
draft-cuellar-ace-pat-priv-enhanced-authz-tokens-01

IETF 94
TOKYO 2015

Our focus Constrained Devices

- ◆ Low-Cost Crypto
 - ✦ Energy, Message Size

- ◆ for low-cost devices
 - ✦ Energy Harvesting
 - ✦ Applications like agriculture in developing countries

Possible (conflicting) Goals

◆ Privacy

- ✦ Confidentiality
- ✦ Consent of the 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

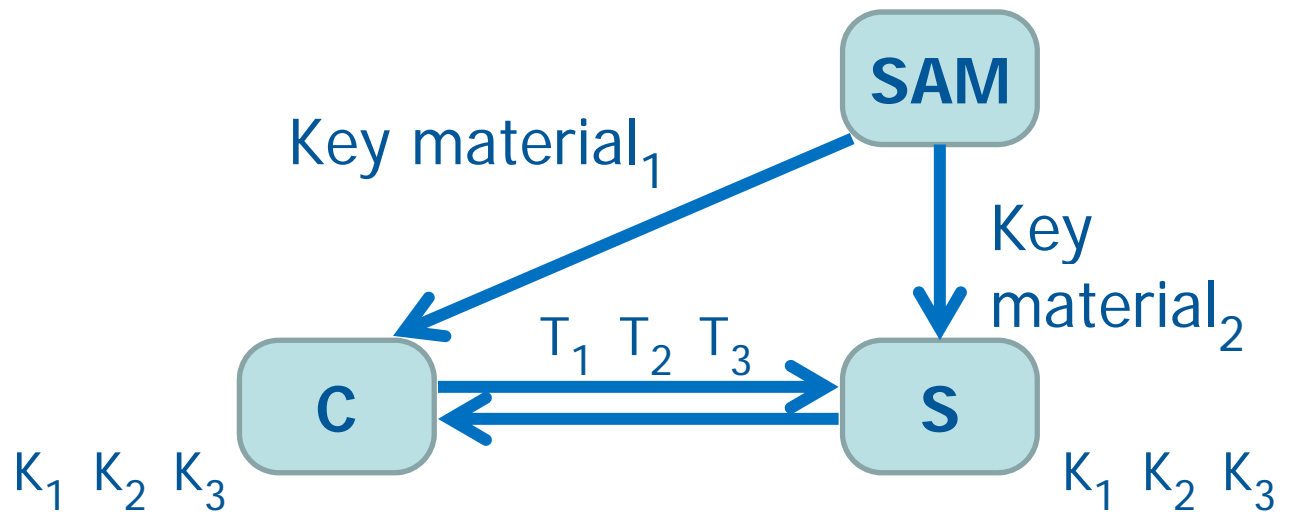
◆ Energy Consumption

◆ Message Size

- ✦ Padding
- ✦ Headers

One solution possibly does not fit all

- ◆ ... Many ways of constructing tokens/keys
 - ✦ Given some key material
- ◆ ... Many ways of using them
 - ✦ As one-time-pads
 - ✦ For DTLS
 - ✦ AES/MACs



A Low-Cost Solution

◆ Use Pseudo-Random Generators

- ◆ An attacker may not distinguish if a (long) bit stream
 - ✧ is purely random
 - ✧ has been generated by a Pseudo-Random Generator $G(k)$
 - where k is a ("small": 128, 256 bits) random key
- ◆ Use the long psuedo-random stream as a set of "Tokens and keys"



A Low-Cost Solution

- ◆ Propose to Use ChaCha 20 (or ChaCha7?) as a pseudo-random generator
- ◆ Use One-Time Pads for Confidentiality
 - ✦ No need for padding