Motivation

- Align draft-cuellar-ace-pat-enhanced-privacy-authz and
  - draft-gerdes-ace-dcaf-authorize
- Other drafts in ACE reuse DCAF message types
  - draft-seitz-ace-core-authz
  - draft-bergmann-ace-dcaf-cose
- Provide common message type classes
  - Describe effects of message types
  - Describe protection requirements for messages transported within such a message
- Provides common content types
- Helps solution designers to determine the security requirements for certain messages
- Solution designers can implement the message type classes they require for their solution
Global View

(0) CAM <=> SAM Security Context Setup
(1) C --> S Unauthorized Resource Req
(2) S --> SAM Token Request
(3) SAM --> S Token Response
(4) S --> C SAM Information
(5) C --> CAM Access Request
(6) CAM --> SAM Ticket Request
(7) SAM --> CAM Ticket Grant
(8) CAM --> C Ticket Transfer
(9) CAM --> C Client Authoriz. Info
(10) C <==> S Security Association
(11) C --> S Authorized Resource Req
(12) S --> C Resource Response
Main Exchange

(3) SAM --> S  Token Response

(7) SAM --> CAM  Ticket Grant
(8) CAM --> C  Ticket Transfer

[(10) C <==> S  Security Association]

(11) C --> S  Authorized Resource Req
(12) S --> C  Resource Response
The Key Material allows C and S to
- generate keys
- generate Tokens
- verify Tokens
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
Future Work

- Provide more detail for existing message type classes
- Provide examples how the messages are used in different solutions
- Add missing message type classes