OAuth 2.0 Security

March 14, 2013

IETF 86, Orlando

Background

- After IETF#85 a series of conference calls were scheduled to progress the security work
  - 11th February 2013
  - 4th February 2013
  - 24th January 2013
  - 11th January 2013
  - 14th December 2013
- References to discussion input docs:
  - http://tools.ietf.org/html/draft-tschofenig-oauth-security-01
  - http://tools.ietf.org/html/draft-tschofenig-oauth-hotk-02
  - http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-03

Goals

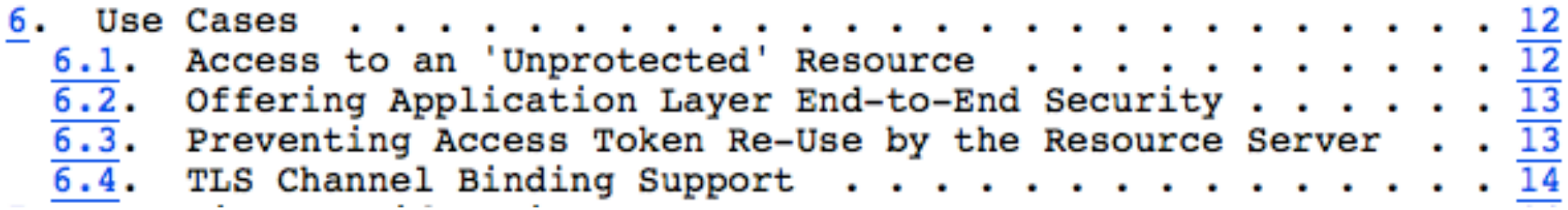
- This talk has two goals:

1) Share information about the progress between IETF#85 and IETF#86

2) Get feedback regarding the directions we are taking.

Scenarios

- Added use cases to draft-tschofenig-oauth-security based on the discussion:
  - http://www.ietf.org/mail-archive/web/oauth/current/msg10280.html



6. Use Cases 12
6.1. Access to an 'Unprotected' Resource 12
6.2. Offering Application Layer End-to-End Security 13
6.3. Preventing Access Token Re-Use by the Resource Server . . 13
6.4. TLS Channel Binding Support 14

- Justin's use case for "signed URL" didn't get enough support to be included.
  - http://www.ietf.org/mail-archive/web/oauth/current/msg10407.html

Questions to the Group

1. Did we cover the relevant scenarios?
2. Are the scenario descriptions understandable?

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.

- More detailed write-up:
  - http://tools.ietf.org/html/draft-tschofenig-oauth-security-01

Scope

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

Questions to the Group

1. Did we capture all the relevant requirements?
2. Do you agree with the scoping?
3. Do you with the requirements?

Open Issues

- Flexible computation of MAC
  - Inspired by DKIM
- Key distribution:
  - Three mechanisms presented. Which one should focus on?
- 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!

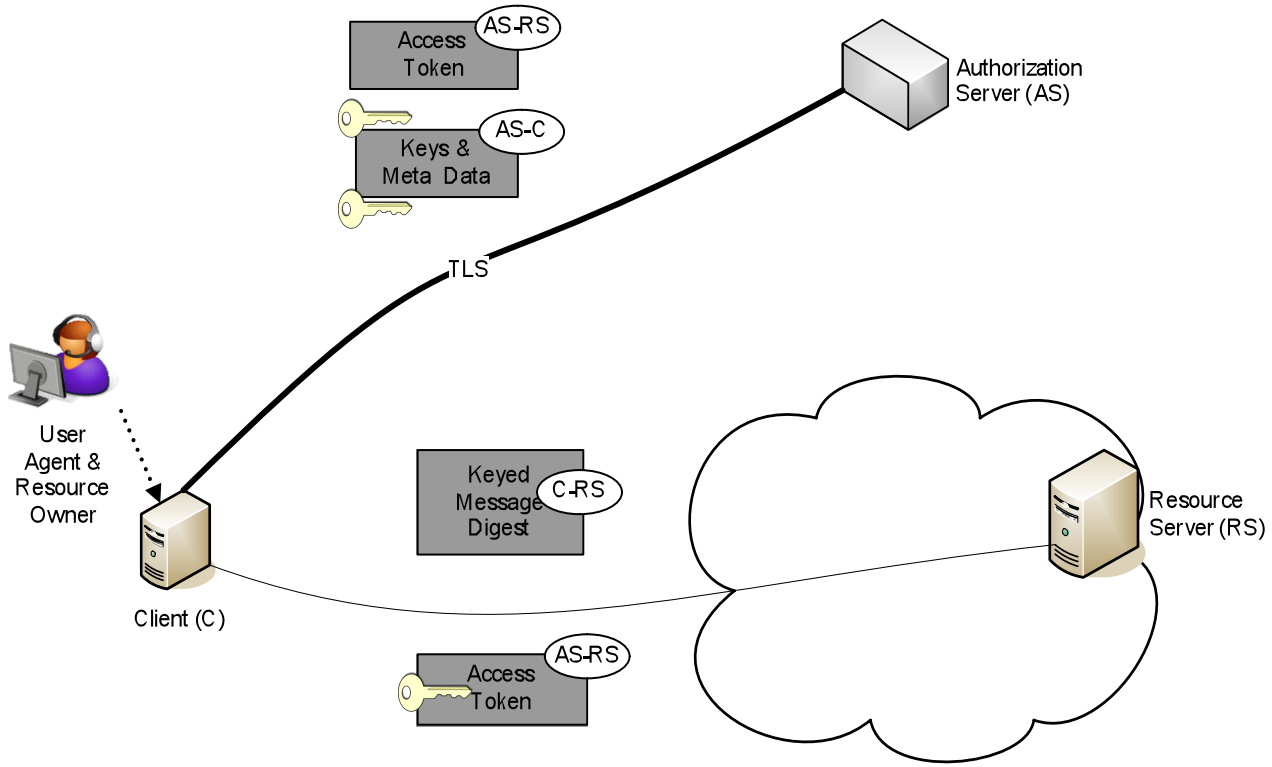
The resulting string is:

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

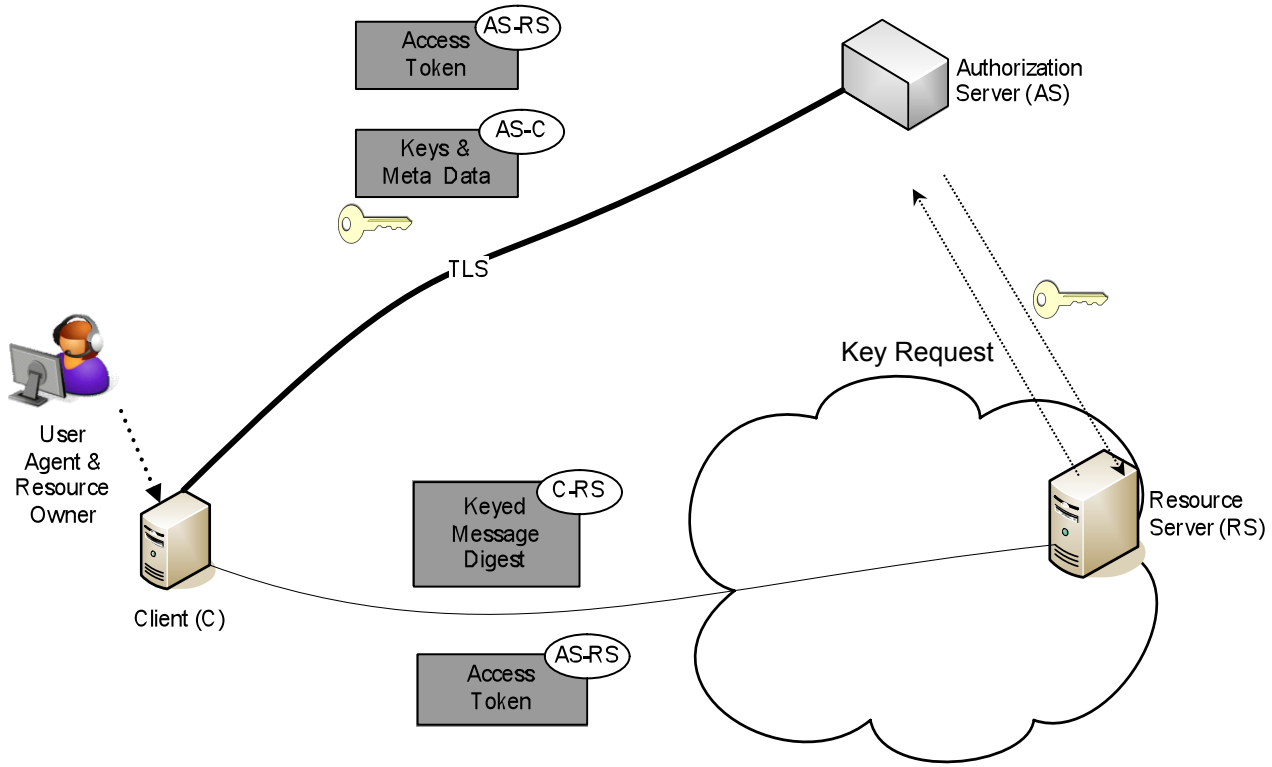
Key Distribution

- Three techniques:
  - Key Transport
  - “Key Retrieval”
  - Key Agreement
- Strawman proposal illustrates key transport approach:
  - http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-03
- Key point: What is MTI?

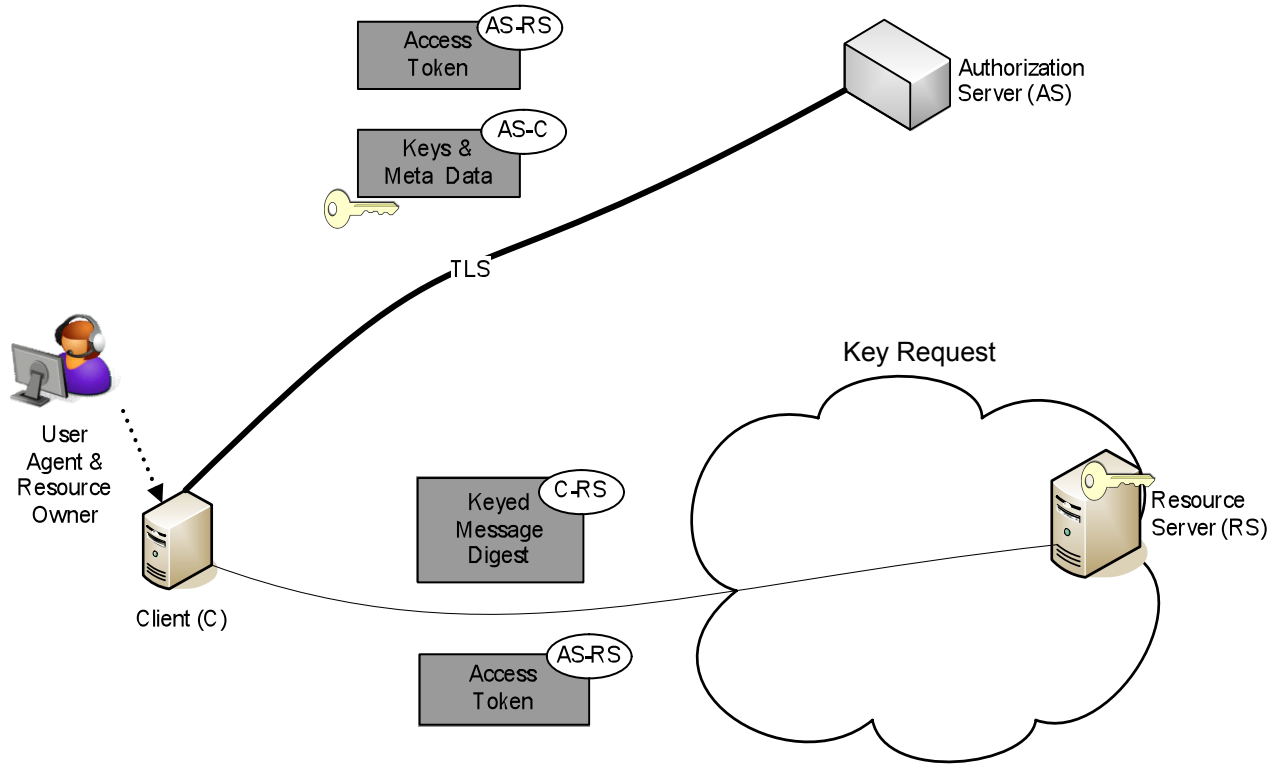
How RS obtains the Session Key? Option#1: Key Transport



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



How RS obtains the Session Key? Option#3: Key Agreement



Questions to the Group

1. Which approach for key management would you like to see described?
2. Which approach should be considered as MTI?

Next Steps

- WG approval of feedback from the meeting next week and incorporate changes in the MAC token specification.