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

![Diagram of device join example](Image)
2.04 payload = CBOR cert. / ref.

message_1 (AD_1 = Voucher info)

message_2 (AD_2 = Voucher)

message_3

POST /sen

core-oscore-edhoc

cose-cbor-cert-compress

AUTHORIZATION

Voucher Request

Voucher Response

ACE-AKE-AUTHZ

Authorization Server

Device

constrained link

message_1 (AD_1 = Voucher info)

message_2 (AD_2 = Voucher)

message_3

POST /sen

payload = CBOR CSR

Certificate Enrollment

lake-edhoc

AKE

Optimization

ACE-EST-COAP-OSCORE

AUTHORIZATION

Voucher Request

Voucher Response

ACE-AKE-AUTHZ

Authorization Server

Device

constrained link

message_1 (AD_1 = Voucher info)

message_2 (AD_2 = Voucher)

message_3

POST /sen

payload = CBOR CSR

Certificate Enrollment

lake-edhoc

AKE

Optimization

ACE-EST-COAP-OSCORE

AUTHORIZATION

Voucher Request

Voucher Response

ACE-AKE-AUTHZ

Authorization Server
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

EDHOC

Encap(g^W)

Authenticator (V)

Authz. V

Voucher = MAC(g^X | ID_U | PK_V)

ID_CRED_R = PK_V

Cert_PK_U

Decap(g^X,W)

E.g., TLS with certs

ECIES, e.g., HPKE

Device (U)

constrained link

Authenticator (V)

unconstrained link

Authorization Server (W)

ID_CRED_I = []

Authz. U

Cert DB

g^X, AEAD(ID_U)

ID_U

Cert_PK_U

Loc_W

PK_V, PoP

EDHOC

ACE mapping

Assumptions

RS $\leftrightarrow$ C
- No prior trust relation
- RS provide location of AS to C

C $\leftrightarrow$ AS
- Web based trust
  - Implicit trust anchors

RS $\leftrightarrow$ AS
- RS know $g^W$ (PK of AS)
- AS can look up Cert_PK_RS using ID_RS

Device (RS) $\leftarrow$ constrained link $\rightarrow$ Authenticator (C) $\leftarrow$ unconstrained link $\rightarrow$ Authorization Server (AS)

- POST /Token
  - ID_RS
  - Cert_PK_RS

- AD1 = AS Request
  - Creation Hints

- AD_2 = Access Token
  - Access Into
  - Authz. C
  - Authz. RS
Content of draft (work in progress)

- 2 new Auxiliary Data types for EDHOC
  - $\text{AD}_1 = ( T0: \text{int}, \text{LOC}_W: \text{tstr}, \text{CC}: \text{bstr}, \text{CIPHERTEXT}_RQ: \text{bstr} )$
  - $\text{AD}_2 = ( T1: \text{int}, \text{Voucher}: \text{bstr} )$

- Ultra-constrained voucher, AEAD with empty plain text of
  - $\text{external_aad_array} = [ \text{V_TYPE}: \text{int}, \text{PK}_V: \text{bstr}, \text{G}_X: \text{bstr}, \text{CC}: \text{bstr}, \text{ID}_U: \text{bstr} ]$

- Voucher Request/Response
  - $\text{VREQ} = [ \text{G}_X: \text{bstr}, \text{CC}: \text{bstr}, \text{CIPHERTEXT}_RQ: \text{bstr} ]$
  - $\text{VRES} = [ \text{G}_X: \text{bstr}, \text{CC}: \text{bstr}, \text{CIPHERTEXT}_RQ: \text{bstr} ]$
  - Independent of transport

- ACE mapping

- Security processing
Next steps

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

— Reviews?