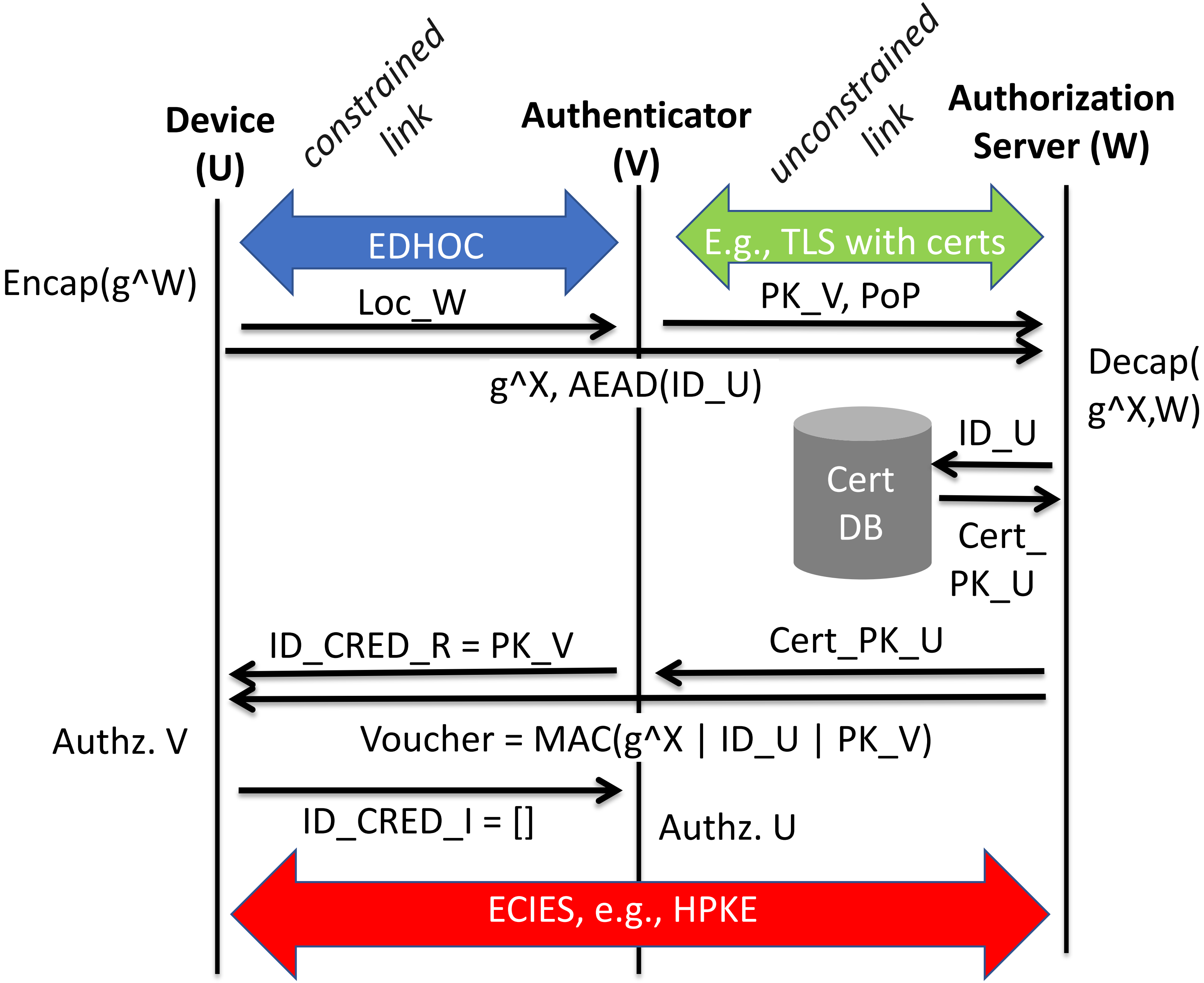
- No prior trust relation
- U provide location of W to V

V ←→W

- Web based trust
  - Implicit trust anchors

U ←→W

- U trust g^W (PK of W)
- W can look up Cert_PK_U using ID_U



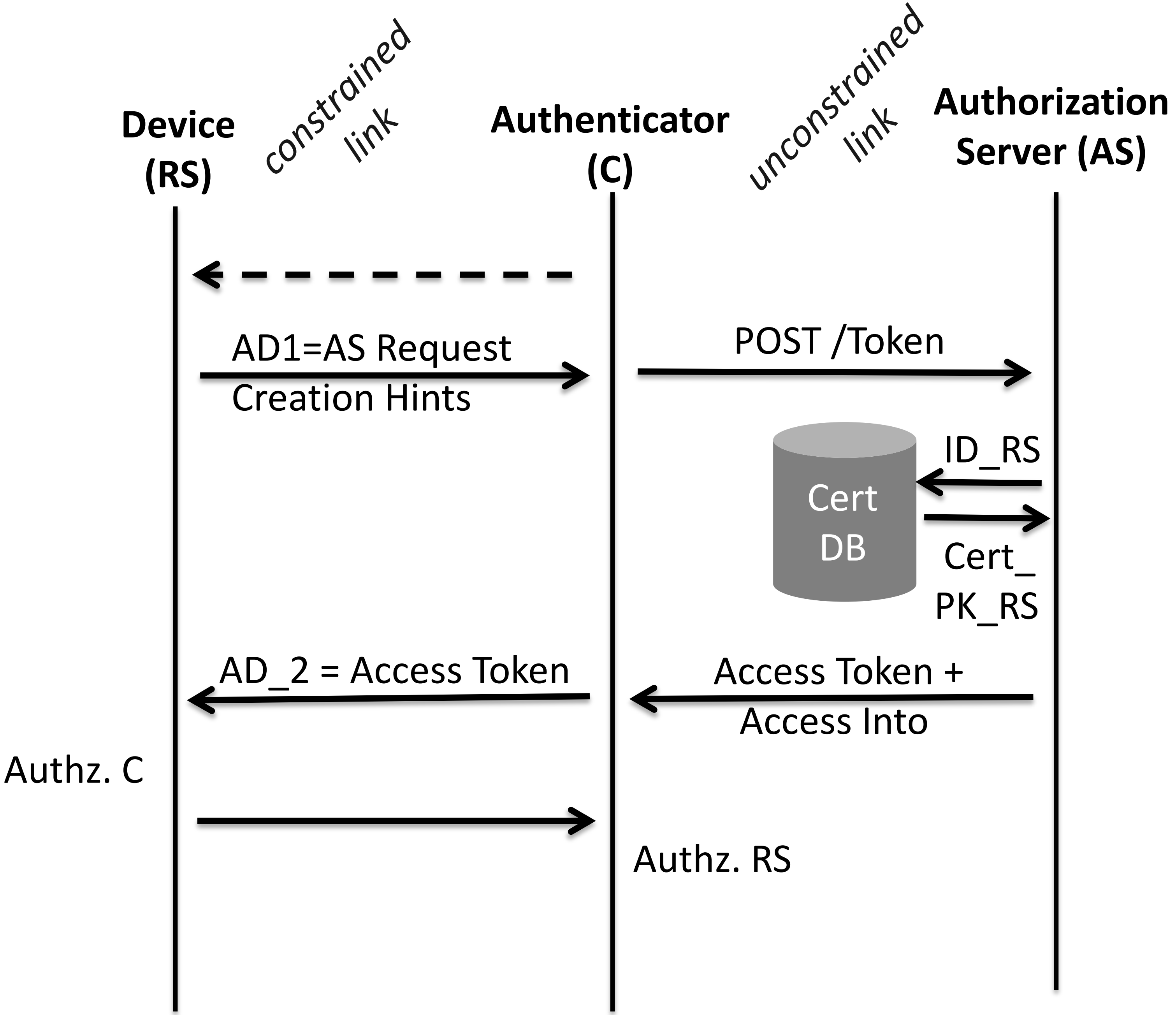
ACE mapping

Assumptions

RS ←→C
- No prior trust relation
- RS provide location of AS to C

C ←→AS
- Web based trust
  - Implicit trust anchors

RS ←→AS
- RS know g^W (PK of AS)
- AS can look up Cert_PK_RS using ID_RS



Content of draft (work in progress)

- 2 new Auxiliary Data types for EDHOC
  - AD_1 = (T0: int, LOC_W: tstr, CC: bstr, CIPHERTEXT_RQ: bstr)
  - AD_2 = (T1: int, Voucher: bstr)

- Ultra-constrained voucher, AEAD with empty plain text of
  - external_aad_array = [V_TYPE: int, PK_V: bstr, G_X: bstr, CC: bstr, ID_U: bstr]

- Voucher Request/Response
  - VREQ = [G_X: bstr, CC: bstr, CIPHERTEXT_RQ: bstr]
  - VRES = [G_X: bstr, CC: bstr, CIPHERTEXT_RQ: bstr]
  - Independent of transport

- ACE mapping

- Security processing

Next steps

- Specify crypto context
- Details of ECIES
- Submit `-03`

- Reviews?