Mobile Connect Client Credentials for Attributes – Configuration B

Version 1.0

06 December 2022

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2022 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

The GSMA Identity programme focuses on positioning Operators as trusted providers of identity and attribute services to third party Service Providers. Within this, the programme identifies a set of products that collectively are referred to as Mobile Connect.

Attribute services in Mobile Connect are typically specified as resources that can be accessed by Service Providers by means of access tokens. These access tokens are assumed to be User specific, meaning each access token is tied to a User and allows queries to be made only for that particular User. These are the kind of access tokens that can be obtained by using the MC Device Initiated OIDC Profile [4] or the MC Server Initiated OIDC Profile [5].

The MC Client Credentials Profile [7] in turn delivers access tokens that are not User specific, i.e. they are not tied to a User, so they could be used by Service Providers to make queries for any User in the scope of a specific attribute service. But that requires changes in the service definition to support the use of this kind of tokens, which is not considered in the specifications by default.

This document specifies the adaptations required in Mobile Connect attribute services so that they can be used with access tokens that are not tied to any specific User.

1.2 Scope

In Scope	Out of Scope
• Adaptations required for MC attribute services to support the use of generic access tokens	• Attribute services description • Legal aspects and regulations

1.3 Audience

The target audience for this document are the Mobile Operator service/technical departments who are considering deploying Mobile Connect attribute services.

1.4 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [8].

The values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

In the context of this specification, the term “generic” referring to an access token indicates it is not tied to any specific User, whereas the term “User specific” indicates the access token is tied to a User.

1.5 Definitions and Abbreviations

The Mobile Connect Technical Overview [1] provides a list of definitions and abbreviations that are used within the Mobile Connect Specifications. It includes terminology from source standards and interprets that terminology in Mobile Connect terms.

1.6 References

1.6.1 GSMA Documentation References

Ref	Doc Number	Title
[1]	IDY.05	Mobile Connect Technical Overview
[2]	IDY.04	Mobile Connect Technical Architecture and Core Requirements
[3]	IDY.03	Mobile Connect Resource Server
[4]	IDY.01	Mobile Connect Device Initiated OIDC Profile
[5]	IDY.02	Mobile Connect Server Initiated OIDC Profile
[6]	IDY.56	Mobile Connect Client Credentials Profile
[7]	IDY.24	Mobile Connect Account Takeover Protection Definition and Technical Requirements

1.6.2 International Standards References

Ref	Doc Number	Title
[8]	RFC 2119	“Keywords for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. https://tools.ietf.org/html/rfc2119
[9]	RFC 6749	“The OAuth 2.0 Authorization Framework”, D. Hardt, Ed, October 2012. https://tools.ietf.org/html/rfc6749
[10]	RFC 6750	“The OAuth 2.0 Authorization Framework: Bearer Token Usage”, M. Jones, D. Hardt, October 2012. https://tools.ietf.org/html/rfc6750
[11]	E.164	“E.164: The international public telecommunication numbering plan”, International Telecommunication Union, 2010. https://www.itu.int/rec/T-REC-E.164-201011-I/en

2 Access to MC Attribute Services using MC Client Credentials

This section specifies the way attribute services MUST be accessed when they are provided in combination with MC Client Credentials.

It is important to note that the adaptations required in the ID GW as a result of this specification do not prevent the provision of the attribute services in exactly the same terms described in their current specifications. This means that, if they are being provided via the Device-Initiated and Server-Initiated modes already specified, it SHOULD still be possible to access them that way (subject to availability depending on the market, ID GW policies, etc.).

2.1 Access Token Request

The access token request MUST be performed as specified in section 4 of MC Client Credentials Profile [7].

The scope `openid` MUST NOT be included in the list of values contained in the `scope` parameter of the request, as MC Client Credentials is not an OIDC-based protocol.

2.2 Access Token Response

The access token response MUST be returned as specified in section 5 of MC Client Credentials Profile [7].

2.3 Resource Request

The resource request MUST be performed as indicated in the corresponding MC attribute service specification (e.g. MC ATP [7]).

However, given that the access tokens delivered by MC Client Credentials are generic, a new mechanism is defined to indicate the MC User whose data is being queried in the request. Namely, the following HTTP headers MUST be used for that purpose:

HTTP Header	Usage Category	Description
`User-ID-Type`	REQUIRED [if the bearer type access token provided in the request is generic]	MC User identification type used in the `User-ID` header. One of these values MUST be used: • `MSISDN`: Indicates the `User-ID` contains a plain MSISDN in international format according to ITU-T recommendation E.164 [11]. The plus sign (+) MUST NOT be included as a prefix. • `ENCR_MSISDN`: Indicates the `User-ID` contains an encrypted MSISDN as specified for the `login_hint` parameter in the Device-Initiated and Server-Initiated flows. See MC Technical Architecture and Core Requirements [2] for details. Support for the `MSISDN` user ID type is REQUIRED, whereas for `ENCR_MSISDN` is OPTIONAL.
`User-ID`	REQUIRED [if the bearer type access token provided in the request is generic]	MC User identification value as per the type indicated in the HTTP header above.

Table 1: New HTTP Headers for MC User Identification

Both the names and the values of these HTTP headers MUST be treated as case insensitive.

Apart from the addition of these two new headers, the resource request specification for the attribute service being adapted is respected. In particular, the HTTP method and HTTP parameters defined for it remain unchanged.

2.4 Resource Response

The resource response MUST be returned as indicated in the corresponding MC attribute service specification (e.g. MC ATP [7]).

However, as the scope `openid` is never requested when using MC Client Credentials (see 2.1) and consequently the access tokens delivered do not grant access to that scope, the `sub` claim MUST NOT be returned in the resource response unless the specific MC attribute service requires it.

Also, as a result of the MC User being indicated in the resource request (see 2.3), new error scenarios are now possible, the details of which can be found in Annex A.2.

2.5 Summary

The following table summarises the main changes introduced in the current definition of attribute services using OIDC-based flows when they need to be provided using the MC Client Credentials flow.

Attribute service aspect	Using MC Device-Initiated / MC Server-Initiated flow	Using MC Client Credentials
Access Token request	The `openid` scope is always requested	The `openid` scope is never requested
MC User identification	The MC User is tied to the user-specific access tokens being delivered	Access tokens are generic and the MC User has to be indicated in the resource request by means of two new HTTP headers: • User-ID-Type • User-ID
Resource response	The `sub` claim is always included in the response	The `sub` claim is never included in the response unless the specific MC attribute service requires it
Error scenarios	Only the error scenarios defined in the current specifications apply	New error scenarios are defined to handle issues related to the new MC User identification mechanism

Table 2: Main Changes to MC Attribute Services When Used with MC Client Credentials

Annex A Specific Error Codes and Descriptions

The following error scenarios are defined in addition to the ones already included in the MC Client Credentials [6], MC Resource Server [3] and attribute service specific (e.g. MC ATP [7]) specifications.

They MUST be considered and, whenever they apply, their associated HTTP responses and error codes MUST be returned as specified in the tables.

A.1 Access Token Response – Error Codes and Descriptions

No additional error scenarios are defined.

A.2 Resource Response – Error Codes and Descriptions

The following error scenarios and associated responses have been defined in accordance with the Oauth 2.0 - Bearer Token Usage specification [10].

Error Scenario	HTTP Status Code	Error Code	Error Description [recommended]
The access token used is generic and no User-ID or User-ID-Type headers have been included in the request	Bad Request 400	invalid_request	User-ID / User-ID-Type header is not used and the Access Token is not tied to an End-User
The access token used is user specific and the User-ID or the User-ID-Type headers have been included in the request	Bad Request 400	invalid_request	User-ID / User-ID-Type header MUST NOT be used if the Access Token is tied to an End-User
User-ID or User-ID-Type value is invalid	Bad Request 400	invalid_request	Invalid User-ID / User-ID-Type value: <reason> (<reason>: unsupported type, wrong format, etc.)
The User-ID specified is unknown	Bad Request 400	invalid_request	Unknown user

Annex B Example: Access to MC ATP using MC Client Credentials

B.1 Access Token Request

This is an example of a token request using the client credentials grant type as specified in MC Client Credentials [6]. The client is authenticated using the HTTP Basic authentication scheme and the scope requested is the one assigned to the MC ATP service (`mc_atp`).

```
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&scope=mc_atp
```

B.2 Access Token Response

The following is an example of a successful response to the previous request. The requested access token is delivered.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
"access_token":"2YotnFZFEjr1zCsicMWpAA",
"token_type":"Bearer",
"expires_in":3600,
}
```

B.3 Resource Request

The following example shows a request to the Resource Server in order to get the ATP information for the MC User indicated via the `User-ID-Type` and `User-ID` HTTP headers. The access token obtained in the previous step is used as a bearer token for the request to be authorized.

```
GET /premiuminfo HTTP/1.1
Host: server.example.com
Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
User-ID-Type: MSISDN
User-ID: 34680947298
```

B.4 Resource Response

The following is an example of a successful response to the previous request. The requested ATP data is returned.

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
"sim_change": "2018-01-30T18:39:50Z"
}
```

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	16/01/2020	First agreed version	Orange, Telefónica, Vodafone, GSMA	Pablo Guijarro / Telefónica
1.0	06/12/2022	Go though TG approval	TG	Yolanda Sanz/GSMA

C.2 Other Information

Type	Description
Document Owner	IDG
Editor / Company	Yolanda Sanz / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You MAY notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.