Mobile Connect KYC Match Definition and Technical Requirements

Version 1.0

22 February 2022

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

Security Classification: Non-Confidential

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 worldwide initiative by mobile Operators to bring a wide portfolio of identity services to market that enable Service Providers and Users to transact with one-another more securely through strong authentication, authorisation and exchange of attributes, subject to User consent.

The Mobile Connect architecture consists of a Core framework around which additional components can be added to support the different Mobile Connect services. The Core framework is based upon the OpenID Connect (OIDC) protocol [1] and allows Users to be identified by their MSISDN (or a related Pseudonymous Customer Reference) to enable authentication.

The serving Mobile Operator selects an appropriate Authenticator based on Operator policy, device capability and the Level of Assurance required by the Service Provider to enable authentication.

This document details the service definition and the technical requirements for the Mobile Connect Know Your Customer (KYC) Match service. KYC Match provides a mechanism by which Service Providers (SP) can check their customer’s information against that held by that customer’s (User’s) mobile Operator.

This document describes the MC KYC Match service, applicable use cases and the associated User experience. It also contains normative sections specifying how the service must be implemented and operated (in conjunction with requirements for the Core framework [6] and Resource Server [9]).

1.2 Scope of the document

In Scope	Out of Scope
• Mobile Connect KYC Match functionality description • Mobile Connect KYC Match technical specifications	• Detailed Privacy and Trust Principles • UI/UX guidelines • Mobile Connect KYC Match commercial propositions • Service provider / developer implementation guidelines • Other Mobile Connect service definitions

1.3 Audience

The target audience for this document are the product managers and service/technical departments at Operators who are considering deploying the Mobile Connect KYC Match service.

Readers of this document are expected to have familiarity with Mobile Connect and some knowledge of the technical architecture and Mobile Connect Core framework technical requirements [6].

1.4 Relationship to Other Mobile Connect Documentation

This document details the Mobile Connect KYC Match service and its usage including the technical requirements (building on the Mobile Connect Core framework) and the relevant technical parameters for the service such as `scope` value and any service specific error codes.

The Mobile Connect Technical Overview document [5] provides a high-level description of Mobile Connect and how it works. It also includes a master list of abbreviations and terminology used within the Mobile Connect Documentation set 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.

The Mobile Connect Technical Architecture and Core Requirements document [6] describes the Mobile Connect Architecture in more detail and also includes the core technical requirements and specification of elements for Mobile Connect that are generic to all Mobile Connect services and modes of operation.

Detailed specifications for the Mobile Connect APIs (Device-Initiated Mode [7] and Server-Initiated Mode [8]) provide details for OIDC Authorization Requests and Responses, and Token Requests (DI Mode) and Responses including examples and error codes.

The Mobile Connect Resource Server Specification [9] provides details on how to handle a Resource request and the associated response for Mobile Connect Identity and Network Attribute services including error codes where this approach is used by a Mobile Connect service. [1]

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 specifications and related documents 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 [5] defines relevant terms that are used within the Mobile Connect Specifications and interprets terminology from source standards in Mobile Connect terms. It also includes a list of abbreviations.

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

[1] Note that the MC KYC Match service does not make use of the split architecture but Resource Server requirements and Attribute service requirements in the Resource Server Specification still apply.

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
[4]	ISO8601-2004	International Organization for Standardization 8601:2004. Data elements and interchange formats - Information interchange - Representation of dates and times, 2004. http://www.iso.org/iso/catalogue_detail?csnumber=40874
[5]	IDY.05	Mobile Connect Technical Overview
[6]	IDY.04	Mobile Connect Technical Architecture and Core Requirements
[7]	IDY.01	Mobile Connect Device-Initiated OIDC Profile
[8]	IDY.02	Mobile Connect Server-Initiated OIDC Profile
[9]	IDY.03	Mobile Connect Resource Server Specification
[10]	IDY.16	Mobile Connect Product Manager's Lifecycle Handbook
[11]	IDY.33	API Exchange Functional Description
[12]	IDY.09	Mobile Connect Authenticator Options
[13]		Mobile Connect Privacy Principles
[14]		GSMA Regulatory considerations for processing personal data and attributes for Mobile Connect
[15]	IDY.35	APIX Discovery API Specification

[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.

2 Mobile Connect KYC Match

The Mobile Connect KYC Match service allows Service Providers to compare personal data that they hold about a User, such as the User's name and address, with the data held by the User's Operator. This supports various practical use cases ranging from protecting the Users' bank accounts from fraud to checks that Service Providers can perform to validate the identity of Users in a convenient and secure way.

- The Service Provider includes within an OIDC Authorization Request the values of the attributes that are to be checked (name, address and, optionally, date of birth) along with the MSISDN of the target user.

- The Service Provider has a choice to provide the data to be matched in a hashed form[3] or in a plain text format.

- The User must provide consent to the use of their personal data for matching purposes. Depending upon the contractual relationship with the Service Provider, it may be that the responsibility for capturing User consent to perform a check against User attributes is carried out by the Service Provider or by the Mobile Operator. If SP captures the consent user must have flexibility to request to Operator for an explicit consent.

- Mobile Connect KYC Match provides a match indicator response for each attribute to indicate whether the match was successful or not. This allows Service Providers the flexibility to work with various degrees of verification based on the number of attribute matches. The match indication can result in the following scenarios:

    - Where there is a match, the attribute identifiers and normalised values (plain text or hashed as in the request) are also included in the response along with a positive match indication for each attribute.
    - If the values do not match, the attribute identifier and value are omitted from the response and only the match indicator is returned.
    - If the data is unavailable, the match indicator will reflect data unavailability and the attribute value will be omitted from the response.
    - If the data is available but access is denied, the match indicator will reflect access denial and the attribute value will be omitted from the response.

- The Operator ID GW may, optionally, return additional attributes relating to the status of the User's mobile account such as:

    - "Billing segment", describing the type of contract the User has with the mobile Operator, for example post-paid, prepaid, business, etc.
    - Lost/stolen flag, indicating if the device has been reported as lost or stolen by the User or not (True/False)

[3] Hashing ensures that the data which is shared cannot be decrypted by any party hence preserving the privacy of the user. It is recommended that Operators do not store hashed data that is processed during KYC Match unless required by legal and regulatory compliance or for transaction logging purposes.

- Mobile phone account status, describing if the account is active or inactive.

2.1 Use Case Examples

Mobile Connect KYC Match provides a mean for Service Providers to validate the identity of the User. Table 1 provides some example use cases for the service.

Product	Example Use Cases
Mobile Connect KYC Match	• ID verification for gov. & other services (e.g.: online casino) • Verification of user details at new account opening • Validating change requests for phone number associated with bank account • Card enrolment/ID verification in mobile wallet • AML (Anti-money Laundering) checks

Table 1: Use case examples

The User can be an existing User or a new User who is in the process of signing up with the SP. For example, when a User is registering to set up a government ID, one of the options offered could be to use the mobile contract of the User to validate the User's name and address. If this option is selected by the User, the Service Provider initiates a Mobile Connect KYC Match service request to the User's Operator ID GW in order to validate the User's data before provisioning the User with a government ID.

Mobile Connect KYC Match offers enhanced fraud management. For example, a Bank may use Mobile Connect KYC Match before completing sensitive transactions such as fulfilling the request to change the mobile number associated with the User's online banking account. In this case, the Bank will initiate a Mobile Connect KYC Match request to the User's Operator to match the personal information associated with the new mobile phone number and confirm that the new phone number actually belongs to the same User (and not just a fraudster trying to set their phone number against a User's bank account). The match provides additional information to the Bank to fulfil the transaction.

3 Mobile Connect KYC Match Functional Overview

3.1 Mobile Connect KYC Match Service Flow

The SP must be registered for Mobile Connect and must register specifically for the MC KYC Match service.

Mobile Connect KYC Match service requests may use Mobile Connect Server-Initiated mode[4] [8] or Device-Initiated mode [7].

The SP would normally acquire “long-lived” consent from the User at the time of the User registering for the SP’s service. This allows the SP to request an KYC Match when required (assuming that the consent is not revoked by the User).

Operators[5] must establish the policy around the provision of the Mobile Connect KYC Match service, which should be reflected within the terms and conditions agreed with Service Providers wishing to use the service.

□ shows a high-level flow for a KYC Match service request. The use case is registration with a Service Provider who wishes to perform checks against the name and address that the User has submitted. This example uses a Server-Initiated request – the KYC Match request is typically performed as a background check.

The differences in using a Device-Initiated request are outlined in Section 3.1.1.

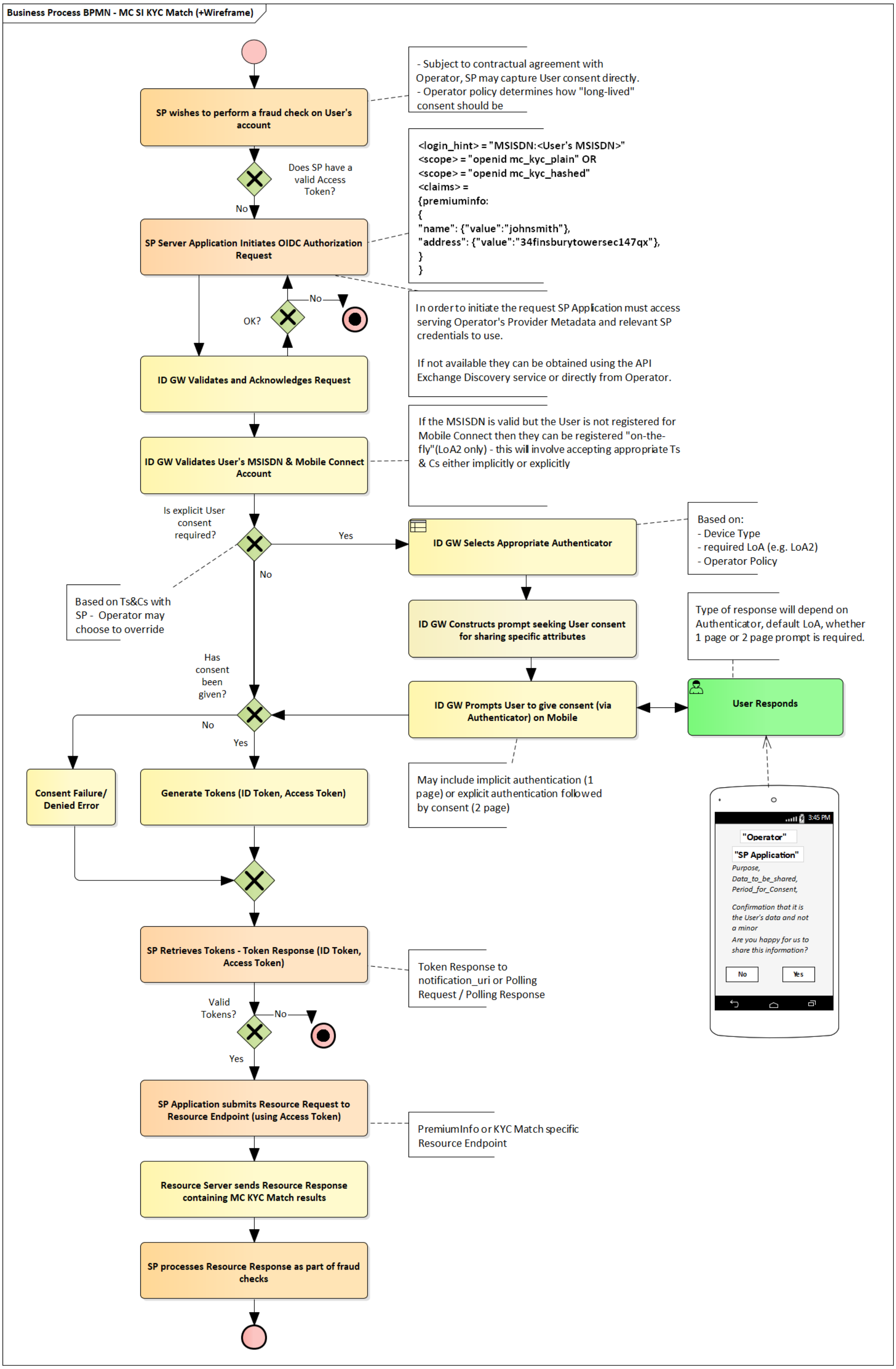
Mobile Connect Technical Architecture and Core Requirements [6] provides more detailed sequence diagrams illustrating the flow for Device-Initiated mode and the Server-Initiated modes. The Mobile Connect Device-Initiated OIDC Profile [7], and the Mobile Connect Server-Initiated OIDC Profile [8] define the API calls and responses for each mode.

The service flow is as follows:

- The Service Provider’s application initiates a MC KYC Match service request towards the Operator’s ID GW Authorization endpoint. The SP specifies the service required using the `scope` parameter to indicate whether a KYC Match using plain text or hashed values for submitting the User’s asserted name and address is required.
    - In this example, it is assumed that the SP already has the relevant Operator ID GW metadata and credentials to be able to initiate a service request to the correct Operator ID GW for that User. If not available, then this can be obtained by using the API Exchange Discovery service [11] or by obtaining the details directly from the Operator.

[4] Server-initiated mode supports two mechanisms for retrieving Tokens from the Authorization Server and the SP must register for one or the other. See the Mobile Connect Server-Initiated OIDC Profile

[5] Operators within the same market must offer a consistent approach to User’s and Service Providers.


Business Process BPMN - MC SI KYC Match (+Wireframe)
SP wishes to perform a fraud check on User's account
Does SP have a valid Access Token?
No
SP Server Application Initiates OIDC Authorization Request
No
OK?
ID GW Validates and Acknowledges Request
ID GW Validates User's MSISDN & Mobile Connect Account
Is explicit User consent required?
Yes
No
ID GW Selects Appropriate Authenticator
ID GW Constructs prompt seeking User consent for sharing specific attributes
Has consent been given?
No
Yes
ID GW Prompts User to give consent (via Authenticator) on Mobile
User Responds
Consent Failure/ Denied Error
Generate Tokens (ID Token, Access Token)
SP Retrieves Tokens - Token Response (ID Token, Access Token)
Valid Tokens?
No
Yes
SP Application submits Resource Request to Resource Endpoint (using Access Token)
Resource Server sends Resource Response containing MC KYC Match results
SP processes Resource Response as part of fraud checks
3:45 PM
"Operator"
"SP Application"
Purpose,
Data_to_be_shared,
Period_for_Consent,
Confirmation that it is the User's data and not a minor
Are you happy for us to share this information?
No
Yes

- Subject to contractual agreement with Operator, SP may capture User consent directly.
- Operator policy determines how "long-lived" consent should be

```
<login_hint> = "MSISDN:<User's MSISDN>"
<scope> = "openid mc_kyc_plain" OR
<scope> = "openid mc_kyc_hashed"
<claims> =
{premiuminfo:
{
"name": {"value":"johnsmith"},
"address": {"value":"34finsburytowersec147qx"},
}
}
```

In order to initiate the request SP Application must access serving Operator's Provider Metadata and relevant SP credentials to use.

If not available they can be obtained using the API Exchange Discovery service or directly from Operator.

If the MSISDN is valid but the User is not registered for Mobile Connect then they can be registered "on-the-fly"(LoA2 only) - this will involve accepting appropriate Ts & Cs either implicitly or explicitly

Based on:
- Device Type
- required LoA (e.g. LoA2)
- Operator Policy

Based on Ts&Cs with SP - Operator may choose to override

Type of response will depend on Authenticator, default LoA, whether 1 page or 2 page prompt is required.

May include implicit authentication (1 page) or explicit authentication followed by consent (2 page)

Token Response to notification_uri or Polling Request / Polling Response

PremiumInfo or KYC Match specific Resource Endpoint

- **: Mobile Connect KYC Match Service Flow**

- The SP includes the name and address asserted by the User in the service request (OIDC Authorization Request) using the `claims` parameter.

  Depending upon the `scope` values specified, the name and address attributes are submitted using an appropriate attribute identifier and a value (See Section 4.3 for more details) that is in plain text or is hashed. KYC Match allows the name and address information to be submitted in a number of different ways. These values should be formatted in line with the agreed data normalisation rules (See Section 3.2).

- The Operator's ID GW validates the request (i.e. that the SP has been registered with the Operator for the MC KYC Match service requested and that the required parameters are included in the correct format)

- The Operator ID GW checks the MSISDN and whether the User is registered for Mobile Connect

  If the MSISDN is not yet registered for Mobile Connect, a new Mobile Connect account can be created "on-the-fly" for that MSISDN, subject to ID GW policy.

- Assuming the request is valid, the Operator processes the request and returns an ID Token and an Access Token which is used to retrieve the requested attributes from the relevant Resource Endpoint.

  - □ also shows the option for the ID GW to explicitly seek User consent via the User's mobile device (Authentication Device). Based on the Operator's policy, the ID GW determines whether explicit User consent needs to be captured. A User should be authenticated before seeking their consent to share information with a Service Provider. This can be either implicit authentication resulting in a single page displayed seeking consent or as a two-stage process – authentication followed by consent. Table 2 shows the appropriate Authenticators for the Mobile Connect KYC Match service.

  - If consent had not already been captured or is not given in response to the prompt, then an error message is generated and returned to the SP.

- The SP can retrieve the ID Token and Access Token using Notification or via a Polling mechanism depending on which variant the SP has registered for and specified in the request. Further details are provided in the Mobile Connect Server-Initiated OIDC Profile specification [8].

- Assuming the request was successful, the SP retrieves the ID Token and Access Token and then uses the Access Token to make a Resource Request to the applicable Resource Endpoint in order to obtain the KYC Match results.

  The Authorization Server matches the attribute values submitted using the `claims` parameter in the OIDC Authorization Request and matches each attribute value, as appropriate, using the same normalisation rules as agreed with the Service Provider.

The results are then made available to the Resource Server and the match results are included within the Resource Response back to the SP. The match indicators are defined in Table 6. The Operator may choose to include additional attributes back to the SP[6].

The name, address and date of birth (if supported) information is based upon the information held by the Operator for their customer. If the User is not the registered customer of the mobile subscription associated with MSISDN being used, then the match is likely to fail. Also, if the data held is inaccurate and differs from that submitted then the match will fail. It is recommended to establish off-line processes to be able to validate the data with the User and to enable the data to be updated.

Due to the nature of the MC KYC Match service where a check involves submitting attributes within the OIDC Authorization Request, the use of a long-lived Access Token or the issue of a valid Refresh Token is not allowed. The full OIDC Authorization followed by a Resource Request / Response to and from the Resource endpoint for KYC Match must be performed for each service call.

3.1.1 Using a Device-Initiated KYC Match service request

Where the User is interacting with a Service Provider's application for example, via a laptop or their mobile device, then the SP application can use a Device-Initiated KYC Match service request. This process is broadly the same as described in □ but with the following differences:

- The format of the request (defined in the Mobile Connect OIDC Device-Initiated OIDC Profile [7]) is different but the same `scope` values are used and the use of the `claims` parameter to submit the User's asserted name and address is the same. The mechanism to obtain the ID Token and the Access Token also differs, but the process of retrieving the Match results from the Resource Server is the same.

- The User may be re-directed to an Operator's ID GW holding page if explicit authentication and User consent is required. The User will always be authenticated on the Authentication Device.

- If User consent is captured as part of the service request, the consent prompt can be displayed on the User's Authentication Device or the Consumption Device depending upon the Operator's consent policy.

3.2 Normalisation of Attribute Data

The Mobile Connect KYC Match service allows attribute values to be included in the OIDC Authorization Request `claims` parameter in a plain text format or in a hashed form.

In plain text form the attributes can be presented in a number of different ways – lower case, upper case, capitalised, use of abbreviations, spurious spaces, etc. While in plain text these forms can be interpreted to a degree, this is not possible if the attribute values are hashed. In order to minimise the number of false negative matches that could occur it is necessary to

[6] This can include parameters such as lost/stolen, billing segment, gender, title etc.

ensure that the Operators within a market[7] establish clear rules to allow data to be normalised which can be shared with registered Service Providers.

An example of a set normalisation rules is where the data is matched with whitespace characters removed, all characters converted to lower case, and all strings truncated to 20 characters.

3.3 Mobile Connect Account Setup and Status

If the User is not previously registered, they should be registered "on the fly" to use Mobile Connect. For some SP implementations, the User may not be involved in the User journey to complete registration. In such scenarios, the Mobile Connect account will be created for the User. Operators are encouraged, in this case, to follow up with the User to complete registration. This is discussed in more detail in the Mobile Connect Product Manager's Lifecycle Handbook [10].

3.4 User Consent Management

Where a Mobile Connect service requires the sharing or matching of personal information relating to the User or their mobile subscription, the User's consent must be obtained before any data is shared. Depending upon the Mobile Connect service or the specific use case within a service, User consent can be captured by the Operator's ID GW or by the Service Provider. For regulatory requirements and privacy principles refer to [13] and [14].

Further discussion on User Consent can be found in the Mobile Connect Product Manager's Lifecycle Handbook [10].

Where consent is captured by the ID GW this would typically be done via the User's Authentication Device. However, depending upon the Authenticator that is used this can create challenges in presenting sufficient information for the User to give informed consent (See Table 2). In Device-Initiated mode, the consent prompt can also be presented to the User via the Consumption Device in order to be able to provide a richer consent prompt. This mechanism is discussed in more detail in the Mobile Connect Resource Server Specification [9].

Table 2: Authenticator suitability for Mobile Connect KYC Match

3.5 Considerations for Lawful Handling of User's Data

Operators may be subject to general data protection laws and telecom specific rules that place conditions and obligations on the use of customer information. Attributes held by Operators may fall into a number of legal categories of regulated and protected data.

Service Providers will also be subject to some of these obligations and must not use the data obtained from a Mobile Connect service request for anything other than the stated purpose.

Operators are recommended to perform due diligence to check that a Service Provider's processes are suitable to meet their obligations and that those obligations are clear within

[7] This will help to ensure that Service Providers and Users have a consistent experience of Mobile Connect services.

the contract between the Operator and the Service Provider. This is discussed in more detail in the Mobile Connect Product Manager's Lifecycle Handbook [10].

4 MC KYC Match Service Specification

4.1 OIDC Authorization Request Parameters - scope

The Mobile Connect KYC Match product is requested by SPs via OpenID Connect API requests in alignment with the Mobile Connect Profile (DI mode or SI mode) and using the appropriate scope parameter based on whether they require the 'plain text' or 'hashed' version of the service:

Mobile Connect KYC Match	scope[8]
Mobile Connect KYC Match with plain text claims values	"mc_kyc_plain"
Mobile Connect KYC Match with hashed claims values	"mc_kyc_hashed"

Table 3: Mobile Connect KYC Match Scope Values

Note that When Operator captures the consent the Level of Assurance required for MC KYC Match is set by Operator policy based upon the sensitivity of the data being shared. The default LoA is LoA2 (single factor authentication). Any value submitted within the acr_values parameter in the OIDC Authorization Request will be ignored.

4.2 API Modes Supported

Mobile Connect KYC Match can be supported in both Device-Initiated and Server-Initiated modes.

4.3 Attribute Set

Both Mobile Connect KYC Match variants support the same attributes: name, address and, optionally, the User's date of birth. In addition, optional additional attributes are identified to enhance the KYC Match service (See Table 7).

Operators may, at their discretion, provide other attributes not specified in this document in their KYC Match service offering. For example, an Operator may offer Title (Mr/Mrs/Dr etc.) or Gender as optional parameters.

All attributes offered in the KYC Match service are provided on a "best-effort" basis.

4.3.1 Submitted Attributes - Claims

Table 4 specifies the possible attribute identifiers that can be included as claims within the OIDC Authorization Request. The attribute identifiers should be appended with "_hash" (e.g. given_name_hash) where the claim values are hashed. The name and address information can either be provided as individual component values (i.e., given_name, family_name) or concatenated into one attribute (e.g., name). Examples of the OIDC Authorization Request are included in Annex C.

[8] "openid" must be included within the scope parameter as a string followed by the relevant Mobile Connect service descriptors separate by spaces

Operators have the flexibility to match given name and surname either as separate parameters or as a single parameter called “name” where the given name and surname are concatenated. The same applies to address, i.e. the Operator can decide to match house number or house name, postal code, town name and country as separate parameters or as a single concatenated parameter called “address”.

Note that the Operator can choose not to use all elements of address to match when using a single attribute for address (e.g.: address = house number + postal code only). Matching all elements (e.g.: address = house number + postal code + town + country) may yield high false negatives.

Attribute Identifier	Usage	Description
`given_name` or `given_name_hash`	**REQUIRED** (`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` or `family_name_hash`		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` or `name_hash`		concatenated `given_name` and `family_name`.
`address` or `address_hash`	**REQUIRED** (`address` (OR) [`houseno_or_housename, postal_code, town, country`]	concatenated `houseno_or_housename, postal_code and optionally town and country`.
`houseno_or_housename` or `houseno_or_housename_hash`		Registered house number or house name.
`postal_code` or `postal_code_hash`		Registered Zip code or post code.
`town` or `town_hash`		Registered city or town name0
`country` or `country_hash`		Registered country0
`birthdate` or `birthdate_hash`	OPTIONAL	End-User's birthday, represented as an ISO 8601:2004 [4] YYYY-`MM-DD` format. The year MAY be `0000`, indicating that it is omitted.

Table 4: Claims Included within the OIDC Authorization Request

4.3.2 Resource Response – Validated Claims

The Operator ID GW processes the request in real time (if request attributes are hashed, then hashes the data it has on record and compares it with hashed data from the SP) and returns a match response. The ID GW also echoes back the attribute identifier and its value if there is a match. If there is no match, the attribute is removed from the response and just an indication of a false match is returned.

Table 5 specifies parameters that are returned within the Resource Response from the appropriate Resource Endpoint for KYC Match.

The attribute identifier is appended with “_hash” where the submitted claim values were hashed (e.g. given_name_hash when the submitted claim included the “given_name_hash” attribute identifier).

In addition, an additional parameter is returned with the suffix ‶_match” to indicate the outcome of the KYC Match. The outcome is indicated using one of the match values defined in Table 6 based on whether the match was successful or unsuccessful. Examples of the Resource Response are shown in Annex C.

Attribute Identifier	Usage
given_name or given_name_hash	**REQUIRED** ([name] (OR) [given_name, family_name])
family_name or family_name_hash	
name or name_hash	
address or address_hash	**REQUIRED** (address (OR) [houseno_or_housename, postal_code, town, country]
houseno_or_housename or houseno_or_housename_hash	
postal_code or postal_code_hash	
town or town_hash	
country or country_hash	
birthdate or birthdate_hash	OPTIONAL
given_name_match	**REQUIRED** (name_match (OR) [given_name_match, family_name_match])
family_name_match	
name_match	
address_match	**REQUIRED** (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

Table 5: Resource Response Parameters

When the service computes a match result, it must return one of the following values for each attribute as shown in Table 6:

Response Match Indicators
“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[9]

Table 6: Resource Response – Match Indicators

4.3.3 Optional Attributes that May be Returned in the Resource Response

In order to enhance the value of the KYC Match service, Operators can optionally include additional attributes relating to the User’s mobile account in the Resource Response as shown in Table 7. Note that Operators must perform legal due diligence on the data shared in the response to ensure the sharing is in accordance with the local rules and regulations.

Attribute Identifier	Usage	Response values
is_lost_stolen	OPTIONAL	Allowed values are Boolean value true or false
billing_segment	OPTIONAL	Allowed values “PAYG”,” PAYM”, “Business”
account_state	OPTIONAL	Allowed values “active” / “inactive”

Table 7: Optional Resource Response Attributes

5 Service-Specific Requirements

Table 8 defines the service-specific requirements relating to the Mobile Connect KYC Match service. These should be used in conjunction with the following requirements in the implementation of this Mobile Connect service:

- Core Requirements specified in the Mobile Connect Technical Architecture and Core Requirements [6]. Note that these are common to all Mobile Connect Services.

- Resource Server and Attribute Services Requirements specified in the Mobile Connect Resource Server Specification [9]. Note that these are common to all Mobile Connect attribute services. Service specific requirements may further refine or qualify the more general requirements for attribute services. Note that MC KYC Match does not make use of the mc_claims parameter in the Resource Request but uses the claims parameter in the OIDC Authorization Request to assert attribute values to be matched.

[9] Note that access may be denied either due to User preference or Operator policy

For terminology and associated specifications please refer to the Mobile Connect Technical Overview [5].

No	Relating To	Requirement
MC_KYCM_01	Service Registration	The ID GW must be able to allow a Service Provider (client application / service) to register for the Mobile Connect KYC Match service and be provisioned with the requisite SP-provided parameters dependent on whether the SP intends to use Device-Initiated mode or Server-Initiated mode when requesting the service and what modes are supported by the ID GW. See the Mobile Connect Device-Initiated OIDC Profile[7] and the Mobile Connect Server-Initiated OIDC Profile[8].
MC_KYCM_02	Attribute Values - Hashing	The Resource Server and the SP are recommended to use the SHA 256 hashing algorithm for hashing attribute values for the KYC Match hashed service variant for interoperability.
MC_KYCM_03	Attribute Values - Normalisation	Mobile Connect KYC Match normalization rules for formatting attribute values should be negotiated offline between Operators and Service Providers for a given geographic region / market.
MC_KYCM_04	Service Invocation	A Service Provider must be able to request either the plain text or hashed variant of the KYC Match service through use of the appropriate `scope` parameter value in the KYC Match service request as specified in Section 4 of MC KYC Match Definition and Technical Requirements. Note that the Operator is free to decide which variant of the KYC Match service (plain or hashed data) they wish to support.
MC_KYCM_06	Service Request - Validation	The ID GW must ensure that the attribute names values to be matched are provided in the `claims` parameter in the OIDC Authorization Request as specified in Section 4 of MC KYC Match Definition and Technical Requirements. The SP should provide attribute values for matching either in plain text form or hashed form. It is not permissible for the SP to mix hashed and plain text attribute values in a single service request. If any REQUIRED attribute values are null, then an appropriate error must be returned. If any OPTIONAL values are null, then that attribute should be ignored. If all attribute values are null, then an appropriate error must be returned as specified in the relevant OIDC Profile (MC Device-Initiated OIDC Profile[7] or MC Server-Initiated OIDC Profile[8]).
MC_KYCM_07	Service Request - Validation	The ID GW must validate that the attribute values submitted in the `claims` parameter of the KYC Match service request based upon the specified `scope` value included in the request. If `scope` contains “mc_kyc_plain”, the attribute values in the `claims` parameter must be in the plain text format. If `scope` contains “mc_kyc_hashed” then the attribute values in the `claims` parameter must be hashed.

		If the scope value and attribute types specified in the claims parameter of the KYC Match service request do not match (e.g. the SP has requested the ‘plain text’ KYC Match service and used the “mc_kyc_plain” scope in the OIDC request but has then provided the claims in hashed form (i.e., "name_hash"), then an "invalid_request" error must be returned as specified in Annex A of this docuemnt.
MC_KYCM_07	Tokens	The ID GW Authorization Server must issue Access Tokens with a zero time-to-live using a very low value (e.g. 10s) for the expires_in parameter in the Token Response or by restricting it to a single-use token. Long-lived consent can be granted, subject to the Operator's ID GW consent policy and the associated contractual agreement with the Service Provider, but an OIDC Authorization Request must be submitted for each service request as the attribute names and values to be matched must be included within the claims parameter for KYC Match services.
MC_KYCM_08	Tokens	The ID GW Authorization Server must not issue a Refresh Token for the KYC Match service.
MC_KYCM_09	Resource Response	For Mobile Connect KYC Match services, for each attribute value for which there is a match, the Resource Server must return a positive match indicator and the attribute name and value. If the attribute values do not match, the ID GW should only return the Match indicator in the response and the attribute name and value must be removed from the response. Match indicators are specified in Section 4 of this document.
MC_KYCM_10	Error Responses	Error Responses may be returned at different stages of the processing of an OIDC Authorization Request as specified in the MC Device-Initiated OIDC Profile and the MC Server-Initiated OIDC Profile and must be supported for the KYC Match service. Error may also be generated as a result of processing of the Resource Request at the Resource Server as specified in the Mobile Connect Resource Server document[9] and must be supported for the KYC Match service. These errors are generic to Mobile Connect services and Mobile Connect attribute services, respectively. Service Specific Error Responses are specified in Annex A of this document and must be supported for the KYC Match service.
MC_KYCM_11	Transaction Logs	A complete Mobile Connect transaction log must be maintained, archived and accessible to resolve any disputes in line with local data protection laws and the Operator's data retention policy. For MC KYC Match this should include: • Phone number (MSISDN or ENCR MSISDN) • Date & Time • KYC Match scope

		• Attributes(s) matched / not matched • PCR • Consent State (active, revoked) • Status (Complete, in-process, Error) • Any Errors (error codes and error description) • Time of consent capture (if Operator captures the consent) • Evidence of consent

Table 8: Mobile Connect KYC Match Service Requirements

Annex A Authenticator Suitability

Mobile Connect Authenticator	Suitable for Mobile Connect Consent Request?	Explanation
Seamless authenticator (e.g. enriched header)	No	Not applicable
SMS + URL (embedded link)	Yes	Supports LoA2
USSD (network-initiated USSD)	Yes	MC KYC Match OK with LoA2.
SIM Applet	Yes	Supports LoA2 and LoA3 but there is limited space to display information - if the requirement is to list out all the attributes and their values within the consent screen, this may require multiple SIM applet pages.
Smartphone app	Yes	The smartphone app authenticator Supports LoA2 and LoA3 and has plenty of space for displaying the consent prompt

Annex B Mobile Connect KYC Match Service Specific Error Codes and Descriptions

This Annex lists the service-specific error codes and associated descriptions that are REQUIRED for the MC National-ID service in addition to the generic error codes and descriptions that are specified in the relevant OIDC Profiles (MC Device-Initiated OIDC Profile [7] and MC Server-Initiated OIDC Profile [8]) and the Resource Server Specification [9].

B.1 Single Page and Two Page Environments

Certain error codes are generated depending on whether the implementation of Mobile Connect KYC Match requires a single page to be displayed or two pages to be displayed on the User's Authentication Device. The default is for a single page to be displayed but there may be a requirement in certain regulatory environments to use a two-page approach. A two-page environment involves authenticating the User on the first page and presenting attributes related information and seeking User consent on the second page.

B.2 Error Responses in Device-Initiated Mode

Table 9 lists the additional error codes and descriptions for Mobile Connect KYC Match.

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
`claims` parameter exists, but REQUIRED parameters inside claims are missing (or) `claims` parameter exist, but the value is empty (or) `claims` parameter does not exist	Redirect 302	`invalid_request`	REQUIRED values in the claims parameter are missing for MC KYC service (or) invalid.
`client_name` parameter does not exist and SP has registered multiple client names	Redirect 302	`invalid_request`	REQUIRED parameter `client_name` is missing.
`client_name` parameter exists but it has invalid value. (SP registered single or multiple client_names)	Redirect 302	`Invalid_request`	REQUIRED parameter client_name value is invalid or name is not registered.
In a single-page environment, the User failed to give consent (or) the ID GW was unable to authenticate the User (authentication failure).	Redirect 302	`consent_failure`	User failed to give consent (or) was not authenticated.

In a single-page environment, the User denied the request for consent.	Redirect 302	`consent_denied`
		`(or)`
		`consent_failure`
		`(or)`
		`access_denied`
			User has not given consent (or) consent failure.

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
The User was unable to give consent – a timeout occurred.	Redirect 302	consent_failure (or) access_denied	Timeout occurred during consent capture.
In a two-page environment, the ID GW failed to authenticate the User on the first page.	Redirect 302	consent_failure (or) access_denied	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but denied the request for consent	Redirect 302	consent_denied (or) consent_failure (or) access_denied	User has not given consent (or) consent failure.

Table 9: MC KYC Match: Errors – Device-Initiated Authorization Response

B.3 Error Responses in Server-Initiated Mode

Table 10, Table 11, Table 12 and Table 13 show the possible error codes and descriptions related to the Mobile Connect KYC Match service.

B.3.1 Error Responses: OIDC Authorization Response

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
client_name parameter does not exist SP has registered multiple client names	Bad Request 400	invalid_request	REQUIRED parameter client_name is missing.
Client_name exists but the value is invalid, SP has register single or multiple client names	Bad Request 400	Invalid_request	REQUIRED parameter client_name value is invalid or name is not registered.
claims parameter does not exist (or) claims parameter exists but REQUIRED parameters within the claims parameter are missing (or) claims parameter exists but the value is empty,	Bad Request 400	invalid_request	REQUIRED claims parameter is missing (or) is invalid.

Table 10: MC KYC Match: Errors – Server-Initiated Authorization Response

B.3.2 Error Responses: Notification

Error Scenario	Error code	Error Description [REOMMENDED text]

In a single-page environment, the User failed to give consent (or) the ID GW was unable to authenticate the User (authentication failure).	`consent_failure`
	(or)
	`access_denied`
		User failed to give consent (or) was not authenticated.

In a single-page environment, the User denied the request for consent.	`consent_denied`
	(or)
	`consent_failure`
	(or)
	`access_denied`
		User has not given consent (or) consent failure.

The User was unable to give consent – a timeout occurred.	`consent_failure`
	(or)
	`access_denied`
		Timeout occurred during consent capture.

In a two-page environment, the ID GW failed to authenticate the User on the first page.	`consent_failure`
	(or)
	`access_denied`
		User was not authenticated.

In a two-page environment, the User was authenticated in the first step, but denied the request for consent	`consent_denied`
	(or)
	`consent_failure`
	(or)
	`access_denied`
		User has not given consent (or) consent failure.

Table 11: MC KYC Match: Errors - Server-Initiated Token Response using Notification

B.3.3 Error Responses: Notification Acknowledgement

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
Invalid ID Token	Bad Request 400	`invalid_request`	Mobile Connect ID Token is not valid.
Invalid Access Token and not tied to the ID Token	Bad Request 400	`invalid_request`	Mobile Connect Access Token is not valid.

Table 12: MC KYC Match: Errors - Server-Initiated Notification Acknowledgement

B.3.4 Error Responses: Polling Response

Error Scenario	HTTP Mode	Error code	Error Description [REOMMENDED text]
In a single-page environment, the User failed to give consent (or) the ID GW was unable to authenticate the User (authentication failure).	Forbidden 403	consent_failure (or) access_denied	User failed to give consent (or) was not authenticated.
In a single-page environment, the User denied the request for consent.	Forbidden 403	consent_denied (or) consent_failure (or) access_denied	User has not given consent (or) consent failure.
The User was unable to give consent – a timeout occurred.	Forbidden 403	consent_failure (or) access_denied	Timeout occurred during consent capture.
In a two-page environment, the ID GW failed to authenticate the User on the first page.	Forbidden 403	consent_failure (or) access_denied	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but denied the request for consent	Forbidden 403	consent_denied (or) consent_failure (or) access_denied	User has not given consent (or) consent failure.

Table 13: MC KYC Match: Errors - Server-Initiated Polling Response

Annex C Example Requests

C.1 Requests from Service Provider

This section shows examples of KYC Match requests from a Service Provider to the ID GW.

Example Request where “`scope = openid mc_kyc_hashed`” without Date of Birth.

```
{
   "response_type": "code",
   "client_id": "s6BhdRkqt3",
   "redirect_uri": "https://client.example.org/cb",
   "scope": " openid mc_kyc_hashed",
   "state": "af0ifjsldkj",
   "nonce": "n-0S6_WzA2Mj",
    "claims":
    {
      “premiuminfo":
      {
            "given_name_hash”:
{“value”:”2fd4e1c67a2d28fced849ee1bb76e7391b93eb12”},
      "family_name_hash”:
{“value”:”3fd4e1c67a2d28fced849ee1bb76e7391b93eb12”},

“given_name_match”: {“essential”: true, values: [“Y”,” N-AV”, “N-AD”, “N-
NA”]},
“family_name_match”: {“essential”:true, values:[“Y”,”N-AV”, “N-AD”, “N-
NA”]},
"address_hash":{“value”:“de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3“},
“address_match”:{“essential”:true, values:[“[“Y”,”N-AV”, “N-AD”, “N-NA”]},
“birthdate”:{“value”:“0000-12-12”},
“account_state” :{“value”:”active”}
    }
}
```

Example Request where “`scope = openid mc_kyc_plain`” with Date of Birth.

```
{
   "response_type": "code",
   "client_id": "s6BhdRkqt3",
   "redirect_uri": "https://client.example.org/cb",
   "scope": " openid mc_kyc_plain",
   "state": "af0ifjsldkj",
   "nonce": "n-0S6_WzA2Mj",
    "claims":
    {
      “premiuminfo":
      {
            "given_name”: {“value”:”john”},
      “given_name_match”:{“essential”:true, values:[“Y”,”N-AV”, “N-AD”, “N-
NA”]},
“family_name”: {“value”:”doe”},
“family_name_match”:{“essential”:true, values:[“Y”,”N-AV”, “N-AD”, “N-
NA”]},
"address":{“value”:“3645finsburytowerec147qx“},
“address_match”:{“essential”:true, values:[“Y”,”N-AV”, “N-AD”, “N-NA”]},
“birthdate”:{“value”:“1984-07-26”},
“birthdate_match”:{“essential”:true, values:[“Y”,”N-AV”, “N-AD”, “N-NA”]},
“account_state” :{“value”:”active”}

}
```

C.2 Resource Response to the Service Provider

Example Response where there is a full match:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
      “sub":"5f90512d-972d-4def-bf90-9ef0ef2e5d2d“,
      "given_name_hash":”2fd4e1c67a2d28fced849ee1bb76e7391b93eb12”,
      “given_name_match”:“Y-AV”,
   "family_name_hash":”3fd4e1c67a2d28fced849ee1bb76e7391b93eb13”,
      “family_name_match”:“Y”,
      "address_hash":”de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3“,
      “address_match”:“Y”,
    “is_lost_stolen”: false,
    “billing_segment”:”PAYM”,
       “barthdate_hash”:” feff2c7fd25e1b3afad3e85a0bd17d9b100db4b1”,
        “birthdate_match”:”Y”,
“account_state” :”active”

   }

}
```

Example Response where there is a partial match (given_name_hash and family_name_hash are not matching):

```
HTTP/1.1 200 OK
Content-Type: application/json
{
      “sub":"5f90512d-972d-4def-bf90-9ef0ef2e5d2d“,
      “given_name_kmatch”:“N-AV”,
   “family_name_match”:“N-AV”,
      "address_hash":”de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3“,
      “address_match”:“Y”,
    “is_lost_stolen”: false,
    “billing_segment”:”PAYM”,
       “birthdate_hash”:” feff2c7fd25e1b3afad3e85a0bd17d9b100db4b1”,
       “birthdate_match”:”Y”,
“account_state” : “active”
}
```

Example Response where there is a partial match (`address_hash` not matching):

```
HTTP/1.1 200 OK
Content-Type: application/json
{
      “sub":"5f90512d-972d-4def-bf90-9ef0ef2e5d2d“,
      "given_name_hash":”2fd4e1c67a2d28fced849ee1bb76e7391b93eb12”,
      “given_name_match”:“Y”,
   "family_name_hash":”3fd4e1c67a2d28fced849ee1bb76e7391b93eb13”,
      “family_name_match”:“Y”,
      “address_match”:“N-AV”,
    “is_lost_stolen”: false,
    “billing_segment”:”PAYM”,
       “birthdate_hash”:” feff2c7fd25e1b3afad3e85a0bd17d9b100db4b1”,
       “birthdate_match”:”Y”,
    “account_state” :”active”

   }

}
```

Example Response where there is No match:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
      “sub":"5f90512d-972d-4def-bf90-9ef0ef2e5d2d“,
      “given_name_match”:“N-AV”,
      “family_name_match”:“N-AV”,
      “address_match”:“N-AV”,
    “is_lost_stolen”: ”false”,
    “billing_segment”:”PAYM”,
    “birthdate_match”:”N-AV”,
    “account_state” :”active”

   }

}
```

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	04/11/2019	Major Update, product definition and technical specificaitons are merged. New document	TG	Gautam Hazari/GSMA

D.1 Other Information

Type	Description
Document Owner	Gautam Hazari/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.