Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 29, 2015

C. Holmberg
Ericsson

May 28, 2015

Authorization server identity
draft-holmberg-sipcore-auth-id-01.txt

Abstract

The 3rd-Generation Partnership Project (3GPP) has defined how the WebRTC framework can be used to provide access to IMS services. Users can use "web credentials" (e.g. a username and password) to obtain an authorization token (e.g. an OAuth 2.0 access token), which is included in the user registration request sent towards the IMS network.

3GPP has specified a requirement, that the eP-CSCF shall be able to include a string value, representing the identity of the WAF, in the REGISTER request forwarded towards the S-CSCF. The S-CSCF can use the identity for e.g. policy decisions.

This document defines a new Authorization header field parameter, 'authorization-entity', which the eP-CSCF can include in a REGISTER request in order to convey the identity of the WAF towards the S-CSCF.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 29, 2015.

Table of Contents

1. Introduction

The 3rd-Generation Partnership Project (3GPP) has defined how the WebRTC framework can be used to provide access to IMS services. Users can use "web credentials" (e.g. a username and password) to obtain an authorization token (e.g. an OAuth 2.0 access token), which is included in the user registration request sent towards the IMS network.

NOTE: The current assumption is that, when SIP [RFC5234] is used between the WIC and the eP-CSCF, together with the OAuth 2.0 framework [RFC6749], the access token will be conveyed in the

REGISTER request using the mechanism defined in [I-D.yusef-sipcore-sip-oauth].

The WWSF (OAuth 2.0 Client role) authenticates the user (OAuth 2.0 Resource Owner role), and obtains the token from the WAF (OAuth 2.0 Authorization Server role). The WWSF then provides the token to user (typically as part of a JavaScript application downloaded by the user), which then includes the token in the registration request (REGISTER request when SIP [RFC3261] is used) towards the IMS network (OAuth 2.0 Resource Server role).

When the eP-CSCF receives the registration request, it contacts the WAF and verifies the token. If the verification is successful, the WAF provides IMS credentials to eP-CSCF, which the eP-CSCF can include in the registration request sent towards the S-CSCF, in order to register the user using legacy IMS registration mechanisms.

3GPP has specified a requirement, that the eP-CSCF shall be able to include a string value, representing the identity of the WAF, in the REGISTER request forwarded towards the S-CSCF. The S-CSCF can use the identity for e.g. policy and routing decisions.

This document defines a new Authorization header field parameter, 'authorization-entity', which the eP-CSCF can include in a REGISTER request in order to convey the identity of the WAF towards the S-CSCF.

The 'authorization-entity' parameter is defined in order to fulfil requirements from the 3rd-Generation Partnership Project (3GPP), but it can also be used in other network environments.

2. Abbreviations

WIC (WebRTC IMS Client): An application (typically a JavaScript application executed in a browser) using the WebRTC 1.0 extensions used to access IMS.

WAF (WebRTC Authorisation Function): Provides and validates access tokens. In the OAuth 2.00 architecture the WAF represents the Authorization Server.

WWSF (WebRTC Web Server Function): obtains access tokens on behalf of a user, and provides the WIC application code to the user. In the OAuth 2.0 architecture the WWSF represents the Client.

CSCF: Call Session Control Function: IMS SIP proxy. Different types of CSCFs perform different functions in an IMS network.

eP-CSCF (P-CSCF enhanced for WebRTC): A SIP proxy which validates the access token, and obtains IMS credentials associated with the access token. In the OAuth 2.0 architecture the eP-CSCF represents verifies the access token on behalf of the Resource Server.

S-CSCF (Serving CSCF): IMS SIP registrar.

3. Requirements

REQ-1: It MUST be possible for a SIP proxy to include a string value, representing the identity of an authorization server, in a REGISTER request sent towards a SIP registrar.

4. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

5. 'authorization-entity' header field parameter

5.1. General

This section defines a new Authorization header field 'authorization-entity' header field parameter. The header field parameter is used in a REGISTER request to convey a string value which represents the identity of an authorization server. The header field parameter is included in the REGISTER request by the entity which verifies the access token received from a SIP UA.

This document only describes the usage of the authorization-entity header field parameter within a REGISTER request. Usage with other SIP methods, or within REGISTER responses, is unspecified.

5.2. Syntax

5.2.1. General

This section defines the ABNF for the SIP Authorization 'authorization-entity' header field parameter. The ABNF defined in this specification is conformant to RFC 5234 [RFC5234].

5.2.2. ABNF

The ABNF [RFC5234] grammar for the 'authorization-entity' header field parameter is:

```
dig-resp    /= "authorization-entity" EQUAL quoted-string
;; quoted-string defined in RFC 3261
```

6. Security Considerations

Security considerations come here.

7. IANA Considerations

[RFC EDITOR NOTE: Please replace RFCXXXX with the RFC number of this document.]

This specification adds one new header field parameter to the IANA registration in the "Header Field Parameters and Parameter Values" registry, as specified in [RFC3969].

Header Field:	Authorization
Parameter Name:	authorization-entity
Predefined Values:	No
Reference:	RFCXXXX

8. Acknowledgments

The author wishes to thank everyone in the 3GPP community that provided input and comments on this document.

9. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

draft-holmberg-sipcore-auth-id-xx

o

draft-holmberg-sipcore-auth-id-00

o Editorial changes/corrections.

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3969] Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)", BCP 99, RFC 3969, December 2004.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC6749] Hardt, D., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012.

[I-D.yusef-sipcore-sip-oauth] Shekh-Yusef, R. and V. Pascual, "The Session Initiation Protocol (SIP) OAuth", draft-yusef-sipcore-sip-oauth-02 (work in progress), April 2015.

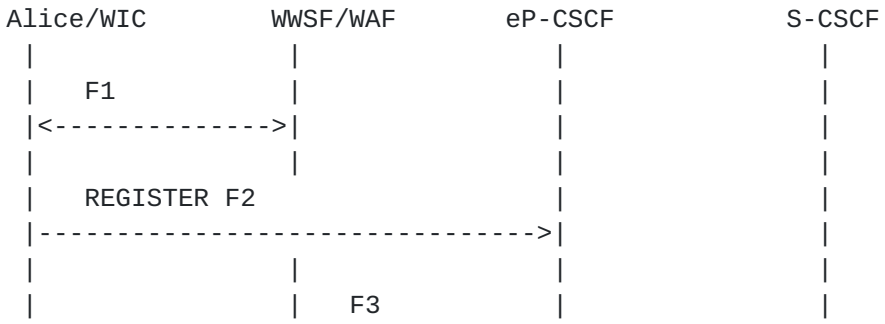
Appendix A. 3GPP Examples

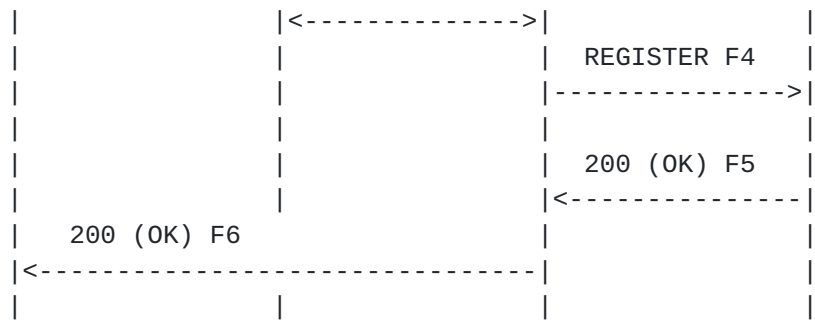
A.1. General

This section contains example call flows based on 3GPP usage of the authorization-entity header field parameter.

A.2. WIC registration using web credentials

The WWSF/WAF authenticates, obtains and provides an access token to, the WIC. The WIC includes the access token in the REGISTER request sent to the eP-CSCF. The eP-CSCF validates the access token with the WAF, and obtains IMS credentials associated with the token. The eP-CSCF includes the IMS credentials, and a string value representing the identity of the WAF, in the REGISTER request before forwarding it towards the S-CSCF.





F1 WIC <-> WWSF/WAF
The WWSF/WAF authenticates Alice, using "web credentials"
(e.g. username and password), and obtains an access
token. The access token and the WIC (typically a JavaScript
application) is provided to Alice.

F2 REGISTER WIC -> eP-CSCF
REGISTER sip:registrar.home1.net SIP/2.0
Authorization: Bearer access_token="O91G451HZ0V......"

F3 eP-CSCF <-> WWSF/WAF
The eP-CSCF validates the access token with the WAF,
and obtains IMS credentials associated with the user,
and a string value representing the identity of the WAF.

F4 REGISTER eP-CSCF -> S-CSCF
REGISTER sip:registrar.home1.net SIP/2.0
Authorization: Digest username="user1_private@home1.net",
 realm="registrar.home1.net",
     nonce="",
     uri="sip:registrar.home1.net",
     response="",
     authorization-entity="webrtc_authserver1@thirdparty.net"

F5 200 OK S-CSCF -> eP-CSCF
200 OK

F6 200 OK eP-CSCF -> WIC
200 OK

Figure 1: The UE registers via P-CSCF

Author's Address

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com