Privacy-Enhanced Tokens for Authorization in ACE

draft-cuellar-ace-pat-priv-enhanced-authz-tokens

Jorge Cuellar [1], Prabhakaran Kasinathan [1], Daniel Calvo [2]

[1] Corporate Technology, Siemens AG, Germany

[2] Atos Research and Innovation, Spain

IETF 96, Berlin
July 20, 2016

RERUM

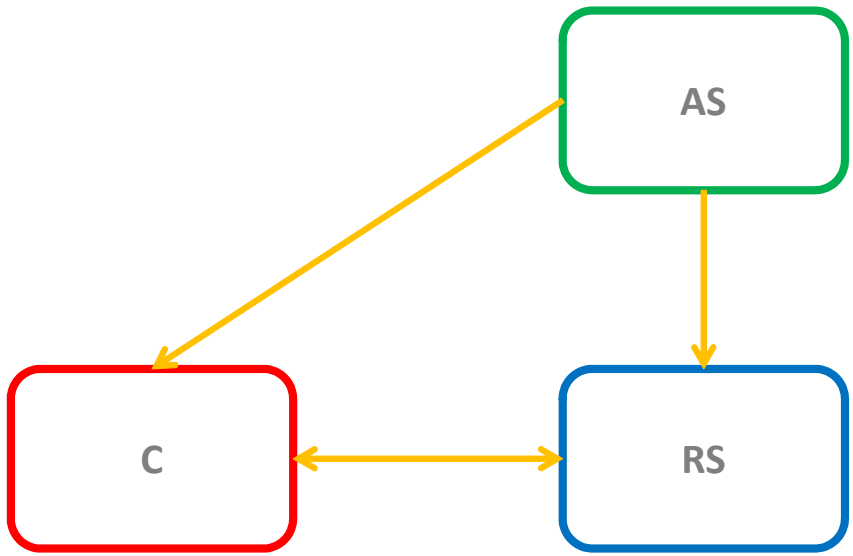
Constrained devices

Memory Constraints	RAM	Flash
C1	10 kB	100 kB

- Powered by battery
- Energy Harvesting

Actors (draft-ietf-ace-actors)

- RS : Resource server
- C : Client
- AS : Authorization Server
- CAS : Client Authorization Server (Optional)



Goals

Privacy

- Confidentiality
- Consent of Resource Owner (RO)
- Non-linkability of Identities of Communication Partners (C & RS)

Authorization & Integrity

- C is allowed to send commands to RS (& replay protection)
- C is allowed to receive data from RS

DoS Resilience

Conflicting Goals . . .

Energy Consumption:

- AES < SHA2 < Transmission < 3DES « ECC

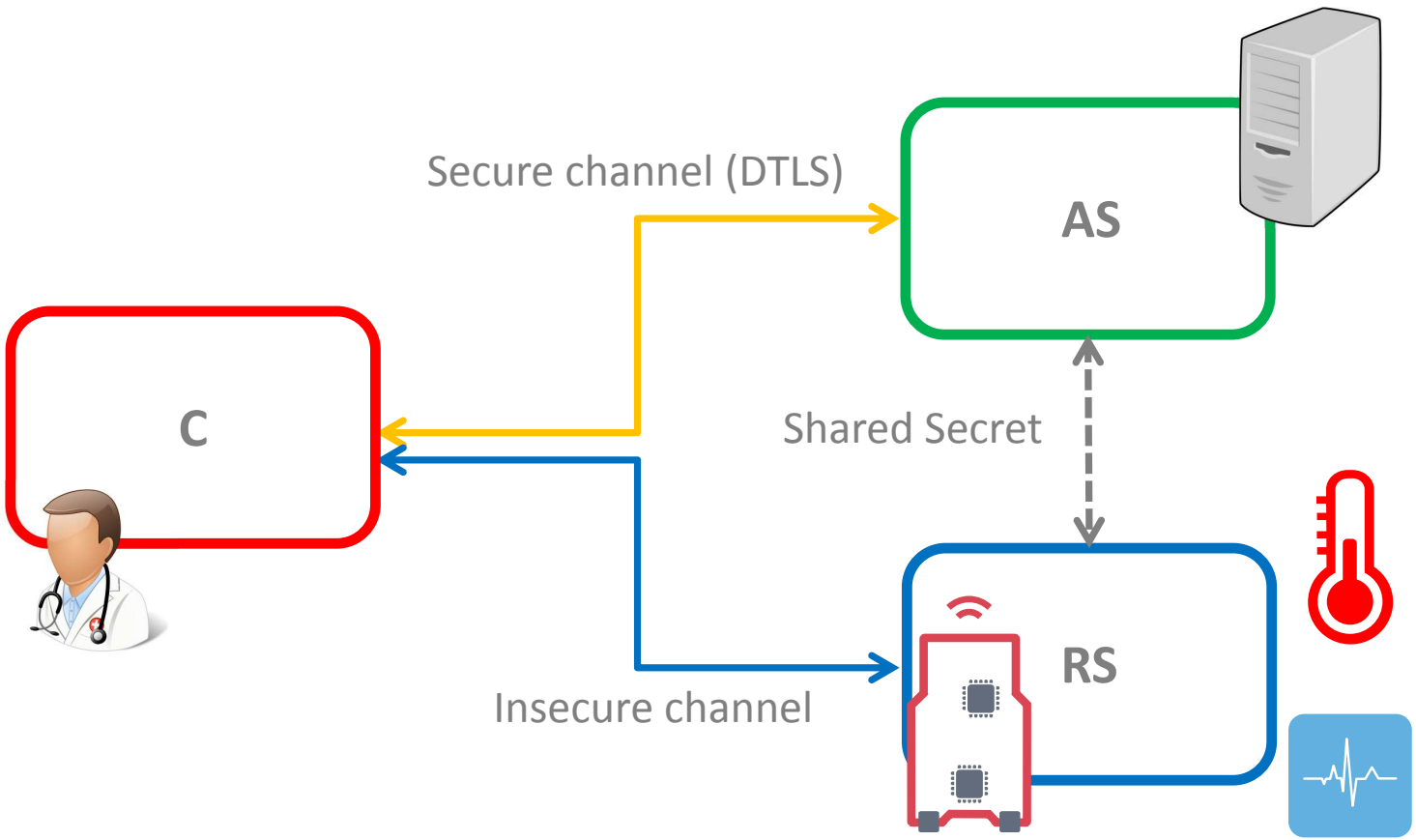
Code Size:

- SHA2 < ECC < 3DES < AES

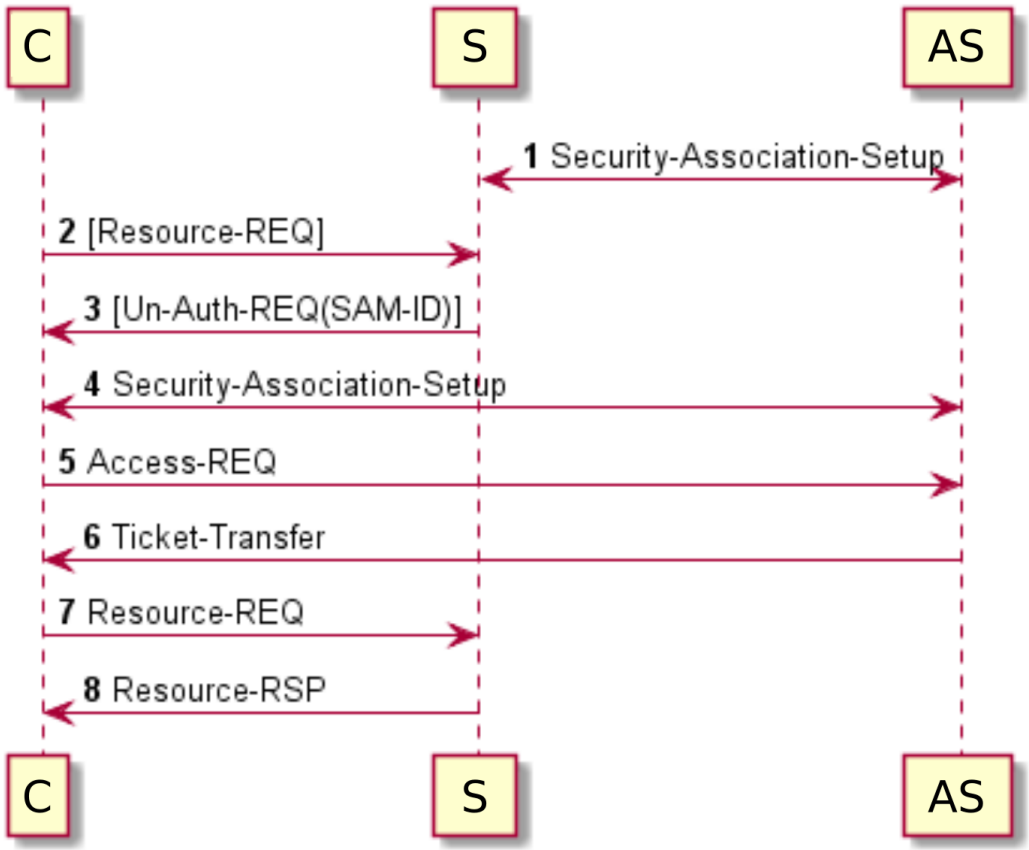
Example: RERUM Remote Board

- DTLS Handshake time (ECC):137 seconds
- DTLS server code footprint: 65 KBytes

DTLS is optional between C<->RS

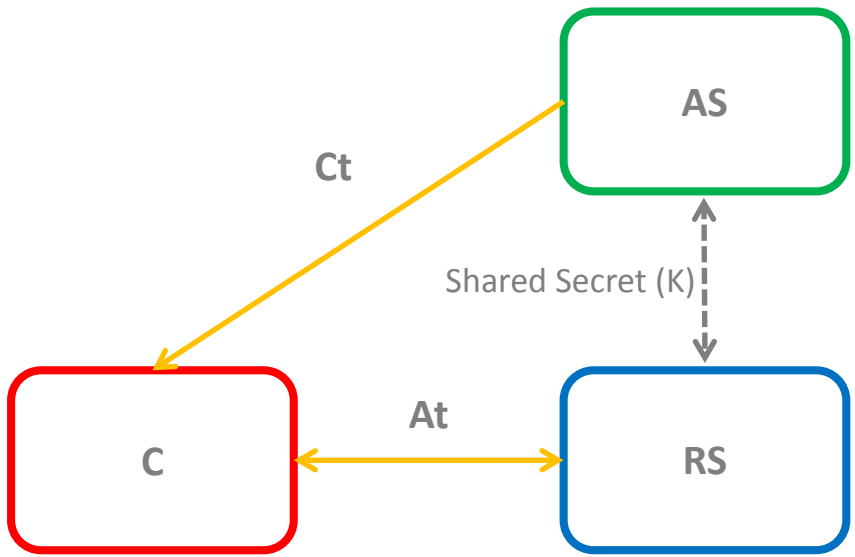


Generic protocol flow



Tokens

- Face
  - Resource
  - Permissions
  - Timestamp
  - Time To Live
- Verifier=f(K,face)
- Client Token (Ct)
  - Face
  - Verifier
  - Additional-Info
- Access Token (At)= [Face,f(Ct, Additional-Info)]



Efficient communication C <-> RS

- Authenticated Encryption (AEAD-CHACHA20-POLY1305) with Verifier
  - Privacy, Confidentiality, Integrity
  - Length(cipherText)= Length(plainText)

Authorization delegated to unconstrained AS

- C and RS can derive keys from the common shared secret

Authenticated Encryption and PoP

- Resilience to DoS and replay attacks
- E.g: Access Token (At)= [Face,f(Ct, CoAP MID)]

Partial implementation in JAVA

- CBOR encoding for token exchanges
- CHACHA20-POLY1305 as one of the Authenticated Encryption Mechanism
- GPL license
- Source Code available in `https://gitlab.atosresearch.eu`

Thank you for your attention!

Questions?

daniel.calvo@atos.net
@danicalvoalonso

Atos Research and Innovation
IoE Lab