

Mobile Connect Technical Reference

Version 2.0

11 August 2017

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 3](#_Toc455570316)

[1.1 Overview 3](#_Toc455570317)

[1.2 Definitions 3](#_Toc455570318)

[1.3 Abbreviations 3](#_Toc455570319)

[1.4 References 4](#_Toc455570320)

[1.5 Conventions 4](#_Toc455570321)

[1.6 Technical documentation map 4](#_Toc455570322)

[2 Scope Reference 5](#_Toc455570323)

[2.1 Mobile Connect Authentication scopes 5](#_Toc455570324)

[2.2 Mobile Connect Authorisation scopes 5](#_Toc455570325)

[2.3 Mobile Connect Identity Services scopes 5](#_Toc455570326)

[3 OIDC Response Amr Values 6](#_Toc455570327)

[4 Error Messages 9](#_Toc455570328)

[4.1 Mobile Connect Core & Authentication 23](#_Toc455570329)

[4.2 Mobile Connect Authorisation **Error! Bookmark not defined.**](#_Toc455570330)

[4.3 Mobile Connect Identity Services **Error! Bookmark not defined.**](#_Toc455570331)

[5 MCIS Attribute Names list 40](#_Toc455570332)

[5.1 Mobile Connect Phone Number 40](#_Toc455570333)

[5.2 Mobile Connect Identity Services Sign-up 40](#_Toc455570334)

[5.3 Mobile Connect Identity Services National ID 40](#_Toc455570335)

[Annex A Document Management 49](#_Toc455570336)

[A.1 Document History 49](#_Toc455570337)

[A.2 Other Information 49](#_Toc455570338)

# Introduction

## 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 Authentication, Authorisation and Identity & Attribute products that collectively are referred to as Mobile Connect.

This document specifies:

* **Error handling mechanism** for both device-initiated and server-initiated Mobile Connect services
* **Error messages**: error messages and example descriptive text to be displayed to the user
* **Identity Services attribute list**: normative claim names for Identity Services attributes.
* **Mobile Connect Attribute services** normative claims names for attribute services [i.e. Mobile Connect Know Your Customer (MC KYC), Mobile Connect Account Takeover Protection (MC ATP) and Mobile Connect Verified MSISDN (MC VM).

## Definitions

| Term  | Description |
| --- | --- |
| Mobile Connect Authentication  | Provides single factor and two-factor authentication using the mobile phone as the authentication device. |
| Mobile Connect Authorisation  | Provides single factor and two-factor authorisation using the mobile phone as the authorisation device. It also supported the first party and 3rd party authorisation.  |
| Mobile Connect Identity Services  | Retrieve Mobile Connect user’s personal data after a successful consent capture.  |
| Mobile Connect Attribute services  | Retrieve specific attributes of the Mobile Connect User, Account related claims or result of operations. |

## Abbreviations

| Term  | Description |
| --- | --- |
| RFC | Request for Comments |
| SP | Service Provider  |
| IOT | Internet Of Things |
| MCIS | Mobile Connect Identity Services |
| OIDC | OpenID Connect |

## References

| Ref | Doc Number | Title |
| --- | --- | --- |
| 1.
 | RFC 2119 | “Keywords for use in RFCs to Indicate Requirement Levels,” S. Bradner, March 1997. Available at <http://www.ietf.org/rfc2119.txt>  |
|  | RFC 2616 | “Hypertext Transfer Protocol (HTTP) an application level protocol,” J Gettys, J. Mogul, L. Masinter, P. Leach, T. Berners-Leem June 1999. Available at <http://www.ietf.org/rfc/rfc2616.txt> |
|  | RFC 6749 | “The Oauth 2.0 Authorization Framework,” D. Hard5, Ed. October 2012 available at <http://www.ietf.org/rfc/rfc6749.txt> |
|  | OpenID Connect | “An interoperable authentication protocol based on the Oauth 2.0 family of specifications” available at <http://openid.net/developers/specs/> |
|  | OpenID Discovery  | OpenID Connect discovery specifications. <https://openid.net/specs/openid-connect-discovery-1_0.html> |

## Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECMMENDED", "NOT RECMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](http://openid.net/specs/openid-connect-core-1_0.html#RFC2119) [1].

## Technical documentation map

The Mobile Connect architecture, technical specifications and implementation guidelines are encompassed by a set of documentation as laid out below:



Figure 1 : Mobile Connect technical documentation map

# Scope Reference

The following scope values are valid for use in the OIDC request parameter “scope”.

## Mobile Connect Authentication scopes

The following table defines the scopes that SHOULD be used for Mobile Connect Authentication products. A release 2 ID GW implementation must support both values.

| Scope | Description |
| --- | --- |
| “openid”  | By default, Mobile Connect authentication must be executed.  |
| “openid mc\_authn” | Same as above, but only supported from Mobile Connect Release 2 onwards.  |

Table : Mobile Connect authentication scopes

## Mobile Connect Authorisation scopes

The following table defines the scopes that SHOULD be used for Mobile Connect Authorisation products.

| Scope | Description |
| --- | --- |
| “openid mc\_authz”  | OIDC scope to identity Mobile Connect Authorisation products.  |

Table : Mobile Connect authorisation scope

## Mobile Connect Identity Services scopes

The following table describes the scopes that SHOULD be used within Mobile Connect Identity Service products.

| Scope | Description |
| --- | --- |
| “openid mc\_identity\_phonenumber” | Execute authentication and capture consent for MC enabled phone number |
| “openid mc\_identity\_signup” | Execute authentication and capture consent for sign up details  |
| “openid mc\_identity\_nationalid” | Execute authentication and capture consent for national ID.  |

Table : Mobile Connect Identity services scopes

## Mobile Connect Attribute Services Scopes

The following table describes the scopes that SHOULD be used within Mobile Connect attribute services.

| Scope | Description |
| --- | --- |
| "openid mc\_atp" | Execute authentication and capture consent to share account call settings, sim status and device change.  |
| "openid mc\_kyc\_plain" | Based on IDGW policies, if required execute authentication and capture consent to compare the SP provided customer information with the Mobile Connect User’s information held by the Operator. The SP provides attributes in plain text format. |
| "openid mc\_kyc\_hashed" | Based on ID GW policies, if required execute authentication and capture consent to compare the SP provided customer information with the Mobile Connect User’s information held by the Operator. The SP provides attributes in hashed format.  |
| "openid mc\_attr\_vm\_share" | Retrieve the device MSISDN from Operator’s network. It works in the On-net scenario only.  |
| "openid mc\_attr\_vm\_match" | Compare the SP provided MSISDN with the device MSISDN, and return the result in Boolean format. The SP provides the attribute values, in a plain text format.  |
| "openid mc\_attr\_vm\_match\_hash" | Compare the SP provided MSISDN with the device MSISDN, and return the result in Boolean format. The SP provides the attribute values, in a plain text format. |

Table : MC Attribute Service Scope values

# OIDC Response Amr Values

The following table defines the OIDC response amr value that must be returned by an ID GW, for the most commonly used authenticators across the different Mobile Connect products.

| Amr claim value  | Mobile Connect Authentication  | MobileConnect Authorisation | Description  |
| --- | --- | --- | --- |
| SIM\_OK | Mobile Connect Authenticate (single factor) | Mobile Connect Authorise(single factor) | SIM Applet authenticator , Uses SIM as a secure element and secure execution environment to support single-factor Mobile Connect authentication / authorisation  |
| SIM\_PIN | Mobile Connect Authenticate Plus(two factor) | Mobile Connect Authorise Plus(two factor) | SIM Applet authenticator, Uses SIM as a secure element and secure execution environment to support Two-Factor Mobile Connect authentication / authorisation |
| SM\_APP\_OK | Mobile Connect Authenticate(single factor) | Mobile Connect Authorise(single factor) | Smartphone app authenticator, to support single-factor Mobile Connect authentication / authorisation.  |
| SM\_APP\_PIN | Mobile Connect Authenticate Plus(two factor) | Mobile Connect Authorise Plus(two factor) | Smartphone app authenticator, to support Two-factor Mobile Connect authentication / authorisation. |
| USSD\_OK | Mobile Connect Authenticate(single factor) | Mobile Connect Authorise(single factor) | Network initiated USSD based authenticator, to support Mobile Connect single-factor authentication/ authorisation.  |
| USSD\_PIN | Mobile Connect Authenticate Plus(two factor) | Mobile Connect Authorise Plus(two factor) | Network initiated USSD based authenticator, to support Mobile Connect Two-factor authentication/ authorisation. |
| SMS\_URL\_OK | Mobile Connect Authenticate(single factor) | Mobile Connect Authorise(single factor) | SMS URL based authenticator, to support Mobile Connect single-factor authentication/ authorisation.  |
| SEAM\_OK | Mobile Connect Authenticate(single factor) | Not Available | Seamless authenticator to support Mobile Connect Single-factor authentication only. For Mobile Connect Authorisation and Mobile Connect Identity Services it MUST not be supported.  |

Table : amr values

# Error Handling Mechanism

Mobile Connect services can be offered either in device-initiated or server-initiated modes. Error messages must be propagated differently in both the scenarios.

## Error Handling in Device Initiated Mode

Mobile Connect follows the OpenID Connect error handling mechanism to send any errors back to the Service Provider. These errors can be returned in a query string to the Service Provider on redirect\_uri [through HTTP redirect 302] when the redirect URI is valid, or HTTP 400 Bad Request with a human readable string OR JSON object [Implementation choice] containing the error code and error description when the redirect URI is invalid. Errors must be returned as a JSON object containing the error code and error description using appropriate HTTP status codes for token and resource endpoints. These errors are returned to the Service Provider as described in the OpenID Connect specifications:

* <https://openid.net/specs/openid-connect-core-1_0-17.html#AuthError>
* <https://openid.net/specs/openid-connect-core-1_0-17.html#TokenErrorResponse>
* <https://openid.net/specs/openid-connect-core-1_0-17.html#UserInfoError> [applicable to service specific resource endpoint]

## Error Handling in Server Initiated Mode

Mobile Connect must return the errors to the Service Provider using HTTP status codes and a JSON object. The errors can be returned in the following scenarios.

* Mobile connect server-initiated authorization endpoint
* Mobile Connect Push Notification [i.e. errors through notification]
* Errors to Operator IDGW through Acknowledgement [from Service Provider]
* [https://openid.net/specs/openid-connect-core-1\_0-17.html#UserInfoError](http://openid.net/specs/openid-connect-core-1_0-17.html#UserInfoError) [applicable to service specific resource endpoint]

# Error Messages

Mobile Connect defines various error messages based on different scenarios that will be returned to the Service Provider and can receive errors from the Service Provider. These error messages are related to:

* Missing MANDATORY parameter(s) in authorization request
* Incorrect parameter values in authorization request
* Incorrect token request
* Incorrect Notification
* Errors to IDGW through acknowledgement to notification
* Errors mapped to abstract errors
* Mobile Connect User interaction failure
* Mobile Connect Service/Product specific errors

## Generic Errors

This section describes Mobile Connect generic errors applicable to all services.

### Mobile Connect in Device Initiated Mode

Operators can offer Mobile Connect services in device-initiated mode where service is initiated through user-agent [i.e. native app, web browser etc.,]. Error responses are returned from authorize, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

If authorization request contains a state parameter, then the error response MUST contain "state “parameter value. The value is set to the value received from the Service Provider. If correlation\_id is provided in the authorization request, then it must be included in the response, and the value must be set to the value received from the Service Provider.

The following is the example error response.



If redirect\_uri is missing or redirect\_uri value is invalid, then Operator IDGW always treat this as a high priority error and MUST return the appropriate error response as described in the following table.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| MSISDN/ENCR MSISDN/ PCR provided does not belong to the Operator.  | Redirect 302 | access\_denied | "Unknown user" [OR] "User is not recognized"  |
| MSISDN/ENCR\_MSDISDN belongs to the Operator, but MC services are not enabled, Note: IDGW policy does not allow to create partially active account  | Redirect 302 | access\_denied | "Mobile Connect User is not registered" [OR] "Unknown Mobile Connect User".  |
| System connection problems [internal to IDGW] (or) Authenticator unreachable (or) Expiration in server (or) Any Unexpected error [internal to IDGW]  | Redirect302 | server\_error (or) temporarily\_unavailable | Internal Server Error.  |
| Multiple requests for the same MSISDN sent at the same time  | Redirect 302 | access\_denied | The user is busy with another transaction.  |
| redirect\_uri value is invalid or not a registered URI.  | Bad Request 400 | invalid\_request   | redirect\_uri is invalid.  |
| response\_type parameter is missing or invalid | Redirect 302 | invalid\_request | MANDATORY parameter response\_type is missing or value is invalid.  |
| client\_id parameter is missing  | Redirect 302 | invalid\_request (or) access\_denied  | MANDATORY parameter client\_id is missing |
| client\_id parameter value is invalid | Redirect 302 | invalid\_request (or) unauthorized\_client (or) access\_denied | The client is not authorized to request an authorization code.  |
| client\_id is valid, but not allowed to make MC service requests  | Redirect 302 | access\_denied (or) unauthorized\_client | The client is not allowed to make MC service requests.  |
| scope parameter is missing (or) scope value "openid" is missing (or) invalid scope values (ex: "abcd") | Redirect 302 | invalid\_request (or) invalid\_scope | MANDATORY parameter scope is missing (or) invalid scope value  |
| version parameter is missing (or) version parameter value is invalid  | Redirect 302 | invalid\_request | MANDATORY parameter version is missing / invalid.  |
| state parameter exists, but the value is invalid | Redirect 302 | invalid\_request | RECOMMENDED parameter state is invalid  |
| nonce parameter is missing or nonce parameter exists, but the value is empty  | Redirect 302 | invalid\_request | MANDATORY parameter nonce is missing (or) invalid.  |
| login\_hint and login\_hint\_token parameters are missing Note: In the following conditions the IDGW SHOULD prompt the user to input MSISDN instead of throwing an error; -- MC service is for stand-alone authentication only in the device-initiated mode. -- If IDGW policy allows to capture MSISDN directly from the user [FC mode only].  | Redirect 302 | invalid\_request | MANDATORY parameters login\_hint\_token (or) login\_hint does not exist.  |
| login\_hint and login\_hint\_token both exist  | Redirect 302 | invalid\_request | Malformed request, duplicate parameter entries  |
| login\_hint (or) login\_hint\_token value is invalid  | Redirect302 | invalid\_request | Invalid value for login\_hint or login\_hint\_token  |
| acr\_values parameter is missing (or) acr\_values exist but contains an invalid value, other than supported values | Redirect 302 | invalid\_request | MANDATORY parameter acr\_values are missing or invalid values.  |
| display parameter exists and it has an invalid value (or)display parameter exists and IDGW does not support the requested value | Redirect 302 | invalid\_request | Invalid display value. / not supported.  |
| The same parameter exists multiple times  | Redirect 302 | invalid\_request | Multiple parameter names in the authorization request. Malformed request.  |
| prompt value exists, and it has an invalid value  | Redirect 302 | invalid\_request | prompt value is invalid  |
| claims parameter exists, but it does not contain any value (or) have invalid values.  | Redirect 302 | invalid\_request  | claims value is invalid,  |
| GET request is used, and the request parameter is NOT serialized using URI string serialization, IDGW able to validate the redirect\_uri.  | Redirect 302 | invalid\_request  | GET request invalid serialization  |
| POST request is used, the request parameters are NOT serialized using form serialization, IDGW can validate the redirect\_uri | Redirect 302 | invalid\_request  | POST request Invalid serialization  |
| response\_mode parameter exists, and it has a value not supported by the Operator IDGW  | Redirect302 | invalid\_request | response\_mode contains same as response\_type (or) invalid.  |
| max\_age parameter exists, and it has an invalid value  | Redirect 302 | Invalid\_request | Invalid max\_age value  |
| Multiple problems in authorization request [redirect URI is valid] | Redirect 302 | invalid\_request | Malformed request multiple problems exist |
| correlation\_id exists, but it has an empty value  | Redirect302 | invalid\_request | Invalid correlation\_id value.  |
| client\_name exists but it has empty value (or)client\_name parameter exists, but the provided value is not a registered client\_name with Operator IDGW and invalid | Redirect 302 | invalid\_request | Invalid client\_name value  |

Table : MC Services: Generic Errors-Device Initiated Authorize Endpoint

#### Error Responses: Device Initiated Token Endpoint

The token request is always a server-initiated request. It must be a POST request. An SP makes a token request by presenting the parameters and the form serialization to the Token endpoint. After validating the request, the token endpoint must return the errors in the following format:



| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| grant\_type parameter is missing (or) grant\_type parameter exists, but value is invalid or not supported | Bad Request400 | invalid\_request (or) unsupported\_grant\_type | MANDATORY parameter grant\_type is missing (or) invalid |
| Authorization code parameter is missing (or)Code parameter exists but value is invalid (or)Code parameter exists, value is already used or expired (or) Authorization code is valid, but not issued to the authenticated client (or) Authorization code is valid, but it is not issued to a MC OpenID Connect request | Bad Request400 | invalid\_grant (or) invalid\_request | MANDATORY parameter code is missing (or) invalid (or) expired  |
| redirect\_uri parameter is missing (or) redirect\_uri parameter exist and it has a value that DOES NOT match the one sent in the authorization request (or) redirect\_uri parameter exists, and it has unregistered value (or) Operator IDGW has multiple redirect URI values registered for a given client\_id. Redirect parameter exist and it has a value that matches one of the redirect URI registered with Operator IDGW, but the value DOES NOT match the one sent in the previous authorization request | Bad request 400 | invalid\_request | MANDATORY parameter redirect\_uri is missing (or) is invalid |
| client\_id parameter does not exist (or) client\_id parameter exists, but it has a value that is not registered at Operator IDGW | Bad Request 400 (or) 401 | access\_denied (or) invalid\_client | Invalid client credentials  |
| client\_secret parameter does not exist (or) client\_secret parameter exists, but it has invalid value (or)  | Bad Request400 (or) 401 | access\_denied (or) invalid\_client | Invalid client credentials  |
| correlation\_id does not exist but previous authorization request and response has correlation ID (or) correlation\_id exists but it has empty value (or) correlation\_id exists but it has value that DOES NOT match the one sent in the previous authorization request | Bad Request400 | invalid\_request | Missing MANDATORY parameter correlation ID (or) invalid |
| Same parameter exists multiple times | Bad Request400 | invalid\_request | Malformed request, the same parameter exists multiple times  |
| Unexpected error  | Internal server Problem 500 | server\_error | Internal error,  |
| System connection problem  | Service Unavailable 503 | server\_error | Service is not available,  |
| SP sends token request through POST, but without form serialization  | Bad Request400 | invalid\_request | No form serialization exists  |
| Multiple problems in token request | Bad Request400 | access\_denied | Multiple problems were in the token request.  |

Table : MC Services: Generic Errors - Device Initiated Token Endpoint

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize endpoint, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

For Mobile Connect server-initiated the authorization request must contain a signed request object. This section describes the error format and error messages returned from server-initiated authorize endpoint.

The following is the example error response.



##### Error Responses: Request Object Parameter Validation

The following tables describe all request object parameters; their validation and corresponding error responses.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| MSISDN/ENCR MSISDN/ PCR provided does not belong to the Operator.  | Bad Request400 | access\_denied | Mobile Connect User is not recognized. [OR] Unknown User |
| MSISDN/ENCR\_MSDISDN belongs to the Operator, but MC services are not enabled, Note: IDGW policy does not allow to create partially active account  | Bad Request400 | access\_denied | "Mobile Connect User is not registered" [OR] "Unknown Mobile Connect User".  |
| response\_type parameter is missing or invalid | Bad Request400 | invalid\_request | MANDATORY parameter response\_type is missing or value is invalid.  |
| client\_id parameter is missing  | Bad Request400 | invalid\_request (or) access\_denied  | MANDATORY parameter client\_id is missing |
| client\_id parameter value is invalid | Bad Request400 | invalid\_request (or) unauthorized\_client (or) access\_denied | The client is not authorized to request an authorization code.  |
| client\_id is valid, but not allowed to make MC service requests  | Bad Request400 | access\_denied (or) unauthorized\_client | The Client is not allowed to make MC service requests.  |
| scope parameter is missing (or) scope value "openid" is missing (or) invalid scope values (ex: "abcd") | Bad Request400 | invalid\_request (or) invalid\_scope | MANDATORY parameter scope is missing (or) invalid scope value  |
| version parameter is missing (or) version parameter value is invalid  | Bad Request400 | invalid\_request | MANDATORY parameter version is missing (or) invalid.  |
| nonce parameter is missing or nonce parameter exists but value is empty  | Bad Request400 | invalid\_request | MANDATORY parameter nonce is missing (or) invalid.  |
| login\_hint and login\_hint\_token parameters are missing  | Bad Request400 | invalid\_request | MANDATORY parameters login\_hint\_token (or) login\_hint does not exist.  |
| login\_hint and login\_hint\_token both exist  | Bad Request400 | invalid\_request | Malformed request, duplicate parameter entries  |
| login\_hint (or) login\_hint\_token value is invalid  | Bad Request400 | invalid\_request | Invalid value for login\_hint (or) login\_hint\_token  |
| acr\_values parameter is missing (or) acr\_values exist but contains invalid value, other than supported values | Bad Request400 | invalid\_request | MANDATORY parameter acr\_values is missing (or) invalid values.  |
| Same parameter exists multiple times  | Bad Request400 | invalid\_request | Multiple parameter names in the authorization request. Malformed request.  |
| claims parameter exists but it does not have any value (or) invalid values.  | Bad Request400 | invalid\_request  | claims value is invalid,  |
| GET request is used, and the request parameters are NOT serialized using URI string serialization, IDGW able to validate the redirect\_uri.  | Bad Request400 | invalid\_request  | GET request invalid serialization  |
| POST request is used, the request parameters are NOT serialized using form serialization, IDGW can validate the redirect\_uri | Bad Request400 | invalid\_request  | POST request Invalid serialization  |
| response\_mode parameter exists, and it has a value not supported by the Operator IDGW  | Bad Request400 | invalid\_request | response\_mode contains same as response\_type (or) invalid.  |
| max\_age parameter exists, and it has an invalid value  | Bad Request400 | invalid\_request | Invalid max\_age value  |
| Multiple problems in authorization request [redirect URI is valid] | Bad Request400 | invalid\_request | Malformed request multiple problems exist |
| correlation\_id exists, but it has empty value  | Bad Request400 | invalid\_request | Invalid correlation\_id value.  |
| client\_name exists, but it has empty value (or)client\_name parameter exists, but the provided value is not a registered client\_name with Operator IDGW and is invalid | Bad Request400 | invalid\_request | Invalid client\_name value  |
| client\_notification\_token MANDATORY parameter is missing (or) client\_notification\_token exists, but it has an invalid value | Bad Request400 | invalid\_request | MANDATORY parameter client\_notification\_token is missing (or) invalid |
| notification\_uri parameter is missing (or) notification\_uri exists but it is not registered with IDGW (or) has an invalid value | Bad Request400 | invalid\_request | MANDATORY parameter notification\_uri is missing (or) invalid.  |
| iss parameter is missing (or) iss parameter exists, but it has an invalid value | Bad Request400 | invalid\_request | MANDATORY parameter SP’s iss parameter is missing (or) invalid |
| aud parameter is missing (or) aud parameter exists, but it has an invalid value | Bad Request400 | invalid\_request | aud parameter is missing (or) invalid.  |

Table : MC Services: Generic Errors - Server Initiated Request Object Validation

##### Error Responses: Server Initiated Authorization Request

The following table describes the MC Authorization Request parameters which includes request object.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
|  response\_type parameter is missing (or) response\_type parameter exists value is invalid (or) response\_type parameter exists and the value is valid, but not matching the request object response\_type value.  | Bad Request 400 | invalid\_request | MANDATORY parameter response\_type is missing (or) invalid (or) malformed request; response\_type values does not match |
| client\_id parameter does not exist | Bad Request400 | access\_denied (or) invalid\_request | MANDATORY parameter client ID does not exist  |
| client\_id parameter exists, but it has invalid value  | Bad Request400 | access\_denied (or) unauthorized\_client | Unknown client ID  |
| client\_id parameter exists, but the value does not match the request object client\_id value | Bad Request400 | invalid\_request | Malformed request, ambiguous client ID values  |
| scope parameter is missing (or)scope parameter exists, it does not contain "openid"  | Bad Request 400 | invalid\_request | MANDATORY parameter scope parameter is missing  |
| scope parameter exists, but it does not match the request object scope value  | Bad Request400 | invalid\_request | Malformed request, ambiguous scope values |
| scope parameter exists, request scope is not supported by the Operator IDGW | Service Unavailable 503 | server\_error | Service is not available.  |
| Request object parameter does not exist (or) request object parameter exists, but value is not valid | Bad Request400 | invalid\_request | MANDATORY parameter request is missing  |
| Signature validation of request object is failed  | Bad Request400 | invalid\_request | Malformed request, invalid signature  |
| System connection problem (or) Expiration in server | Service Unavailable 503 | server\_error | Service is not available,  |
| Multiple requests for the same MSISDN sent at the same time  | Internal Server Error 500 | server\_error | The user is busy with another transaction.  |
| Unexpected error [Internal to IDGW] | Internal Server Error500 | server\_error | Internal Server Error |
| IDGW time-out due to internal error.  | Internal Server Error 500 | server\_error | Timeout: Server internal error.  |

Table : MC Services: Generic Errors – Server Initiated Authorize Request Validation

#### Error Response: Notification [IDGW to SP]

The following table describes the generic errors that can be returned to SP’s notification endpoint from Operator IDGW.

The error format will be like the following:



| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| Authenticator unreachable/ expiration in server  | server\_error | Service is not available,  |
| System connection problems [internal to IDGW] | server\_error | Connection problem.  |
| Unexpected error [Internal to IDGW] | server\_error | Internal server error.  |

Table : MC Services: Generic Errors - Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to Operator IDGW]

This section describes the error responses from SP to Operator IDGW through acknowledgement.

The Error format is like the following.



| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid JWT received from Operator IDGW [ID Token] | Bad Request 400 | invalid\_request | Invalid JWT [ID Token] is received.  |
| Invalid access\_token is received  | Bad Request400 | invalid\_request | Invalid access\_token is received |
| Invalid auth\_req\_id | Bad Request 400 | invalid\_request | Malformed request, unable to identify the response.  |
| Invalid correlation\_id  | Bad Request400 | invalid\_request | Malformed request, unable to correlate the response.  |
| token\_type parameter is missing | Bad Request400 | invalid\_request | MANDATORY parameter token\_type is missing  |
| token\_type parameter exists, but the value is not Bearer | Bad Request400 | invalid\_request | Invalid token type value  |
| expires\_in parameter does not exist  | Bad Request400 | invalid\_request | MANDATORY parameter expires\_in does not exist.  |
| expires\_in parameter exists, but value is invalid  | Bad request400 | invalid\_request | Invalid expires\_in value  |
| ID Token parameter does not exist | Bad Request400 | invalid\_request | MANDATORY parameter ID Token does not exist |
| Access Token parameter does not exist | Bad Request400 | invalid\_request | MANDATORY parameter access token does not exist  |
| System connection problem (or) Expiration in server | Service Unavailable 503 | server\_error | Service is not available,  |
| Unexpected error [Internal to SP] | Internal Server Error500 | server\_error | Internal Server Error |
| SP server time-out due to an internal error.  | Internal Server Error 500 | server\_error | Timeout: Server internal error.  |

Table : MC Services: Generic Errors - Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

There are two different types of resource endpoints for attributes in Mobile Connect. One is to share Mobile Connect User attributes through PremiumInfo endpoint and another one is Service specific resource endpoint. This section describes generic errors that can be returned from both the endpoints.

#### Error Responses Service Specific/ PremiumInfo Resource Endpoint

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Unexpected error  | Internal Server Error 500  | server\_error | Internal server error,  |
| System connection problems  | Service Unavailable 503 | server\_error | Service is not available,  |
| Access token is sent but is not obtained through Mobile Connect OIDC request (or) Access token exists, but it is invalid (or) (or) the expired access token  | Unauthorized 401 | invalid\_request (or) invalid\_token | Invalid access token (or) access token does not exist (or) expired invalid access token |
| Resource request is sent using POST and "access\_token" parameter does not exist in the Form encoded body | Unauthorized 401 | If the access token does not exist, then the following error SHOULD be returned. Error code and error description must not be returned. Example: HTTP/1.1 401 Unauthorized WWW-Authenticate: Bearer  |
| The resource request is sent through POST entity-header includes the "Content-type header and the value is NOT "application/x-www-form-urlencoded".  | Bad Request400 | invalid\_request |   |
| The resource request is sent through POST and it is not form url encoded as described in RFC 6750  | Bad Request400 | invalid\_request | Malformed request, invalid url encoding |
| The resource request is sent through POST, and the content to be encoded in the entity-body contains non-ASCII characters as defined In RFC 6750  | Bad Request400 | invalid\_request | Malformed request, invalid non-ascii characters |
| Any unsupported parameters exist in the request | Bad Request400 | invalid\_request | Malformed request, invalid parameters  |
| Multiple problems in the resource request | Bad Request400 | invalid\_request | Malformed request, invalid parameters.  |
| The request requires higher privileges than provided by the access token  | Forbidden 403 | insufficient\_scope (or) access\_denied | Insufficient scope.  |
| Unexpected error [Internal to Resource Server] | Internal Server Error500 | server\_error | Internal Server Error |
| Resource server time-out due to internal error.  | Internal Server Error 500 | server\_error | Timeout: Server internal error.  |

Table : MC Services: Generic Errors - Resource Endpoint

## Mobile Connect Core & Authentication

###  Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Authentication service in the device-initiated mode where service is initiated through user-agent [i.e. native app, web browser, etc.,]. Error responses are returned from authorize endpoint, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

|  Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Mobile Connect User failed to authenticate [ example: invalid pin] | Redirect 302 | authentication\_failure[or]access\_denied | Mobile Connect user failed to authenticate |
| Mobile Connect User cancelled or rejected the authentication request on his/her mobile device | Redirect 302 | authentication\_denied (or) authentication\_failure (or)access\_denied | Mobile Connect user rejected / cancelled the authentication  |
| Mobile Connect User unable to authenticate timeout occurred | Redirect 302 | authentication\_failure(or)access\_denied | Timeout occurred during authentication.  |

Table : MC Authentication: Errors - Device Initiated Authorize endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in the generic errors section.

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize endpoint, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service specific error responses in the server-initiated model.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Requested authentication strength is not implemented.  | Bad Request 400 | invalid\_request | Requested authentication is not supported.  |
| Authentication for the given strength is implemented, but service is not available now due to internal error.  | Service Unavailable 503 | server\_error | Request authentication is temporarily not available. |

Table : MC Authentication: Errors - Server Initiated Authorize Endpoint

#### Error Responses: Notification [IDGW to SP]

| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| Mobile Connect User failed to authenticate | authentication\_failure (or)access\_denied | Mobile Connect user failed to authenticate |
| Mobile Connect User cancelled or rejected the authentication request on his/her mobile device | authentication\_denied (or)authentication\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the authentication  |
| Mobile Connect User is prompted with authentication, the timeout occurs.  | authentication\_failure (or) access\_denied | Timeout occurred during authentication. |

Table : MC Authentication: Errors - Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error Code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid authentication proof token [ID Token] | Bad Request400 | invalid\_request | Mobile Connect Authentication proof token [ID token] is invalid.  |

Table : MC Authentication: Errors – Server Initiated ACK SP to IDGW

## Mobile Connect Authorisation

### Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Authorisation service in the device-initiated mode where service is initiated through user-agent [i.e. native app, web browser, etc.,]. Error responses are returned from authorize, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| In the single-page environment Mobile Connect User failed to approve the requested prompt (or) IDGW unable to assert the user’s identity | Redirect 302 | authorisation\_failure (or)access\_denied | Mobile Connect user failed to approve the requested prompt |
| In the single-page environment Mobile Connect User cancelled or rejected the MC authorisation request on his/her mobile device | Redirect 302 | authorisation\_denied (or) authorization\_failure(or)access\_denied | Mobile Connect user rejected / cancelled the authentication  |
| Mobile Connect User unable to authorise timeout occurred | Redirect 302 | authorisation\_failure(or)access\_denied | Timeout: User is not available to respond, later.  |
| Requested authorisation strength is not implemented.  | Redirect 302 | invalid\_request | Requested authorisation service is not implemented.  |
| Authorisation for the given strength is implemented, but service is not available at this moment due to internal error.  | Redirect 302 | server\_error | Authorisation for the given strength is implemented, but service is not available now due to internal error.  |
| In a two-page environment, IDGW unable to assert the identity of the user.  | Redirect 302 | authorisation\_failure(or)access\_denied | User is not identified, unable to get the approval from MC User |
| In a two-page environment, user is identified in the first step, but rejects or cancels the approval  | Redirect 302 | authorisation\_failure (or) authorisation\_denied(or)access\_denied | User is identified, but unable to get the approval from MC User |
| Binding message does not exist (or) invalid | Bad Request400 | invalid\_request | MANDATORY parameter binding\_message is missing  |
| context parameter does not exist (or) invalid  | Bad Request400 | invalid\_request | MANDATORY parameter context is missing  |

Table : MC Authorisation: Errors - Device Initiated Authorize endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in the generic errors section.

### Mobile Connect in Server Initiated Mode

Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service-specific error responses in the server-initiated model.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Requested authorisation strength is not implemented.  | Bad Request 400  | invalid\_request | Requested authorisation service is not implemented.  |
| Authorisation for the given strength is implemented, but service is not available at this moment due to an internal error.  | Service Unavailable 503 | server\_error | Authorisation for the given strength is implemented, but service is not available now due to an internal error.  |
| client\_name does not exist  | Bad Request 400 | invalid\_request | MANDATORY parameter client\_name is missing.  |
| client\_name exists, but value is not a registered client\_name at Operator IDGW | Bad Request400 | invalid\_request | Malformed request. Invalid / unregistered client\_name.  |
| binding\_message does not exist (or) invalid | Bad Request400 | invalid\_request | MANDATORY parameter binding\_message is missing  |
| context parameter does not exist (or) invalid  | Bad Request400 | invalid\_request | MANDATORY parameter context is missing  |

Table : MC Authorisation: Errors - Server Initiated Authorize endpoint

#### Error Responses: Notification [IDGW to SP]

| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| In the single-page environment Mobile Connect User failed to approve the requested prompt (or) IDGW unable to assert the user’s identity | authorisation\_failure(or)access\_denied | Mobile Connect user failed to approve the requested prompt.  |
| In the single-page environment Mobile Connect User cancelled or rejected the MC authorisation request on his/her mobile device | authorisation\_denied (or) authorisation\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the authentication  |
| Mobile Connect User unable to authorize, timeout occurred | authorisation\_failure (or) access\_denied | Timeout occurred during capturing approval from the user.  |
| Authorisation for the given strength is implemented, but service is not available at this moment due to internal error.  | server\_error | Request authentication is temporarily not available |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | authorisation\_failure (or)access\_denied | User is not identified, unable to get the approval from MC User |
| In a two-page environment, user is identified in the first step, but rejects or cancels the approval.  | authorisation\_denied (or) access\_denied(or) authorisation\_failure | User is identified, but unable to get the approval from MC User |

Table : MC Authorisation: Errors – Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid authorisation proof token [ID Token] | Bad Request400 | invalid\_request | Mobile Connect authorisation proof token is invalid.  |
| Invalid access token and not tied to the MC authorization proof token  | Bad Request 400 | invalid\_request | Mobile Connect Authorisation access token is not valid.  |

Table : MC Authorisation: Errors – Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| The Access token is submitted to resource endpoint to process MC authorization transaction, and resource server finds it is invalid.  | Unauthorized 401 | invalid\_request (or) invalid\_token | Invalid token, unable to proceed with the transaction. |

Table : MC Authorisation: Errors - Resource Endpoint

## Mobile Connect Identity Phone Number

### Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Identity Phone Number service in the device-initiated mode where service is initiated through user-agent [i.e. native app, web browser, etc.,]. Error responses are returned from authorize endpoint, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

In a two-page environment, all authentication failures must be same as described in Section 5.2.

|  Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | Redirect 302 | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | Redirect 302 | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | Redirect 302 | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | Redirect 302 | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | Redirect 302 | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MCIS Phone Number: Errors - Device Initiated Authorize Endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in Generic errors section.

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service specific error responses in the server-initiated mode.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| client\_name parameter does not exist (or) invalid | Bad Request400 | invalid\_request | MANDATORY parameter client\_name is missing.  |

Table : MCIS Phone Number: Errors - Server Initiated Authorize Endpoint

#### Error Responses: Notification [IDGW to SP]

In a two-page environment, all server-initiated authentication failures must be same as described in Section 5.2.

| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | consent\_failure (or) access\_denied | Timeout occurred during consent capture for phone number.  |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MCIS Phone Number: Errors - Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid identity phone number proof token [ID Token] | Bad Request400 | invalid\_request | Mobile Connect phone number proof token is invalid.  |
| Invalid access token and not tied to the MC phone number proof token  | Bad Request400 | invalid\_request | Mobile Connect phone number access token is not valid.  |

Table MCIS Phone Number: Errors - Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

None. Already covered in Generic errors section.

## Mobile Connect Identity National ID

### Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Identity NationalID service in device-initiated mode where service is initiated through user-agent [i.e. native app, web browser, etc.,]. Error responses are returned from authorize, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

 In a two-page environment, all authentication failures must be same as described in Section 5.2.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure] for national ID  | Redirect 302 | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | Redirect 302 | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent for National ID |
| Mobile Connect User unable to give consent timeout occurred | Redirect 302 | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | Redirect 302 | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | Redirect 302 | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure for MC National ID.  |

Table : MCIS National ID: Errors – Device Initiated Authorize endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in Generic errors section.

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize endpoint, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service-specific error responses in the server-initiated model.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| client\_name parameter does not exist  | Bad Request400 | invalid\_request | MANDATORY parameter client\_name is missing.  |

Table : MCIS National ID: Errors - Server Initiated Authorize endpoint

#### Error Responses: Notification [IDGW to SP]

In a two-page environment, all server-initiated authentication failures must be same as described in Section 5.2.

| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | consent\_failure (or) access\_denied | Timeout occurred during consent capture for National ID.  |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MCIS National ID: Errors – Server Initiated Notification IDGW to SP

#### Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid identity NationalID proof token [JWT - ID Token] | Bad Request400 | invalid\_request | Mobile Connect NationalId proof token is invalid.  |
| Invalid access token and not tied to the MC NationalID proof token  | Bad Request400 | invalid\_request | Mobile Connect National ID access token is not valid.  |

 Table :MCIS National ID: Errors – Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

None. Already covered in Generic errors section.

## Mobile Connect Identity Sign-Up

### Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Identity Sign-Up service in the device-initiated mode where service is initiated through user-agent [i.e. native app, web browser, etc.,]. Error responses are returned from authorize endpoint, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

In a two-page environment, all authentication failures must be same as described in Section 5.2.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | Redirect 302 | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | Redirect 302 | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | Redirect 302 | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | Redirect 302 | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | Redirect 302 | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MCIS Sign-Up: Errors - Device Initiated Authorize Endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in Generic errors section.

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize endpoint, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service-specific error responses in the server-initiated model.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| client\_name parameter does not exist (or) invalid | Bad Request400 | invalid\_request | MANDATORY parameter client\_name is missing.  |

Table : MCIS Signup: Errors – Server Initiated Authorize Endpoint

#### Error Responses: Notification [IDGW to SP]

In a two-page environment, all server-initiated authentication failures must be same as described in Section 5.2.

| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MCIS Sign-Up: Errors – Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid identity Signup proof token [JWT - ID Token] | Bad Request400 | invalid\_request | Mobile Connect Signup proof token is invalid.  |
| Invalid access token and not tied to the MC Signup proof token  | Bad Request400 | invalid\_request | Mobile Connect Signup access token is not valid.  |

Table : MCIS Sign-Up: Errors - Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

None. Already covered in Generic errors section.

## Mobile Connect Attributes Know Your Customer [KYC]

### Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Attributes KYC service in device-initiated mode where service is initiated through user-agent [i.e. native app, web browser etc.,]. Error responses are returned from authorize endpoint, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

 In a two-page environment, all authentication failures must be same as described in Section 5.2.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| claims parameter exists, but MANDATORY parameters inside claims are missing (or) claims parameter exist, but the value is empty (or) claims parameter does not exist | Redirect 302 | invalid\_request | MANDATORY values in the claims parameter are missing for MC KYC service (or) invalid |
| client\_name parameter does not exist (or) invalid | Redirect302 | invalid\_request | MANDATORY parameter client\_name is missing.  |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | Redirect 302 | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | Redirect 302 | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | Redirect 302 | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | Redirect 302 | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | Redirect 302 | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MC KYC: Errors – Device Initiated Authorize Endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in Generic errors section.

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize endpoint, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service-specific error responses in the server-initiated model.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| client\_name parameter does not exist (or) invalid | Bad Request400 | invalid\_request | MANDATORY parameter client\_name is missing.  |
| claims parameter does not exist (or) claims parameter exist but MANDATORY parameters inside claims are missing (or) claims parameter exist but the value is empty | Bad Request 400 | invalid\_request | MANDATORY parameter claims are missing in the request for MC KYC service (or) invalid  |

Table : MC KYC: Errors – Server Initiated Authorize Endpoint

#### Error Responses: Notification [Operator IDGW to SP]

In a two-page environment, all server-initiated authentication failures must be same as described in Section 5.2.

| Error Scenario | Error code | Error Description [REOMMENDED text] |
| --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | consent\_failure (or)access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | consent\_failure (or)access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MC KYC: Errors - Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid identity KYC proof token [JWT - ID Token] | Bad Request400 | invalid\_request | Mobile Connect KYC proof token is invalid.  |
| Invalid access token and not tied to the MC KYC proof token  | Bad Request400 | invalid\_request | Mobile Connect KYC access token is not valid.  |

Table : MC KYC: Errors - Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

None. Already covered in Generic errors section.

## Mobile Connect Attributes Account Takeover Protection [ATP]

MC ATP MUST operate in server-initiated mode. By default, no prompt will be displayed to the user. If IDGW policy mandates to capture the consent from MC User, then it will be prompted.

### Mobile Connect in Device Initiated Mode

MC ATP product does not operate in the device-initiated mode.

### Mobile Connect in Server Initiated Mode

The Operator can offer Mobile Connect services in server-initiated mode where service is initiated from a Server. Error responses are returned from authorize endpoint, push notification service and resource endpoints as described below.

####  Error Responses: Server Initiated Authorize Endpoint

This section describes service-specific error responses in the server-initiated model.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| client\_name parameter does not exist (or) invalid | Bad Request400 | invalid\_request | MANDATORY parameter client\_name is missing.  |
| claims parameter does not exist (or) claims parameter exist but MANDATORY parameters inside claims are missing(or)claims parameter exist but value is empty | Bad Request 400 | invalid\_request | MANDATORY parameter claims are missing for MC ATP service (or) invalid |

Table : MC ATP: Errors – Server Initiated Authorize Endpoint

#### Error Responses: Notification [Operator IDGW to SP]

In a two-page environment, all server-initiated authentication failures must be same as described in Section 5.2.

| Error Scenario | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | consent\_failure(or)access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | consent\_failure (or)access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |

Table : MC ATP: Errors - Server Initiated Notification IDGW to SP

#### Error Responses: ACK To Notification [SP to IDGW]

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| Invalid identity ATP proof token [JWT - ID Token] | Bad Request400 | invalid\_request | Mobile Connect ATP proof token is invalid.  |
| Invalid access token and not tied to the MC ATP proof token  | Bad Request400 | invalid\_request | Mobile Connect ATP access token is not valid.  |

Table : MC ATP: Errors - Server Initiated ACK SP to IDGW

### Error Responses: Resource Endpoint

None. Already covered in Generic errors section.

## Mobile Connect Attributes Verified MSISDN Match & Share

### Mobile Connect in Device Initiated Mode

The Operator can offer Mobile Connect Attributes VM service in device-initiated mode only where service is initiated through user-agent [i.e. native app, web browser, etc.,]. Error responses are returned from authorize endpoint, token and resource endpoints as described below.

#### Error Responses: Device Initiated Authorize Endpoint

 The following errors are applicable if Operator captures the consent.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| In the single-page environment Mobile Connect User failed to give consent (or) IDGW is unable to assert the user’s identity. [authentication failure]  | Redirect 302 | consent\_failure(or) access\_denied | Mobile Connect user failed to give consent (or) unable to identify.  |
| In the single-page environment Mobile Connect User cancelled or rejected the consent request on his/her consent device | Redirect 302 | consent\_denied (or) consent\_failure (or) access\_denied | Mobile Connect user rejected / cancelled the consent  |
| Mobile Connect User unable to give consent timeout occurred | Redirect 302 | consent\_failure (or) access\_denied | Timeout occurred during consent capture |
| In a two-page environment, IDGW failed to assert the user’s identity the first step when prompted for authentication.  | Redirect 302 | consent\_failure (or) access\_denied | Mobile Connect User is not identified.  |
| In a two-page environment, user is identified in the first step, but rejects or cancels the consent approval.  | Redirect 302 | consent\_denied (or)consent\_failure (or)access\_denied | Mobile Connect User has denied the consent (or) consent failure.  |
| Network MSISDN is not available in the HTTP header | Redirect302 | access\_denied | Device MSISDN is not available.  |

Table : MC VM: Errors – Device Initiated Authorize Endpoint

#### Error Responses: Device Initiated Token Endpoint

None. Already covered in Generic Errors section.

### Error Responses: Resource Endpoint

Resource endpoint common errors are already covered in Generic section.

| Error Scenario | HTTP mode | Error code | Error Description [RECOMMENDED text] |
| --- | --- | --- | --- |
| mc\_claims parameter does not exist | Bad Request 400 | invalid\_request | MANDATORY parameter mc\_claims are missing  |
| mc\_claims parameter exist but has MANDATORY parameter device\_msisdn is missing [VM share] | Bad Request400 | invalid\_request | MANDATORY parameter is missing from mc\_claims.  |
| mc\_claims parameter exist, but has no entries.  | Bad Request400 | invalid\_request | MANDATORY parameter values from mc\_claims are missing.  |

Table : MC VM: Errors – Resource Endpoint

# MCIS & Attribute Services Names list

This section provides information about normative claim names for the Mobile Connect Identity Services.

## Mobile Connect Phone Number

This section provides MCIS Phone number product claim names that must be used in the MCIS Phone number product OIDC request and responses.

| Attribute Name | Description |
| --- | --- |
| phone\_number | User's Mobile Connect designated mobile number |

Table : MCIS Phone Number Attributes

## Mobile Connect Identity Services Sign-up

This section provides MCIS Sign-up product claim names that must be used in the MCIS Signup product OIDC request and responses.

| Attribute Name | MANDATORY | Description |
| --- | --- | --- |
| phone\_number\_alternate | Yes | User's alternate/secondary telephone number [E.164] |
| title | No | Salutation |
| given\_name | Yes | Given name(s) or first names |
| family\_name | Yes | Surname(s) or last name(s) of the user  |
| middle\_name | No | Middle name(s) of the user  |
| street\_address | Yes | User’s street (incl. house name/number)  |
| city | No | User’s city  |
| state | No | User’s State / County  |
| postal\_code | Yes | User’s Zip/ Postcode |
| country | Yes | User’s postal country  |
| email | No | User’s e-mail |

Table : MCIS Sign Up Attributes

## Mobile Connect Identity Services National ID

This section provides MCIS National ID product claim names that must be used in the MCIS National ID product OIDC request and responses.

| Attribute Name | MANDATORY | Description |
| --- | --- | --- |
| phone\_number | No | User's Mobile Connect designated mobile number.  |
| title | No | Salutation |
| given\_name | Yes | Given name(s) or first names |
| family\_name | Yes | Surname(s) or last name(s) of the user  |
| middle\_name | No | Middle name(s) of the user  |
| street\_address | Yes | User’s street (incl. house name/number)  |
| state | No | User’s State / County  |
| postal\_code | No | User’s Zip/ Postcode |
| country | No | User’s postal country  |
| email | No | User’s e-mail |
| birthdate | Yes | User’s birth date  |
| national\_identifier | Yes | User’s Identifier (eIDAS), any national identifier like Social Security Identifier, passport e t c. (depends on the local regulations) |

Table : MCIS National ID Attributes

## MC KYC Attribute List

This section provides MC KYC (Know Your Customer) Attribute list

| **Response Match Values**  |
| --- |
| "Y"– match is successful"N-NA"- match failed, data is not available"N-AV"– match failed; data is available "N-AD"– match failed, data is available but access is denied |

 Table : MC KYC Response Values

The following table identifies the request attributes for the plain text KYC Match service variant; for the hashed variant, the attribute names SHOULD be appended with "\_hash"(i.e., given\_name\_hash).

| **Attribute Name** | **Usage** | **Description** |
| --- | --- | --- |
| given\_name | **MANDATORY** ([name](OR)[given\_name, family\_name]) | Given name(s) or first name(s) of the End-User. Note that in some cultures, people can have multiple given names; all can be present, with the names being separated by space characters. Always used in conjunction with the family\_name attribute.  |
| family\_name | Family name(s), surname(s) or last name(s) of the End-User. Note that in some cultures, people can have multiple family names or no family name; all can be present, with the names being separated by space characters. Always used in conjunction with the given\_name attribute.  |
| name | concatenated given\_name and family\_name.  |
| address | **MANDATORY** ([address] (OR)[houseno\_or\_housename, postal\_code, town, country] | concatenated houseno\_or\_housename, postal\_code and optionally town and country.  |
| houseno\_or\_housename | Registered house number or house name  |
| postal\_code | Registered Zip code or post code  |
| town | Registered city or town name  |
| country | Registered country  |
| birthdate | OPTIONAL | End-User's birthday, represented as an [**ISO 8601:2004**](https://openid.net/specs/openid-connect-basic-1_0.html%22%20/l%20%22ISO8601-2004) [ISO8601‑2004] YYYY-MM-DD format. The year MAY be 0000, indicating that it is omitted.  |

Table MCKYC Request Attributes

For each attribute, if there is a successful match, the attribute name+value SHOULD be echoed back to the TSP in the response.

| **Attribute Name** | **Usage**  |
| --- | --- |
| given\_name | **MANDATORY** ([name](OR)[given\_name, family\_name]) |
| family\_name |
| name |
| address | **MANDATORY** ([address] (OR) [houseno\_or\_housename, postal\_code, town, country] |
| houseno\_or\_housename |
| postal\_code |
| town |
| country |
| birthdate | OPTIONAL |
| given\_name\_match | **MANDATORY** ([name\_match] (OR)[given\_name\_match, family\_name\_match]) |
| family\_name\_match |
| name\_match |
| address\_match | **MANDATORY** ([address\_match] (OR) [houseno\_or\_housename\_match, postal\_code\_match, town\_match, country\_match]] |
| houseno\_or\_housename\_match |
| postal\_code\_match |
| town\_match |
| country\_match |
| birthdate\_match | OPTIONAL |

| **Attribute Name** | **Usage**  | **Response values** |
| --- | --- | --- |
| is\_lost\_stolen | OPTIONAL | Allowed boolean values are true / false |
| billing\_segment | OPTIONAL | Allowed values "PAYG","PAYM", "Business" |
| account\_state | OPTIONAL | Allowed values "active"/ "inactive" |

Table : MC KYC Response attributes

## MC ATP Attribute List

The attribute set returned within the Account Takeover Protection service is described in this section. The ID GW SHOULD only offer the ATP service if it has access to all the MANDATORY attribute values.

| **Attribute Name** | **Usage Category** | **Description** |
| --- | --- | --- |
| is\_unconditional\_call\_divert\_active | MANDATORY | Mobile phone account has an unconditional call divert set to a number; allowed boolean values true or false |
| is\_lost\_stolen | OPTIONAL | Boolean values true or false |
| sim\_change | MANDATORY | Timestamp[[1]](#footnote-2) of last MSISDN <-> IMSI pairing change |
| device\_change | OPTIONAL | Timestamp[[2]](#footnote-3) of last MSISDN <-> IMEI pairing change |
| account\_state | OPTIONAL | "active"or "inactive"[[3]](#footnote-4).  |

Table : MC ATP Attribute Set

## MC VM Attribute List

This section describes the attributes used in MC VM Share and MC VM Match services.

### Mobile Connect Verified MSISDN Share

For Mobile Connect Verified MSISDN Share any one of the following parameters must be supported based on the service variant being requested (see section **Error! Reference source not found.**). The values must be returned through attribute share endpoint.

|  |  |  |
| --- | --- | --- |
| **Attribute name**  | **Type**  | **Description**  |
| device\_msisdn | string  | MSISDN returned to the SP (via UserInfo). [**E.164**](http://openid.net/specs/openid-connect-core-1_0.html#E.164) [E.164] is RECOMMENDED as the format of this Claim, for example, +441234567890 |

Table : MC VM Attribute Set

### Mobile Connect Verified MSISDN Match

#### Resource Request Using ‘claims’ Parameters

For Mobile Connect Verified MSISDN Match any one of the following claims must exist in the resource request.

|  |  |  |
| --- | --- | --- |
| **Claim parameter name**  | **Type**  | **Description**  |
| device\_msisdn | String  | The value is the MSISDN to verify. [E.164] is RECOMMENDED as the format of this Claim, for example, +441234567890 |
| device\_msisdn\_hash | String | Hashed value of device\_msisdn. SHA256 algorithm is RECOMMENDED for backward interoperability to current implementations[[4]](#footnote-5). New implementations SHOULD NOT use SHA256[[5]](#footnote-6) unless backward interoperability is required. Hashing algorithms can be negotiated offline[[6]](#footnote-7) |

Table : MC VM Resource Request Attribute Set

#### Resource Response Parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Claim parameter name**  | **Type**  | **Usage Category** | **Description**  |
| device\_msisdn\_verified | Boolean | MANDATORY | True or False. Match result.  |

Table : MC VM Resource Endpoint Response

# Mobile Connect Provider Metadata

This section describes required Mobile Connect Provider Metadata configuration based on OpenID Provider Metadata and with Mobile Connect specific amendments. The RECOMMENDED location to host provider metadata is:

<https://idgw-operator.example.com/mc_examplepath/.well-known/openid-configuration>

### OpenID Provider Metadata

| **Field Name** | **Usage Category** | **Description** |
| --- | --- | --- |
| issuer | MANDATORY | Same as defined in [5] |
| authorization\_endpoint | MANDATORY | The device-initiated authorization endpoint only. It is same as defined in [5].  |
| bc\_authorize\_endpoint | MANDATORY | The server-initiated authorization end point only. It is same as defined in [xx].  |
| token\_endpoint | MANDATORY | Same as defined in [5] |
| jwks\_uri | MANDATORY | Same as defined in [5] |
| scopes\_supported | MANDATORY | The default scope "openid" must be supported. This parameter must contain all the Mobile Connect scopes supported by the Operator IDGW. Operators must register their own Mobile Connect innovation product scopes before exposing them through this parameter. The syntax is same as defined in the [5].  |
| response\_types \_supported | MANDATORY | This parameter must list down all response types used in Mobile Connect. [i.e. for FC and BC]. The syntax is same as defined in [5].  |
| grant\_types\_supported | MANDATORY | This parameter must list down all Mobile Connect grant\_types. The syntax is same as defined in [5]. It must have a value "authorization\_code" |
| acr\_values\_supported | MANDATORY | It must have Mobile Connect acr values i.e. [1,2,3,4] based on ISO29115. The syntax is same as defined in [5].  |
| id\_token\_signing\_alg\_values\_supported | MANDATORY | Same as defined in [5]  |
| id\_token\_encryption\_alg\_values\_supported | OPTIONAL [for future] | Same as defined in [5]. Placeholder for future requirements.  |
| id\_token\_encryption\_enc\_values\_supported | OPTIONAL [for future] | Same as defined in [5]. Placeholder for future requirements. |
| request\_object\_signing\_alg\_values\_supported | OPTIONAL [MANDATORY if server-initiated is supported] | Same as defined in [5].  |
| request\_object\_enryption\_alg\_values\_supported | OPTIONAL | Same as defined in [5]. Place holder for future requirements.  |
| claims\_parameter\_supported | OPTIONAL [MANDATORY if MC KYC and ATP are supported] | Same as defined in [5]. This parameter must be true, if MC KYC and MC ATP products are supported.  |
| request\_parameter\_supported | OPTIONAL [MANDATORY if server-initiated is supported] | Same as defined in [5].  |
| ui\_locales\_supported | MANDATORY | Same as defined in [5].  |

Table : MC Provider Metadata [Derived from OIDC]

## Hashing Algorithms

This section lists hashing algorithms that can be used to obfuscate attribute values, allowing an exact match to be recognised without directly revealing the value. The identifiers can appear in the mc\_hash\_algs\_supported metadata member.

The only currently defined value is "SHA-256". It is used by early implementations but SHOULD NOT be used unless backwards compatibility with those implementations is required as the hash algorithm in this situation SHOULD be deliberately slow to mitigate dictionary attacks. Better algorithms exist (such as PBKDF2 and Argon2id). It is expected that a better algorithm will be RECOMMENDED in the future.

| **Hashing Algorithm** | **Identifier**  |
| --- | --- |
| SHA-256, as hex digits | SHA-256 |
| PBKDF2 using HMAC with SHA-256 | PBKDF2-HMAC-SHA256[[7]](#footnote-8) |
| Argon2id | ARGON2ID[[8]](#footnote-9) |

Table : RECOMMENDED Hashing Algorithms

## Mobile Connect Specific Provider Metadata Parameters

This section describes Mobile Connect specific parameters.

| **Field Name** | **Usage Category** | **Description** |
| --- | --- | --- |
| mc\_version  | MANDATORY | A JSON array containing the list of the Mobile Connect profile versions [i.e. mc\_v1.0, mc\_v1.1, mc\_v2.0 etc]  |
| mc\_amr\_values\_supported  | MANDATORY | The parameter must all amr values supported by the Operator IDGW  |
| mc\_hash\_algs\_supported | MANDATORY | JSON array containing a list of hash algorithms supported by the MC provider, for where there a requirement in MC services to obfuscate attribute values [e.g., MC KYC, MC VM etc.,]. See section 7.2. |
| mc\_di\_scopes\_supported | MANDATORY | This parameter will list all MC services supported by the IDGW in device-initiated mode |
| mc\_si\_scopes\_supported | MANDATORY | This parameter will list all MC services supported by the IDGW in server-initiated mode.  |
| mc\_claims\_paramter\_supported | MANDATORY | 'true'; if mc\_claims is supported in the resource call 'false': if mc\_claims is NOT supported in the resource call. The mc\_claims parameter is used to request that specific claims be returned from resource end point. The value is a JSON object listing the requested Claims and is part of the resource request. |
| login\_hint\_types\_supported | MANDATORY | The values must be MSISDN, ENCR\_MSISDN and PCR |

Table : MC Specific Provider Metadata Parameters

The following is an example of Mobile Connect Provider Metadata configuration.

HTTP/1.1 200 OK

Content-Type: application/json

 {

 "issuer": "https://mc-idgw-operator.example.com",

 "authorization\_endpoint":

 "https://mc-idgw-operator.example.com/connect/authorize",

 "token\_endpoint":

 "https://mc-idgw-operator.example.com/connect/token",

 "premiuminfo\_endpoint":

 "https://server.example.com/connect/userinfo",

 "jwks\_uri": "https://mc-idgw-operator.example.com/jwks.json",

 "scopes\_supported": ["openid","mc\_authn","mc\_authz","mc\_kyc\_hash"],

 "response\_types\_supported": ["code", "mc\_bc\_async\_code"],

 "acr\_values\_supported": ["2", "3"],

 "id\_token\_signing\_alg\_values\_supported": ["RS256","ES256", "HS256"],

 "request\_object\_signing\_alg\_values\_supported": ["none","RS256", "ES256"],

 "claims\_parameter\_supported": true,

 "ui\_locales\_supported": ["en-US","en-GB","en-CA","fr-FR", "fr-CA"],

 "mc\_version": ["mc\_v1.0", "mc\_v1.1", "mc\_v2.0", "mc\_v2 .2"],

 "mc\_amr\_values\_suppored": ["SIM\_OK", "SIM\_PIN", "FIDO\_OK", "FIDO\_PIN"],

 "mc\_hash\_algs\_supported": ["SHA-256"],

 "mc\_di\_scope\_values\_supported": ["openid mc\_authn", "openid mc\_attr\_vm\_share"],

 "mc\_si\_scope\_values\_supported": ["openid mc\_authn", "openid mc\_atp"],

 "mc\_claims\_parameter\_supported": true

 }

1. Document Management
	1. Document History

| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
| --- | --- | --- | --- | --- |
| 1.0 | 27/05/2016 | New document  | PDATA/PSMC | Siva (Venkatasivakumar Boyalakuntla) / GSMA |
| 1.1 | 12/05/2017 | Transfer of PRD from Personal Data |  | Nick Cheung / GSMA |
| 2.0 | 11/08/2017 | Major update with new error messages (member´s feedback) and reorganised per Mobile Connect product | TG | Venkatasivakumar Boyalakuntla / GSMA |

* 1. 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.

1. It must adhere to the RFC 3339 absolute timestamp format. [↑](#footnote-ref-2)
2. Please refer above footnote [2]. [↑](#footnote-ref-3)
3. The values always depend on mobile account status. [↑](#footnote-ref-4)
4. Changing RECOMMENDED hashing algorithm for interoperability is for future study by CPAS. [↑](#footnote-ref-5)
5. SHA256 is fast but to mitigate brute force attacks on the hash the hashing algorithms should be slow like e.g. PBKDF2 [↑](#footnote-ref-6)
6. Currently identified algorithms are PBKDF2, SHA256\_crypt, Argon2 and SHA256. An operator and SP can negotiate any of these algorithms offline. Changing RECOMMENDED algorithms for interoperability is for future study. [↑](#footnote-ref-7)
7. CPAS defined identifier, once PBKDF2 standard sets out a new one, MC specs will adopt the same. Implementation details are out of scope for this document. [↑](#footnote-ref-8)
8. CPAS defined identifier, once ARGON2ID standard sets out a new one, MC specs will adopt the same. Implementation details are out of scope for this document. [↑](#footnote-ref-9)