3rd-Party Authentication for SIP

Rifaat Shekh-Yusef, Christer Holmberg, Victor Pascual

IETF100, SIPCore WG, Singapore

November 13, 2017

Overview

- The mechanism allows a user to use his **non-sip credentials** to get access to **SIP services**.
- This enables the **Single-Sign-On** feature where the user is expected to use **one set of credentials** to get access to **SIP and non-SIP services**.

UA Types

- **Confidential**: a UA that is capable of maintaining the confidentiality of the user credentials and any tokens obtained using these user credentials.

- **Public**: a UA that is incapable of maintaining the confidentiality of the user credentials and any obtained tokens.

Public UA with Rich UI

```
User                            Proxy                   Authorization
Agent                                                          Server
---------------------------------------------------------------------
   |                               |                               |
   | F1 REGISTER                   |                               |
   |------------------------------>|                               |
   |                   F2 401      |                               |
   |                      Location |                               |
   |<------------------------------|                               |
   |                               |                               |
   |                        F3 [AuthZ Code]                        |
   |<------------------------------------------------------------->|
   |                               |                               |
   |                               |                               |
   | F4 REGISTER [AuthZ Code]      |                               |
   |------------------------------>|                               |
   |                               | F5 Exchange code for tokens   |
   |                               |<----------------------------->|
   |                               |                               |
   |                     F6 200 OK |                               |
   |<------------------------------|                               |
   |                               |                               |
```

Both UA and Proxy create a shared-key based on F6 200 OK request, as follows:

Shared-key = HMAC-SHA256(AuthZ Code, call-id | from-tag | to-tag)

Public UA with Limited UI

```
        User
--------------------
                User                           Proxy                   Authorization
   Browser     Agent                                                          Server
 ------------------------------------------------------------------------------------
       |          |                               |                               |
       | F1 Authenticate to AS and obtain a shorted-lived numeric access code     |
       |<------------------------------------------------------------------------>|
       |          |                               |                               |
       |     F2 The UA collects the numeric code from the user through the key-pad|
       |          |                               |                               |
       |          |                               |                               |
       |          | F3 REGISTER [AuthZ Code]      |                               |
       |          |------------------------------>|                               |
       |          |                               |                               |
       |          |                               | F4 Exchange code for tokens   |
       |          |                               |<----------------------------->|
       |          |                               |                               |
       |          |                     F5 200 OK |                               |
       |          |<------------------------------|                               |
       |          |                               |                               |
```

Both UA and Proxy create a shared-key based on F6 200 OK request, as follows:
Shared-key = HMAC-SHA256(AuthZ Code, call-id | from-tag | to-tag)

Re-Registration

- The UA uses the **shared-key** to re-register with the proxy.
- This is useful in case the connection with the proxy was lost to avoid the need to re-authenticate the user.
- The proxy could invalidate the shared-key at any time, and require the user to re-authenticate.

Confidential UA with Rich UI

```
User                            Proxy                   Authorization
Agent                                                          Server
---------------------------------------------------------------------
   |                               |                               |
   | F1 Authenticate to AS and obtain access and refresh tokens    |
   |<------------------------------------------------------------->|
   |                               |                               |
   |                               |                               |
   | F2 REGISTER access-token      |                               |
   |------------------------------>|                               |
   |                               |                               |
   |                               | F3 Introspection (optional)   |
   |                               |<----------------------------->|
   |                               |                               |
   |                     F4 200 OK |                               |
   |<------------------------------|                               |
   |                               |                               |
```

Open Issues

- **Location**
  - **401** with **Location** header (RFC7231)
- **Proof-of-Possession (PoP)**
  - PoP is calculated based on the **digest-string** defined in **RFC4474**.
  - Should PoP not be limited to re-registrations?
    - If so, a new header needs to be defined, instead of sending the pop in the request body.