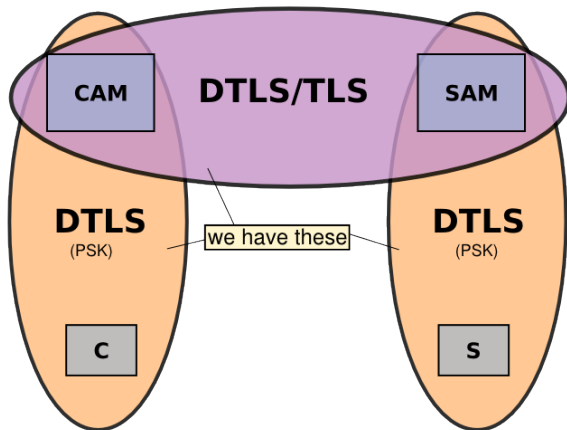# Using DCAF with Less Constrained Devices
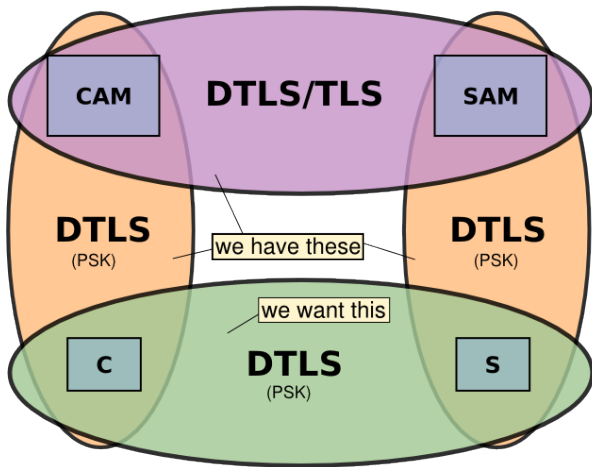
draft-gerdes-ace-dcaf-examples

Stefanie Gerdes, **Olaf Bergmann**, Carsten Bormann
{gerdes | bergmann | cabo}@tzi.org
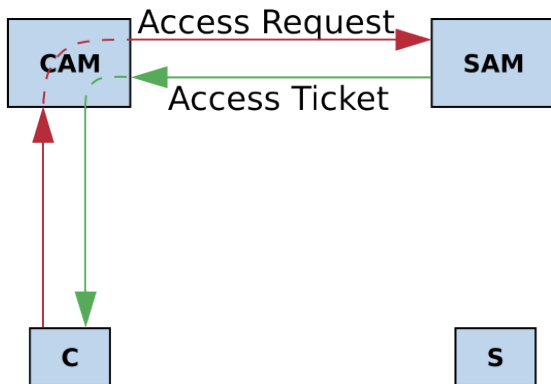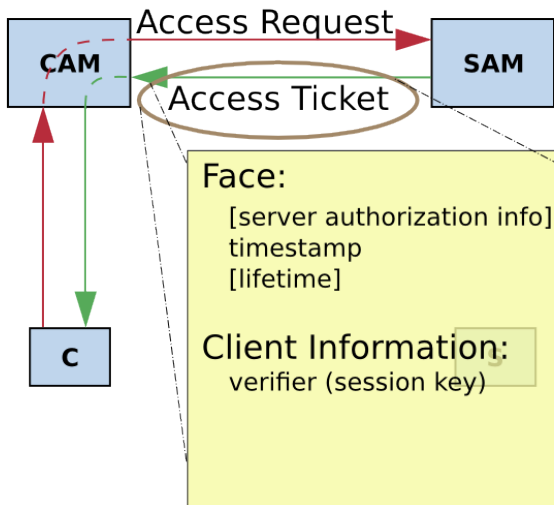
2015-07-22

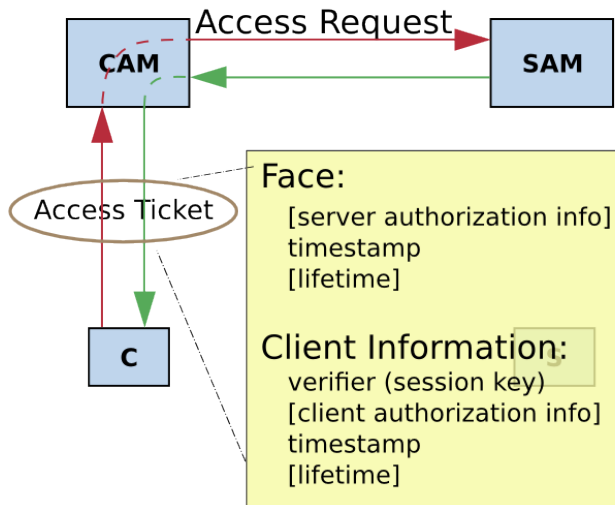# Initial Trust Relationships

Trust: The Complete Picture

Contact S's Less Constrained Device for Authorization

Access Ticket

Access Ticket: Obtaining an Access Ticket

CAM

Access Request

SAM

Access Ticket

C

Face:
[server authorization info]
timestamp
[lifetime]

Client Information:
verifier (session key)
[client authorization info]
timestamp
[lifetime]

Access Ticket Parts

PSK Derivation

CAM

SAM

DTLS channel
psk_identity = Ticket Face

C

S

PSK = Verifier

derive PSK from
Ticket Face and
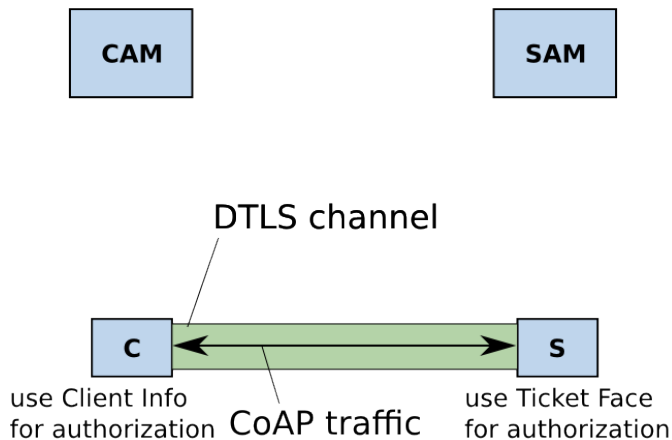$K_{S,SAM}$
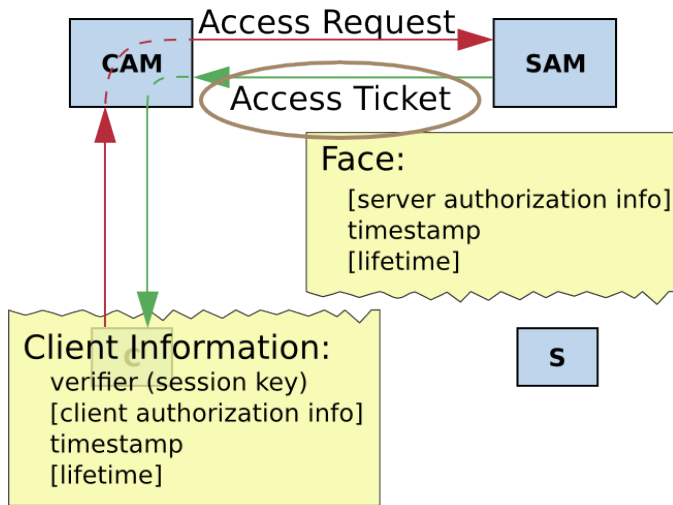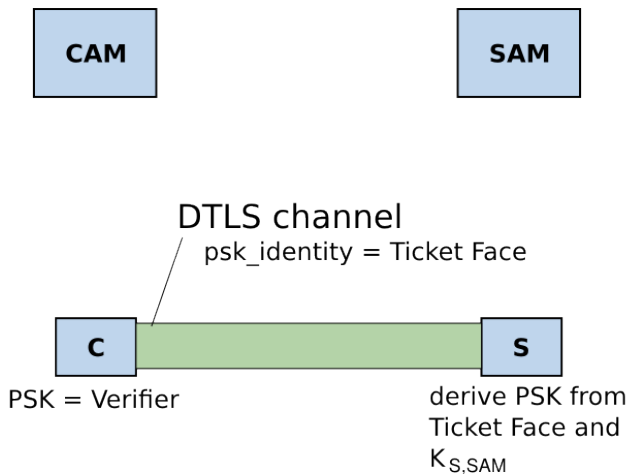
Authorized Requests Over DTLS

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.

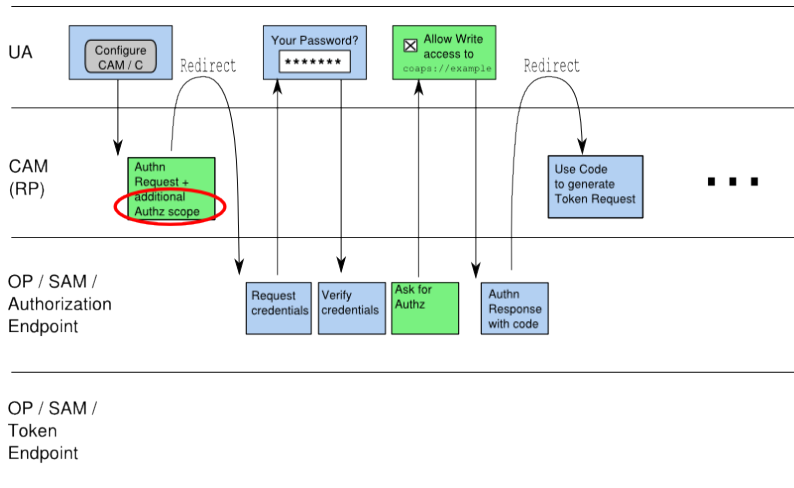# Authenticated Authorization on the Less Constrained Level
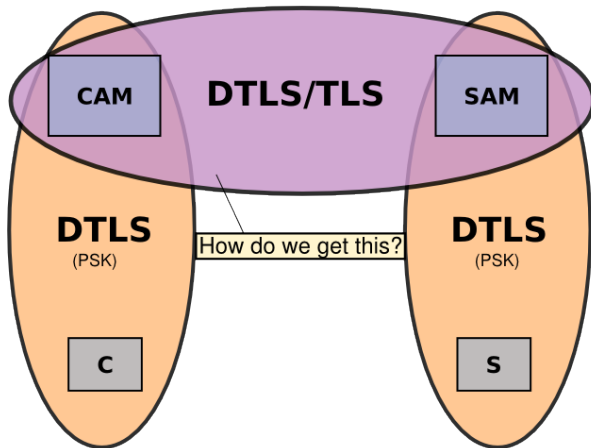
Example: Posting Temperature Values on a Blog

- ▶ Sarah has a blog where she posts details about her daily work
- ▶ During a heat wave, she wants her temperature sensor to autonomously post the current room temperature of her office in the blog.
- ▶ She is registered with an OpenID Provider

Use OpenID Connect with OAuth and DCAF

- ▶ Use OpenID Connect for authentication on the less constrained level.
- ▶ Use OAuth for authorization on the less constrained level.
- ▶ Use an OAuth Authorization Endpoint that can speak OAuth and DCAF and issues DCAF Tickets.
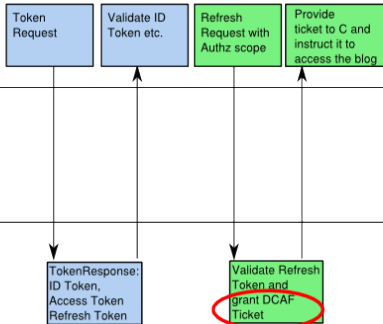
Flow Part 1: Authentication with OpenID Connect

Flow Part 2: Authorization with OAuth/DCAF

Summary

- Use DCAF to provide simplified authentication and authorization to constrained devices.
- Enable constrained devices to enact the principals' security objectives.
- Use less constrained nodes for the more difficult tasks.
- Use common protocols on the less constrained level that interoperate with DCAF.

Next Steps

- Describe more interaction examples (please feel free to contribute).
- Standardize DCAF as one of the ACE building blocks.