Delegated CoAP Authentication and Authorization Framework (DCAF)

draft-gerdes-ace-dcaf-authorize-02

Stefanie Gerdes, Olaf Bergmann, **Carsten Bormann**
{gerdes | bergmann | cabo}@tzi.org

IETF-92, ACE Meeting, 2015-03-24

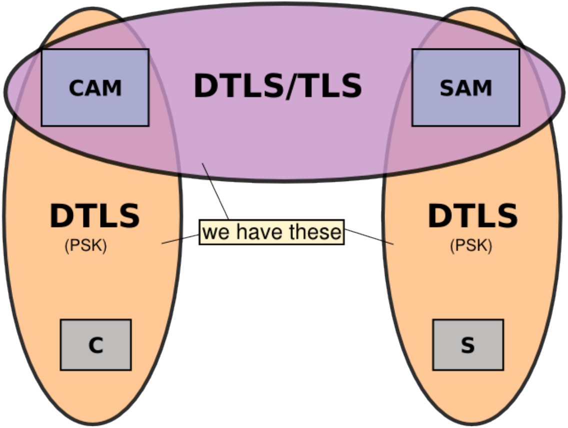
Communication in Constrained Environments

- Constrained Application Protocol (CoAP, RFC 7252)
  - designed for special requirements of constrained environments
  - Similar to HTTP (RESTful architecture style)
    - server has items of interest
    - client requests representation of current state
- Datagram Transport Layer Security (DTLS) binding

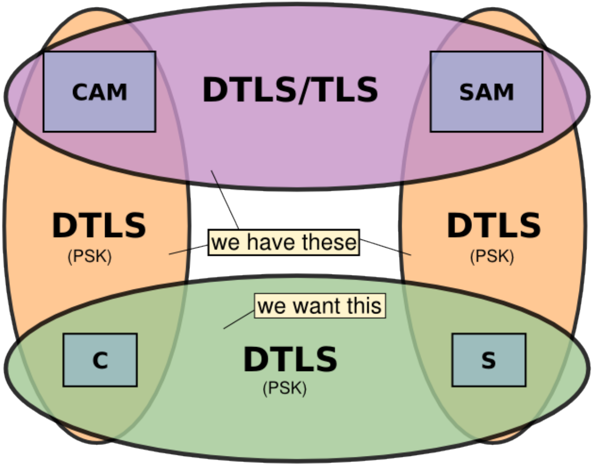
Features of DCAF

- Secure exchange of authorization information.
- Establish DTLS channel between constrained nodes.
- Establish DTLS channel between a constrained and a less-constrained nodes.
- Support of class-1 devices (RFC 7228).
- Use only symmetric key cryptography on the constrained nodes.
- Support of CoAP Observe and blockwise transfer without additional overhead.
- Relieve constrained nodes from managing complex authentication and authorization tasks.

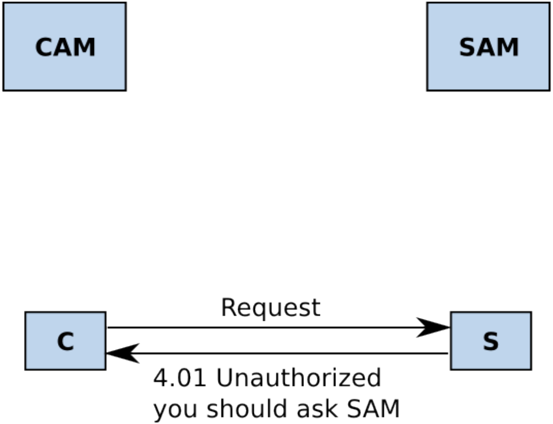
Initial Trust Relationships



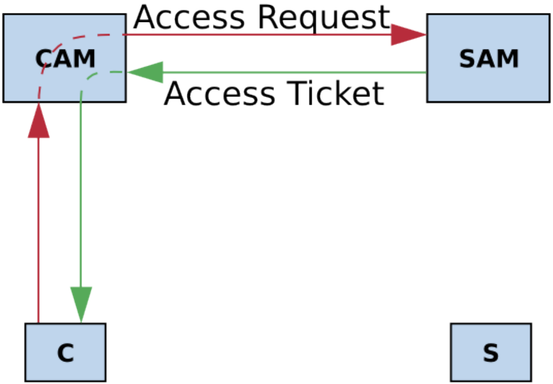
Trust: The Complete Picture



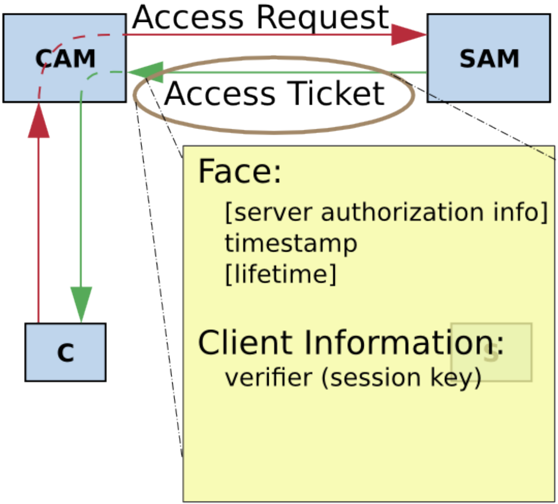
Unauthorized Access Request



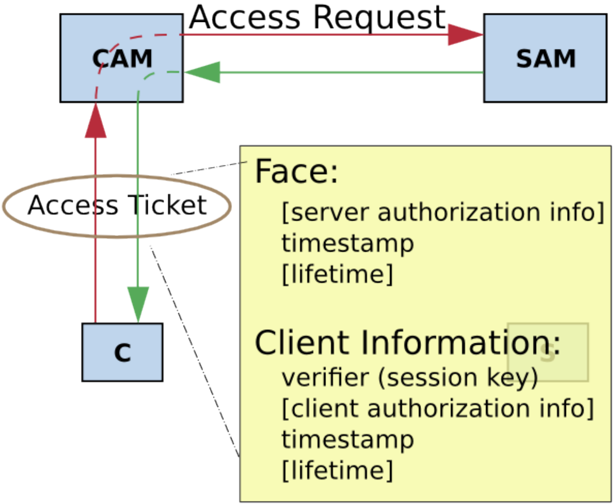
Contact S's Less Constrained Device for Authorization



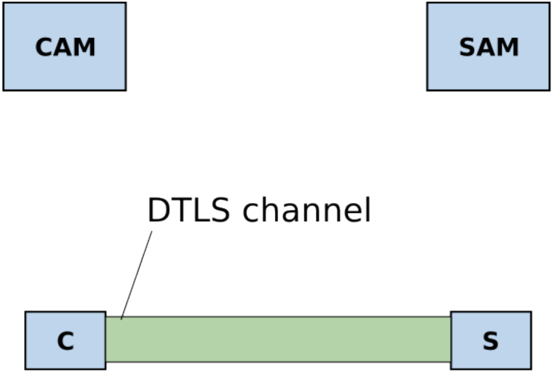
Access Ticket



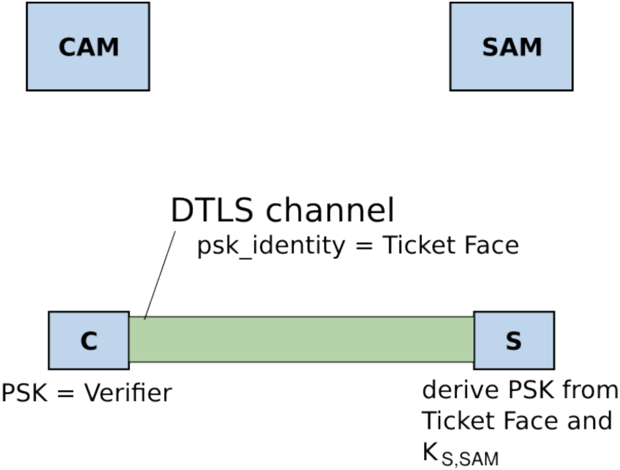
Access Ticket: Adding Client Information



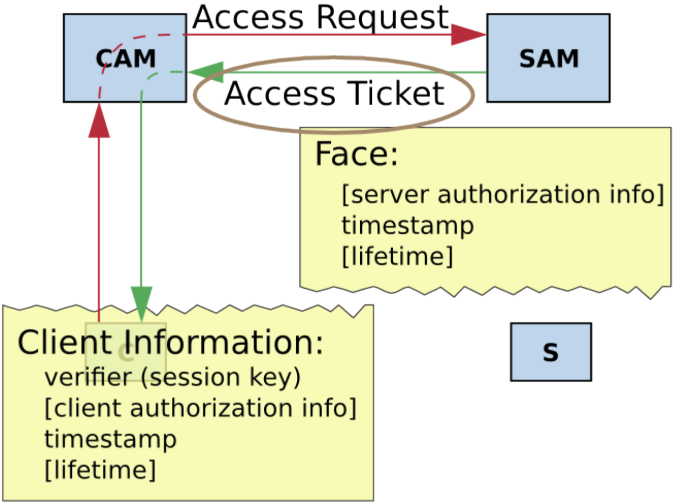
Use Access Ticket to Establish DTLS Channel



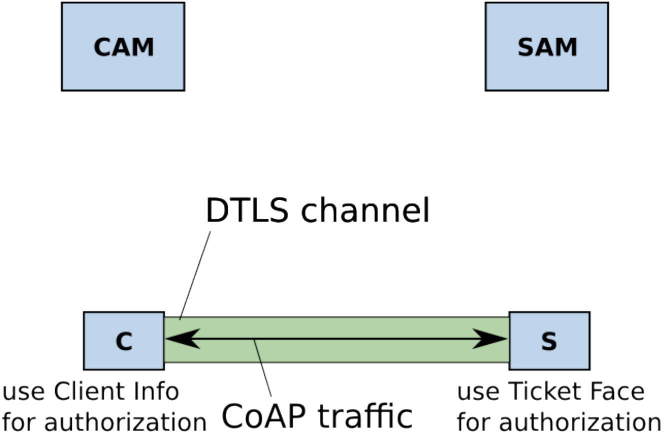
PSK Derivation



Access Ticket Parts



RS Permits Authorized Requests Over DTLS



Lessons learned from the Use Cases:

- In some cases, binary authorization (all authenticated entities have the same authorization) is sufficient.
- Use Cases often require more sophisticated authorization on the client and/or on the server side.

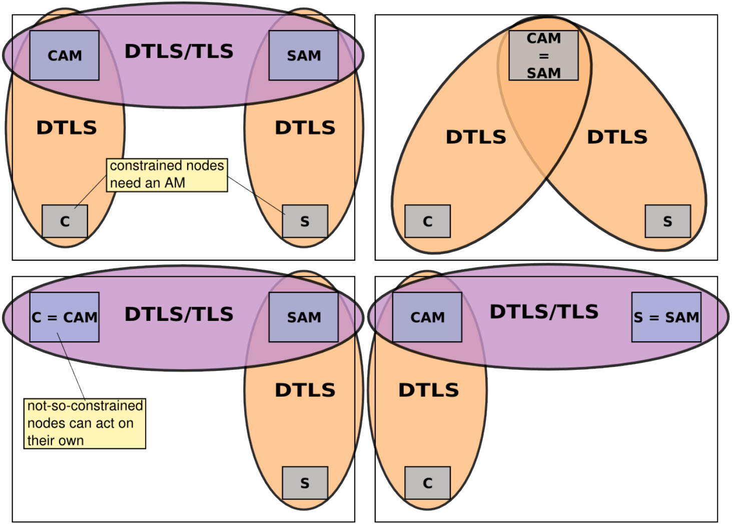
Consequence:

- A solution that always transmits authorization information generates unnecessary overhead.
- Authorization information must be securely transmitted when needed.

Flexibility

- DCAF can be used as a simple protocol for secure transmission of DTLS pre-shared keys (implicit authorization).
- DCAF can additionally securely transmit authorization information to the server and / or the client.
- DCAF defines how combinations of actors work together.
- DCAF can be used as needed.

Combined Actors



Evaluation

Reference implementation adds

- about 440 Bytes Code
- 54 Bytes data for ticket face
- 722 Bytes parser for CBOR payload

to existing CoAP/DTLS server (ARM Cortex M3).

How to proceed

- Define interaction with protocols on the less-constrained level (how to use DCAF with existing solutions such as OAuth)
- Accept DCAF as one of the building blocks that ACE is working on.