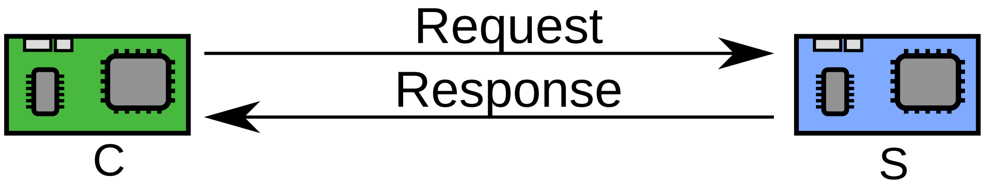
2014-05-05: ACE formed

- “Authentication and Authorization
  for Constrained Environments”
- Informational documents:
  - RFC 7744: “**Use Cases** for ACE”
  - draft-ietf-ace-actors:
    “An **architecture** for ACE”, **problem statement**
- Solution drafts:
  - currently: applying OAuth framework to IoT

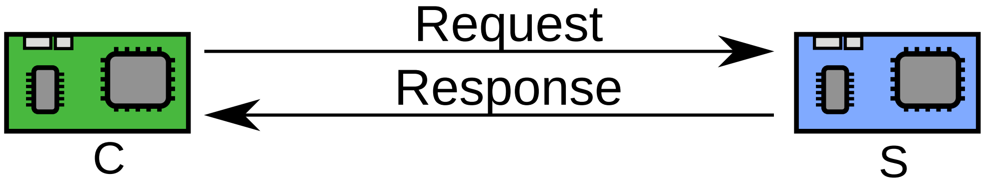
ACE: Scenario to be protected

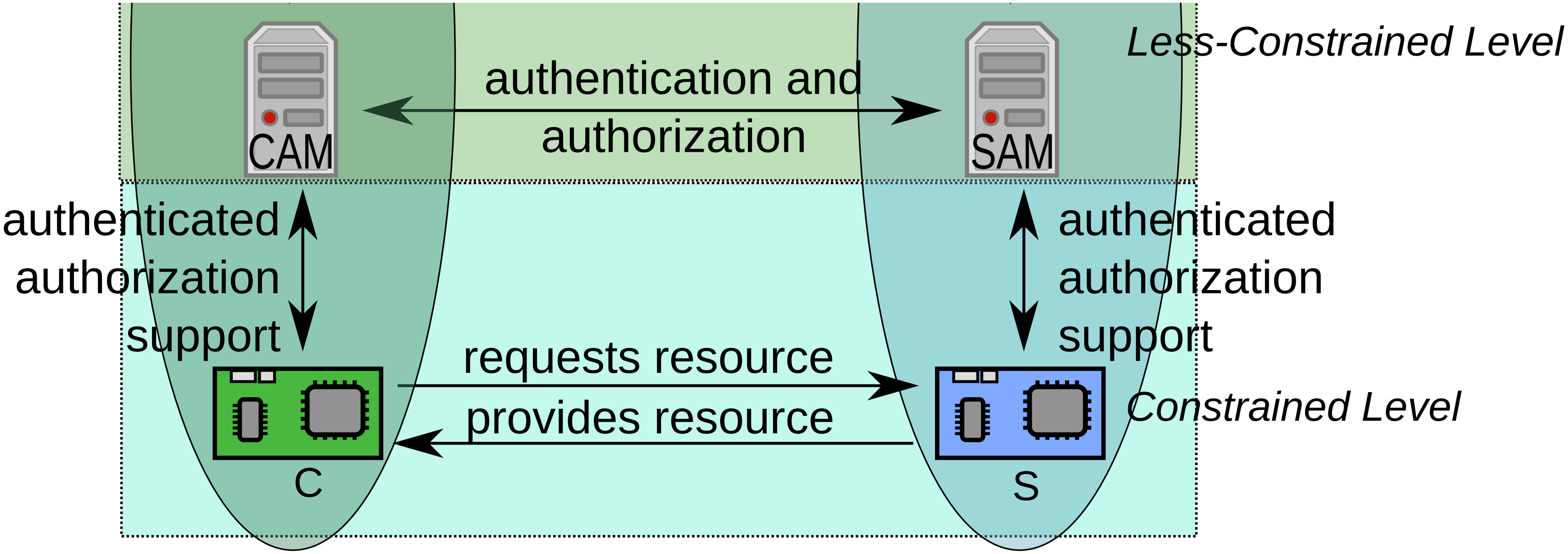
- C and (R)S may not know each other
- C and (R)S may not have the same principal
- C and (R)S may be constrained nodes

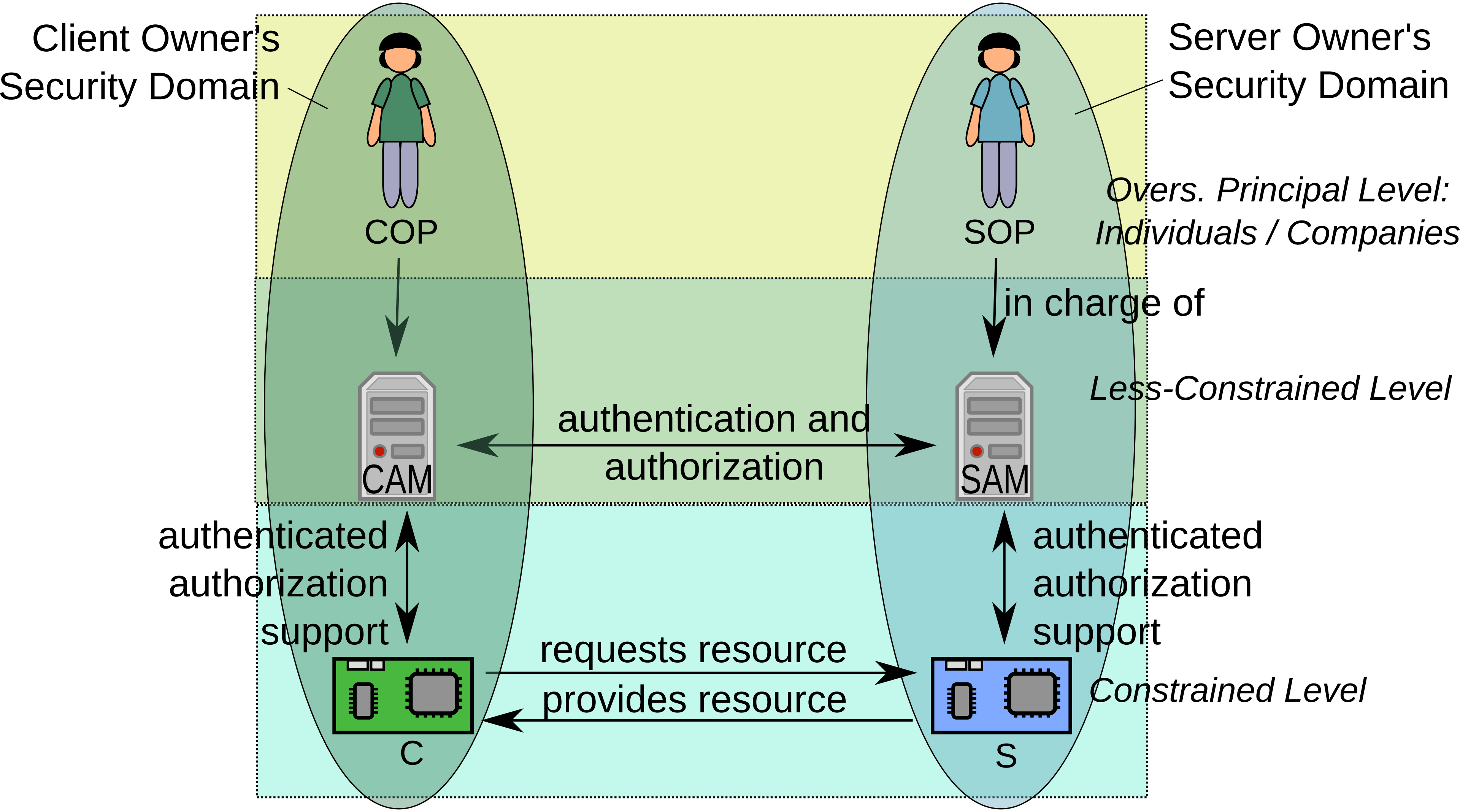


Make good use of less-constrained nodes

- C and RS may be too simple to run detailed business logic
  - Much more straight-forward to employ existing web-based systems for that
- Pair C and RS with a less-constrained node for running the business logic: C ➔ CAM, RS ➔ SAM


Request
Response
C
S


Less-Constrained Level
CAM
authentication and
authorization
SAM
authenticated
authorization
support
authenticated
authorization
support
requests resource
provides resource
Constrained Level
C
S



Client Owner's Security Domain

Server Owner's Security Domain

COP

SOP

Overs. Principal Level: Individuals / Companies

in charge of

Less-Constrained Level

CAM

SAM

authentication and authorization

authenticated authorization support

authenticated authorization support

requests resource

provides resource

C

S

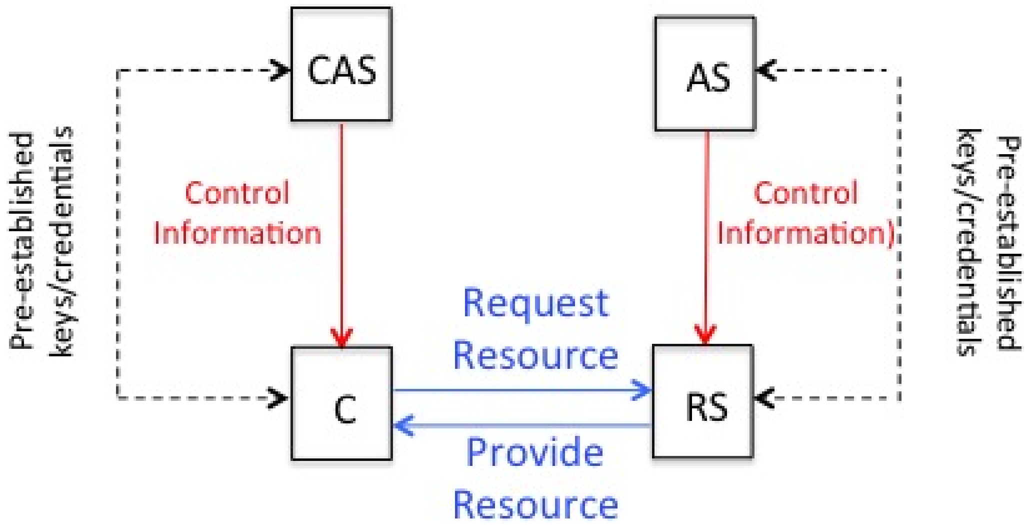
Constrained Level

ACE Architecture

- Covers all variants including cross-domain settings.

Legend:

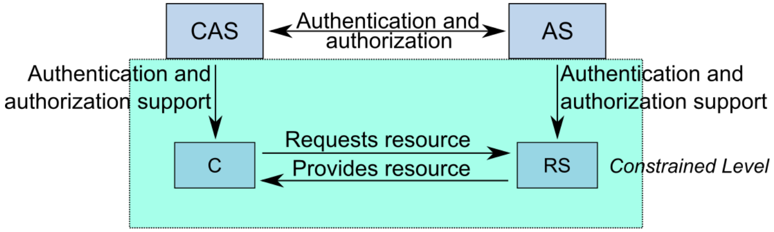
- Information flows in solid lines (actual message flow between the actors may be different).
  - Resource access (based on CoAP)
  - Control information (authorization information, keys, etc.)
  - Information flow may need to be secured end-to-end through intermediary devices

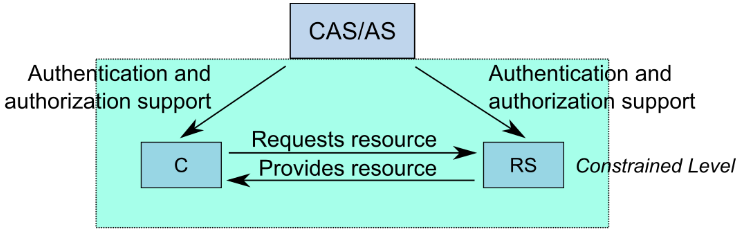


Information flows may be protected with session-based security (DTLS) or data object based security (COSE)

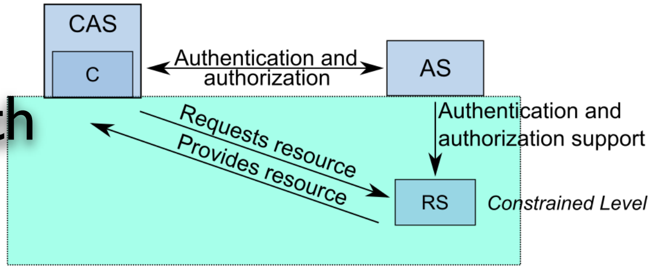
Comprehensive model: map to fewer components

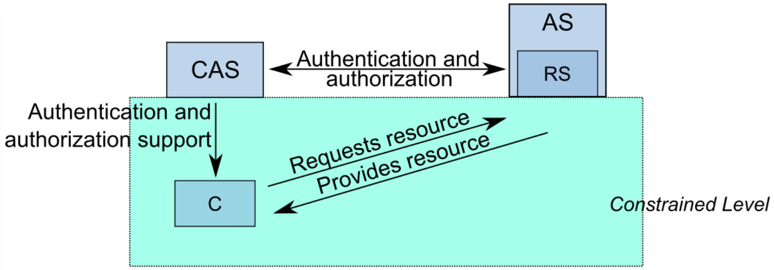
- Roles can be combined into a single instance


CAS
Authentication and authorization
AS
Authentication and authorization support
Authentication and authorization support
C
Requests resource
Provides resource
RS
Constrained Level

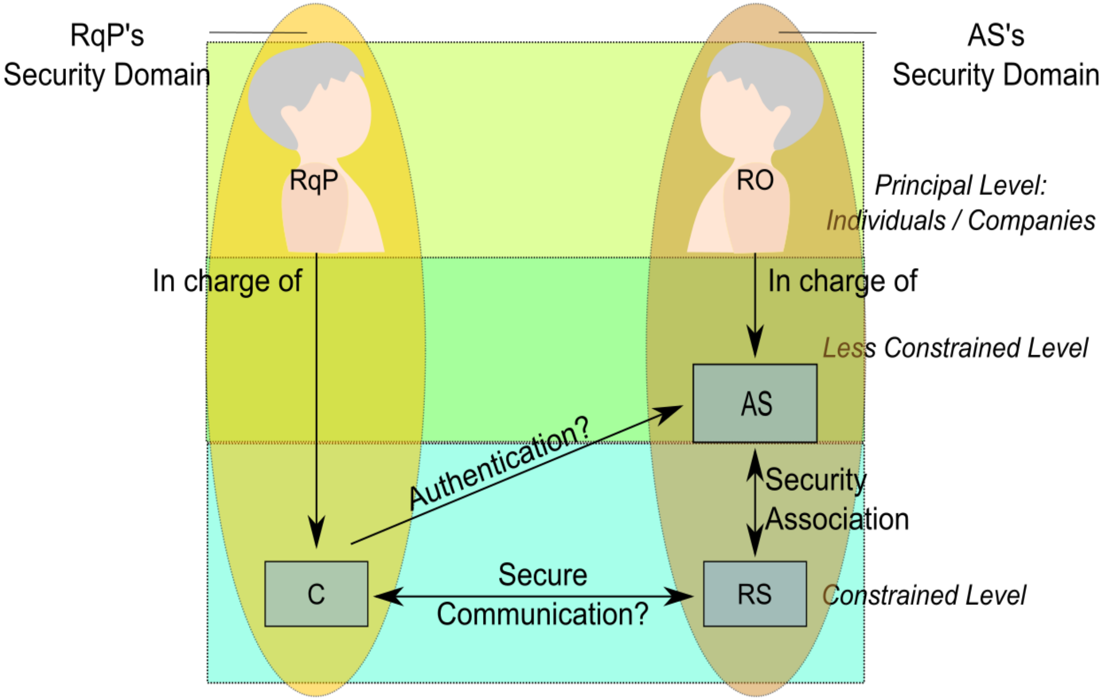

CAS/AS
Authentication and authorization support
Authentication and authorization support
C
Requests resource
Provides resource
RS
Constrained Level

OAuth 2.0


CAS
C
Authentication and authorization
AS
Requests resource
Provides resource
Authentication and authorization support
RS
Constrained Level


CAS
Authentication and authorization
AS
RS
Authentication and authorization support
Requests resource
Provides resource
C
Constrained Level

- C needs Authentication and Authorization policies for AS and RS
- These now need to be pre-installed in C
- Mechanisms for that not defined in ACE today



Shaping the Security Workflows

- Stakeholders, Principals
- Less-constrained nodes
- Constrained nodes

- Device Lifecycle
- Authorized, authenticated delegation