draft-cuellar-ace-pat-priv-enhanced-authz-tokens-00

# IETF 93
# PraGue 2015

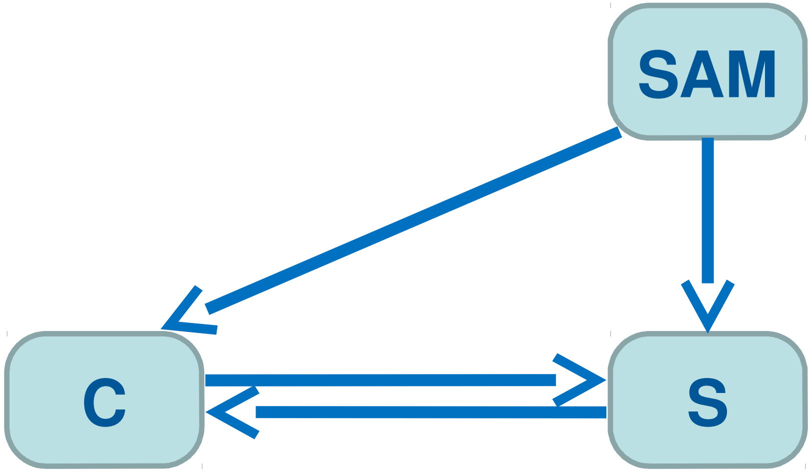
# Our focus: Constrained Devices

- Powered by battery
  - Button cell
  - AA battery
- Energy Harvesting

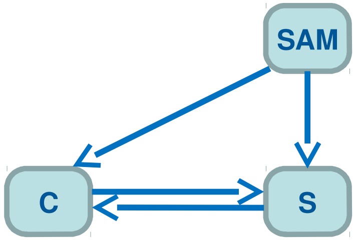
| Memory Constraints | RAM | Flash |
|---|---|---|
| C1 | 10 kB | 100 kB |

# Actors (as in DCAF)

- **S** Server: hosts & represents CoAP resource(s)
- **C** Client: attempts to access a resource on S
- **SAM** Server Authorization Manager: prepares and endorses authentication and authorization data for S



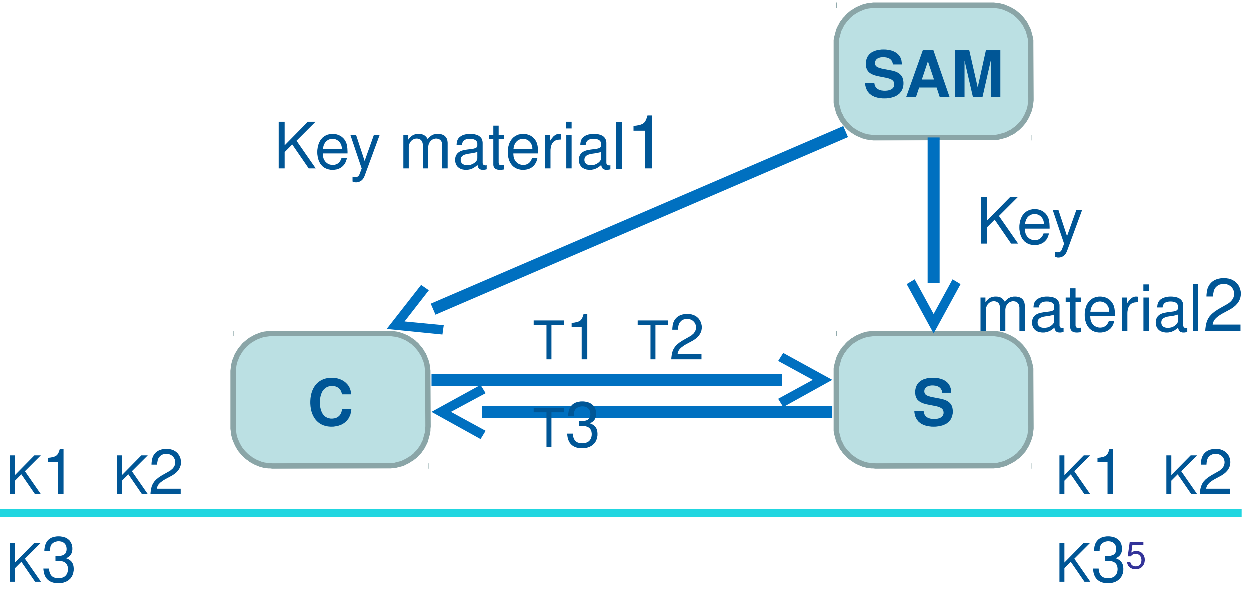
# Possible (conflicting) Goals



- **Privacy**
  - Confidentiality
  - Consent of Resource Owner (RO)
  - Non-linkability of Identities of Communication Partners (C & S)
- **Authorization & Integrity**
  - C is allowed to send commands to S
  - C is allowed to receive data from S
- **DoS Resilience**
- **Energy Consumption:**
  - AES < SHA2 < Transmission < 3DES << ECC
- **Code Size:** SHA2 < ECC < 3DES < AES

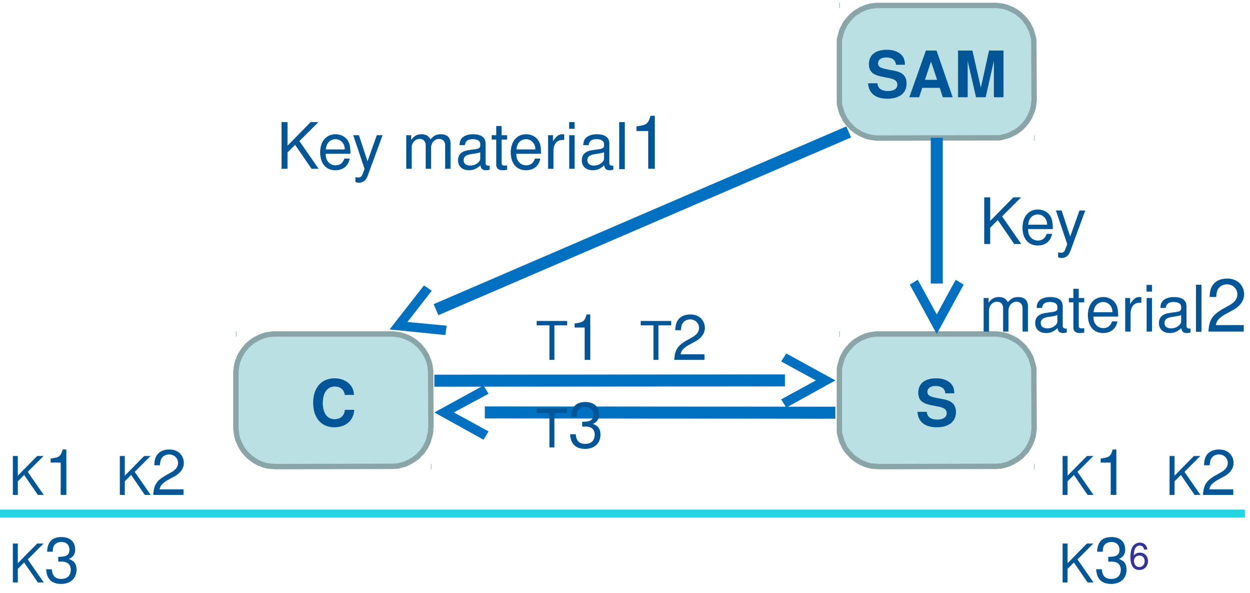
# One solution possibly does not fit all

- In some cases Privacy is not an issue
- In some cases, C gets one response per request
  - in others, C subscribes to a stream
- In some cases DoS resilience only under stress…



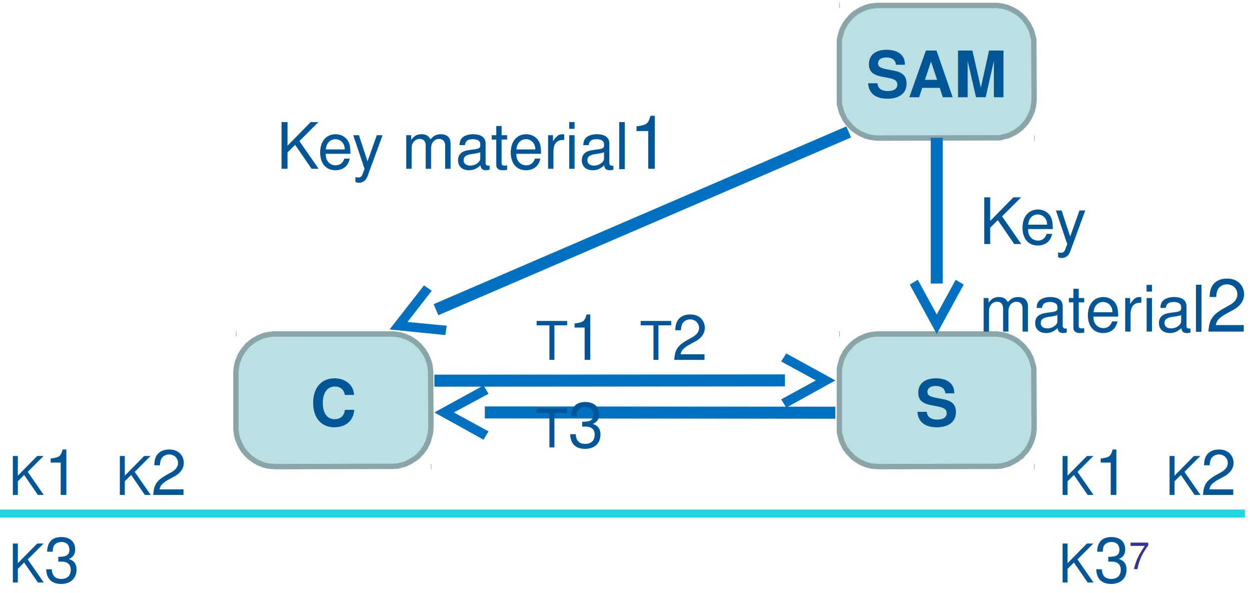
# One solution possibly does not fit all

- … Many ways of constructing tokens/keys
  - Given some key material
    - The has trees in the draft ia only one example
- … Many ways of using them
  - As One-Time-Pads
  - For DTLS
  - AES/MACs
  - TESLA



# A possible way forward

- Define a generic protocol
- … with some very lightweight versions
- Based on CoAP
  - But not necessarily on DTLS (optional)


SAM
Key material1
Key material2
C
S
T1 T2
T3
K1 K2 K3
K1 K2 K3