Mobile Connect Product Guidelines

Version 1.1

06 December 2022

This is a General of the GSMA

Security Classification: Non-confidential

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

Copyright Notice

Copyright © 2022 GSM Association

Disclaimer

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

Antitrust Notice

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

Table of Contents

1 Introduction 3
1.1 Executive summary 3
1.2 Scope of the document 3
1.3 References 3
1.4 Glossary and abbreviations 4
1.5 Conventions 4
2 Product Guidelines 5
2.1 Development guidelines 5
2.2 Technical design principles 7
2.3 User Experience (UX) guidelines 8
2.4 Mobile Connect License 9
2.5 Product Registration via the GSMA Product Directory 9
3 Mobile Connect Product Directory 9
3.1 Information required for product registration 10
3.2 Plan for a simple implementation 10
Annex A An example of how and when to create a new product 12
Annex B Attributes list (non-exhaustive) 13
Annex C Document History 16

1 Introduction

1.1 Executive summary

The purpose of this document is to provide guidance for the development of products and services using the existing Mobile Connect framework and in particular for Mobile Operators developing and deploying products to meet their own local market needs.

To ensure that a Service Provider can consume the services in a consistent manner, it will be important that Mobile Operators work together on the definition of said products within their local market, and do so in compliance with a set of Mobile Connect criteria to ensure interoperability. Doing so also ensures that these products can easily be offered consistently by mobile operators across different markets as well.

In short, a new Product should follow the product development guidelines outlined in this document and in particular the technical design principles defined in section 2.2. The Products should also adhere to the Mobile Connect licence agreement [2] and Mobile Connect Privacy Principles [6] and be registered in the Product Directory managed by GSMA to ensure uniqueness of the product identifier hence avoiding conflicting product naming and duplication of effort (see section 2.5).

1.2 Scope of the document

In Scope	Out of Scope
• Product development guidelines • Product compliancy requirements • Product registration (Product Directory)	• Go to market including Service Provider onboarding and contracts • In-life management of Products including Service Provider support

1.3 References

Ref	Doc Number	Title
[1]	RFC 2119	"Keywords for use in RFCs to Indicate Requirement Levels," S. Bradner, March 1997. Available at http://www.ietf.org/rfc2119.txt
[2]		Mobile Connect Operator Licence Agreement
[3]	IDY.01	Tech Mobile Connect Device Initiated OIDC Profile
[4]	IDY.02	Tech Mobile Connect Server Initiated OIDC Profile
[5]		Quick reference UI flows and Designs. Available at https://infocentre2.gsma.com/gp/pr/Identity/User%20Flow%20Design%20Kit/1.%20Quick%20referencee%20UI%20flows%20and%20Designs
[6]		Mobile Connect Privacy Principles
[7]	IDY.16	Product Manager's Lifecycle Handbook
[8]	IDY.21	Prod Mobile Connect National ID product definition v1
[9]	IDY.03	Mobile Connect Resource Server Specification

Table 1: References

1.4 Glossary and abbreviations

Term	Description
API	Application Programming Interface
Attribute	Piece of information about a user that is shared with an SP
CIBA	Client Initiated Backchannel Authentication
Global Product	Globally defined Mobile Connect product described in GSMA reference documents including Product Definition and Technical Specification
Identity Token	Provides a set of metadata regarding the Authentication to the Service Provider. This includes the PCR, authenticator used, Level of Assurance etc.
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
KYC	Know Your Customer
LoA	Level of Assurance
MSISDN	Mobile Station International Subscriber Directory Number
Operator	Mobile Network Operator
OTP	One-Time Password
PAYG	Pay as you go (prepaid contract)
PAYM	Pay monthly (postpaid contract)
PRD	Public Reference Document
SP	Service Provider (The application/service that needs the authentication and identity services)
SIM	Subscriber identity module
T&C	Terms and conditions
UI	User Interface
UX	User Experience

Table 2: Glossary and abbreviations

1.5 Conventions

The keywords “must”, “must not”, “required”, “shall,” “shall not,” “should,” “should not,” “recommended,” “may”, and “optional” in this document are to be interpreted as described in RFC2119 [1].

2 Product Guidelines

The Product guidelines comprise the following three parts:

- Development
  Adherence to the Mobile Connect product development guidelines (further detailed in sections 0, 2.2 and 2.3)

- License
  Adherence to the Mobile Connect license agreement [2] including the Mobile Connect Privacy Principles [6] (see section 2.4)

- Product Registration
  Registration of all Products in a GSMA centrally managed repository [the Product Directory] (see section 2.5).

In order to be considered Mobile Connect compliant, a Product:

- Must adhere to the Mobile Connect technical design principles (see section 2.2)
- Must build upon the Mobile Connect User Experience guidelines (see section 2.3)
- Must rely on the mobile device as the mechanism through which the user authenticates or authorises a transaction

2.1 Development guidelines

When designing a new Product, it is vital that Mobile Operators work together within the market to form a common agreement on the product definition hence ensuring that SPs are able to consume the same service consistently irrespective of the serving Mobile Operator within the local market. Mobile Operators should agree on a suitable process in each market for the development of the product and allocate roles and responsibilities to deliver:

- A product Definition & Technical Specification document which explains:
  - functionality of the Product
  - use cases and scenarios in which it might be used
  - user experience/user flows
  - which attributes are used and the format for these attributes
  - all other applicable product requirements
  - technical specification including how the Open ID Connect Mobile Connect API should be used in the deployment of the product and associated error handling
- An SDK if needed, which may be built as an evolution of a relevant Global Product SDK
- Interoperability testing across MNO deployments in the target market; this may be performed with a friendly SP
- A go-to-market plan covering those aspects which need to be discussed jointly x-MNO including channels to market, contractual model, SP onboarding, billing and

settlement and customer care and the potential opportunity of using MC Link in this regard

Mobile Operators may find it useful to leverage the existing Global Product documentation (Service Definition & Technical Requirements) to generate local variants. An example is discussed in annex A.

For reference, Annex A lists a wide range of potential attributes that Mobile Operators may choose to share or verify as part of their Products. Of course Mobile Operators may also have other attributes of interest which are not listed. The table below provides an attribute short-list that addresses many of the current SP needs:

Attribute Name	Description
User identity & contact details	
`title`	Salutation
`given_name`	Given name(s) or first names
`family_name`	Surname(s) or last name(s) of the user
`middle_name`	Middle name(s) of the user
`gender`	User's gender
`birthdate`	User's birth date[1]
`street_address`	User's street (incl. house name/number)
`city`	User's city / town
`state`	User's state / county
`postal_code`	User's Zip/ Postcode
`country`	User's postal country
`phone_number`	User's Mobile Connect designated mobile number
`email`	User's e-mail
Mobile account details	
`billing_segment`	"PAYG","PAYM","Business"
`account_tenure`	Date from which the user is known as a customer at the MNO
`account_state`	"active","inactive"
Contextual signals	
`is_roaming`	True/False
`country_code`	Last-known country of the user
`is_lost_stolen`	True/False
`is_unconditional_call_divert_active`	Mobile phone account has an unconditional call divert set to a number (True/False)
`sim_change`	Timestamp of last MSISDN <-> IMSI pairing change
`device_change`	Timestamp of last MSISDN <-> IMEI pairing change
`device_msisdn`	MSISDN of the device accessing the SP service[2]

Figure 1 Attribute short-list

[1] Enables additional derived attributes to be generated such as `Age` or `Is_Adult`

[2] Captured and used specifically for the Verified MSISDN service

2.2 Technical design principles

This section defines a set of key principles that MUST be adhered to in the deployment of a Product:

1. Mobile Connect API:
   a. The Product MUST use the Mobile Connect API (Device Initiated [3] or Server Initiated [4] OpenID Connect Profiles) for the exposure of Mobile Connect services towards Service Providers
2. There MUST be a logical separation between the “Authorization Server” and the “Resource Server(s)”:
   a. The Authorization Server is part of the ID GW which exposes the protocol endpoints: Authorization and Token
   b. The Resource Server exposes the resource endpoints which can either be UserInfo/PremiumInfo or a service-specific resource endpoint. The Resource Server can be implemented as part of the ID GW or separately; more information on the Resource Server is available in [9]
3. ID GW endpoints:
   a. The ID GW Authorisation Server MUST use the same endpoints (Authorisation; Token or Notification endpoints) irrespective of use case (product/service). For the resources, UserInfo/PremiumInfo or service-specific Resource Server endpoints SHOULD be used
4. Adherence to OIDF standards:
   a. The flows MUST use either a Device-Initiated approach based on the Authorisation Code flow as described in the Mobile Connect Device Initiated OpenID Connect Profile or a Server-Initiated approach based on asynchronous communication.
   b. Device Initiated Mode
      i. The following core OpenID Connect protocol aspects MUST be adhered to:
         1. Authorization Code: OIDC Authorization call
         2. ID Token and Access Token: OIDC Token call
         3. Resource Access: UserInfo/PremiumInfo call or call to service-specific Resource Server endpoint
   c. Server Initiated Mode
      i. The following CIBA[3] related protocol aspects MUST be adhered to
         1. Server initiated call: OIDC Authorization call
         2. ID Token and Access: through Notification or Polling
         3. Resource Access: UserInfo/PremiumInfo call or call to service-specific Resource Server endpoint
   d. There MUST NOT be any additional flows introduced for the Mobile Connect protocol interactions (e.g., additional redirects, additional notifications) unless needed for specific architecture options like aggregator integration, hub based integration etc. The usage of additional flows MUST be discussed and agreed with the GSMA and Mobile Connect MNO community.

[3] Client Initiated Backchannel Authentication

5. OIDC <scope> parameter:
   a. The <scope> parameter in the OIDC Authorization request MUST be used as the "control channel" for identifying the product/service being requested by the SP
   b. The <scope> value MUST align with the Mobile Connect pattern (mc_<<product>>_<<country>>)
   c. Registration of <scope> value via GSMA Product Directory (see sections 2.5 & 3
      i. The Product Directory will check the uniqueness of the <scope> value across the directory and also check for consistency in naming[4]
      ii. A Mobile Operator creating a Product should submit a <scope> entry for the directory and use the registered <scope> to identify the product
6. Mobile Connect API extension:
   a. Additional parameters for the Mobile Connect calls [Authorization, Token, Notification and UserInfo] SHOULD NOT be introduced as this may result in fragmentation and interoperability issues
   b. If additional parameters are needed, this MUST be discussed and agreed within the wider Mobile Connect MNO community to minimise the risk of fragmentation
7. The ID Token MUST ONLY be used for providing claims for the Authentication/Authorisation metadata. All user attributes MUST be exchanged using the UserInfo/PremiumInfo endpoint or service-specific Resource Server endpoints.
8. User or Mobile Connect Tokens (PCR, Access Token, ID Token) MUST be used within APIs as parameters and MUST NOT be shared using cookies due to their limitations
9. Mobile Operators must follow local legislation to ensure that users accept T&Cs pertaining to the use of the Mobile Connect Product

2.3 User Experience (UX) guidelines

A clean, simple & intuitive UX is key to the adoption and repeat usage of Mobile Connect Products by end users. Towards this view, Mobile Operators should invest in the UI/UX testing and design of Products to ensure that the most optimised versions are deployed in-market. Similarily, Mobile Operators should acknowledge the importance of user education and incorporate where necessary into the product flow as well as through a wider marketing and communications strategy to drive higher take-up of the product.

For products that include the provision or verification of attributes / personal data, specific attention must be paid to establish the lawful data processing basis. Where user consent is required, the method of consent capture and how to manage the user journey will form an important element of the end-end User Experience. General guidance on consent management is provided in the Product Manager's Lifecycle Handbook [7] and Mobile Operators will also be able to review other Products listed in the Product Directory to study Best Practice approaches that have worked in other markets.

Additional guidance with regards to UX is currently available in [5].

[4] to avoid two products being registered with different names but very similar functionality; e.g., avoid the following: <mc_kycmatch_uk> <mc_kyccompare_es>

2.4 Mobile Connect License

A Product which uses the Mobile Connect Service Mark must abide by the Mobile Connect License agreement [2]. The Mobile Connect Licence agreement grants Mobile Operators a worldwide license to use the Mobile Connect brand assets subject to them meeting the following contractual terms[5]:

- Usage of the Mobile Connect Service Mark
- Communication guidelines for the Service Mark
- Mobile Connect minimum Service Mark requirements[6]
- Mobile Connect Privacy Principles [6]

A Product that does not use the Mobile Connect Service Mark should still be designed in accordance with the Mobile Connect Product Guidelines as outlined in section 2 and the Mobile Connect Privacy Principles [6] in order to be considered Mobile Connect compliant.

2.5 Product Registration via the GSMA Product Directory

It is vital that Mobile Operators register any Products they develop (and the associated `<scope>` product identifier they intend to use) within the Product Directory in order to avoid conflicts between different markets (for instance two markets developing different products under the same product identifier). As an additional benefit, by sharing Products through the Product Directory Mobile Operators will benefit from reduced development cost and an increased flow of ideas. Starting the product registration whilst Mobile Operators are still in the development stages is encouraged, both to confirm the correct product identifier and to identify synergies across markets hence avoiding duplication of effort.

Once a Mobile Operator has submitted a product registration request, the GSMA will confirm the product meets the Product Guidelines before publishing it to the Product Directory. More details about the Product Directory and the Product registration process can be found in section 3.

3 Mobile Connect Product Directory

The aim of the Product Directory is to provide a single reference point for all Mobile Connect products that are in development or have been deployed in order to support best practise sharing and avoid duplication of effort and/or conflict in product naming (`<scope>`) etc.

[5] This license can't be sub-licensed and therefore any SPs and distribution partners entering into contracts with a Mobile Operator would be required to sign a license agreement with GSMA for access to the Mobile Connect Service Mark

[6] Minimum requirements that a Mobile Operator must self-certify in order to use the Mobile Connect Service Mark include: The Mobile device must be the mechanism the end user uses to be authenticated, the API exposed must comply with the OpenID Connect standard and global discovery must be enabled. For a complete list please refer to Annex D of the Mobile Connect License Agreement [2].

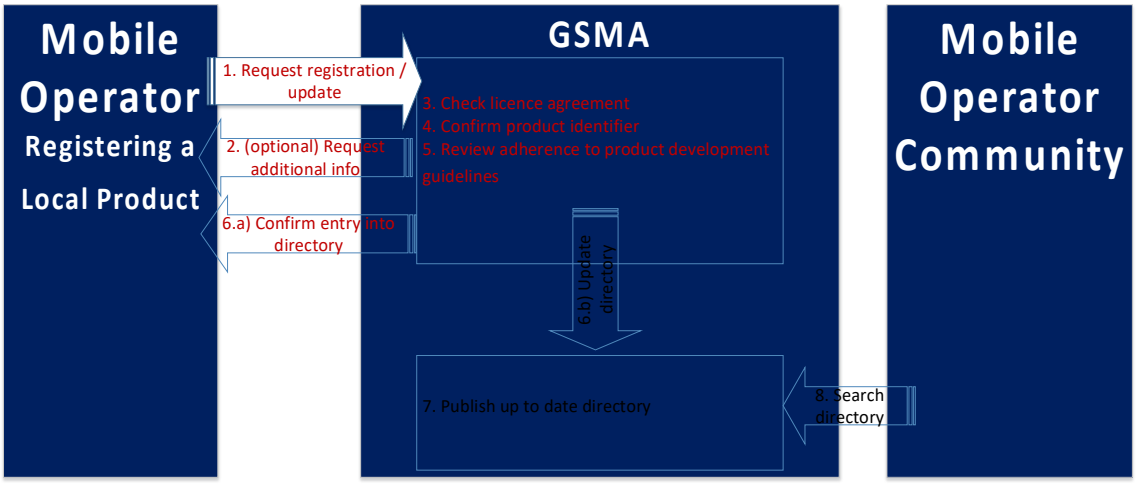
3.1 Information required for product registration

To register a Product a Mobile Operator will need to provide the following registration information:

- Product name
- Country
- Product identifier (`<scope>`)
- Authenticator/s used (where applicable)
- Assurance level used (where applicable)
- How the service is requested (Device-Initiated and/or Server-Initiated invocation) and what Profile version is being used
- Attributes used (where applicable)
- Comments, such as:
  - Technical assets such as SDKs (if and when avaialble)
  - What restrictions (if any) are put on the visibility of the Product, e.g. restrictions as to how it should be promoted to SPs (some products are not publicly advertised due to commercial sensitivities e.g. SP does not want to publicise their anti-fraud solutions)
  - What consent model is used (where applicable)
  - User flow information including a 30 second video of the Product in action (the video can be provided once the product has been developed)
  - Use cases supported by the product

3.2 Plan for a simple implementation

The Product Directory has been implemented as an Excel spreadsheet. GSMA will be responsible for coordinating and tracking the overall progress of new product requests and ensuring that the latest version of the Product Directory is available online.

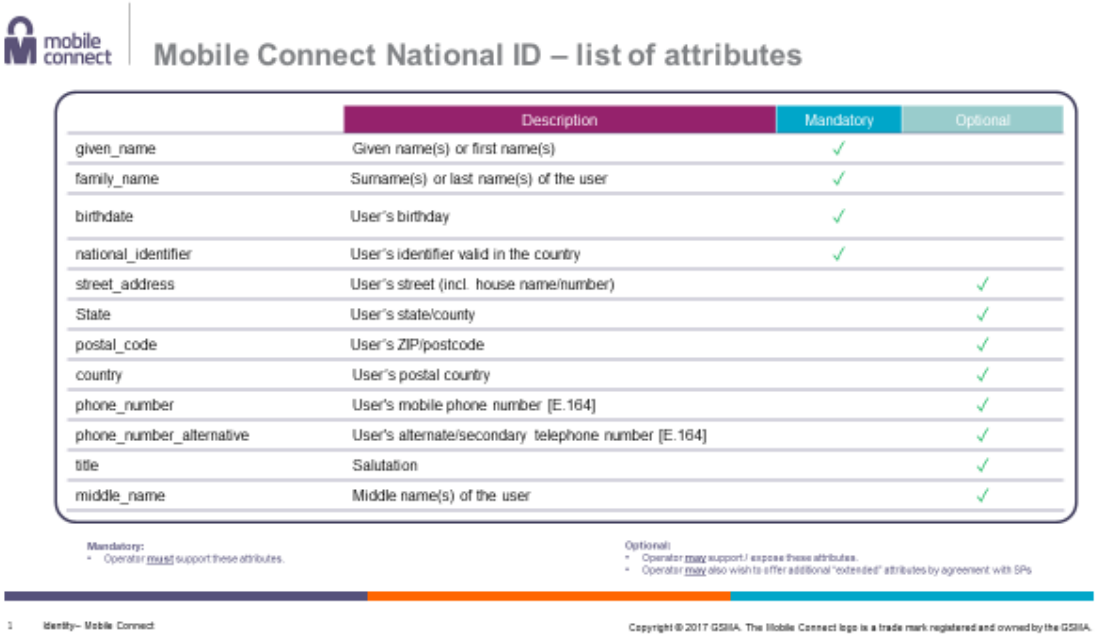


New product requests (or updates to existing products) should be submitted to mc_productdirectory@gsma.com. The GSMA will review all submissions, request any additional information where required and register the new product into the Product Directory. In doing so, it will perform the following checks:

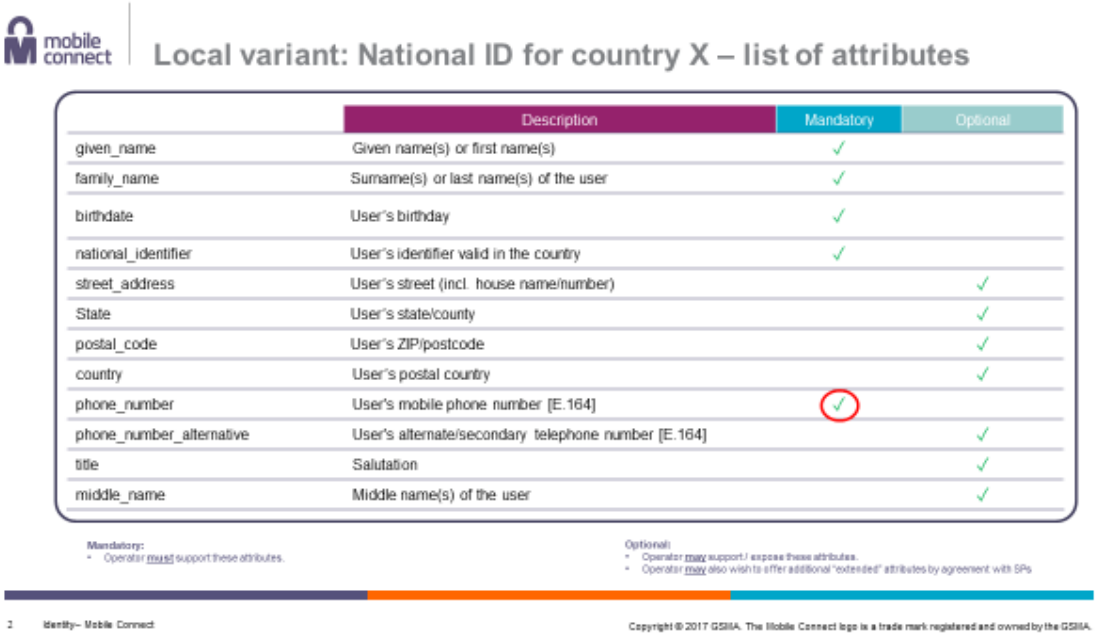
- ensure that each product has a unique identifier (via the `<scope>` parameter)
- validate that Mobile Operators are not developing a Product that is the same or similar to one that already exists.
  - Should the Product being registered be similar to another product registered in the Product Directory, the GSMA may suggest that the submitted Product use the same Product Identifier and align with the existing registered product; any slight variations to this existing registered product can be accommodated by using the same Product Identifier but appended with the name of the country where the variant is being deployed.
- ensure that the Product abides by the Product Guidelines requirements as set out in this document; if non-conformant, the GSMA will suggest corrections before the product can be considered as Mobile Connect compliant and registered in the Product Directory.
- in case of a change request to an existing product, confirm if the proposed change can be made under the existing registration or if a new product registration is required. If changes are made under the existing registration, GSMA will consider the associated impact for other markets who have already adopted the Product in its initial version and ensure that the same product name is not used in different markets for product variants that are significantly different.
- store the Product Directory [spreadsheet] and make it available online to Mobile Operators and GSMA via InfoCentre2 (only GSMA will have read/write access). Note that Mobile Operators can search the Product Directory directly or request support from the GSMA regional teams.

Annex A An example of how and when to create a new product

Mobile Connect National ID is a Global Product which delivers the following attributes:



Mobile Operators in a particular market may decide that the user's mobile phone number should also be included as a mandatory attribute to meet local regulations and/or SP expectations hence would need to create a new variant as identified below:



In such a scenario, the most efficient approach would be for the Operators to modify the existing Mobile Connect National ID Definition & Technical Requirements document [8] rather than writing their own product documentation from scratch.

Annex B Attributes list (non-exhaustive)

This annex lists a range of attributes which Mobile Operators may decide to share or verify as part of their Products. This list is not intended to be exhaustive and local variations are expected in the availability of attributes.

Attribute Name	Description
Mobile Connect	
sub	Subject Identifier, used as a unique reference for the user (i.e., PCR)
creation_date	Registration date of the user on Mobile Connect
updated_at	Time the user's information was last updated
User profile	
title	Salutation
name	User's full name in displayable form
given_name	Given name(s) or first name(s) of the user
family_name	Surname(s) or last name(s) of the user
middle_name	Middle name(s) of the user
nickname	Casual name of the user that may or may not be the same as the given_name. For instance, a nickname value of Mike might be returned alongside a given_name value of Michael
preferred_username	Shorthand name by which the user wishes to be referred to at the SP, such as janedoe or j.doe
displayname	Preferred name for display purposes
alias	Default alias of the user
locale	User's (preferred) locale/language code; e.g., en-US or fr-CA
gender	User's gender
birthdate	User's birthday; the year MAY be 0000, indicating that it is omitted
age	The age of the user in years (rounded)
age_verified	TRUE if the age of the user is verified, FALSE otherwise
is_adult[7]	0=Unknown 1=Subscriber Verified (verified by the holder) 2=Owner Verified (verified by the bill payer) 3=barred (set to non-verified by the owner/bill payer)
profile	URL of the user's profile page (describing the user)
picture	URL of the user's profile picture
website	URL of the user's Web page or blog
msisdn	Designated MSISDN for the Mobile Connect service
phone_number	User's preferred telephone number [E.164]
phone_number_verified	TRUE if the user's phone number has been verified; otherwise FALSE
phone_number_country_code	E.164 Country Code for the user's phone number
phone_number_alternate	User's alternate/secondary telephone number [E.164]
voicemail_PIN_enabled	TRUE if user has changed the voicemail PIN from the MNO-defined default
email	User's email
email_verified	TRUE if the user's e-mail address has been verified; otherwise FALSE

[7] Age threshold for an individual being legally considered an adult will be dependent on local legislation

Attribute Name	Description
address	User's preferred full postal address. . Concatenated houseno_or_housename, postal_code and optionally city and country
formatted	Full postal address formatted for display purpose (as a text string)
houseno_or_housename	Registered house number or house name
street_address	User's street (incl. house name/number)
city	Registered city or town name (residence)
state	Registered state / county (residence)
postal_code	Postal code (Zip code) (residence)
country	Country (residence)
address_verified	TRUE if the address is verified at the IDP, FALSE otherwise
zoneinfo	Registered (home) timezone of the user; e.g., Europe/Paris or America/Los_Angeles
passport	Passport number of the user
social_security_number	Social Security Number or NIC of the user
national_identifier	National identifier (e.g., in accordance with eIDAS) in the following format: CC/Type/Identifier CC: ISO 3166-1 Alpha-2 country code Type: ID document type (ID card, passport etc.) Identifier: ID number
segmentation	Socio-demographic segmentation of the user (e.g., MOSAIC)
Account info	
is_lost_stolen	TRUE if device reported as lost or stolen; otherwise FALSE
account_type	"Consumer","Enterprise"
billing_segment	Allowed values "PAYG","PAYM","Business"
account_tenure	Date from which the user is known as a customer at the MNO
account_start_date	Time since last renewal in days; False if unknown or unsupported
account_type	Primary; Sub
length_of_tenure	0=unknown 1=less than 30 days 2=30-90 days 3=90-360 days 4=over 360 days
tariff_group	Tariff group: prepaid, postpaid, hybrid
is_billpayer	TRUE If the user has been verified as the bill payer, FALSE otherwise
parental_control	Flag set by the parent on the account to indicate that the user is a minor (e.g., <18yrs)
ported_in	Has the user ported in from another MNO
phone_number_recycling	MSISDN has been released and not currently allocated[8]: Boolean: 0: currently not released 1: currently released and not currently allocated
account_state	'active', 'inactive'
device_type	User's device type (TAC code)
device_msisdn	MSISDN of the device accessing the SP service[9] [E.164]

[8] Note: this would apply to the situation where a Trusted SP is providing an MSISDN and requesting information about that number

[9] Captured and used specifically for the Verified MSISDN service

Attribute Name	Description
smartphone_upgrade	Smartphone upgrade = TAC code change + TAC code now indicating smartphone
type_tokens	MNO identity tokens assigned to the user's device: IMSI, ICCID, IMEI
ID_hash	Hash of MSISDN, IMSI and IMEI
device_change	Timestamp of last MSISDN <-> IMEI pairing change
SIM_change	Timestamp of last MSISDN <-> IMSI pairing change
is_unconditional_call_divert_active	Call divert status - activated, not-activated
date_last_bill_payed	Last bill payment date
date_last_topup	Last top up date for pre-paid user
payment_type_used	Payment method used by user - Direct Debit, Bank Transfer, Credit/Debit card
channel_of_purchase	Channel of purchase used by user - online, PoS, partner
Network session	
network_presence	Network presence: connected_home_nw, not_connected, connected_roaming
subscription_activity_30	Either the number of calls / texts in the last 30 days or a simple Boolean (TRUE/FALSE) indicating activity within this period
subscription_activity_365	Either the number of calls / texts in the last 12 months or a simple Boolean (TRUE/FALSE) indicating activity within this period; will depend on whether the intention is to indicate 'liveliness'
is_roaming	True/False
country_code	The country or last-known country of the user (ISO 3166-1 Alpha-2 country code)
latitude	The current or last-known latitude of the user's location
longitude	The current or last known longitude of the user's location
location_accuracy	Degree of confidence on the location accuracy: HIGH, MEDIUM, LOW
proximity	Indication of whether the user is within a search area (True/False)[10]
cell_id	The current or last known cell id of the mobile device used by the user
reverse-coded POI	Nearest POI reverse geo-coded from Lat/Long or Cell ID
state	The current or last-known state of the user derived from the Lat/Long and/or cell_id
city	The current or last-known city of the user derived from the Lat/Long and/or cell_id
location_time	The time at which the location data of the user was collected
location_age	The age of the location information expressed as the time between when the attribute request is made and the time at which the location data of the user was collected (location_time)
current_zoneinfo	Current or last-known timezone of the user; e.g., Europe/Paris or America/Los_Angeles
dwell_location	TRUE/FALSE indication of whether the device is currently in a common, habitual location; will be dependent on location pattern analysis and acquiring necessary user consents to collect this information and create these insights (the dwell locations: home, work[11] etc.)

[10] SP provides target Lat/Long; MNO compares against a pre-defined search radius and returns a True/False indication

[11] Note: the aim is not to identify the locations or infer anything about the user based on the locations they visit but to determine whether a location is common to the behavioural patterns of a given user; nevertheless, this is clearly privacy sensitive so any capability/service would have to be carefully and considerately designed & deployed

Annex C Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	07/07/2017	Initial draft	David Pollington	Helene Vigue / GSMA
0.2	10/07/2017	GSMA team revisions	David Pollington	Helene Vigue / GSMA
0.3	25/07/2017	GSMA team revisions (updates to Product Directory strawman implementation)	David Pollington	Helene Vigue / GSMA
0.4	02/08/2017	GSMA team revisions (updates to Annexes)	David Pollington	Helene Vigue / GSMA
0.6	07/09/2017	GSMA team revisions (simplification of Product Directory chapter 3, addition of section **Error! Reference s ource not found.** and Annex A)	David Pollington	Helene Vigue / GSMA
1.0	28/09/2017	Finalised version	Marie Austenaa	Helene Vigue / GSMA
1.1	30/10/18	Revised version	David Pollington	Niklas Bergvall / GSMA
1.1	06/12/2022	Go through TG approval	TG	Yolanda Sanz/GSMA

C.1 Other Information

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

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

Your comments or suggestions & questions are always welcome.