Mobile Connect Resource Server Technical Requirements

Version 1.0

03 June 2019

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

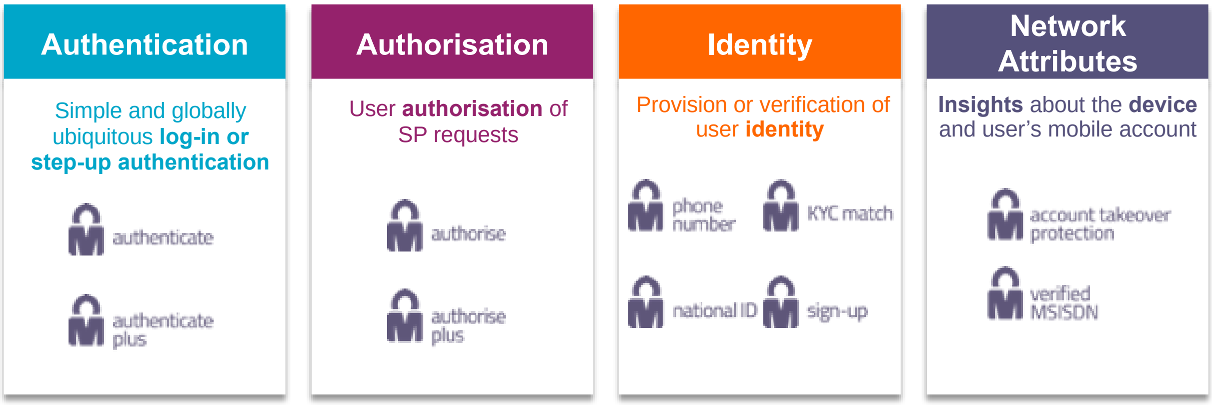
The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

Mobile Connect is a portfolio of mobile-enabled services that can be integrated into a SP's application to support access to services provided by the SP. Mobile Connect provides authentication, authorisation, and permissioned access to a User's attributes.


Authentication
Simple and globally ubiquitous log-in or step-up authentication
authenticate
authenticate plus
Authorisation
User authorisation of SP requests
authorise
authorise plus
Identity
Provision or verification of user identity
phone number
KYC match
national ID
sign-up
Network Attributes
Insights about the device and user's mobile account
account takeover protection
verified MSISDN

- : Mobile Connect Portfolio of Services

Mobile Connect is based upon the OpenID Connect (OIDC) protocol [1] which provides an identity

layer on top of the OAuth 2.0 protocol [5]. It allows Users to be identified by their MSISDN (or a related Pseudonymous Customer Reference) and authenticated via their mobile device.

Mobile Connect defines two profiles to support Device-Initiated and Server-Initiated requests for authentication, authorisation or permissioned access to User attributes.

The serving Mobile Operator supports and selects an appropriate Authenticator to present the authentication, authorisation or permissioned access requests to the User on their mobile device depending on device capability and Level of Assurance required.

Mobile Connect provides access to a set of User attributes[1] provided by the Mobile Operator, that can be shared or validated with a SP, subject to User consent.

The Mobile Connect architecture consists of a Core framework around which additional components can be added to support different Mobile Connect services that utilise the Core framework.

[1] Open ID Connect specifies a set of attributes that can be obtained from the OIDC Provider's Resource Server (i.e. the serving Operator's IDGW) also referred to as 'Protected Resources'. Mobile Connect provides an enriched set of attributes that also includes information relating to a User's mobile account and status – this information can be made available by the same Resource Server or a separate one depending on use case and implementation choice

This document describes the use of a Resource Server for supporting Mobile Connect attribute services. Based upon a successful OIDC Authorization Request, resulting in the SP receiving an ID Token and a valid Access Token from the Operator's IDGW, the Access Token can be used to request the sharing or matching of the attributes based upon the requested services in the original OIDC Authorization Request (via the `scope` parameter). A Resource Server exposes the appropriate Resource endpoint to which Resource Requests are made and from which Resource Responses are received by the SP. This document describes the format for the Resource Request and the associated Resource Response, includes the technical requirements for the implementation of the Resource Server and also includes the error responses that may be received back from the Resource endpoint.

This document is normative - it includes examples for illustrative purposes that are non-normative.

1.2 Scope

In Scope	Out of Scope
• Resource Request and Resource Response to and from a Resource endpoint / Resource Server • Generic Error Responses from the Resource endpoint	• Detailed specification of Mobile Connect services

1.3 Audience

The target audience for this document are mobile Operators' service / technical departments who are considering deploying Mobile Connect Identity and Network Attribute services.

1.4 Relationship to Other Mobile Connect Documentation

This document describes the use of a Resource Server for the processing of Resource Requests and the return of an appropriate response for Mobile Connect attribute services. It includes the requirements associated with the deployment of a Resource Server, including the format of Resource Requests and associated responses. It also includes generic requirements relating to the deployment of attribute services. A Resource Server is only deployed to support Mobile Connect attribute services and builds upon the Core framework and associated Core requirements. A Resource Request can only be initiated upon a successful OIDC Authorization through which the specific MC service is requested and the issue of valid ID and Access Tokens once the User has been authenticated and User consent given, if required.

The Mobile Connect Technical Architecture and Core Requirements document [13] along with the Mobile Connect API profiles – Mobile Connect Device-Initiated OIDC Profile [14] and the Server-Initiated OIDC Profile [15] together define the Mobile Connect Core framework upon which specific Mobile Connect services can be built. This also includes the provision of appropriate Authenticators on a User's mobile device (i.e. the Authentication Device) to support OIDC Authorization.

The Mobile Connect Technical Overview [12] provides a high-level description of Mobile Connect and how it works. It also includes a master list of abbreviations and terminology used within Mobile Connect documents and a map of that documentation set. It serves as a starting point for understanding how Mobile Connect works and also references the relevant documents for the reader to obtain further detail.

Each individual Mobile Connect service has its own service "Definition and Technical Requirements" 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 RFC 2119 [3].

1.6 Terminology & Definitions

Mobile Connect technical specifications and related documentation make use of terms that are defined by the OpenID Connect Core Specification [1] and supporting specifications and extended in the OIDF CIBA (Client Initiated Backchannel Authentication Flow) [2].

The Mobile Connect Technical Overview document [12] 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.

Due to potential confusion with OIDC and OAuth 2.0 terminology, the initial Mobile Connect service request which underpins Mobile Connect Authentication, Authorisation and User consent associated with attribute services, is referred to as an OIDC Authorization Request[2] (spelled with a 'z') throughout this document.

1.7 References

Ref	Doc Number	Title
[1]	OpenID Connect Core Specification	"An interoperable authentication protocol based on the OAuth 2.0 family of specifications" available at https://openid.net/specs/openid-connect-core-1_0.html
[2]	OIDF CIBA	OpenID Connect MODRNA Client Initiated Backchannel Authentication Flow 1.0 https://openid.net/specs/openid-connect-modrna-client-initiated-backchannel-authentication-1_0.html
[3]	RFC 2119	"Keywords for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at https://tools.ietf.org/html/rfc2119

[2] In OAuth2.0 the initial request is referred to as an "Authorization Request", whereas in OIDC it is referred to as an "Authentication Request". Mobile Connect offers several services including MC Authentication and MC Authorisation, hence MC specifications have adopted the term "OIDC Authorization Request" to describe this initial service request in the protocol flow.

[4]	RFC 2616	“Hypertext Transfer Protocol (HTTP) an application level protocol”, J Gettys, J. Mogul, L. Masinter, P. Leach, T. Berners-Lee, June 1999. Available at http://www.ietf.org/rfc/rfc2616.txt
[5]	RFC 6749	“The OAuth 2.0 Authorization Framework”, D. Hard5, Ed. October 2012 available at https://tools.ietf.org/html/rfc6749
[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
[7]	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
[8]	RFC 6819	Lodderstedt, T., McGloin, M., and P. Hunt, “OAuth 2.0 Threat Model and Security Considerations,” RFC 6819, January 2013 (TXT). https://www.ietf.org/rfc6819.txt
[9]	RFC 7519	M. Jones, J Bradley, N. Sakimura “JSON Web Token (JWT)”, RFC 7519, MAY 2015 https://tools.ietf.org/html/rfc7519
[10]	RFC 7515	JSON Web Signature (JWS) https://tools.ietf.org/html/rfc7515
[11]	RFC 7516	Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, http://www.rfc-editor.org/info/rfc7516
[12]	IDY.05	Mobile Connect Technical Overview
[13]	IDY.04	Mobile Connect Technical Architecture and Core Requirements
[14]	IDY.01	Mobile Connect Device-Initiated OIDC Profile
[15]	IDY.02	Mobile Connect Server-Initiated OIDC Profile
[16]	IDY.16	Mobile Connect Product Manager’s Lifecycle Handbook
[17]		Mobile Connect Privacy Principles
[18]		GSMA Regulatory considerations for processing personal data and attributes for Mobile Connect

2 OpenID Connect

OpenID Connect (OIDC) is a simple Identity layer that sits on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of a User based on the authentication performed by an Authorization Server as well as to obtain basic profile information about the User in an inter-operable and REST-like manner.

OpenID Connect provides an additional token (an ID Token) along with the OAuth 2.0 Access Token. The ID Token is represented as a signed JWT [9] and contains a claim set related to the authentication context of the subject (i.e. User).[3].

OpenID Connect doesn't specify how users should actually be authenticated - Mobile Connect is a specific implementation of Open ID Connect (OIDC) that uses the User's MSISDN (and an associated Pseudonymous Customer Reference) as an identifier and their mobile device as the Authentication Device. Additionally, it specifies a range of information about the User that can be shared with a Client, subject to the User's consent.

The OpenID Connect Core Specification [1] defines the core OIDC functionality that underpins Mobile Connect and Device-Initiated mode. This includes the mechanism for requesting User attributes (referred to as "claims"), using an Access Token, and the associated response[4].

3 Mobile Connect Resource Server

Mobile Connect is based upon a split architecture that consists of an Authorization Server which handles OIDC Authorization and the issue of tokens to a SP, and a Resource Server which manages the sharing or validation of User attributes with a SP based upon a Mobile Connect service request (i.e. an OIDC Authorization Request) and the issue of a valid Access Token by the Authorization Server.

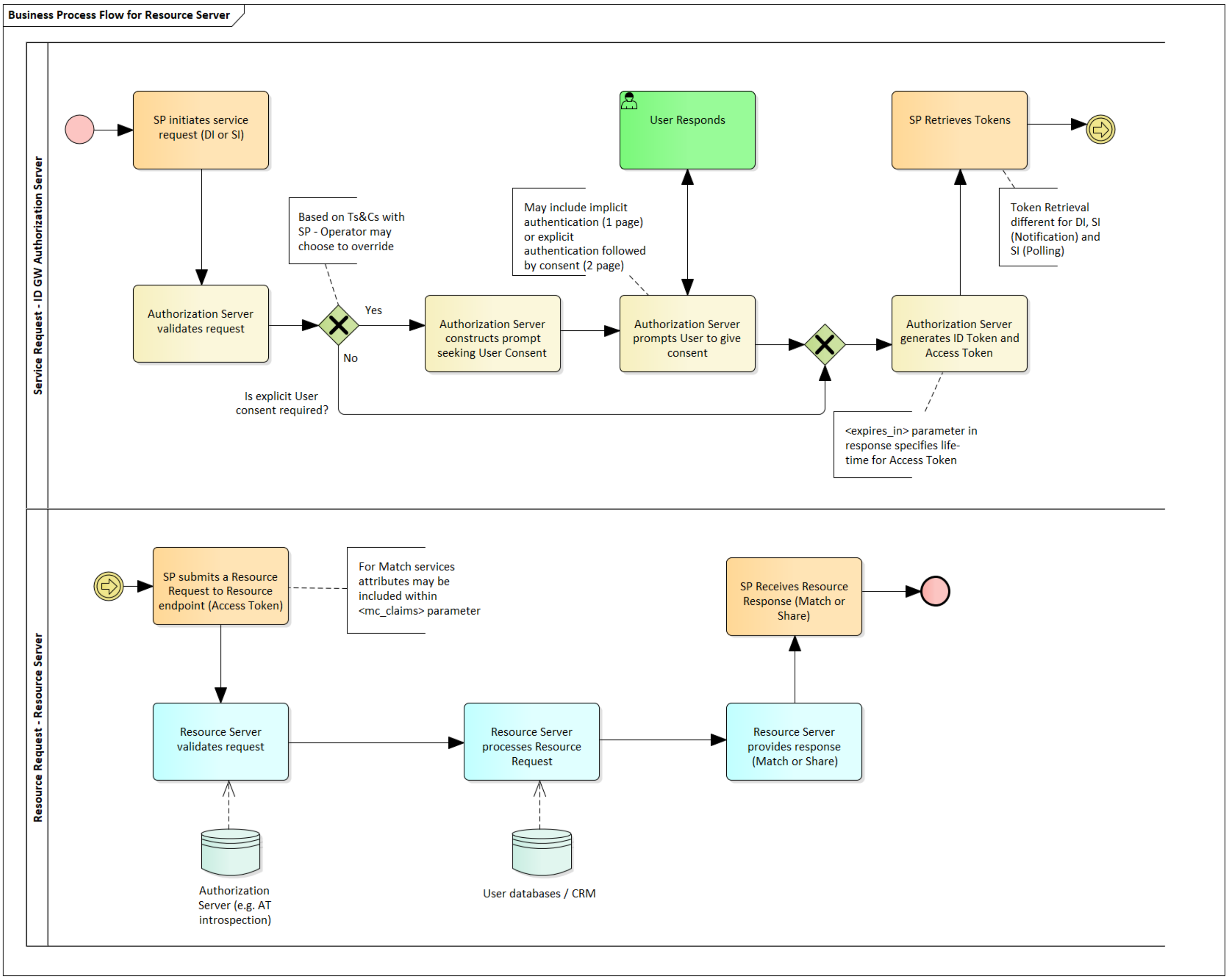
□ illustrates the flow. A service request is submitted by the SP to the IDGW Authorization Server using a Device-Initiated or Server-Initiated request. The submitted `scope` parameter value specified the Mobile Connect services being requested.

The Authorization Server validates and processes the request. A User must give their consent before any attributes can be shared or validated with the SP.

If User consent is required then this can be captured by the Authorization Server or it can be captured by the SP, subject to the contractual agreement with the Operator IDGW. However, the Operator may choose to override this and enforce an explicit consent as part of the service request.

[3] The JWT can be a plain text JWT or cryptographically protected JWT – represented as a signed JWT using JSON Web Signatures (JWS) [10] or as an encrypted JWT using JSON Web Encryption (JWE) [11]. Within Mobile Connect the ID Token is a signed JWT using JWS and is not encrypted

[4] Note that OIDC refers to the Resource Request and Resource Response as "UserInfo Request" and "UserInfo Response" respectively.


Business Process Flow for Resource Server
Service Request - ID GW Authorization Server
SP initiates service request (DI or SI)
Authorization Server validates request
Based on Ts&Cs with SP - Operator may choose to override
Yes
No
Is explicit User consent required?
Authorization Server constructs prompt seeking User Consent
May include implicit authentication (1 page) or explicit authentication followed by consent (2 page)
User Responds
Authorization Server prompts User to give consent
Authorization Server generates ID Token and Access Token
<expires_in> parameter in response specifies life-time for Access Token
SP Retrieves Tokens
Token Retrieval different for DI, SI (Notification) and SI (Polling)
Resource Request - Resource Server
SP submits a Resource Request to Resource endpoint (Access Token)
For Match services attributes may be included within <mc_claims> parameter
Resource Server validates request
Authorization Server (e.g. AT introspection)
Resource Server processes Resource Request
User databases / CRM
Resource Server provides response (Match or Share)
SP Receives Resource Response (Match or Share)

- : Service Request Flow for Attribute Services

Assuming that consent has been given, the Authorization Server then generates the ID Token and Access Token. The ID Token acts as a security token and also used to enable the Access Token to be validated by the SP for security reasons. The Access Token may have an extended period of validity (i.e. long-lived) which means that it can be used to retrieve the relevant attributes (defined by the service request) at any time as long as the Access Token remains valid. However by default all MC services are defined to have one time use of Access Token due to security reasons. The mechanism for Token retrieval differs depending upon the MC OIDC Profile and mode being used. Mobile Connect Technical Architecture and Core Requirements [13] provides more detailed sequence diagrams illustrating the flow for Device-Initiated mode and the Server-Initiated modes. The Mobile Connect Device-Initiated OIDC Profile [14], and the Mobile Connect Server-Initiated OIDC Profile [15] define the API calls and responses for each mode.

The Resource Server is not part of the Core framework as it is only deployed for those services that involve the sharing or validation of MC attributes associated with a User. However, it is dependent upon the Core framework and relies on the issue of a valid Access

Token as a result of a Mobile Connect service request. The physical deployment of the Resource Server is an implementation choice for the Operator.

The lower half of □ illustrates the process of the SP initiating a Resource Request to the relevant Resource endpoint exposed by the Resource Server. The Resource Server receives the request which contains a valid Access Token (generated by the originating service request). If the service request was for a match service where the SP submits the relevant attributes and associated values that is wishes to be validated, the Resource Request may also contain these attributes and values in the Resource Request[5]. The Resource Server interfaces with the IDGW Authorization Server (e.g. via an introspection backend) to be able to validate the Access Token as well as identifying which User profile the SP is requesting.

The Resource Server then processes the request, interfacing with the relevant internal systems to be able to retrieve the requested User attributes (relating to the User and the status of their mobile subscription) and responds back to the SP with the results (Resource Response).

4 Attribute Services

4.1 Claims[6]

As described in the OpenID Connect Core Specification [1], claims can be requested using specific `scope` values or via individual claims that can be requested using the `claims` parameter in the OIDC Authorization Request. For Mobile Connect, only specific `scope` values are used for requesting claims and must be present within the OIDC Authorization Request otherwise an error will be generated.

Table 1 summarises three models for supplying claims (attributes) as defined in the OIDC Core Specification [1]. The Normal Claims approach MUST be supported for Mobile Connect attribute services; the Operator may also support Aggregated and Distributed Claims (authorising use of attributes served by a 3rd party Attribute/Claims Provider) where appropriate.

Claim Type	Description
Normal Claims	Claims that are directly asserted by the Operator via an appropriate Resource Server
Aggregated Claims	Claims that are asserted by a Claims Provider other than the Operator but are returned by the Operator

[5] Note that MC KYC Match uses a different approach where attributes and values are asserted by the SP using the `claims` parameter in the service request which are processed in the Authorization Server and results made available to the Resource Server. However, new any new MC services will make use of the `mc_claims` parameter in the Resource call for this as described above.

[6] OIDC specifications make use of the terms: “claim” or “claims”. A claim refers to a piece of information asserted about an entity – e.g. a User. This is used interchangeably with the term “attributes” and is typically used when referencing elements that are described in the OIDC specifications.

Distributed Claims	Claims that are asserted by a Claims Provider other than the Operator but are returned as references by the Operator.

Table 1: Claim Types

4.2 Supported Attributes

Attributes are specified as REQUIRED or as OPTIONAL within the relevant service "Definition and Technical Requirements" document. In order for an Operator IDGW to support a particular Mobile Connect attribute service it MUST provide the REQUIRED attributes and MAY return attributes that are marked as OPTIONAL. In addition, the Operator MAY choose to return other attributes to enrich the Mobile Connect service offering to SPs[7].

The particular attribute set supported by an Operator (i.e., REQUIRED + OPTIONAL attributes) should be communicated to SPs as part of the service proposition (and ultimately the Operator will price the service based on the particular set of attributes they include within the service). This would typically be agreed when the SP is contracting for the service and be reflected within the contractual agreement. The Operator may decide to offer the same attributes to all SPs, or to offer an enhanced service variant (with a few more attributes) to select SPs.

Within Mobile Connect, the specific attributes and the quality of those attributes are provided by the Operator on a "best-efforts" basis although Operators should put in place appropriate procedures to improve and/or ensure the accuracy of the User information that will be returned, wherever possible.

Whilst an Operator must endeavour to supply (or match) all the attributes defined within the service definition, it is recognised that the Operator may not always be able to provide or match values for every attribute for a particular User. Likewise, in the case of a match service, it is recognised that the SP may not have values for every attribute for a particular User.

Note that it may not be possible to support Mobile Connect attribute services for some end-users where there is limited information available on that User unless processes are in place to capture and check the accuracy of that information. In a similar way, it may not[8] be possible for example to support Mobile Connect attribute services where the User is a minor (based on local legislation) or where the User's MSISDN is part of company account, or similar, where data for the individual User may not be available.

4.3 Share and Match Services

Mobile Connect supports both the sharing of attributes and an ability for an SP to submit attributes (attribute names and values) in either a plain text or hashed form for the Operator to compare against its own data and return a match result. Each Mobile Connect service is requested using a specific `scope` value - further details can be found in the relevant service "Definition and Technical Requirements" document.

[7] Ideally the supported attributes would be the same across all Operators within a market to provide a consistent service towards SPs.

[8] There might be other reasons and scenarios where the data may not be captured or managed by the Operators to rely on. (example : MVNOs held MSISDNs etc.).

For share services the SP submits a service request and the Operator returns the supported attributes (defined by the `scope` value). If the User profile does not contain a particular attribute, this is returned as an empty value. The Resource Server returns all attributes that are supported (including empty values) - the SP cannot specify a subset of attributes.

For MC attribute opreation[9] services, attribute names and the values to be matched are typically included using the Mobile Connect specific `mc_claims` parameter within the Resource Request to the relevant Resource endpoint[10].

For a match service, the SP submits attribute names and values based upon the information that it has available. There is no restriction on what must be submitted - it is based purely on what the SP wishes to validate within the supported attribute set.

- An error is returned if there is any inconsistency within the submitted attributes e.g. a plain text identifier is used as an input for a hashed scope. i.e. for hashed scope, hashed attribute must be used as an input.
- An error is returned if the request (Resource Request) is malformed (e.g. missing parameters, etc.)
- If the request includes an attribute name and value that is not supported by the IDGW (i.e. the SP includes some attributes for matching that are not part of the service), it is ignored by the IDGW and the remaining submitted attribute names and values are processed. If the request only includes attribute names and values that are not supported, then the request is rejected, and an error is returned.

The Resource Server processes the request based upon the submitted attribute names and values (claims) and returns a match indicator. Only those valid claims that are submitted by the SP return a result. The match indicators for a specific service are defined in the relevant service “Definition and Technical Requirements” document.

The Resource server may also return the attribute value along with the match indicator where a match has been achieved. If the submitted data is hashed, then the hashed value is returned. If a match is not achieved no value is returned. This is specified within the relevant Mobile Connect service “Definition and Technical Requirements” document.

5 Resource Endpoints

A Resource Server must expose a Resource endpoint to the SP which may be the general PremiumInfo endpoint or a service-specific Resource endpoint. Resource endpoints supported by an Operator are specified within the Mobile Connect Provider Metadata,

[9] For example matching the attribute values.

[10] Some older MC services utilise the `claims` parameter in the OIDC Authorization Request. All new Mobile Connect match attribute services should utilise the submission of claims via the Resource call using the `mc_claims` parameter. At the time of writing this specification, old MC services are not changed. If required after assessing the commercial impact a CR will be raised to align with the new resource principle.

available from the Operator’s openid-configuration URL, as described in Mobile Connect Technical Architecture and Core Requirements [13].

Mobile Connect has defined the PremiumInfo endpoint and associated data set for returning User attributes to SPs. It is based on the UserInfo endpoint, specified within the OIDC Core Specification [1] and encompasses the majority of the UserInfo data set of standard claims[11] whilst extending it further with claims (attributes) that Operators can provide, related not only to User information but adding in data categories around the User’s account with the Operator, the device they use and their network status etc.

Whilst a full set of attributes are defined within the PremiumInfo data set, the Operator only needs to implement whichever attributes are needed for the particular Mobile Connect attribute services that they deploy, as defined in the respective “Definition and Technical Requirements” document for that service.

Mobile Connect Resource endpoints are Protected Resources, as defined in OAuth 2.0 [5] that return claims about an authenticated User, subject to the appropriate User consent. If required these claims are normally represented by a JSON object that contains a collection of name and value pairs for the claims using mc_claims parameter.

A Mobile Connect Resource endpoint is represented by an HTTPS URL, and MAY have a port, path, and query parameters. Communication with the Resource endpoint MUST utilise the latest version of TLS.

The Resource endpoint MUST support the use of the HTTP GET and HTTP POST methods defined in RFC 2616 [4].

The Resource endpoint MUST accept a Bearer Access Token as described in Section 2 of RFC6750 [6].

6 Resource Request / Response Flow

□ shows a high-level sequence diagram for a Mobile Connect service request illustrating the Resource Request and associated Resource Response. Note that the diagram assumes that an SP has the necessary IDGW metadata and credentials to initiate an OIDC Authorization Request for the service.

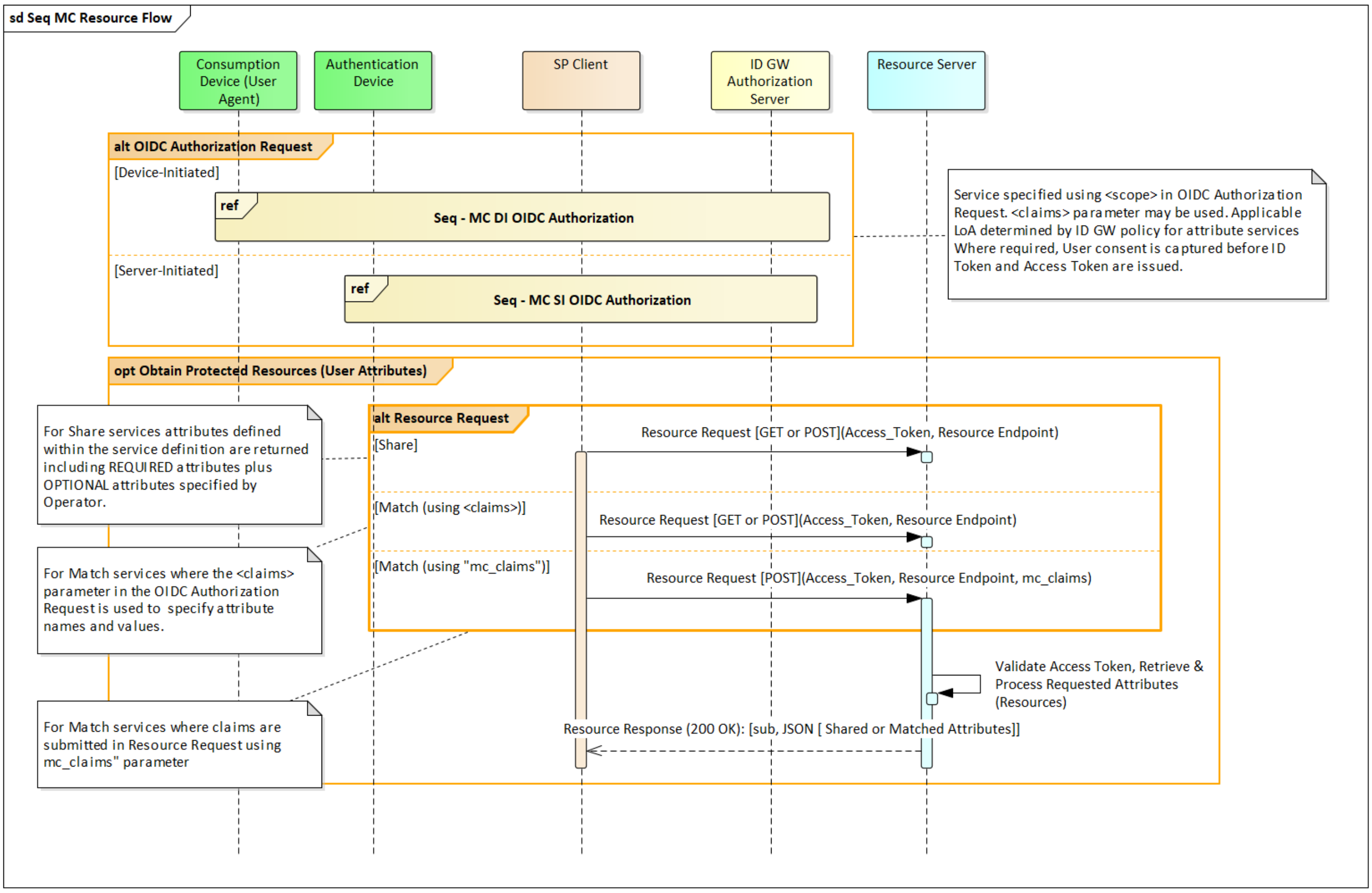
The request can be Device-Initiated or Server-Initiated although specific Mobile Connect attribute services will specify which modes are supported. The Mobile Connect service is requested using the `scope` parameter in the OIDC Authorization Request. The Mobile Connect service definition specifies which attributes or claims are to be shared or matched.

For Mobile Connect attribute services, User consent must be obtained before attributes can be shared or match results returned to a SP. A User must be identified (i.e. asserting the user's identity) before consent is obtained. This can be done within the OIDC Authorization

[11] Some Operators may choose to also support the UserInfo endpoint and associated data set, for example, for backwards compatibility.

process, where the User consent represents an additional step within the flow. This is described in more detail in Section 7.

After a successful authentication and capturing User consent (where required), the SP receives a valid Access Token which can then be used to retrieve the requested attributes or match values. The SP then submits a Resource Request to the relevant Resource endpoint using the Access Token and supplying the attributes (claims) to be matched where relevant.


sd Seq MC Resource Flow
Consumption Device (User Agent)
Authentication Device
SP Client
ID GW Authorization Server
Resource Server
alt OIDC Authorization Request
[Device-Initiated]
ref
Seq - MC DI OIDC Authorization
[Server-Initiated]
ref
Seq - MC SI OIDC Authorization
opt Obtain Protected Resources (User Attributes)
alt Resource Request
[Share]
Resource Request [GET or POST](Access_Token, Resource Endpoint)
[Match (using <claims>)]
Resource Request [GET or POST](Access_Token, Resource Endpoint)
[Match (using "mc_claims")]
Resource Request [POST](Access_Token, Resource Endpoint, mc_claims)
Validate Access Token, Retrieve & Process Requested Attributes (Resources)
Resource Response (200 OK): [sub, JSON [Shared or Matched Attributes]]

Service specified using <scope> in OIDC Authorization Request. <claims> parameter may be used. Applicable LoA determined by ID GW policy for attribute services Where required, User consent is captured before ID Token and Access Token are issued.

For Share services attributes defined within the service definition are returned including REQUIRED attributes plus OPTIONAL attributes specified by Operator.

For Match services where the <claims> parameter in the OIDC Authorization Request is used to specify attribute names and values.

For Match services where claims are submitted in Resource Request using mc_claims" parameter

- **: Resource Request and Response**

6.1 Resource Request

The SP Client sends the Resource Request using either HTTP GET or HTTP POST (server-initiated). The Access Token MUST be sent in the HTTP authorization header field using the "Bearer" authentication scheme (bearer access token) as described in Section 2 of RFC6750 [5].

For legacy Mobile Connect “match” services that make use of the `claims` parameter in the OIDC Authorization Request to submit values to be matched, the use of GET is recommended.

For all other Mobile Connect match services, the Resource Request should include a JSON object containing the claims and their values using the `mc_claims` parameter. This Resource Request should use the POST method. The `mc_claims` parameter is analogous to the `claims` parameter in the OIDC Authorization Request but provides a more robust mechanism for submitting claims and their associated values for match services.

Annex B contains examples of Resource Requests.

6.2 Resource Response

Upon receipt of the Resource Request, the Resource endpoint MUST return the JSON Serialization of the JSON object containing the response claims. The content-type of the HTTP response MUST be application/json. The response body SHOULD be encoded using UTF- 8.

A successful request returns an HTTP 200 OK response or an appropriate error response as defined in Annex A. There may also be service specific error responses which are defined in the relevant Mobile Connect service "Definition and Technical Requirements" document.

The claims returned in the Resource Response are returned as members of a JSON object.

The "sub" (subject) claim containing the PCR MUST always be returned in the Resource Response so that the Resource Response is tied with the ID Token and the User in this context. This allows the SP to validate the response.

For an attribute share service, the Resource Response will return the supported attributes. If for some reason an attribute cannot be returned (e.g. data is missing from a particular User's profile) then the attribute identifier with an empty value will be returned.

For attribute match services, a match will be performed based upon the attribute values provided within the request (e.g. via the `mc_claims` parameter in the Resource Request) and a match result will be returned (e.g. match successful, match failed - data is unavailable, as appropriate) as defined within the relevant Mobile Connect service "Definition and Technical Requirements" document.

Annex B contains examples of Resource Responses.

7 Capturing User Consent

For Mobile Connect services that involve sharing or matching User attributes with a SP, the User must give their consent for the information to be shared or matched. In such cases it is imperative that the User is authenticated before being asked to provide their consent to ensure that the right person is providing such consent. This may be an explicit authentication prior to asking for consent to share the attribute data or it may be an "implicit" authentication via the User demonstrating that they are in possession and control of their mobile device (i.e. the Authentication Device) when giving consent.

Depending upon the Mobile Connect service or the specific use case, User consent can be captured by the Operator IDGW or by the SP subject to the contractual agreement with the Operator and in line with local regulations around data protection and privacy. Each Mobile Connect service "Definition and Technical Requirements" document provides guidelines on consent considerations for that particular service.

Consent can be given on a per transaction basis or can be long-lived to remove the need for the user to have to repeatedly authorise an SP each time the SP needs to access the User's information. A long-lived approach can be supported by the IDGW issuing a long-lived Access Token (long expiration time) hence enabling the SP to go directly to the Resource Server with the Access Token to request the attributes (removes the need for the SP to issue an OIDC Authorization Call to the IDGW every time they need to access the User's information)[12].

The Mobile Connect Product Manager's Lifecycle Handbook contains further discussion on User Consent [16].

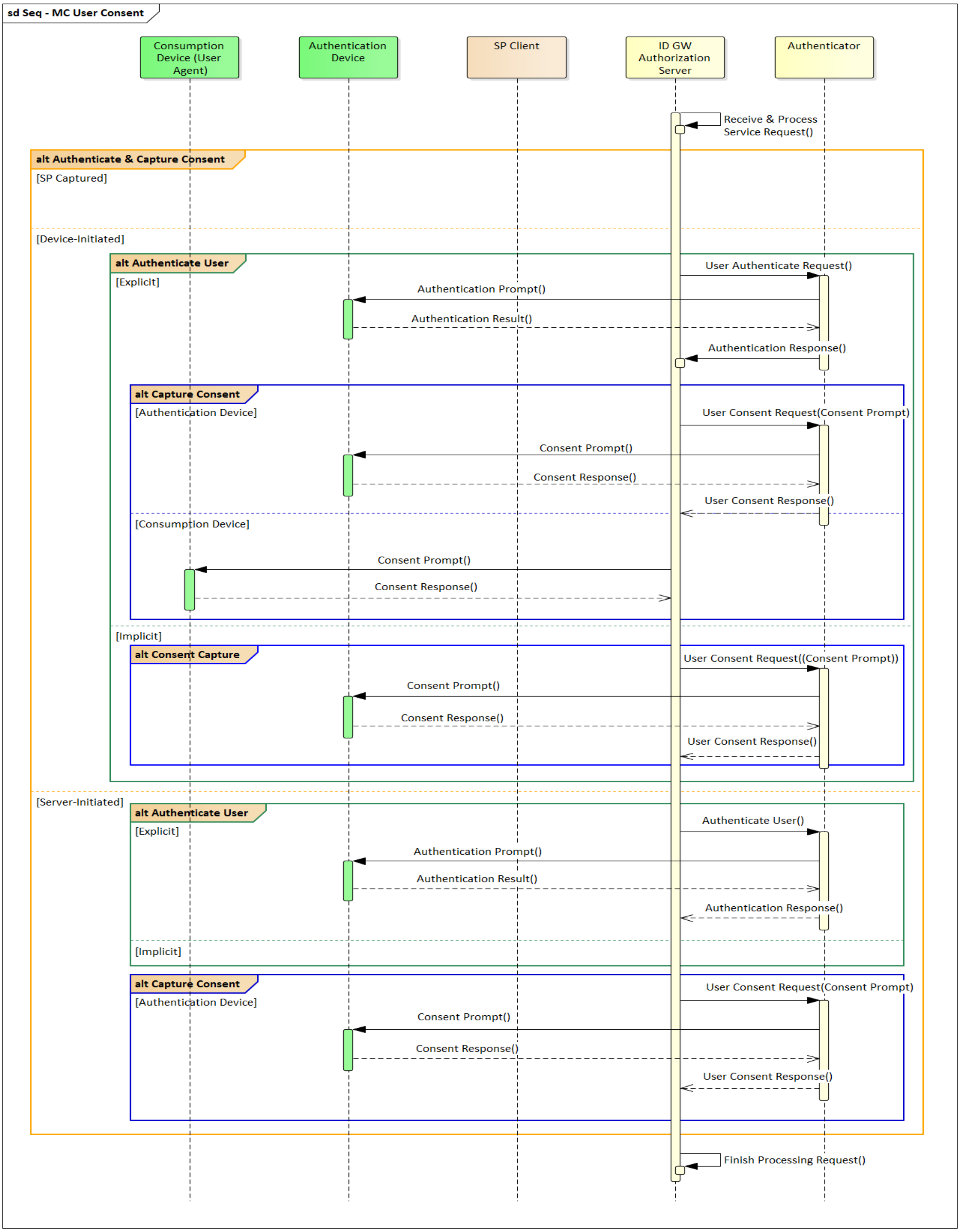
Where the Operator IDGW is capturing User consent on a per transactional basis, there will be an additional step within the processing of an OIDC Authorization Request to display a consent prompt to the User and to capture their response. presents a sequence diagram outlining the different options for authentication and capturing User consent in the context of an OIDC Authorization Request.

In Device-Initiated mode, the IDGW can present a consent prompt requesting the User to give their consent on their Authentication Device using the appropriate Authenticator or, after being authenticated on their Authentication Device, the consent prompt can be displayed, and the response captured via the User's Consumption Device. This approach may be required where the Authenticator has limited capacity to provide an appropriate consent prompt to ensure that the User is fully informed of what they are giving consent for and the larger screen of a laptop, for example, as the Consumption Device makes this more practical.

In Server-Initiated mode, where the Operator IDGW is capturing consent, the consent must be captured via the Authentication Device as there is no Consumption Device available in Server-Initiated mode.

The choice of how to capture User consent is based on the Operator's policies depending upon the Mobile Connect services being requested, the profile used, the contractual agreement with the SP and any local regulations relating to data protection and privacy. Note that where the SP is responsible for capturing User consent, the Operator IDGW can also enforce a transaction-based User consent, if required.

[12] OIDC specifies the use of an optional Refresh Token, which may also be used to allow the Access Token to be refreshed – this is a possible future option for Mobile Connect



- : Capturing User Consent

8 Requirements for the Resource Server and associated Mobile Connect attribute Services

8.1 Attribute Services

No	Relating To	Requirement
MC_ATTR_01	Attribute Services	A Mobile Connect attribute service can only be offered by an Operator IDGW if the REQUIRED attributes, defined in the relevant Mobile Connect service "Definition and Technical Requirements" document, can be supported. Note that attributes marked as REQUIRED MUST be supported; attributes marked as OPTIONAL MAY be supported (at the discretion of the Operator). An Operator may also choose to return additional parameters (not included within the service definition) to enhance the service proposition. Note that Mobile Connect services are provided on a best-effort basis hence the Operator is not expected to always be able to provide REQUIRED attributes for every User.
MC_ATTR_02	Attribute Services	For Mobile Connect attribute services, additional OPTIONAL attributes may be returned by the Resource Server if supported by the Operator implementation.
MC_ATTR_03	Attribute Services	The IDGW must implement appropriate Policy Management to determine the best method of displaying the attributes being requested by the SP and capturing consent for a given User (where needed). See the Mobile Connect Product Manager's Lifecycle Handbook for further details
MC_ATTR_04	Attribute Services	The IDGW should select the authentication method based on the LoA pre-configured for the service being requested. The IDGW must ignore the `acr_values` parameter in the OIDC authorisation request and select the authentication method based on its own policies. This is typically influenced by the sensitivity of the attributes being requested within a specific Mobile Connect service.
MC_ATTR_05	Attributes Services	Where Mobile Connect attribute services are provided (within a market), each Operator must implement an appropriate process to validate User identity and personal information to support those services, subject to local data protection regulations. Attributes and quality of information are provided on a best-effort basis.
MC_ATTR_06	Consent Capture	For Mobile Connect attribute services, consent for the sharing or validation of User attributes must be obtained from the User. Subject to the Operator IDGW policy and the type of attribute service requested, User consent can be captured by the Operator IDGW or the SP. Obligations on the SP when capturing User consent will be reflected in the terms and conditions with the SP. See the Mobile Connect Product Manager's Lifecycle Handbook for further details.
MC_ATTR_07	Consent Capture - Authentication	Where the Operator IDGW is responsible for capturing User consent, the IDGW must ensure that the Mobile Connect User is successfully authenticated before or as part of the consent capture to ensure that the right person is

No	Relating To	Requirement
		being asked for consent. Where supported and where service requirements allow, a single-factor, Seamless Authentication can be used for authentication but not for consent capture.
MC_ATTR_08	Consent Capture - Device	Where the Operator IDGW is capturing User consent and the Mobile Connect service request is a Device-Initiated request as defined in the MC Device-Initiated OIDC Profile, the consent can be captured either on the Authentication Device via the Authenticator or can be captured on the Consumption device. The decision as to which device is used is down to the Operator's policy for consent capture which will be influenced by the type of Authenticator and the specific attribute services requested.
MC_ATTR_09	Consent Capture - Device	Where the Operator IDGW is responsible for capturing User consent and a Mobile Connect attribute service request is made as a Server-Initiated request as defined in the MC Server-Initiated OIDC Profile , consent must be captured via the Authentication Device (i.e. mobile device). Note that a Seamless Authenticator cannot be used for authentication or consent capture for Server-Initiated mode as there will be no Consumption device for displaying the consent prompt and capturing the User's response.
MC_ATTR_10	Consent Capture - Prompt	Where the Operator IDGW is responsible for capturing User consent, the request for User consent MUST identify the data to be shared and prompt the User for a Yes/No response.
MC_ATTR_11	Consent Capture - Prompt	Where the Operator IDGW is capturing User consent, the IDGW must construct a consent prompt providing as much detail as possible to the User on the attributes being requested. This should include SP application short name (passed in the `client_name` parameter in the OIDC Authorization Request - up to 16 bytes) as well as one of the possible formats for indicating the attributes to be shared or validated. This could be (in order of preference): - Attribute names + values (e.g., first_name = Marie) - Attribute names only (e.g., first_name, last_name, etc.) - Attribute group (e.g., 'name, 'address details') The Operator will need to select the most appropriate attribute presentation format based on the capabilities of the device on which the consent is captured.
MC_ATTR_12	Consent Capture - Prompt	Where the Operator IDGW captures User consent, if the display space on the device permits, the consent prompt should get assurance from the User that the data being shared belongs to them and no one else and that they are not a minor (as defined by local regulations)
MC_ATTR_13	Consent Capture - Prompt	If the consent device is the Authentication Device (i.e. the User's mobile device), then for interoperability purposes the maximum prompt length should be <= 220 bytes, otherwise no restrictions on prompt le ngth apply.
MC_ATTR_14	Consent Capture - Prompt	gsm7, ucs2, and utf-8 encoding schemes must be supported for generation of the consent prompt
MC_ATTR_15	Consent Capture - Prompt	The device used to display the prompt for User consent must render prompt details correctly i.e. without breaking a word into multiple lines.

No	Relating To	Requirement
MC_ATTR_16	Consent Capture - Prompt	For a better User experience, it is recommended that the consent prompt is displayed on a single screen (not a sequence of multiple screens) unless local regulations require otherwise or it is beyond the capabilities of the Authenticator being used for displaying the consent prompt
MC_ATTR_17	Consent Capture - USSD Authenticator	If a USSD Authenticator is used to capture consent, the IDGW must capture the authentication and consent in a single interaction. The IDGW must not use a 2-stage approach that would result in an additional round-trip delay.
MC_ATTR_18	Access Token	Where a Mobile Connect service warrants or an SP requires User consent to be long-lived, the Operator IDGW can issue the SP with a long-lived Access Token. The decision on whether to issue a long-lived, transactional (short-lived) or a one-time-use Access Token is at the discretion of the Operator. For transactional Access Tokens, the IDGW must issue Access Tokens with TTL = zero, using the `expires_in` parameter with a very low value (e.g. 10s). If the Access Token is issued as a one-time-use token then if the SP uses the issued Access Token a second time, the IDGW must throw an error.
MC_ATTR_19	Consent Capture - Notification to User	Based on the Operator's IDGW Policy, the IDGW MAY issue a notification to the User if it receives a request from an SP (i.e., even when the SP has already captured the User's consent). Doing so ensures that the User is aware that a particular Mobile Connect attribute service has been invoked against their MSISDN.
MC_ATTR_20	Consent Revocation	Where an SP is responsible for capturing long-lived consent, a mechanism must be provided to allow the User to revoke consent and the SP must honour the revocation of consent. The revocation mechanism may be provided by the SP or by the IDGW depending upon Operator policy and configuration of the Mobile Connect services (e.g. if long-lived consent is provided via a long-lived Access Token). A means for the User to flag an SP who does not revoke consent upon User request should be provided and the IDGW should then support blacklisting that SP.
MC_ATTR_21	User Validation	The IDGW should reject OIDC Authorization requests if it is known that the corresponding Mobile Connect User is a minor (based on local legislation) based on IDGW policies, regulations [18] and privacy principles[17].
MC_ATTR_22	Service Request	For match services, if the SP submits an attribute name and value (claim) that is not part of the supported attribute set for that service (as specified by the Operator IDGW) then that claim is ignored and the remaining (valid) claims are processed. If all such claims are not part of the supported attribute set then the request should be rejected and an error returned. Note that this may occur in response to an OIDC Authorization Request if the `claims` parameter is being used or in response to the Resource Request where the `mc_claims` parameter is being used in the request.
MC_ATTR_23	Resource Request	The SP Client sends a Resource Request using either HTTP GET or HTTP POST to the Resource Server. The request is server-initiated irrespective of which OIDC Profile is used for the OIDC Authorization Request.

No	Relating To	Requirement
		The Access Token MUST be sent in the HTTP authorization header field using the "Bearer" authentication scheme (bearer access token) as described in Section 2 of RFC6750.
MC_ATTR_24	Resource Request	Mobile Connect match services should make use of a Resource Request which includes a JSON object containing a set of claims and their values using the `mc_claims` parameter. This Resource Request should use the POST method
MC_ATTR_25	Resource Response	The Resource Response MUST return the JSON Serialization of a JSON object containing the response claims. The content-type of the HTTP response MUST be application/json. The response body SHOULD be encoded using UTF- 8.
MC_ATTR_26	Resource Response	If the Resource Request is unsuccessful, the Resource Server must return an error response. Generic error responses, which are relevant for all attribute services, are defined in Annex A of the Mobile Connect Resource Server Specification. Service specific error responses may also be applicable which are defined in the relevant Mobile Connect service "Definition and Technical Requirements" document
MC_ATTR_27	Resource Response	For match services, the Resource Server must return a plain-text match response (as specified in the relevant Mobile Connect service "Definition and Technical Requirements" document) for each attribute match. The Resource Server must only return a match for the attributes and associated values specified in claims parameter in the service request or the mc_claims parameter in the Resource Request, and which are included within the service definition, as appropriate. If data is not available to perform a match for a specific attribute then the match indicator should provide the appropriate indication Note that for some Mobile Connect services, the attribute name and value submitted in the `claims` or `mc_claims` parameter may also returned as part of the response if there is a match - this is specified within the relevant Mobile Connect service "Definition and Technical Requirements" document.
MC_ATTR_28	Resource Response	The attribute service should match and return match indicators or requested attributes on a best effort basis in terms of data quality (i.e. based on whatever information the Operator already has for a given User as a result of the Operator's prevailing KYC processes)
MC_ATTR_29	Resource Response	For share services, if any supported attributes (REQUIRED attributes plus OPTIONAL attributes that the Operator supports) are not available for a specific request (i.e. information is not available for a particular User), the Resource Server must return those parameters with empty values.
MC_ATTR_30	Resource Response	The `sub` (subject) claim, containing the PCR, MUST always be returned in the Resource Response so that the Resource Response is tied with the ID Token and the User in this context. This allows the SP to validate the response.
MC_ATTR_31	Transaction Logs	The IDGW must provide a consent audit trail to support Operator customer service teams, SP Service teams, etc.

No	Relating To	Requirement
		Log files of all Mobile Connect attribute services requests and consent responses must be kept with all necessary data to resolve disputes.
MC_ATTR_32	Transaction Logs	The IDGW should provide a mechanism for the consent audit trail to be viewed by the User e.g. via a Mobile Connect self-care portal.

8.2 Resource Server

No	Relating To	Requirement
MC_RES_01	Resource Endpoints	A Resource Server must expose either a PremiumInfo endpoint or a service-specific Resource endpoint to support Mobile Connect attribute services. The PremiumInfo Endpoint is a single Mobile Connect defined endpoint to support a range of Mobile Connect services. It is NOT REQUIRED that an Operator provides the full PremiumInfo data set from the PremiumInfo endpoint. The choice of which endpoints are exposed is down to the Operator depending upon which specific Mobile Connect services are to be supported. Resource endpoints are published to SPs via the Mobile Connect Provider Metadata via the openid-configuration URL as described in Mobile Connect Technical Architecture and Core Requirements
MC_RES_02	Resource Endpoints	A Mobile Connect Resource endpoint is represented by an HTTPS URL, and MAY have a port, path, and query parameters. Communication with the Resource endpoint MUST utilise the latest version of TLS.
MC_RES_03	Resource Endpoints	The Resource endpoint MUST support the use of the HTTP GET and HTTP POST methods defined in RFC 2616
MC_RES_04	Resource Endpoints	The Resource endpoint MUST accept an Access Token as a "Bearer Access Token" as described in Section 2 of RFC6750
MC_RES_05	Resource Server	A Resource Server must be able to validate the Access Token submitted in a Resource Request (e.g. via the IDGW AT introspection point) in order to retrieve the relevant User Profile and to be able to service the Resource Request as described in the Mobile Connect Resource Server Specification.
MC_RES_06	Resource Server	The Resource Server must be able to retrieve the REQUIRED User attributes and the supported OPTIONAL attributes for the supported Mobile Connect attribute services using relevant Operator CRM and other databases that hold customer profile information, as appropriate.
MC_RES_07	Resource Server	Consistent with the IDGW (see Mobile Connect Technical Architecture and Core Requirements), the Resource Server must also use a high availability deployment
MC_RES_08	Resource Server	The IDGW should try to return the Resource Response to the SP promptly [13]following the SP's Resource Request
MC_RES_09	Security	The Resource Server implementation must consider RFC 6819 threats and security considerations. Appropriate counter measures must be implemented

[13] Performance metrics are out of scope of this specification. IDGW should define certain performance standards as part of their deployment & sytem engineering.

No	Relating To	Requirement
MC_RES_10	Security	All counter measures to security threats as mentioned in the Section 16 of the OpenID Connect Core specification must be implemented (wherever applicable)

Annex A Generic Error Responses from the Resource Endpoint

Mobile Connect follows the OpenID Connect error handling mechanism to send any errors back to the SP.

Errors must be returned as a JSON object containing the error code and error description using the appropriate HTTP status codes for Resource endpoints. Generic error codes for the Resource Response are listed in Table 2. Specific Mobile Connect services may also return service-specific error codes which are returned using the same format. Please refer to the relevant Mobile Connect service “Definition and Technical Requirements” document.

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 was issued but was not obtained through a Mobile Connect OIDC request (or) Access token exists, but it is invalid (or) (or) the Access Token has expired	Unauthorized 401	invalid_request (or) invalid_token	Invalid access token (or) access token does not exist (or) expired access token
Resource request is sent using POST and the "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 using POST - the entity-header includes the "Content-type header but the value is NOT "application/x-www-form-urlencoded" or "application/json"(when mc_claims are submitted)	Bad Request 400	invalid_request	Conent type is wrong .
The resource request is sent using POST was not form url encoded as described in RFC 6750 [6].	Bad Request 400	invalid_request	Malformed request, invalid url encoding
The resource request is sent using POST, and the content to be encoded in the entity-body contains non-ASCII	Bad Request 400	invalid_request	Malformed request, invalid non-ascii characters

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
characters as defined In RFC 6750 [6].			
Any unsupported parameters exist in the request	Bad Request 400	invalid_request	Malformed request, invalid parameters
Multiple problems in the resource request	Bad Request 400	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 Error 500	server_error	Internal Server Error
Resource server time-out due to internal error.	Internal Server Error 500	server_error	Timeout: Server internal error.

Table 2: MC Services: Generic Errors - Resource Endpoint

Annex B Example Resource Requests and Responses

B.1 Resource Request

The following example show a Resource Request for a share service

```
GET /connect/mc_vm HTTP/1.1.
User-Agent: XXXXXXXXXX.
Host: mc-idgw-Operator.example.com.
Authorization: Bearer LTRjZDMtNDUyYi1iNjk.
Accept: application/json.
```

The following example shows the Resource Request for a match service using the `mc_claims` parameter in the Resource Request which uses an HTTP POST request with the “Bearer Access Token” and a JSON payload.

```
POST /connect/mc_vm HTTP/1.1.
User-Agent: XXXXXXXXXX
Host: mc-idgw-Operator.example.com.
Authorization: Bearer LTRjZDMtNDUyYi1iNjk.
Content-Type: application/json.
Accept: application/json.
Content-Length: 73.
.
{"mc_claims" :  {"device_msisdn" : "+44123456789"}}
```

B.2 Resource Response

The following example shows the Resource Response for a share service

```
HTTP/1.1 200 OK.
Date: Tue, 03 Oct 2017 09:37:43 GMT.
Server: XXXXXXX
Expires: Thu, 19 Nov 1981 08:52:00 GMT.
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0.
Pragma: no-cache.
Content-Length: xx.
Content-Type: application/json.
.
{
  "sub": "s6BhdRkqt3"
  "device_msisdn": "+44123456789"
}
```

The following example shows the Resource Response for a match service

```
HTTP/1.1 200 OK.
Date: Tue, 03 Oct 2017 09:37:43 GMT.
Server: XXXXXXX
Expires: Thu, 19 Nov 1981 08:52:00 GMT.
```

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0.
Pragma: no-cache.
Content-Length: xx.
Content-Type: application/json.
.
{
  "sub": "s6BhdRkqt3"
  "device_msisdn_verified": true
}
```

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	03/06/2019	A new document for resource server specification decoupled from main profile. Updated with DQRT and david's inputs.	TG	Siva [Venkatasivakumar Boyalakuntla]/GSMA

A.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.