OAuth 2.0 Security

IETF 87

Requirements

- Main requirements:
  - Lifetime of session key = Lifetime of access token
  - Replay protection: Timestamp + [sequence number]
  - Support for TLS channel bindings
  - Integrity protection for data exchange between the client and the resource server, and vice versa.
  - “Flexibility” regarding keyed message digest computation
  - Crypto-Agility: Algorithm indication from Authorization Server to the Client.

Scope

- Focus on symmetric key cryptography initially
- Use MAC token draft as a starting point

Design

- Flexible computation of MAC
- Key distribution: Key Transport
- Allow Client to indicate to which RS is wants to talk to.
  - http://tools.ietf.org/html/draft-tschofenig-oauth-audience-00

MAC Computation

- Introduces an additional header – ‘h’
- This field contains a colon-separated list of header field names that identify the header fields presented to the keyed message digest algorithm.

MAC Computation, cont.

Parameters: h=host, timestamp=1361471629

```
POST /request?b5=%3D%253D&a3=a&c%40=&a2=r%20b&c2&a3=2+q HTTP/1.1
Host: example.com

Hello World!
```

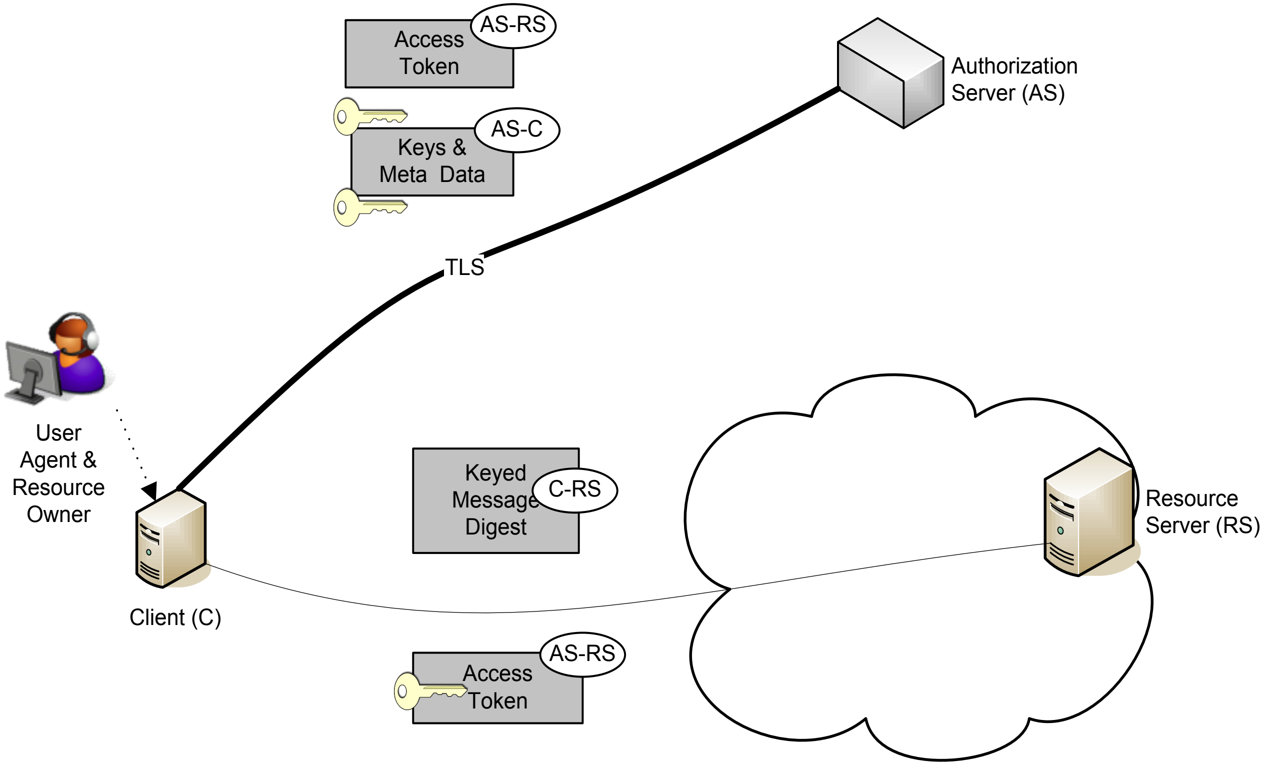
The resulting string is:

```
POST /request?b5=%3D%253D&a3=a&c%40=&a2=r%20b&c2&a3=2+q HTTP/1.1\n
1361471629\n
example.com
```

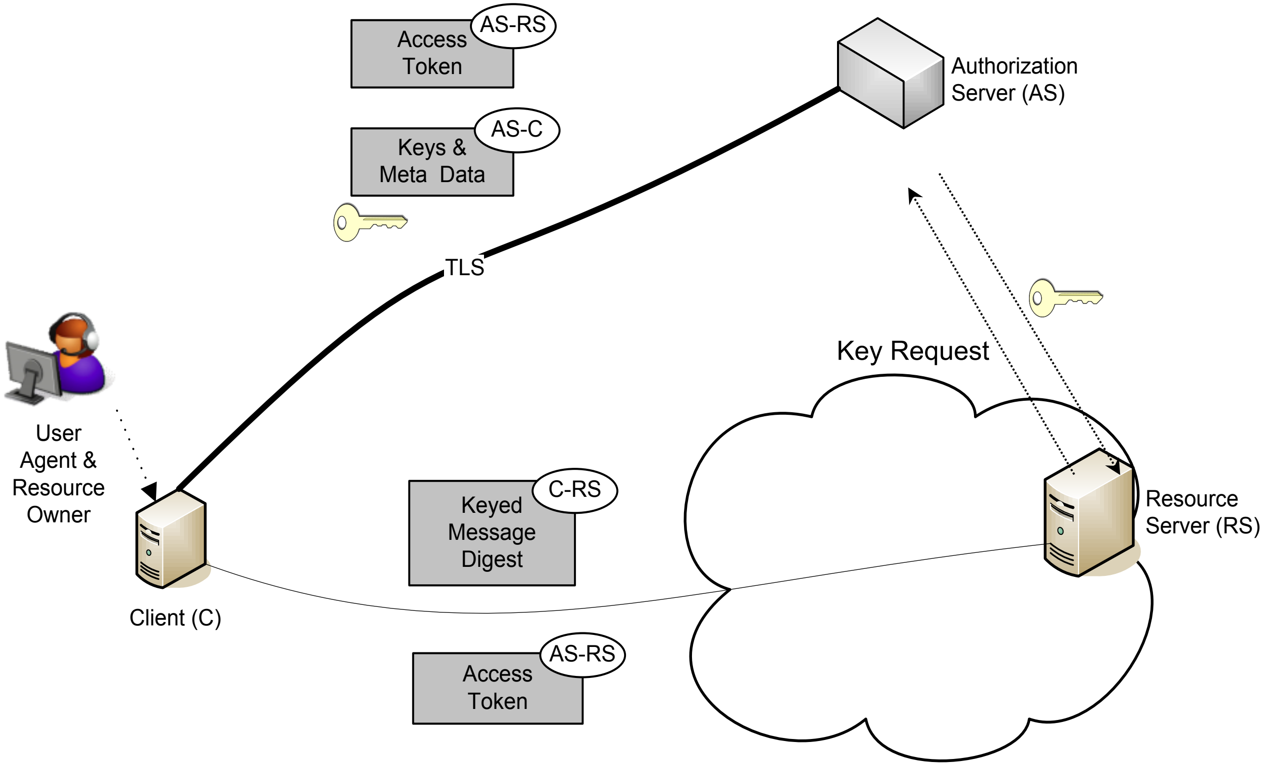
Key Distribution

- Three techniques:
  - Key Transport
  - “Key Retrieval”
  - Key Agreement

How RS obtains the Session Key? Option#1: Key Transport



How RS obtains the Session Key? Option#2: “Key Retrieval”


Access Token
AS-RS
Keys & Meta Data
AS-C
Authorization Server (AS)
TLS
Key Request
User Agent & Resource Owner
Resource Server (RS)
Keyed Message Digest
C-RS
Client (C)
Access Token
AS-RS