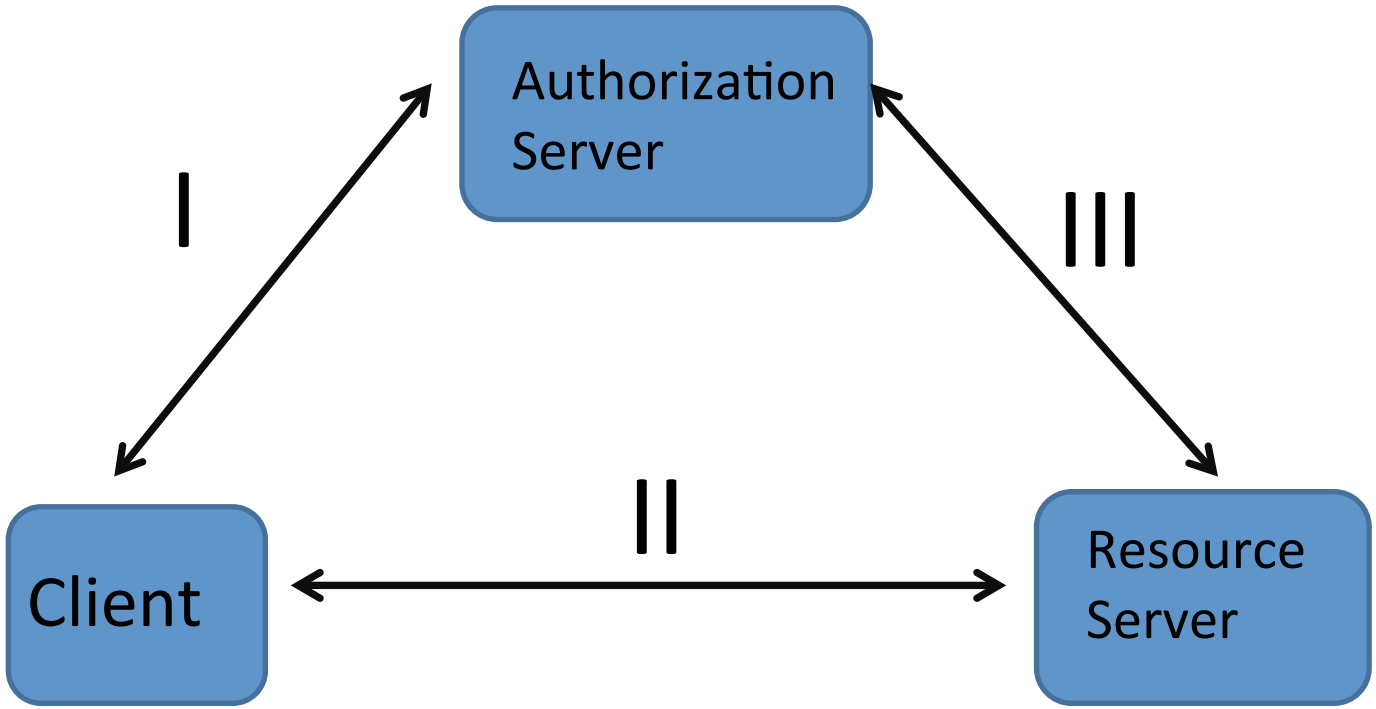
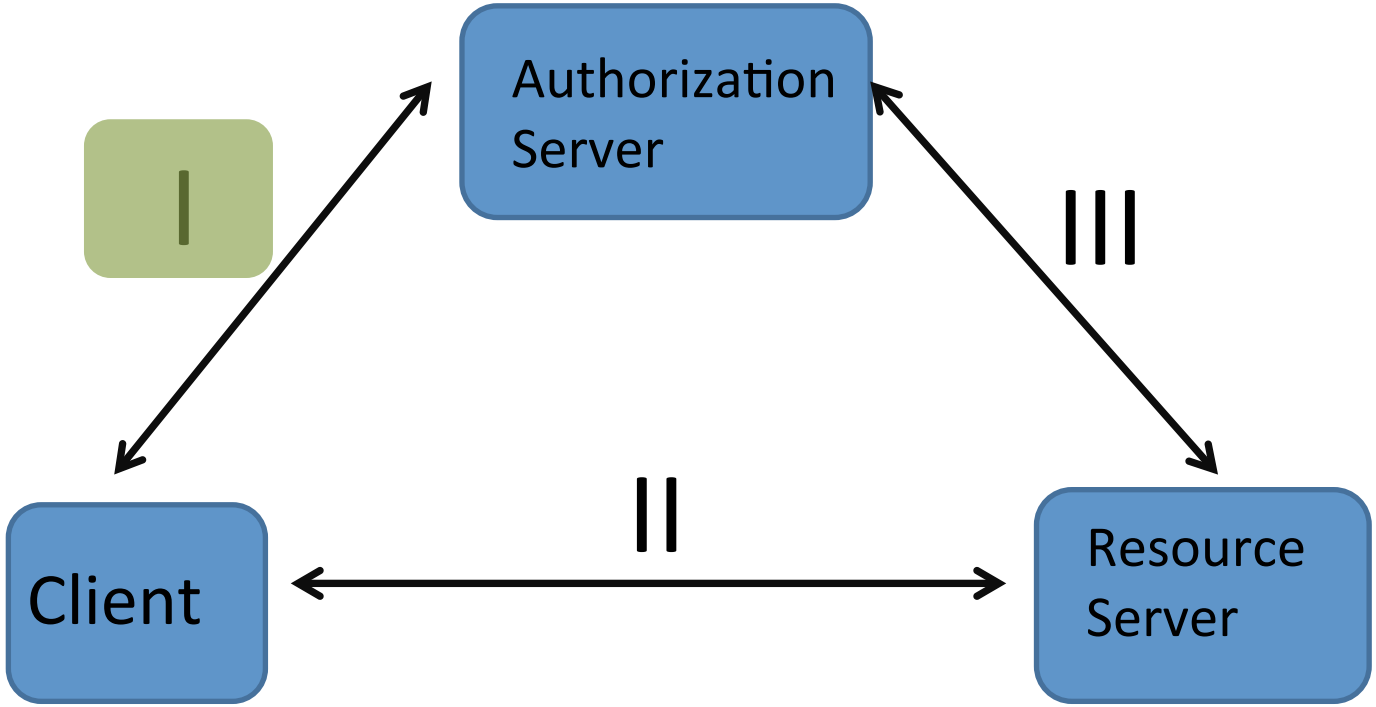
OAuth Security

Hannes Tschofenig
Derek Atkins

State-of-the-Art

- Design Team work late 2012/early 2013
- Results documented in Appendix 3 (Requirements) and in Appendix 4 (Use Cases) of http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-05
- Two solution approaches documents available in the group:
  - MAC Token: draft-ietf-oauth-v2-http-mac-05
  - HOTK: draft-tschofenig-oauth-hotk-03


Authorization Server
I
III
Client
II
Resource Server

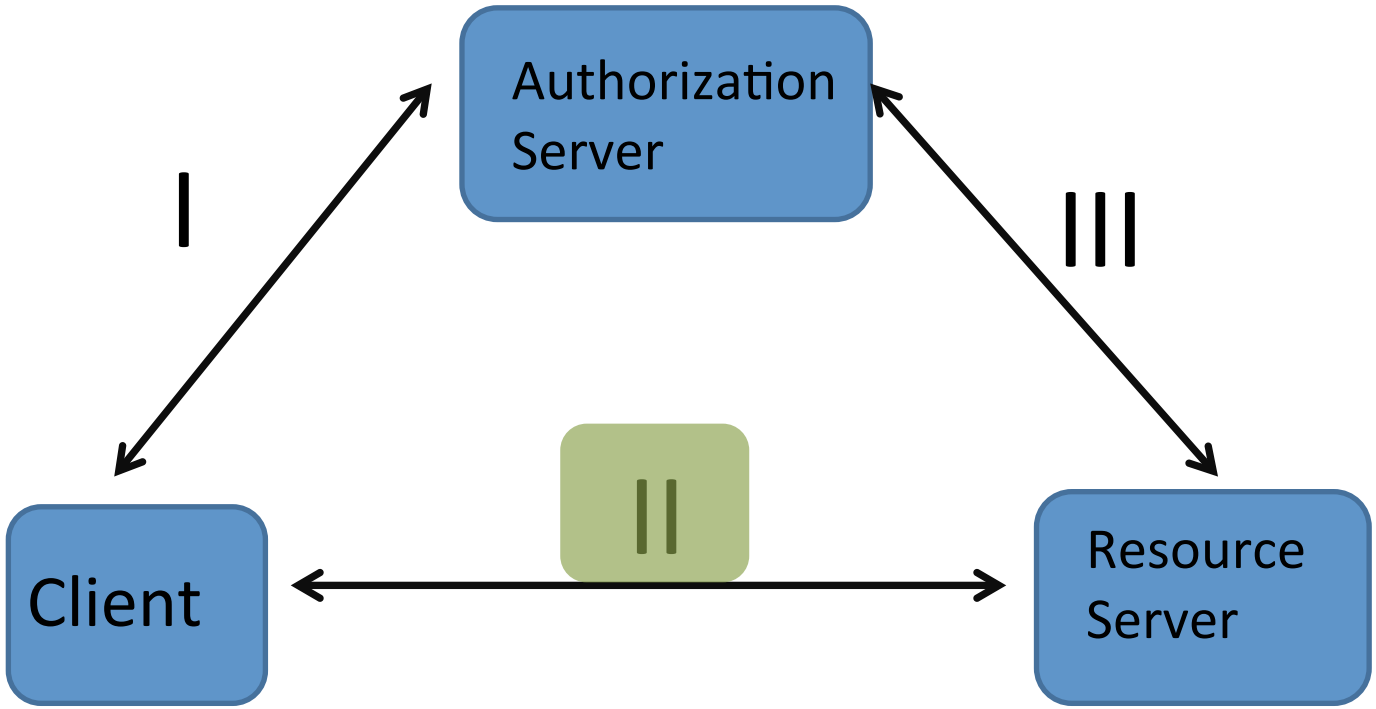

Authorization Server
I
III
Client
II
Resource Server

I: Key Distribution AS <-> Client

- Variants:
  - Key Distribution at Token Issuance
  - Key Distribution at Registration
- Approaches:
  - Server-provided key
  - Client-provided key
  - Joint key control / key agreement
- Examples:
  - Section 3.1.2 of HOTK for asymmetric keys
  - Section 4.1 of MAC Token for symmetric keys

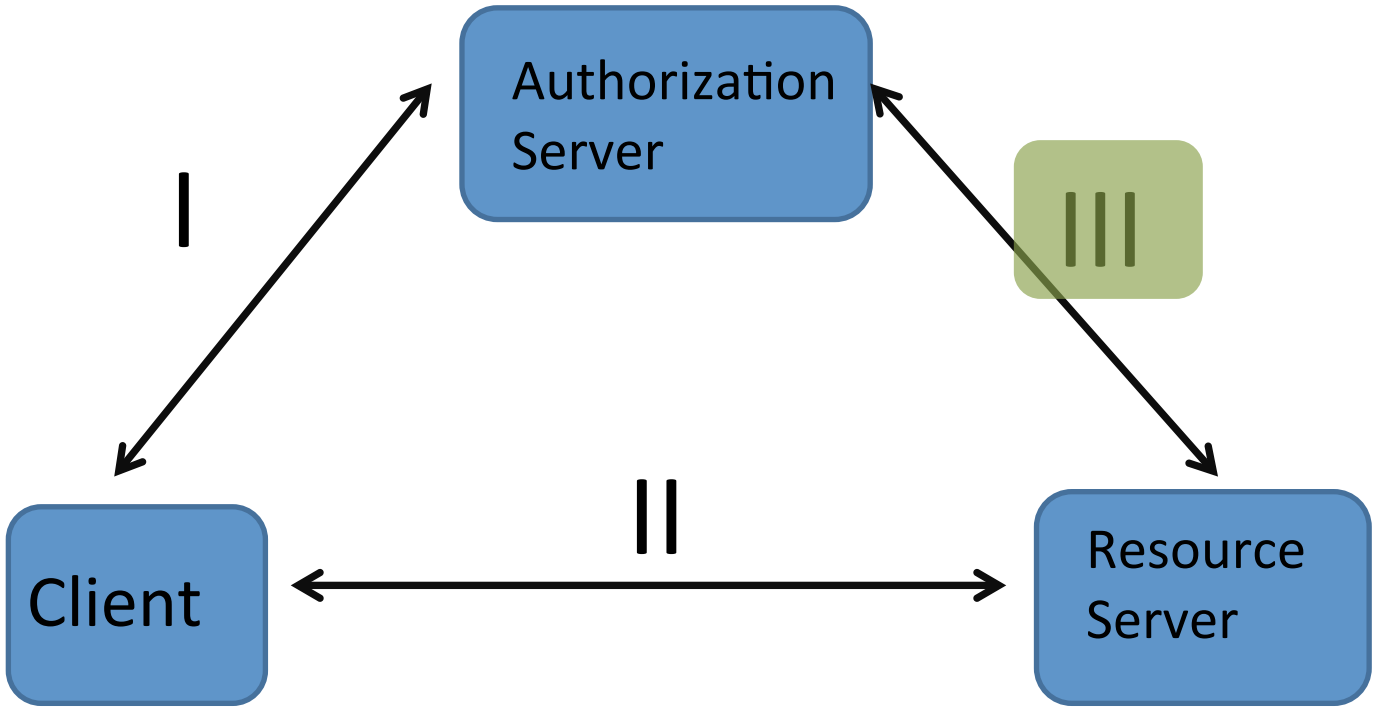
Lifetime Hierarchy

Oauth	Kerberos
Client Secret / Assertions	Long-term Username/Passwd
Refresh Tokens	Ticket Granting Ticket
Access Token-based key	Service tickets


Authorization Server
I
III
II
Client
Resource Server

II: Client <-> RS Interaction

- Components:
  a) Proof of possession of client key
  b) Message integrity / Channel Binding
  c) Server-to-client authentication
     a) As part of TLS
     b) Custom application-layer solution
- Examples:
  - Section 5 of MAC Token for symmetric keys (encoded as HTTP header)
  - Section 3.2.2 of HOTK for asymmetric keys
  - Section 3.2.1 of HOTK for symmetric keys (encoded as JSON structure)


Authorization Server
I
III
Client
II
Resource Server

III: Key Distribution AS <-> RS

- Variants:
  a) Embedded key
  b) Token introspection
  c) Out-of-band

- Examples:
  Ad a) Section 4.2 of HOTK
  Ad b) draft-richer-oauth-introspection
  Ad c) PKI

Next Steps: Document Restructuring

- Use Cases, Requirements and Design Rational
  - Currently in the appendix of MAC Token
  - Update to reflect new use cases
- Key Distribution AS <-> Client
  - Cover symmetric as well as asymmetric case
- Client <-> RS Communication
  - Section 5 of MAC Token & Section 3.2 of HOTK.
  - Includes keyed message digest/signature calculation algorithm.
  - Includes binding to transport
  - Includes JSON structure.
- Token introspection
- Encoding of PoP in JWT (symmetric & asymmetric)