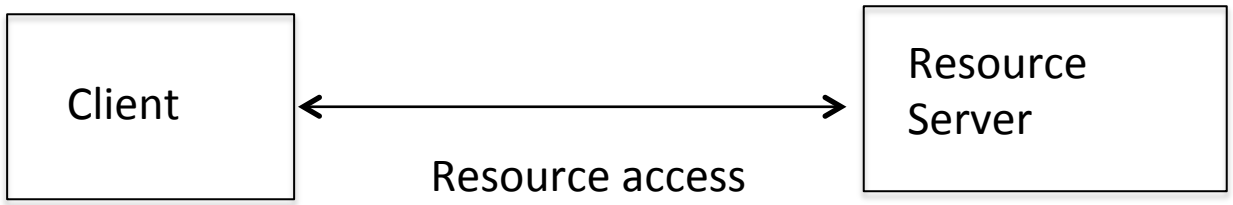
Authorization architecture sketches

draft-selander-core-access-control-02
draft-gerdes-core-dcaf-authorize-02
draft-seitz-ace-design-considerations-00

Göran Selander
IETF 89 ACE BOF
March 5, 2014

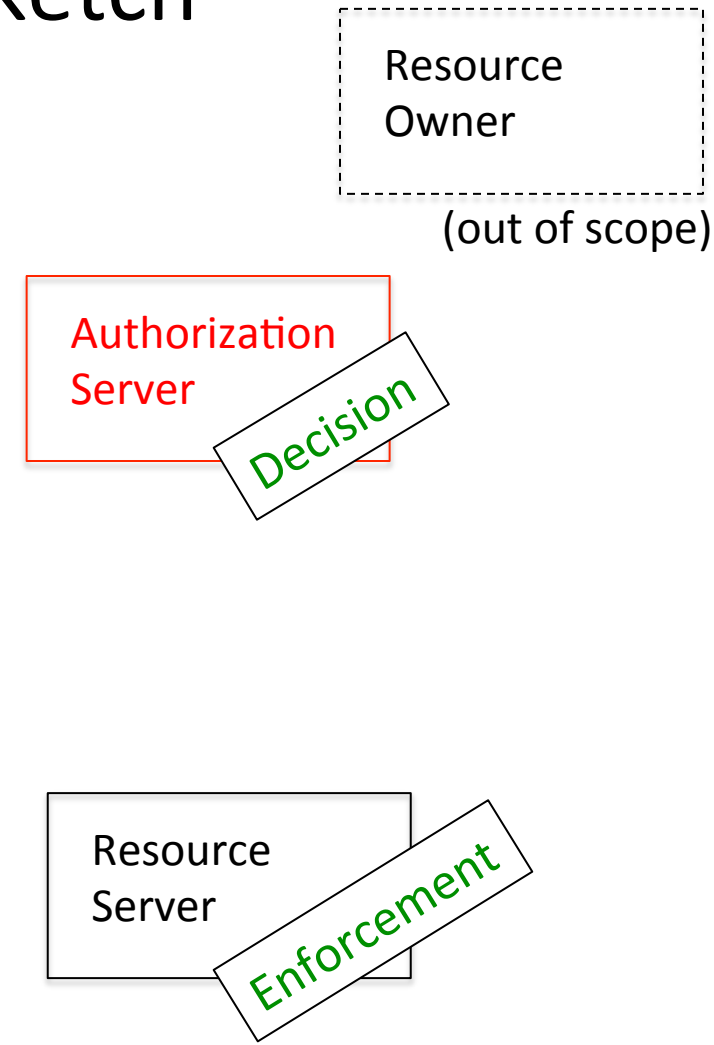
Architecture sketch

- Goal: Protected access for authorized client C to resources on RS allowing explicit and dynamic access policies



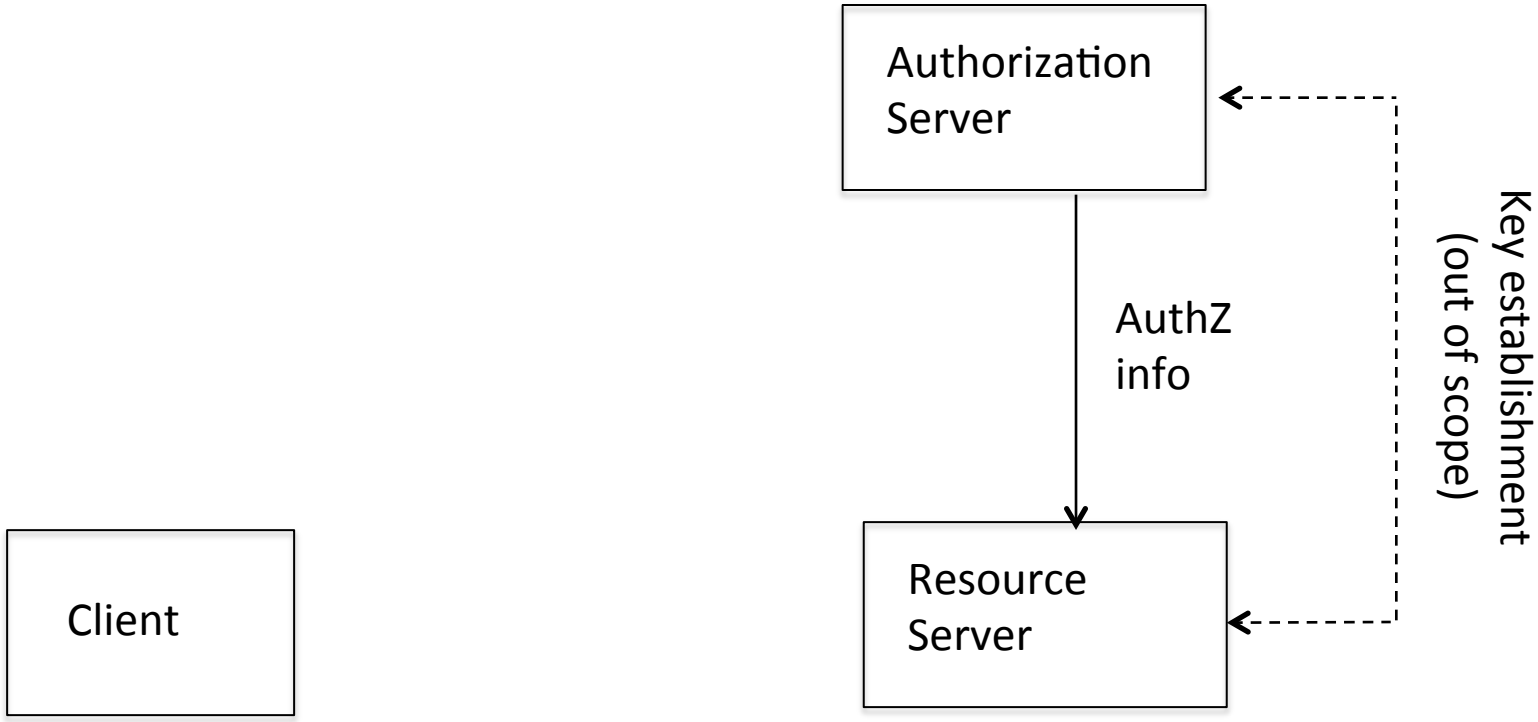
- But constrained devices may be unable to handle management and decisions with generic access control polices

Architecture sketch



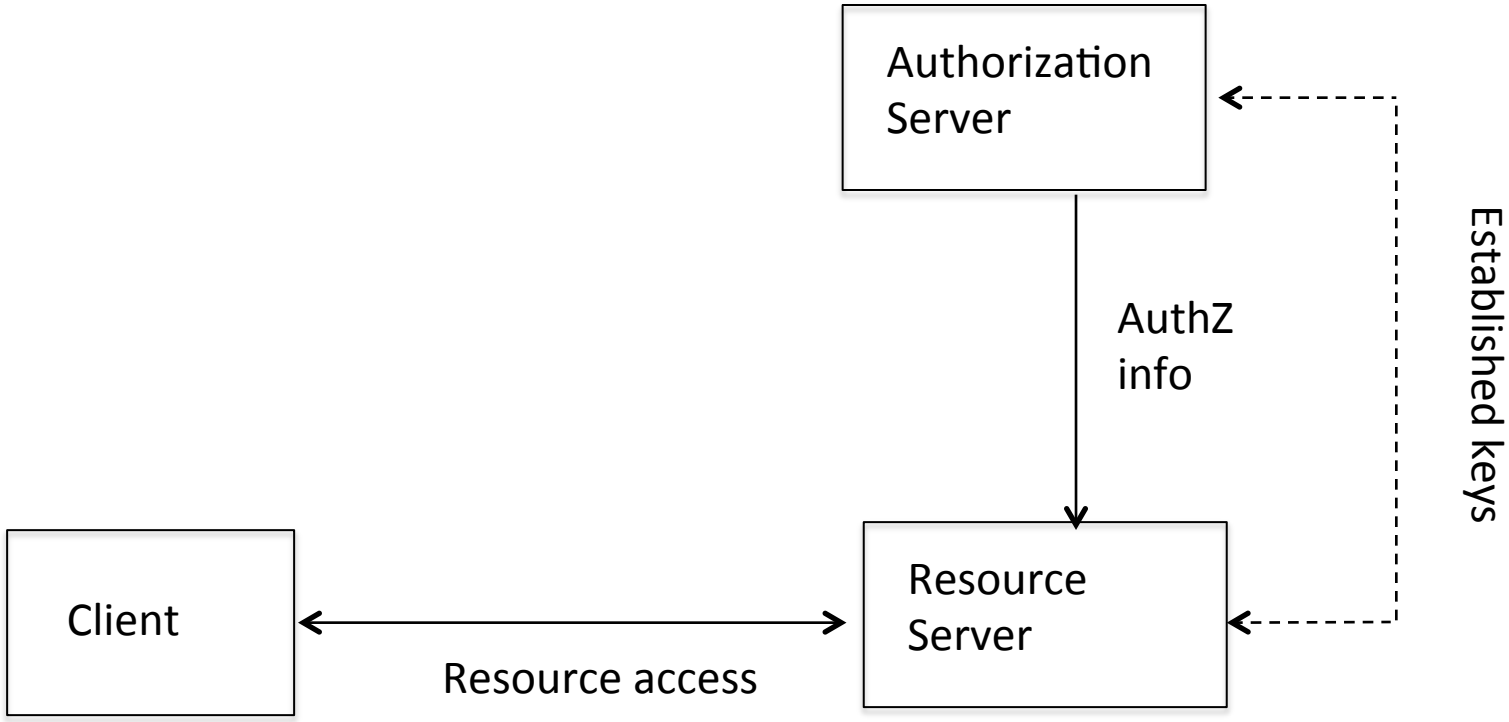
- Separate authorization decision from enforcement
- Introduce less constrained node called AS

Information flow: authorization info



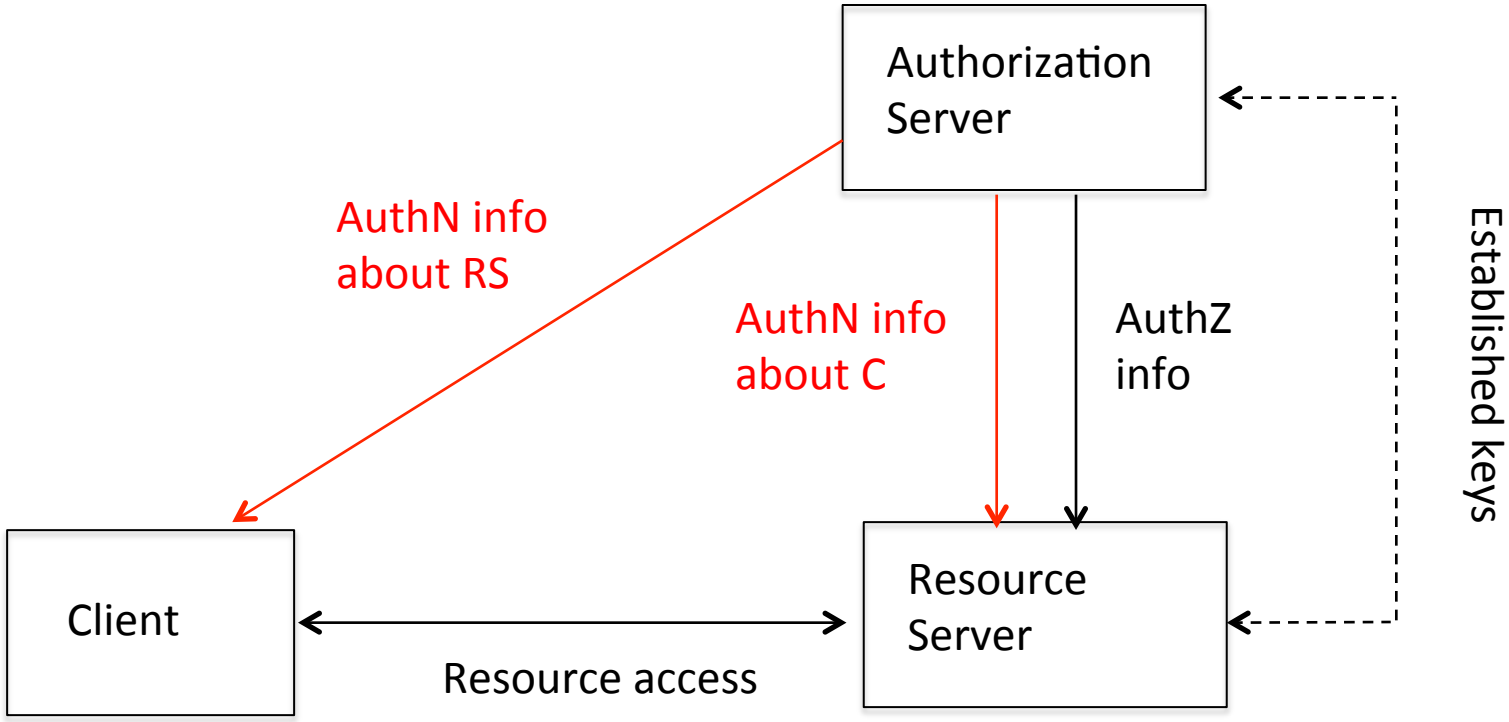
- The RS must authenticate the authorization info and that it comes from a trusted AS

Information flow: resource access



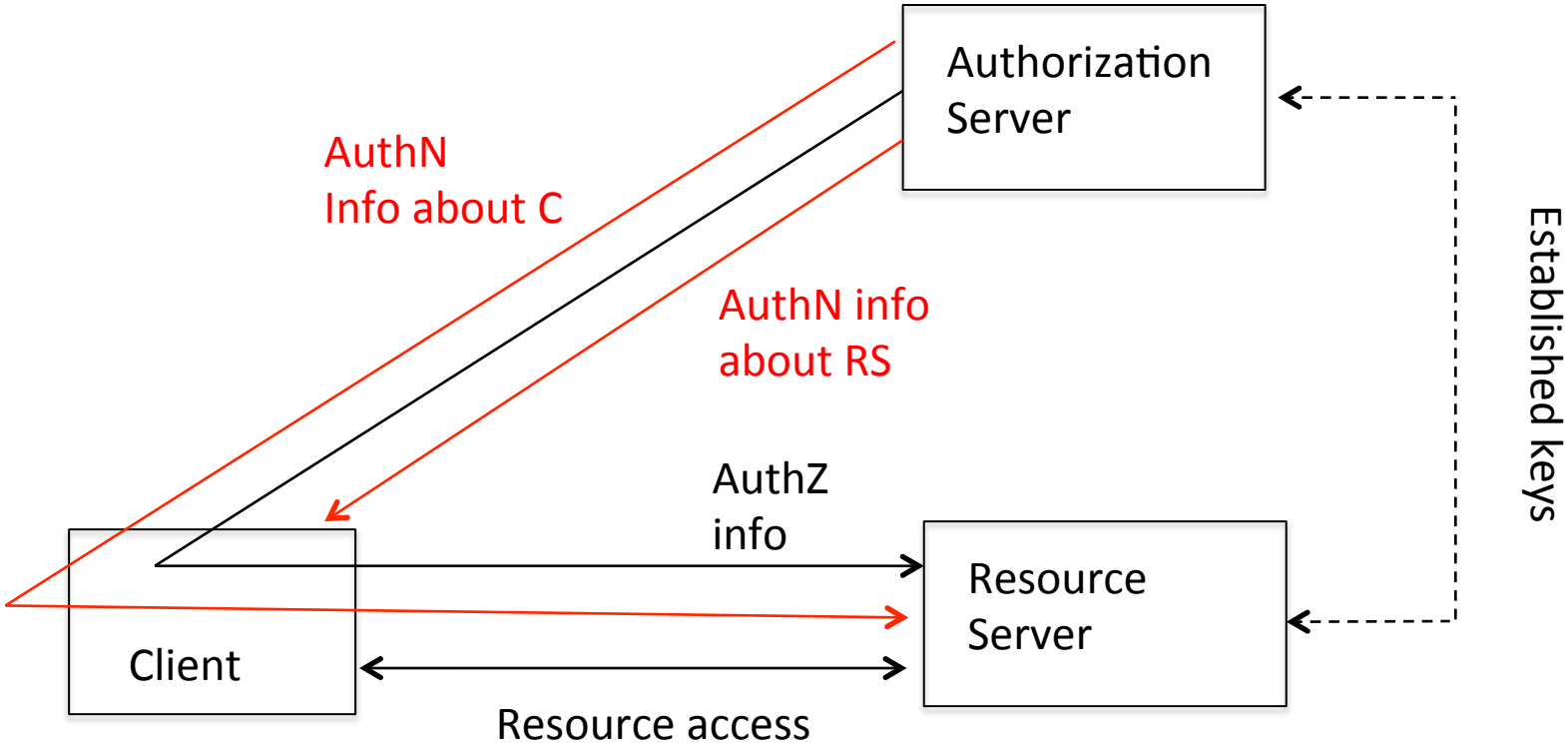
- The RS enforces access control based on authZ info
- Multiple resource requests as long as authZ info is valid

Information flow: Keys for protecting resource access



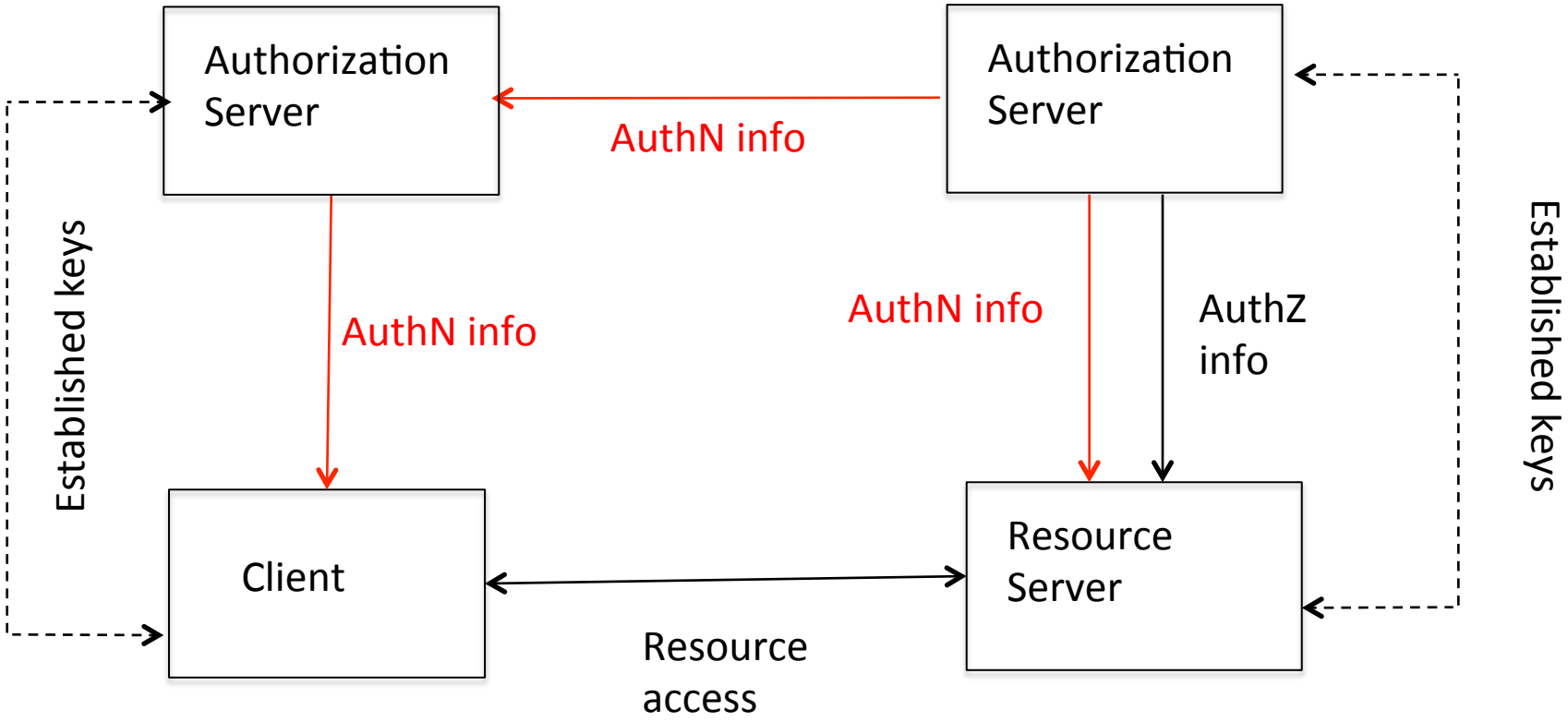
- The RS must be able to verify that a requesting Client is encompassed by the authorization information
- AS may support key management between C and RS

Alternative information flow



- RS and AS may not be connected at the time of the request

Cross domain



- Alternative information flows are possible

Design considerations

- Need multi-party security protocol
  - Profile existing security protocol? Which protocol?
  - Consider tradeoffs e.g. between messaging and crypto relevant for constrained environments
- Session security or object security or hybrid?
  - E.g. securing transfer of authorization information
- Symmetric or asymmetric keys
  - for verifying authorization information?
  - for establishing security between the parties
- Is revocation required or is authZ info with short time validity sufficient?
  - Access to revocation information?

Thank you!

Questions/comments?