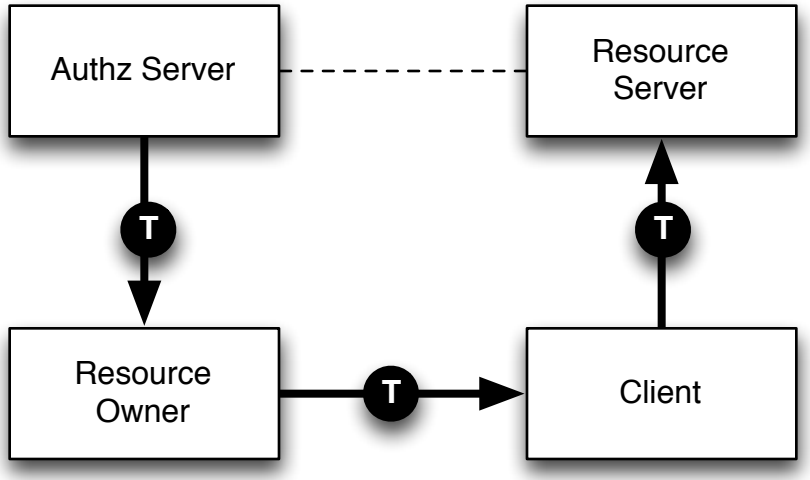
Use Cases / Requirements for JOSE

What do we want to do?

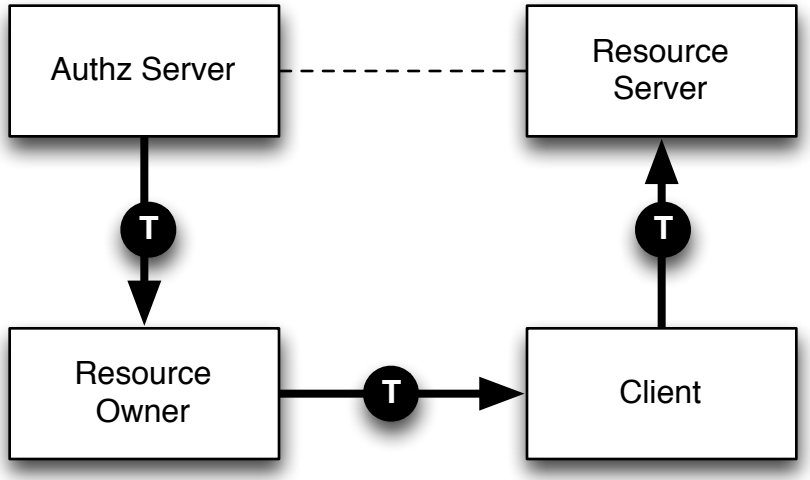
- Obvious: Sign and Encrypt JSON Objects!
- What's the next level of detail?
- Couple of levels of requirements
  - Cryptographic properties
    - Which features do we want to port over from S/MIME
  - Encoding properties

OAuth / Tokens



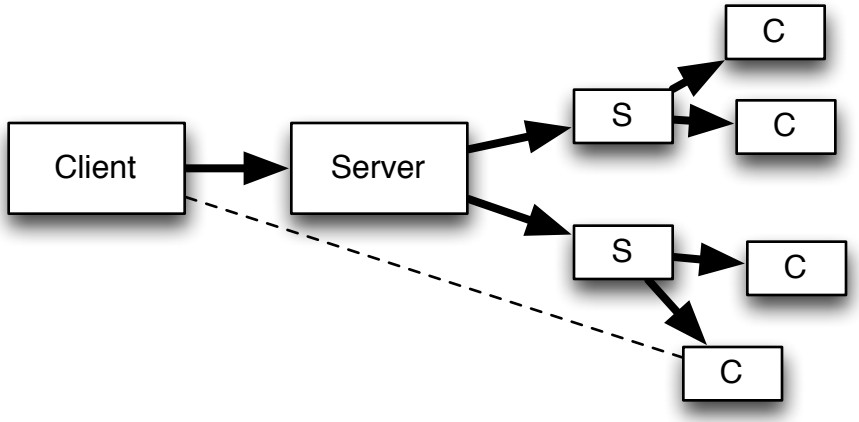
- Goal: Pass authorization from an authz server to the resource server that enforces the authz policy [draft-ietf-oauth-v2]
  - Authz server delivers token to client via RO
  - Client presents token to access resources
  - RS verifies that token encodes a valid authz from the AS

OAuth / Tokens



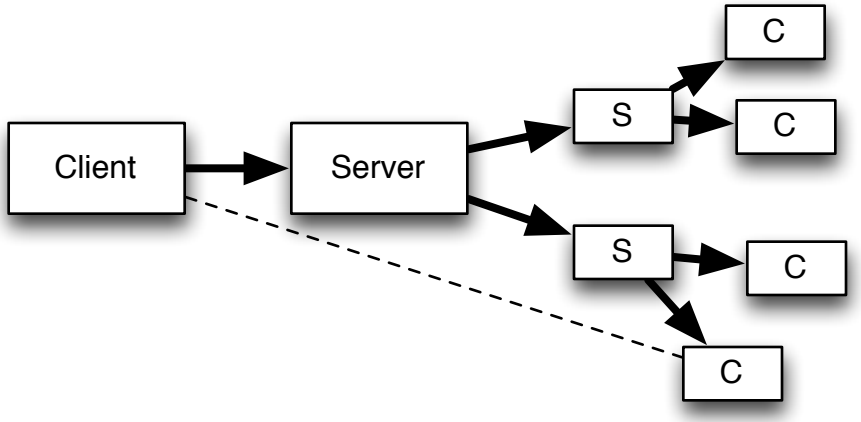
- Passes through untrusted RO and Client, so it needs **integrity** and **confidentiality** (symm or asymm)
- Passed in small fields (e.g., HTTP query params), so it needs to be **compact**

XMPP E2E Security



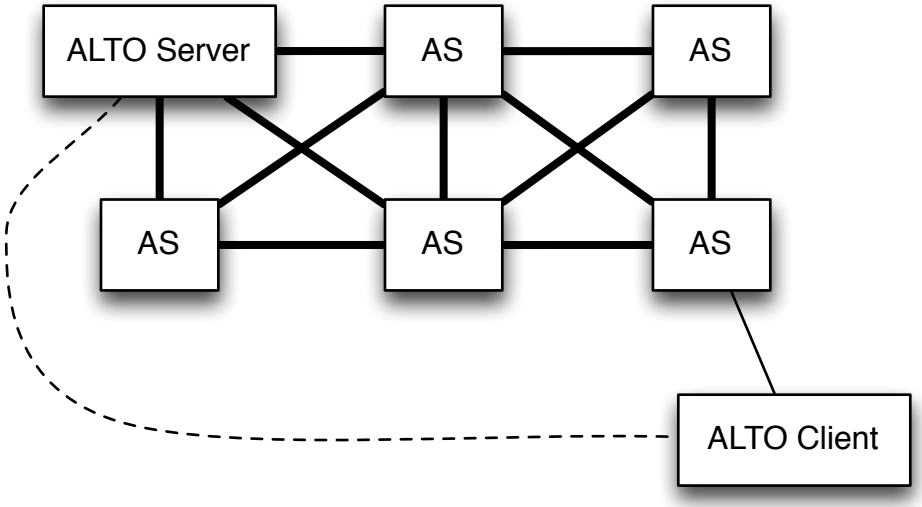
- Goal: Messaging between clients that is protected from intermediate servers [draft-miller-xmpp-e2e-00]
  - Sender encrypts object and sends to recipients
  - Recipients “dial back” and provide public key
  - Sender sends wrapped content encryption key
- Secure assuming XMPP routing is secure

XMPP E2E Security



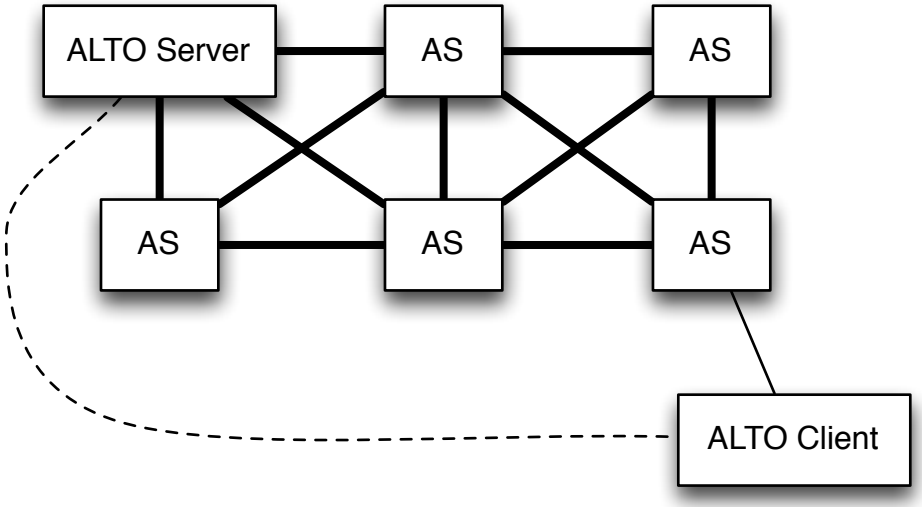
- Primary need is **confidentiality** (with integrity), less need for **integrity without encryption**
- Need to **separate key encryption** from message encryption ("detached RecipientInfos")
  - For multiple recipients even if not separate transmission
- Need **key references** for initial transmission

ALTO Server Federation



- Goal: Distribute ALTO mapping information through a network of ALTO servers
- JSON object signed by authoritative server
- Key distribution still being worked out

ALTO Server Federation



- Primary need is **signing** of JSON objects
  - … potentially **large objects** (KB/MB)
- Impact of JSON as payload format on **encoding**?

Derived Requirements Summary

- Confidentiality
  - Symmetric encryption
  - Wrapped private keys, detachable from content
  - Key references/identifiers
- Integrity
  - MAC within encrypted object
  - MAC/Signing with symmetric and asymmetric keys
- Encoding
  - How to manage wide range size constraints
  - Where is base64 applied?

What else?

<rbarnes@bbn.com>