Mobile Connect Client Credentials Profile

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

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

Mobile Connect is a portfolio of mobile-enabled services to provide Authentication, Authorisation, Identity Services and Network Attribute Services to be used in conjunction with services offered to a User by Service Providers.

This specification enables a Service Provider to make a request to the Operator's Identity Gateway (ID GW) for an access token not tied to the User.

This specification is normative - it includes examples for illustration purposes that are non-normative.

1.2 Scope

Mobile Connect Client Credential Profile to deliver access token not tied to the user.

1.3 Audience

The target audience for this document are the Operator service/technical departments who are considering deploying Mobile Connect services in Client Credentials grant mode.

1.4 Relationship to Other Mobile Connect Documentation

This document describes and specifies the Mobile Connect Client Credentials grant mode. As no authorization request is needed (the client authentication is used as the authorization grant), It includes details of mechanisms for then obtaining tokens. It also includes examples and generic error codes.

The Mobile Connect Technical Architecture and Core Requirements document describes the Mobile Connect Architecture in more detail and also includes the core technical requirements and specification of elements for Mobile Connect that are generic to all Mobile Connect services and modes of operation.

The Mobile Connect Resource Server Specification provides details on how to handle a Resource request and the associated response for Mobile Connect Identity and Network Attribute services including error codes where this approach is used by a Mobile Connect service.

Each individual Mobile Connect service has its own definition document which includes service specific parameters, such as <scope> value and any service specific error codes. It also includes technical requirements that relate to that specific Mobile Connect service.

1.5 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 RFC2119 **Error! Reference source not found.**.

1.6 Terminology & Definitions

The Mobile Connect Technical Overview document **Error! Reference source not found.** 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.

1.7 Abbreviations

Term	Description
HTTP	Hyper Text Transfer Protocol
ID GW	Identity Gateway
JSON	Java Script Object Notation
SP	Service Provider (e.g. banks, webstores, government)
URI	Uniform Resource Identifier

1.8 References

Ref	Doc Number	Title
[1]	IDY.51	Mobile Connect Technical Architecture and Core Requirements
[2]	IDY.03	Mobile Connect Resource Server Specification
[3]	RFC 2119	"Keywords for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at https://tools.ietf.org/html/rfc2119
[4]	RFC 6749	"The OAuth 2.0 Authorization Framework", D. Hard5, Ed. October 2012 available at http://www.ietf.org/rfc/rfc6749.txt
[5]	RFC 5246	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008 https://tools.ietf.org/html/rfc5322
[6]	RFC 6750	M. Jones and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," RFC 6750, October 2012 https://tools.ietf.org/html/rfc6750

2 Client Credential flow

In specific use cases, the SP (Service Provider) server needs to have access to a Resource Server with an access token not tied to the user. This MUST be done by using the Client Credentials grant (OAuth2.0 [4]). In other words, the Client Credentials grant type is used by an SP to obtain an access token outside of the context of a user.

This specification describes the Mobile Connect Client Credentials mode including the structure of the Access Token Request and the various responses to that request including possible error codes.

Client Credentials mode MUST only be used where its use has been pre-agreed and configured for both participating servers (i.e. the SP server application and the Operator ID GW) and in business contexts where the legal conditions and regulative requirements for processing data are met.

The use of Client Credentials profile implies that personal data are not involved in the exchanges between the SP and the Resource Server unless:

1. the service logic and the lawful data processing basis allow it
2. the SP and the Operator agree that the Operator is not involved in the customer consent management (i.e.: legitimate interest and/or consent managed exclusively on Service Provider side).

The Operator ID GW should expose in its ID GW metadata that it supports the client_credentials grant type:

{…

“grant_types_supported”: […, “client_credentials”],

…

}

Figure 1 illustrates the Client Credential mode flow. This specification details the parameters involved in the Access Token Request and Response.

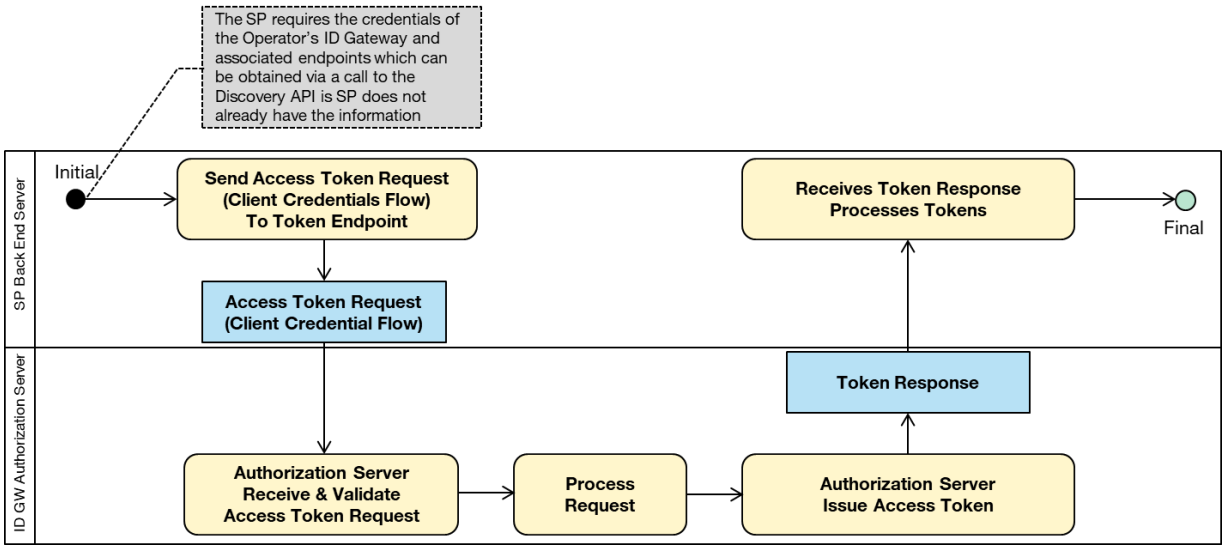

Figure 1: Mobile Connect Client Credentials Mode Flow

The high level flow is as follows:

- The SP needs an Access Token not tied to the user for a specific use case. This assumes that the SP is already registered with Mobile Connect.
- The SP sends an Access Token request to the ID GW (Authorization Server) with a grant type “client_credentials” and optional scope(s) (representing the resource(s) requested).

- The ID GW authenticates the SP using its client credentials. If the request is valid, the ID GW sends an Access Token for the scope(s).
- Where requested, the SP can then call the relevant resource endpoint (Mobile Connect Service-Specific Endpoint) by submitting the received Access Token to retrieve the requested attributes/claims (not shown in Figure 1).

3 Client Credential Authorization Request

Mobile Connect Providers may support one or both of the following mechanisms to cater for Service Provider applications with different capabilities.

3.1 Service Provider Authentication using HTTP Basic Authentication

In Mobile Connect, all Service Providers are issued with a client_id and client_secret during registration (and through the Discovery process). Service Providers in possession of a client_secret SHOULD use the HTTP Basic authentication scheme as defined in [RFC 2617] to authenticate. The client identifier is encoded using the "application/x-www-form-urlencoded" encoding algorithm and the client_secret is encoded using the same algorithm and used as the password. The authorization server MUST support the HTTP Basic authentication scheme for authenticating clients.

This is the recommended mechanism for client authentication.

3.2 Service Provider Authentication with Client Credentials in the Request Body[1]

Mobile Connect Providers MAY support including the client credentials (i.e. client_id and client_secret) in the request-body. Including the client credentials in the request-body using the two parameters is not recommended and SHOULD be limited to clients unable to directly utilize the HTTP Basic authentication scheme. The parameters can only be transmitted in the request-body and MUST NOT be included in the request URI. This is an optional feature.

4 Access Token Request

For Client Credential mode, an Access Token Request is submitted to the Operator's ID GW Token Endpoint.

- The communication with the ID GW MUST use HTTPS/TLS [5].
- The request MUST use POST as specified in Section 4.4.2 of the OAuth2.0 specification

[1] In a real-life scenario, few Operators have Service Providers who use request body to authenticate to the authorization server. This is not a recommended feature and Mobile Connect does not use this method for compliance, whereas HTTP Basic authentication mechanism must be supported by the IDGW.

4.1 Access Token Request Parameters

Table 11 lists the parameters to be included within a Client Credentials Access Token Request.

Parameter	Usage Category	Description
`grant_type`	REQUIRED	Value MUST be set to "`client_credentials`".
`scope`	REQUIRED	The scope of the access request as described in Section 3.3 of the OAuth2.0 specification **Error! Reference source not found.**.

Table 1: Access Token Request parameters

4.2 The <scope> Parameter

<scope> values determine the specific Mobile Connect services being requested by the Service Provider, subject to the SP being registered to use those services.

The Mobile Connect Client Credentials Access Token Request MUST contain the <scope> parameter which is a space delimited, case-sensitive list of ASCII strings (scope values). The scope values are depending on the specific Mobile Connect services being requested. Multiple scope values can be requested simultaneously, subject to the SP being registered to use those "scopes".

Scope values are defined for each Mobile Connect service in the relevant service "Definition and Technical Requirements" document.

5 Access Token Response

If the access token request is valid and authorized, the ID GW Authorization Server issues an Access Token. A refresh token SHOULD NOT be included.

Access Tokens are credentials used to access protected resources. An Access Token is a string representing an authorization issued to the SP Client. The string is opaque to the SP Client. Tokens represent specific scopes and durations of access, and enforced by the ID GW Resource Server and ID GW Authorization Server. Further information on the Access Token can be found in RFC6749 and RFC6750.

The authorization server issues an access_token and constructs the response by adding the following parameters to the entity-body of the HTTP response with a 200 (OK) status code:

Parameter	Usage Category	Description
`token_type`	REQUIRED	the type of the token issued.
`access_token`	REQUIRED	the access token issued by the authorization server, and to be used for calling resource end-points for Mobile Connect services
`expires_in`	RECOMMENDED	the lifetime in seconds of the Access Token.
`scope`	OPTIONAL	if identical to the scope requested by the client; otherwise, REQUIRED

Table 2: Access Token Response parameters

6 Security Considerations

The security considerations listed in the OAuth2.0 specifications SHALL be considered in the Mobile Connect implementation:

- Section 10, OAuth2.0 Specification **Error! Reference source not found.**.

Annex A Generic Error Codes and Descriptions for Client Credentials Mode: Error Responses for Access Token Request – Error Codes and Descriptions

The generic error response for an Access Token request listed in the OAuth2.0 specifications SHALL be considered in the Mobile Connect implementation (see Section 5.2, OAuth2.0 Specification). The following text is extracted from the OAuth 2.0 specification for convenience.

The authorization server responds with an HTTP 400 (Bad Request) status code (unless specified otherwise) and includes the following parameters with the response:

Parameter	Usage Category	Error code	Description
error	REQUIRED (a single ASCII [USASCII] error code from the following)	invalid_request	The request is missing a required parameter, includes an unsupported parameter value (other than grant type), repeats a parameter, includes multiple credentials, utilizes more than one mechanism for authenticating the client, or is otherwise malformed.
		invalid_client	Client authentication failed (e.g., unknown client, no client authentication included, or unsupported authentication method). The authorization server MAY return an HTTP 401 (Unauthorized) status code to indicate which HTTP authentication schemes are supported. If the client attempted to authenticate via the "Authorization" request header field, the authorization server MUST respond with an HTTP 401 (Unauthorized) status code and include the "WWW-Authenticate" response header field matching the authentication scheme used by the client.
		invalid_grant	The provided authorization grant (e.g., authorization, resource owner credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used in the authorization request, or was issued to another client.
		unauthorized_client	The authenticated client is not authorized to use this authorization grant type.
		unsupported_grant_type	The authorization grant type is not supported by the authorization server.
		invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.
error_description	OPTIONAL		Human-readable ASCII [USASCII] text providing additional information, used to assist the client developer in understanding the error that occurred.
error_uri	OPTIONAL		A URI identifying a human-readable web page with information about the error, used to provide the client developer with additional information about the error.

Table 3: Error Responses for Access Token Request – Error Codes and Descriptions

Values for the "error" and "error_description" parameters MUST NOT include characters outside the set %x20-21 / %x23-5B / %x5D-7E.

Values for the "error_uri" parameter MUST conform to the URI-reference syntax and thus MUST NOT include characters outside the set %x21 / %x23-5B / %x5D-7E.

The parameters are included in the entity-body of the HTTP response using the "application/json" media type as defined by [RFC4627]. The parameters are serialized into a JSON structure by adding each parameter at the highest structure level. Parameter names and string values are included as JSON strings. Numerical values are included as JSON numbers. The order of parameters does not matter and can vary.

For example:

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
  "error":"invalid_request"
}
```

Annex B Example Requests and Responses

B.1 Access Token Request (§4.4.2)

For example, the client makes the following HTTP request using transport-layer security (with extra line breaks for display purposes only):

```
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded
grant_type=client_credentials&scope=my_scope
```

B.2 Access Token Response (§4.4.3)

An example successful response sent by the ID GW

```
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,
  "scope":"my_scope"
 }
```

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	20/01/2020	New document for Approval	GSMA TG	Hubert Mariotte /ORANGE
1.0	06/12/2022	Go through 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.

stions & questions are always welcome.