SIP OAuth Use Cases

Rifaat Shekh-Yusef, Victor Pascual, Christer Holmberg
IETF 95, SIPCore WG, Buenos Aires, Argentina
April 8, 2016
Enterprise SSO

• An enterprise is interested in providing its users with an SSO capability to the various corporate services.

• The user is expected to provide his corporate credentials to login to the corporate network and get access to all configured services, including SIP services, without the need to create different accounts for these different types of services.
IMS-WebRTC

• The 3GPP network has a requirement to allow a user using a WebRTC IMS Client (WIC) to authenticate to a WebRTC Authorization Function (WAF) and in response be given an access token that allows the user to register and get service from the 3GPP IMS SIP network.

• The WIC then requests an access token from the WAF using HTTP, which the WIC then uses to register to the 3GPP IMS SIP network.
Confidential SIP Hardphone

- A **SIP hardphone** with **rich UI**, that has the capability to maintain the **confidentiality** of user's credentials, is used to authenticate to an authorization server, get a **token**, and use that token to register and get service from the **SIP** network.

- When the phone interacts with the authorization server and gets challenged to provide credentials, the phone will prompt the user to enter his credentials which will be used to authenticate to the authorization server.
Public SIP Hardphone

- A SIP hardphone with limited UI capabilities, that is incapable of maintaining confidentiality of user's credentials, is used to register with the SIP network by providing an access code obtained from an authorization server.
- The user will use an out of band method, e.g. browser, to authenticate to the authorization server and get a short-lived numeric access code.
- The user will then use the phone's keypad to provide the numeric access code to the SIP phone. The phone will then use the access code to register and get service from the SIP network. The SIP Proxy will exchange the access code with access token from the authorization server.
QUESTIONS?