3rd-Party Authentication for SIP

Rifaat Shekh-Yusef, Christer Holmberg, Victor Pascual

IETF98, SIPCore WG, Chicago, USA

March 30, 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**.

3ʳᵈ Party AuthN vs SIP OAuth

- The **SIP OAuth** draft defines a general **SIP services authorization** framework.

- The **3ʳᵈ Party Authentication** draft defines an authentication and authorization mechanism for **SIP registration** to enable the **SSO** feature.

UA Types

- **RFC6749** defines two types of UAs:

  - **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 302 |                           |
    |<----------------------------|                           |
    |                             |                           |
    |               F3 [AuthZ Code]                           |
    |<--------------------------------------------------------|
    |                             |                           |
    |                             |                           |
    | F4 REGISTER [AuthZ Code]    |                           |
    |---------------------------->|                           |
    |                             | F5 Exchange code for tokens |
    |                             |<------------------------->|
    |                             |                           |
    |                   F6 200 OK |                           |
    |<----------------------------|                           |
    |                             |                           |
    |                             |                           |
```
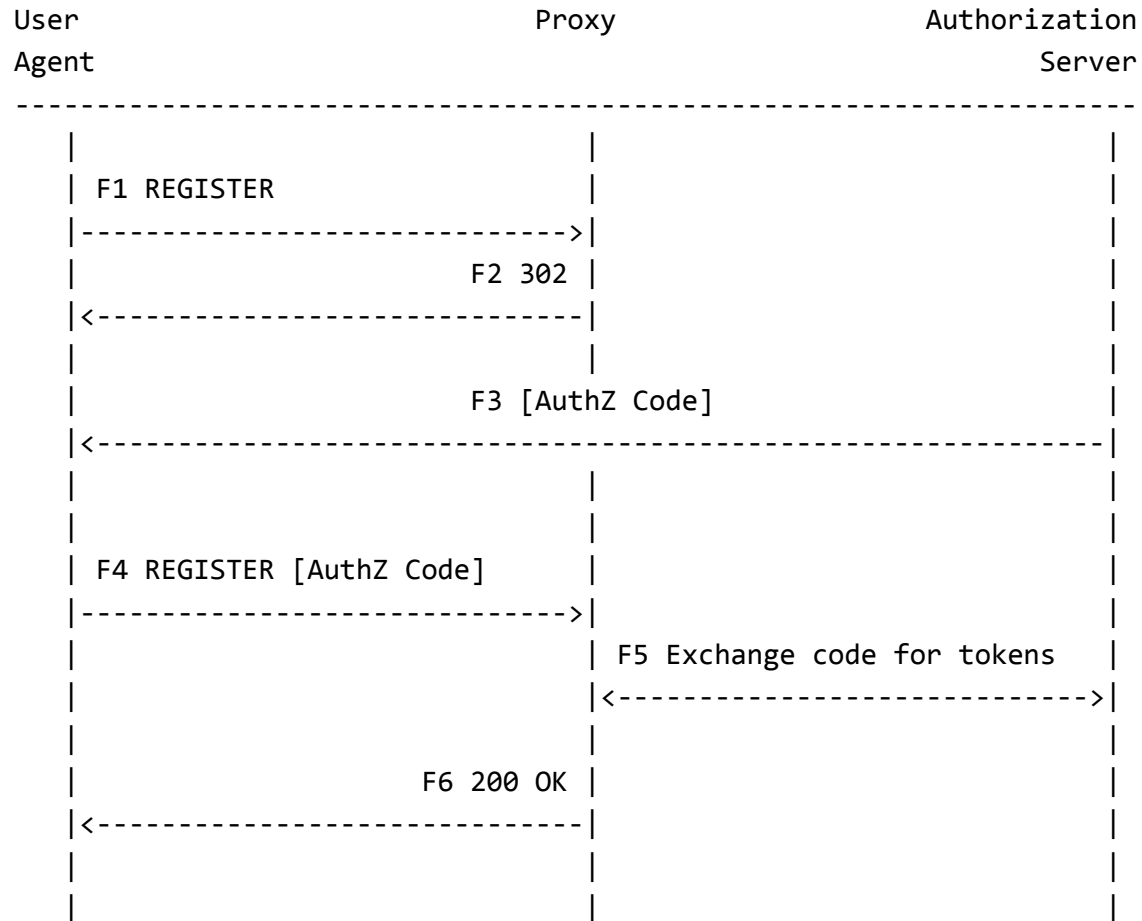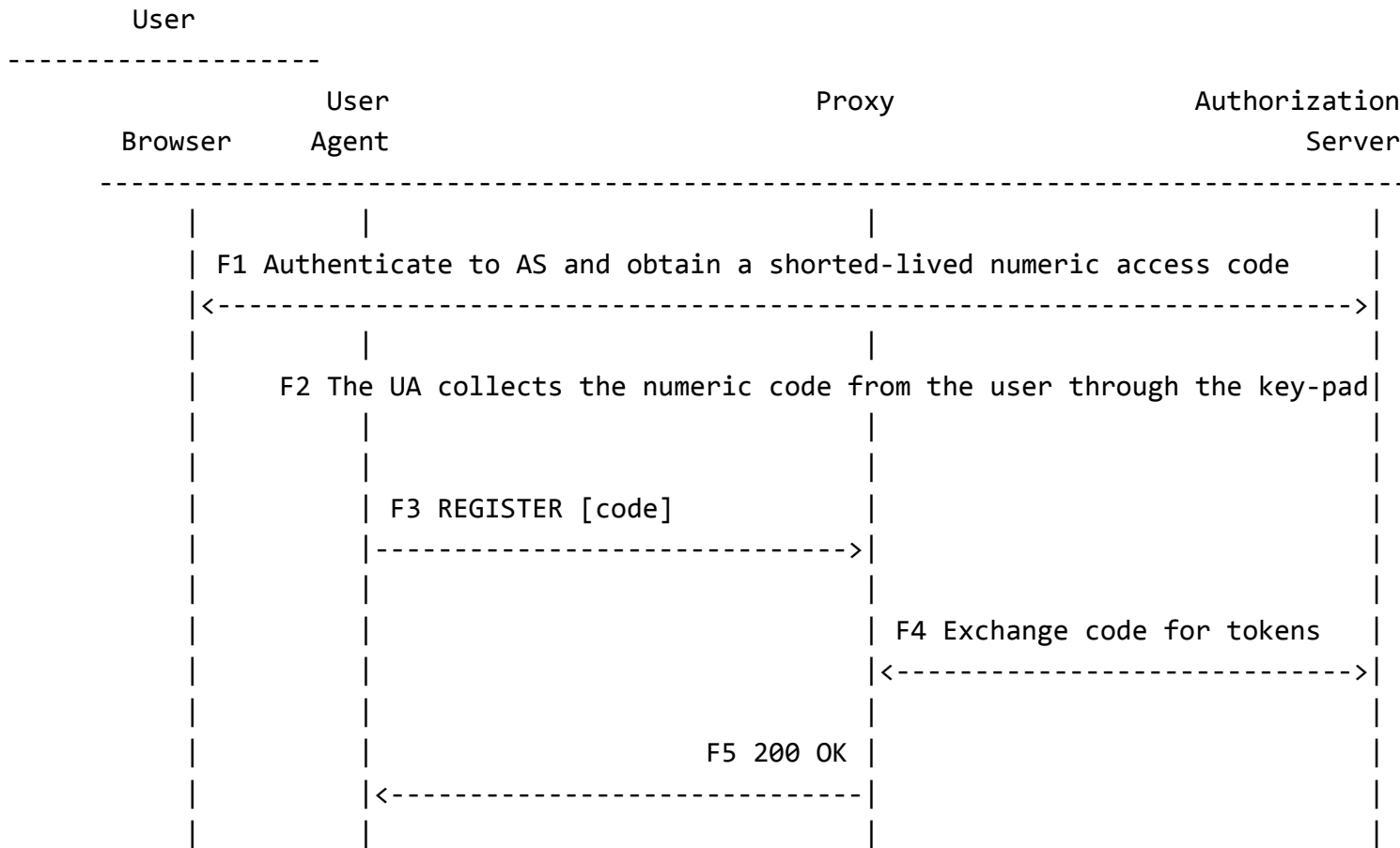
Public UA with Limited UI

```
         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 [code]              |                       |
       |          |-------------------------------->|                       |
       |          |                                 |                       |
       |          |                                 | F4 Exchange code for tokens |
       |          |                                 |<--------------------------->|
       |          |                                 |                       |
       |          |                      F5 200 OK  |                       |
       |          |<--------------------------------|                       |
       |          |                                 |                       |
```

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       |                            |
     |<--------------------------|                            |
     |                            |                            |
```
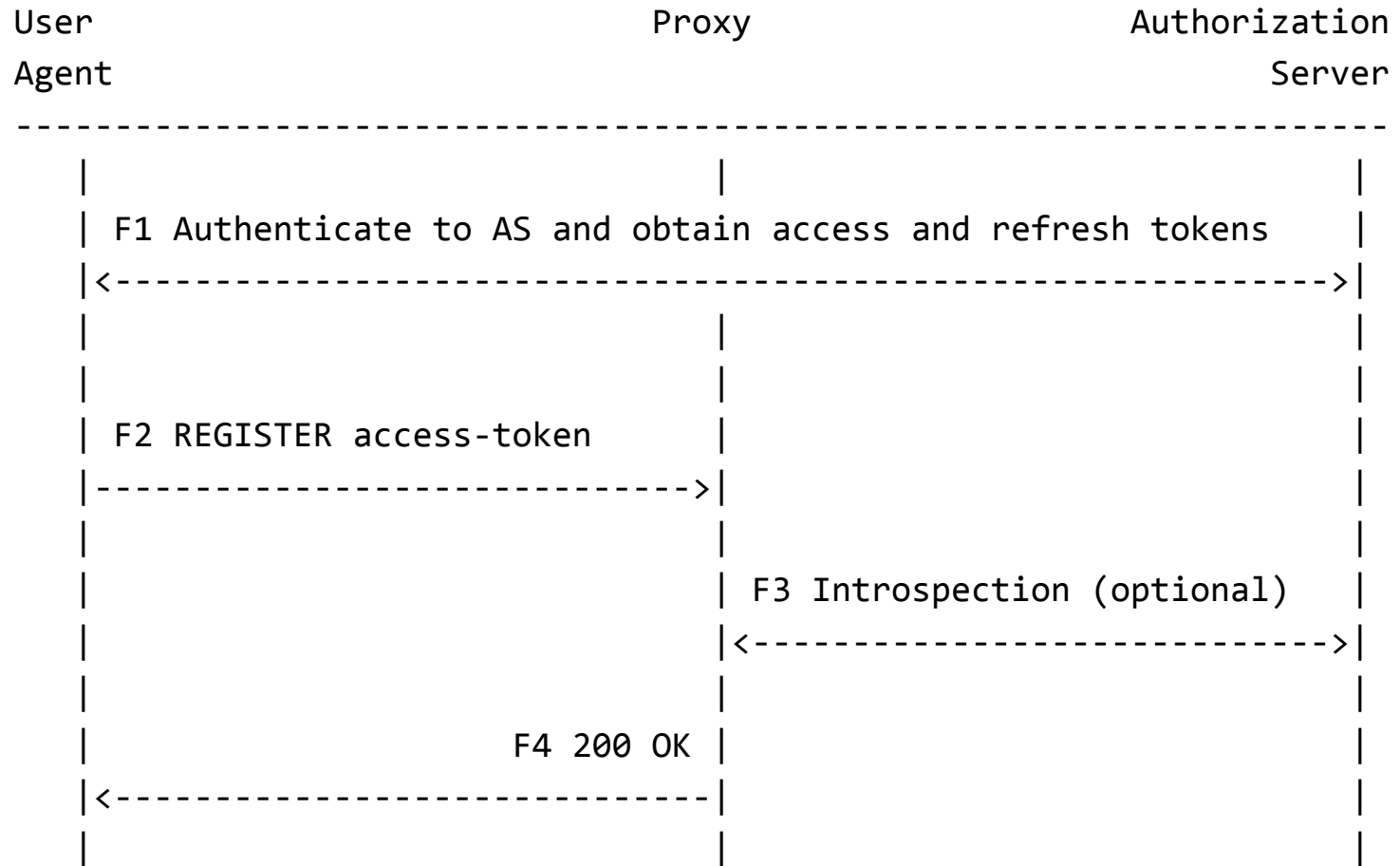
IMS-WebRTC

- Access IMS services using web credentials
  - Non-legacy IMS authentication methods
- Entities
  - WIC (**W**ebRTC **I**MS **C**lient)
    - E.g., JavaScript application in browser
  - WWSF (**W**ebRTC **W**eb **S**erver **F**unction)
  - WAF (**W**ebRTC **A**uthorisation **F**unction)
    - Issues authorization tokens
    - IMS operator or 3rd party

IMS-WebRTC
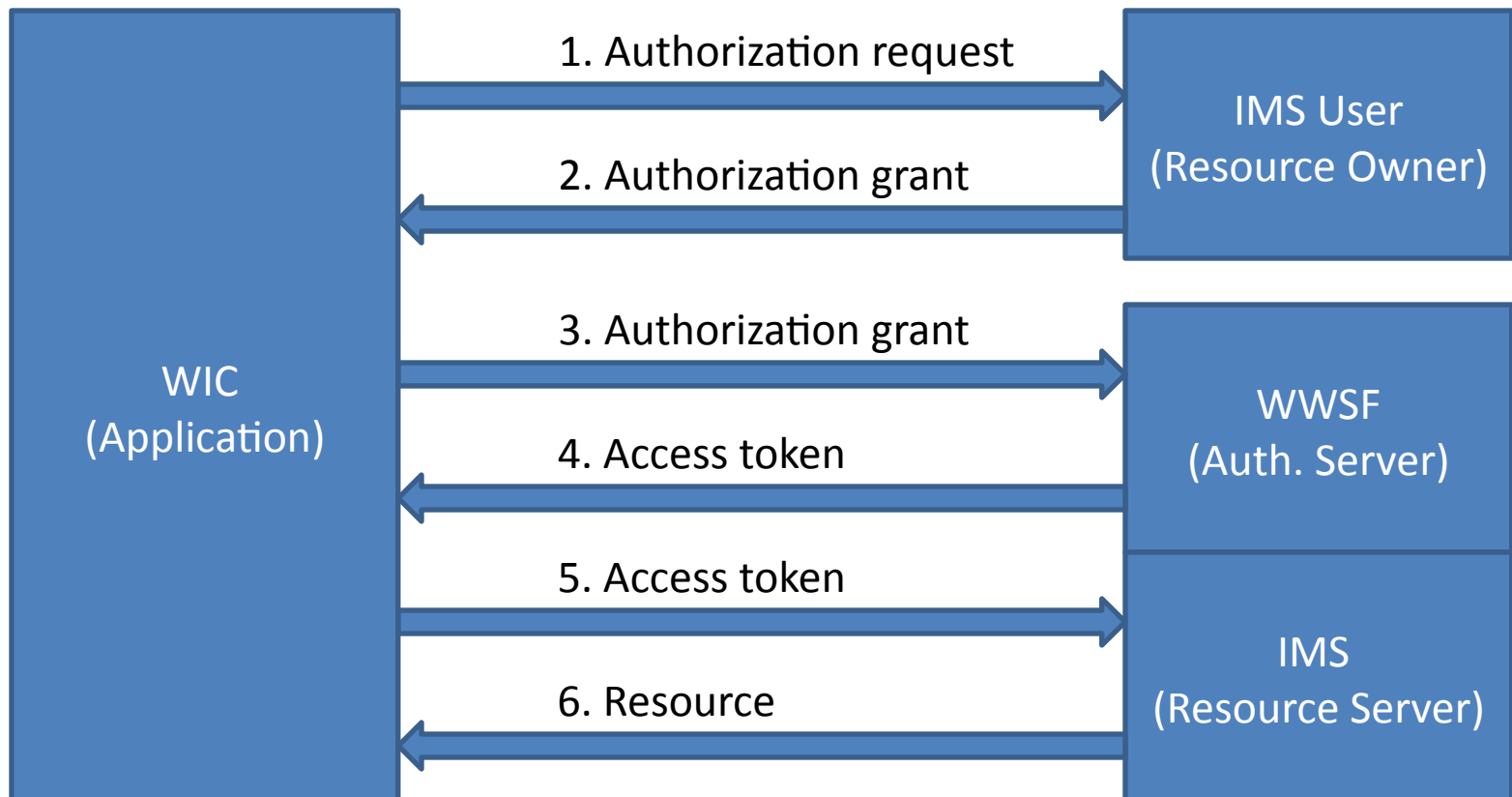
Open Issues

- Redirection
  - 302? 4xx?
- Flow recovery with PoP?