Mobile Connect Identity Services Technical Requirements

Version 1.1

12 May 2017

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

The GSMA Personal Data Programme is focused on positioning operators as trusted providers of identity and attribute services to third party service providers. Within this, the programme identifies a set of authentication, authorisation and identity services products that collectively are referred to as Mobile Connect.

This document specifies the technical requirements for Mobile Connect Identity, a new product category within the Mobile Connect service portfolio for Release 2.

The Mobile Connect Identity product category encompasses three products: Mobile Connect Phone Number, Mobile Connect Sign-up, and Mobile Connect National ID, all of which provide information about the user to a service provider based on one-time user consent.

- **Mobile Connect Phone Number**: provision of the MSISDN associated with the user's Mobile Connect account
- **Mobile Connect Sign-up**: provision of name, address and phone number for simple sign-up/account registration use cases
- **Mobile Connect National ID**: assertion of a nationally recognised identity (where identity proofing has been conducted sufficiently to meet local requirements).

For the full attribute set that should be supported within each product, please refer to PDATA.27 Mobile Connect Product Definition [9].

1.2 Scope

In Scope	Out of Scope
• Mobile Connect Phone-number technical requirements • Mobile Connect National ID technical requirements • Mobile Connect Sign-up technical requirements	• Mobile Connect user information verification requirements • Support for consent capture by Trusted service providers (SP) • Support for 3rd party data sources (Aggregated or distributed claims)

1.3 Audience

The target audience of this document is operator's service/technical departments who are considering deploying Mobile Connect Identity service (MCIS) products.

Readers of this document are expected to be familiar with and have a good understanding of the documents PDATA.13 Mobile Connect Core Technical Requirements [2] and PDATA.17 Mobile Connect Technical Architecture [6].

1.4 Definitions

Term	Description
Mobile Connect Authentication	Provides single factor and two-factor authentication using the mobile phone as the authentication device.
Mobile Connect Authorisation	Captures authorisation from a user for a third party to perform an action on their behalf. The Mobile Connect Authorisation product category provides two products: simple and two-factor authorisation. The user is authenticated as part of the flow to ensure that they have the right to provide the authorisation.
Mobile Connect Authorisation device	A mobile device (identified by an SIM card associated with the Mobile Connect user) used to approve/reject Mobile Connect authorisation requests.
Mobile Connect Authentication device	A mobile device (identified by an SIM card associated with the Mobile Connect user) used to approve/reject Mobile Connect authentication challenge.
Mobile Connect Consent device	The device through which the user reviews the attributes being requested by the SP and provides their permission for their operator to share the information with the SP.
Consent management	The system and process enable a user to control what information or access they are willing to share with the Service Provider.

1.5 Abbreviations

Term	Description
API	Application Program Interface
CPAS	Core Products And Solutions
HTTP	Hyper Text Transport Protocol
ID GW	Identity Gateway
LoA	Level of Assurance
MCIS	Mobile Connect Identity services
MSISDN	Mobile Station Integrated Services Digital Network
OIDC	OpenID Connect
PCR	Pseudonymous Customer Reference
RFC	Request for Comments
RQ	Requirement
SP	Service Provider
TTL	Time To Live
UI	User Interface

1.6 Document References

Ref	Doc Number	Title
[1]	PDATA.01	Mobile Connect Profile V1.2.
[2]	PDATA.13	Mobile Connect Core Technical Requirements V1.0

Ref	Doc Number	Title
[3]	PDATA.02	Mobile Connect Authorisation Technical Requirements V1.0
[4]	PDATA.08	Mobile Connect Identity services Technical Requirements V1.0
[5]	PDATA.41	Mobile Connect Technical Reference V1.0
[6]	PDATA.17	Mobile Connect Technical Architecture V2.0
[7]	PDATA.28	Mobile Connect Lifecycle Events V1.2
[8]	PDATA.40	Mobile Connect Lifecycle Technical Solutions V1.0
[9]	PDATA.27	Mobile Connect Product definition V2.2
[10]	PDATA.18	1AP.06 API Exchange System Architecture V1.0
[11]	PDATA.19	1AP.03 API Exchange Business Process Guide V1.0
[12]	PDATA.24	EH.V3 Discovery API Specification
[13]	PDATA.03	Mobile Connect Authenticator options CPAS4 V1.2
[14]	PDATA.04	Mobile Connect SIM applet authenticator CPAS8 V0.1
[15]	PDATA.09	Mobile Connect Smartphone Application Authenticator V1.0
[16]	PDATA.43	Mobile Connect Release 2 Technical Overview (MNOs) V0.2
[17]		Mobile Connect Brand Communication Guidelines_v2_06_15
[18]		Mobile Connect User Flow Design kit V1.2

1.6.1 International Standards References

Ref	Doc Number	Title
[30]	OpenID Connect	"An interoperable authentication protocol based on the OAuth 2.0 family of specifications" available at http://openid.net/specs/openid-connect-core-1_0.html https://openid.net/specs/openid-connect-basic-1_0.html
[31]	RFC 2119	"Keywords for use in RFCs to Indicate Requirement Levels," S. Bradner, March 1997. Available at http://www.ietf.org/rfc2119.txt
[32]	RFC 2616	"Hypertext Transfer Protocol (HTTP) an application level protocol," J Gettys, J. Mogul, L. Masinter, P. Leach, T. Berners-Leem June 1999. Available at http://www.ietf.org/rfc/rfc2616.txt
[33]	RFC 6749	"The OAuth 2.0 Authorization Framework," D. Hard5, Ed. October 2012 available at http://www.ietf.org/rfc/rfc6749.txt
[34]	RFC 4112	A Universally Unique Identifier (UUID) URN Namespace. https://www.ietf.org/rfc/rfc4122.txt
[35]	RFC 2246	Dierks, T. and C. Allen, "The TLS Protocol Version 1.0," RFC 2246, January 1999
[36]	RFC 3339	Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps," RFC 3339, July 2002
[37]	RFC 3986	Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," STD 66, RFC 3986, January 2005
[38]	RFC 4627	Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)," RFC 4627, July 2006
[39]	RFC 5246	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008
[40]	RFC 5322	Resnick, P., Ed., "Internet Message Format," RFC 5322, October 2008

[41]	RFC 5646	Phillips, A. and M. Davis, "Tags for Identifying Languages," BCP 47, RFC 5646, September 2009
[42]	RFC 6750	Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," RFC 6750, October 2012
[43]	RFC 6819	Lodderstedt, T., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations," RFC 6819, January 2013 (TXT).
[44]	RFC 7519	M. Jones, J Bradley, N. Sakimura "JSON Web Token (JWT)", RFC 7519, May 2015
[45]	ISO 29115	International Organization for Standardization, "ISO/IEC 29115:2013 -- Information technology - Security techniques - Entity authentication assurance framework," ISO/IEC 29115, March 2013
[46]	ISO 3166-01	International Organization for Standardization, "ISO 3166-1:1997. Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes," 1997
[47]	ISO 639-1	International Organization for Standardization, "ISO 639-1:2002. Codes for the representation of names of languages -- Part 1: Alpha-2 code," 2002
[48]	ISO 8601-2004	International Organization for Standardization, "ISO 8601:2004. Data elements and interchange formats - Information interchange - Representation of dates and times," 2004

1.7 Technical Documentation Map

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

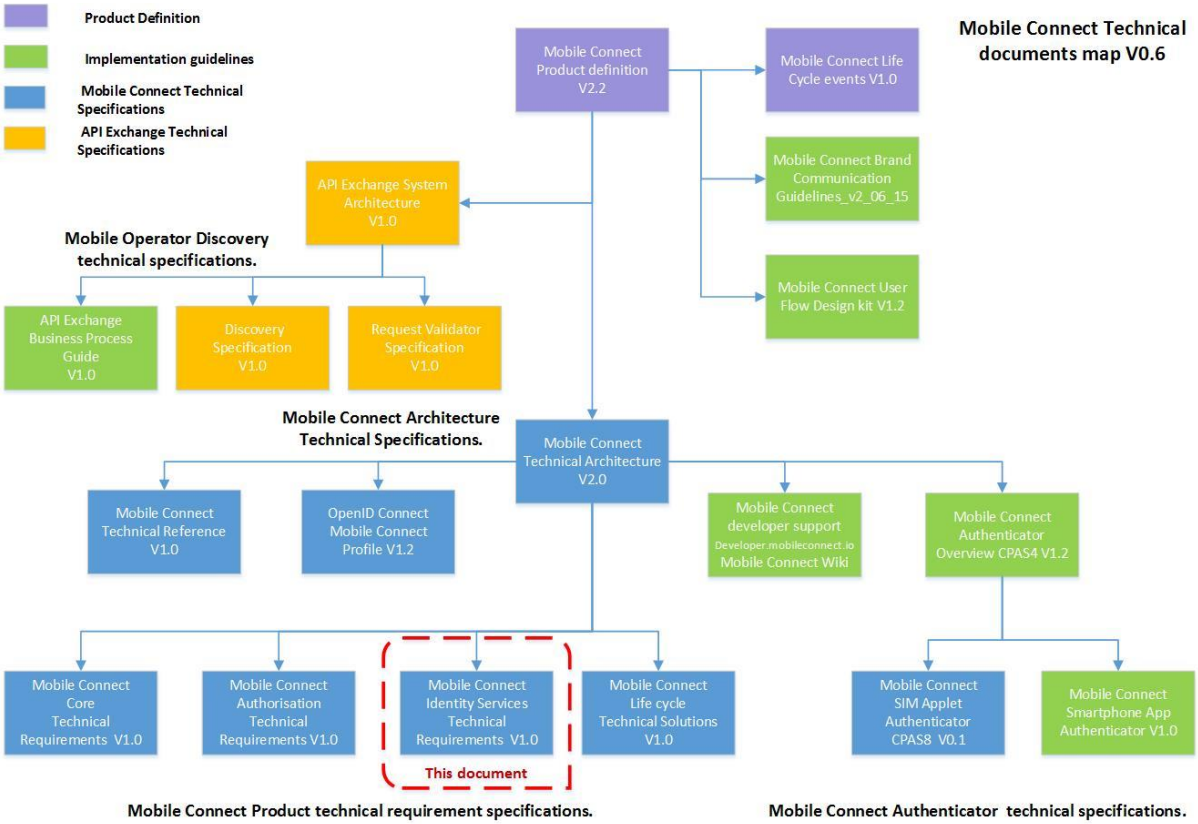

Figure 1: Mobile Connect technical documentation map

1.8 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 [31].

The values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

2 Mobile Connect Actors

The following diagram illustrates the interactions between different Mobile Connect actors for the Mobile Connect Identity services products and consent capture mechanism.

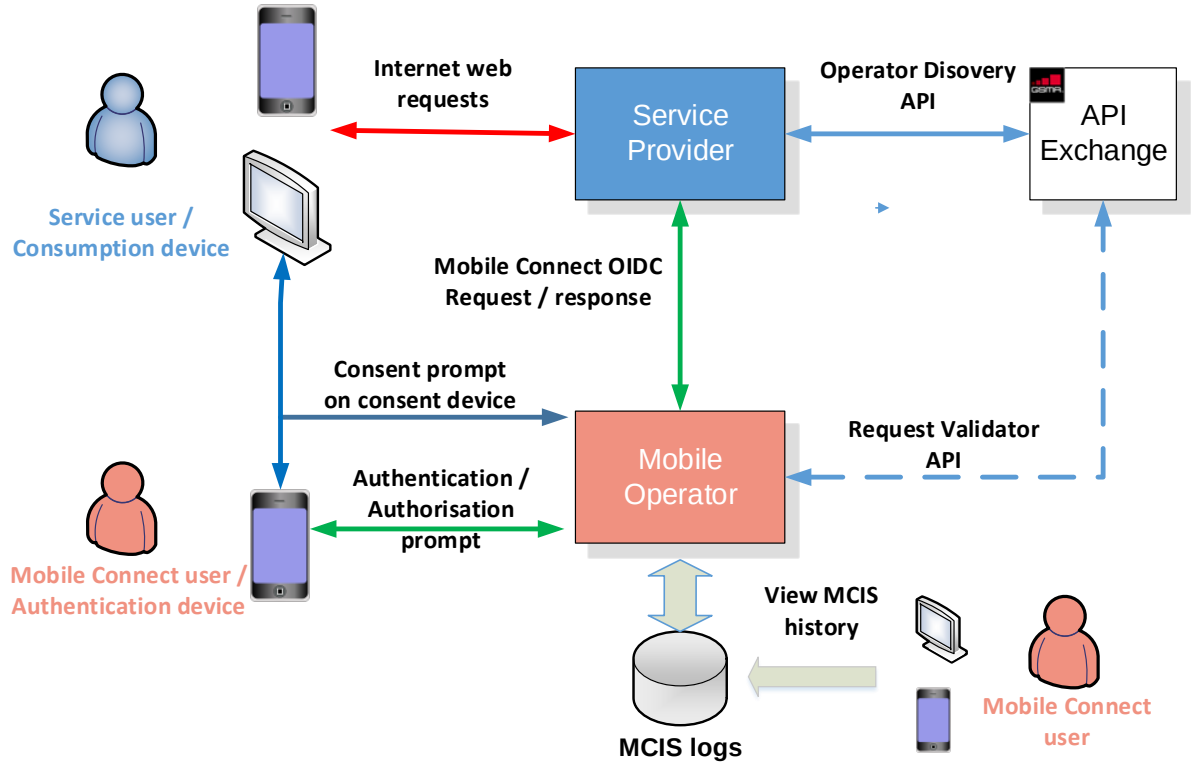

Figure 1: Mobile Connect actors

2.1.1 Service Provider

A service provider integrates with Mobile Connect and uses the Mobile Connect Identity Services products as part of their service to the end-user (the Service User).

2.1.2 Service User

The service user consumes services from the Service Provider. As part of the user flow for giving consent for a specific Mobile Connect Identity Services product, the Service User may need to identify themselves to the Discovery Service so that the SP knows which operator to submit the OIDC (OpenID Connect) request to.

Note that typically the Service User is the individual that needs to provide consent for their information to be shared (aka Mobile Connect user – see 2.1.5). However, in the case of

delegated consent (e.g., a parent consenting on behalf of their child) the SP must acquire consent from a 3rd party. In these situations, it is important that the MSISDN (Mobile Station Integrated Services Digital Network) Discovery flow isn't used hence the SP must provide an identifier for the individual who needs to provide consent - a Normal SP must use the PCR (Pseudonymous Customer Reference) whilst a Trusted SP can use either plain MSISDN or PCR; in both cases, these identifiers would have been acquired during the registration process when the SP set up 3rd party consent for their service.

2.1.3 Discovery

Discovery is used to identify the operator for a specific Mobile Connect user and the relevant API (Application Program Interface) endpoints supporting the Mobile Connect Identity services. For security/privacy reasons Discovery does not disclose any Mobile Connect user personal information to the SP. See [12] for Mobile Connect Discovery API information.

2.1.4 Operator Identity Gateway (ID GW)

The operator's Identity Gateway is the provider of Mobile Connect Identity Services. It implements Mobile Connect OpenID Connect flows and interacts with the Mobile Connect user.

The main characteristics of the ID GW are:

1. A main logical component called by the SP to consume the Mobile Connect service.
2. Provides an abstraction layer between the SP and the Mobile Connect system components.
3. Implements OpenID Connect Mobile Connect Profile endpoints for the SP to call. The Discovery service returns the ID GW endpoints to the SP.
4. Optionally, invokes Validation API of API Exchange to validate the credentials passed by the SP in OIDC request.

2.1.5 Mobile Connect User

The Mobile Connect user interacts with the operator to authenticate via the mobile device and provides their consent for the identity information being requested by the SP. Note that the Mobile Connect user is typically the Service User but by separating the two roles allows for delegated consent use cases in which case a 3rd party (the Mobile Connect user) may provide consent for identity information to be shared on behalf of the Service User (e.g., a parent giving consent on behalf of a child).

2.1.6 Authentication Device

The device authenticating a Mobile Connect user is always a mobile device that is addressed via the MSISDN of the user. It receives authentication requests from the operator and is used by the Mobile Connect user to approve or reject authentication requests.

2.1.7 Consumption Device

The device used to consume a SP's services, by the Service User. Consumption of SP services can be through different channels including directly via mobile and desktop/tablet browsers and mobile applications, and indirectly via voice systems, interaction with Customer Care agents, etc.

Any of these channels can integrate with Mobile Connect and use the Mobile Connect Identity Services products for requesting information about a user.

2.1.8 Consent Device

The device used to capture consent from a Mobile Connect user to share their Mobile Connect personal information with the Service Provider. The consent device can be any of the following:

- Consumption device (desktop/tablet) with user agent (i.e. web browser etc.)
- Consumption device (mobile device) with user agent (i.e. mobile browser etc.); note that a WebView within an SP app running on the device would not be suitable
- Mobile device (Mobile Connect authenticator mechanism)

For more information on consent device options please see section 4.2.4.

3 Identity Services Product Design Principles

The Identity Services products offer a mechanism through which a Service Provider can request the operator to share identity attributes for a target user. Based on the requested product (identified by the scope value in the SP request), the ID GW presents the consent capture question to the end user either via the authentication device or the consumption device.

3.1 Design Principles and Prerequisites

Mobile Connect Identity services products use the same infrastructure as the Mobile Connect Authentication products and reuse Mobile Connect Authentication logical components wherever applicable.

A few important differences:

- An explicit response is required from the user hence any form of seamless consent capture cannot be used.
- The operator will need to utilise the Mobile Connect consent capture mechanism to generate a consent prompt to be displayed to the user, as specified in this document.
- A complete identity services consent log must be maintained, archived and accessible to both SPs and end-users to resolve any disputes.

The following pre-requisites are assumed for the operation of the service:

- The Mobile Connect user is already registered to Mobile Connect with their operator.
- If the Mobile Connect user does not have a Mobile Connect account, before serving any Mobile Connect Identity Service requests, the operator must offer on-the-fly registration and must register the user for Mobile Connect.
- For all server-based invocation requests, the Mobile Connect user must be registered to Mobile Connect with their operator. In this scenario, no on-the-fly registration is supported.
- Attribute values must be provided by the operator from its data sources through the ID GW. For full details on the mandatory and optional attributes for each Identity Service product, please refer to the Mobile Connect Product Definition [9].
- The Mobile Connect user must have access to the mobile device to authenticate.

- The Mobile Connect user must have access to the consent device (consumption device or mobile device) to respond to consent requests from the ID GW.

3.2 Identity Services product requirements

The following high-level requirements have been derived from the Mobile Connect Product Definition [9]:

Requirement	Description
MC_RQ01.4.1 Consent capture	The operator must authenticate and capture consent from the Mobile Connect user for the attributes that have been requested
MC_RQ01.4.2 Authentication device	The Mobile Connect Identity services must authenticate the user only on the Authentication device (i.e. mobile device).
MC_RQ01.4.3 Consent device	The Mobile Connect Identity services must support the following devices for capturing consent: • Authentication device (i.e. mobile device) • Consumption device (i.e. desktop /tablet or mobile device).
MC_RQ01.4.4 Consent prompt	The Mobile Connect Identity services product must construct a consent prompt providing as much detail as possible to the user on the attributes being requested.
MC_RQ01.4.5 Consent screens	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 regulation requires otherwise.
MC_RQ01.4.6 Supported authenticators	Given that explicit consent is required, seamless authenticators must not be used for consent capture. Note that a seamless authentication mechanism may still be used for identifying the user to the operator.
MC_RQ01.4.7 Identity Services requests	The Mobile Connect Identity services should support server-initiated as well as client-initiated OIDC requests
MC_RQ01.4.8 Attributes data quality	The Mobile Connect Identity services should return attributes on a best effort basis regarding data quality (i.e., based on whatever information the operator already has for a given user based on the prevailing KYC processes).

Table 1: Mobile Connect Identity services product requirements

3.3 High Level Overview

A high level overview of how Mobile Connect Identity services work end-end is as follows:

1. SPs register for, and request attributes based on a set of pre-defined groups as defined for each of the Identity Service products

    a) Doing so enables operators to control individual SP privileges on a per service level
    b) Operators can extend the services with additional attributes and/or use the underlying framework to offer other attribute services to SPs at their discretion

2. SPs submit service requests to the operator[1] using the Mobile Connect API[2]

    a) It is assumed in the default scenario that the user is already registered to Mobile Connect with their operator.

3. All services will provide customer information (attribute values) to the SPs[3]

    a) The SP may request a subset of the customer information supported within a given service[4]
    b) The operator may choose to provide only a subset of the customer information[5]
    c) Data quality is best effort[6] for the Phone-number, Sign-up and Sign-up Plus services; for National ID, data quality should be in accordance with local legislation
    d) Note that the operator will share whatever information they have on file for the given MSISDN hence this might reflect either the primary account holder or the user of the phone (sub-account); if this information is incorrect for any reason, the user can either update at the SP (e.g., in a form-fill scenario) or using the operator's existing CRM self-care portal (for the Sign-up product); any updates to National ID information will require additional KYC checks to be conducted to ensure the authenticity of this new information.
    e) Note that the technical solution will not support a user updating the Sign-up information at point of presentation and consent before it is shared with the SP[7]

4. Customer information is only provided following explicit consent from the user

    a) The SP name and attributes that have been requested are presented to the user

        - Note that either the attribute names or names+values can be presented; whilst it is preferable to display attribute names+values so that a) the user is fully aware of the information being shared and b) the user by consenting gives assurance that the data being shared belongs to them and no-one else, in practise, there will be a dependency on the method of capturing consent.

[1] Either directly or via an Aggregator/Channel Partner; only direct interaction with the operator is fully defined within this document although options for utilising an Aggregator/Channel Partner should also be considered

[2] OIDC Mobile Connect Profile v1.2

[3] Verification of information provided by the SP to the operator is out of scope and will be handled by a separate service (currently entitled KYC Match) in Rel 3

[4] In accordance with the privacy principles, the SP should only request information that is proportionate to the intended purpose so shouldn't automatically include all attributes (claims) for a given scope within their service request; doing so also risks the user declining their request.

[5] e.g., due to unavailability of particular pieces of customer information, or due to local legislation on what can be shared or to reflect individual user preferences where applicable

[6] For the first iteration of the services the operators will provide whatever information they currently have available (e.g., based on what is captured when issuing a PAYM contract); it is for further study whether a minimum quality level could be defined (e.g., in terms of identity proofing when registering a user's identity).

[7] Doing so would place additional constraints on the consent method and require the Mobile Connect infrastructure (i.e., ID GW) to integrate back into the operator's CRM systems to update the information (and hence would introduce additional non-functional requirements around security and data handling etc.)

b) The user must always be authenticated before being asked to provide permission for the requested attributes to be shared

- LoA2 is the default for acquiring consent; LoA3 can be utilised at operator discretion (or if needed by local legislation) and is mandatory for the National ID service

c) The user provides binary consent (yes/no) for all the customer information requested within a given transaction from the SP[8]

5. Consent is captured by the operator

a) Consent is based on one-time use only (i.e., SPs need to seek consent every time they would like to request customer information)

4 Technical Requirements

4.1 Core Technical Requirements References

The Mobile Connect Identity Service products are built on and extend the core Mobile Connect system capability. As such, implementations of the Mobile Connect Identity Service products must abide by the Mobile Connect Core Technical Requirements [2]. The following table highlights key areas that must be complied with:

Requirement	Description
MC_RQ03.2.1 PCR	The ID GW must issue PCRs as defined in the Mobile Connect Core Technical Requirements spec [2]
MC_RQ03.2.2 Trusted/Normal Service provider	The ID GW must support Trusted[9] as well as normal (untrusted) Service Providers as defined in the Mobile Connect Core Technical Requirements spec [2].
MC_RQ03.2.3 Server-based invocation	The ID GW must implement support for server-based invocation[10] as defined in the Mobile Connect Core Technical Requirements spec [2].

Table 2: Core technical requirements references

4.2 ID Gateway Requirements

This section details the new requirements which need to be implemented by the ID GW to support the Mobile Connect Identity Service products.

[8] The user is not asked to pick and choose which particular aspects of the customer information they are happy to share; taking such an approach minimises complexity for the user

[9] Provides an SP with the ability to stipulate the user they would like to authorise a transaction (via the MSISDN)

[10] i.e., support for Mobile Connect service requests to be initiated directly by the SP server rather than from the User Agent (e.g., browser)

4.2.1 Service Registration

Requirement	Description
MC_RQ04.2.1 Identity services variants	The ID GW should enable the Service Provider (application/service) to register for any of the three variants of Identity Services i.e. Mobile Connect Phone-number, Mobile Connect Sign-up and Mobile Connect National ID based on what the operator supports/offers.
MC_RQ04.2.2 Mandatory attribute support	The ID GW should only offer those products for which it has access to all the mandatory attribute values defined for that particular product (as defined in the Mobile Connect Product Definition [9]).
MC_RQ04.2.3 Single set of credentials	The Mobile Connect deployment must provide a single set of credentials (client id/secret) to a Service Provider (application) for accessing all Mobile Connect Identity services, either through the API Exchange or directly; for further information see the Mobile Connect Core Technical Requirements [2].

Table 3: Service registration

4.2.2 Service Invocation

The Mobile Connect Identity Service products are requested by SPs via OpenID Connect API requests in alignment with the Mobile Connect Profile v1.2 [1]. These requests must identify the specific Mobile Connect Identity Service product that is being requested through the <scope> parameter:

Mobile Connect Identity Service	Scope
Mobile Connect Phone Number	“openid mc_identity_phonenumber”
Mobile Connect Sign-up	“openid mc_identity_signup”
Mobile Connect National ID	“openid mc_identity_nationalid”

Table 4: Mobile Connect Identity service scopes

Requirement	Description
MC_RQ04.2.4 MCIS requests	The SP should submit Identity Service OIDC requests using the Mobile Connect API, and the ID GW must process these requests if they comply with the Mobile Connect profile 1.2. [1]
MC_RQ04.2.5 MCIS product type	The SP must be able to specify the required type of Mobile Connect Identity Service through the use of the scope value (as defined in).
MC_RQ04.2.6 MCIS login hint type	The ID GW must be able to serve Identity Service OIDC requests through supplied encrypted MSISDN or PCR provided via the `login_hint` parameter (for normal SPs). Note: Encryption of MSISDN is done by API Exchange only.
MC_RQ04.2.7 Trusted Service Provider semantics	The ID GW must be able to serve identity services OIDC requests through plain MSISDN/encrypted MSISDN and PCR provided via the `login_hint` parameter (for Trusted SPs). Note: Encryption of MSISDN is done by API Exchange only.
MC_RQ04.2.8 Header Enrichment	The operator can also identify the user through header enrichment (if on-net).

Requirement	Description
MC_RQ04.2.9 Subset attributes claims	The Service Provider may request a subset of the attributes supported by a given identity service through the claims request parameter. If claims parameters are included in the OIDC request, the ID GW must process these claims parameters from the request object and only return the claims about those attribute values to the Service Provider.
MC_RQ04.2.10 SP application short name	The Service Provider must be able to specify the SP application short name to display along with the attribute list by the ID GW in the consent prompt. The SP can only provide a pre-registered application short name, using the `client_name` parameter in the OIDC request. The ID GW must check whether the incoming `client_name` OIDC request parameter matches one of the pre-registered application short names[11] for that SP, by comparing with its registry database. If it doesn't match, the ID GW must return an `invalid_request` error as per the Mobile Connect Technical Reference [5].
MC_RQ04.2.11 Combo Identity Services	The ID GW must be flexible to support OIDC requests that combine a Mobile Connect Identity Service with Mobile Connect Authenticate or Mobile Connect Authorise to cater for various scenarios.
MC_RQ04.2.12 MCIS requests using Plain MSISDN through `login_hint`	Only Trusted Service Providers must be able to invoke Mobile Connect Identity Service requests using plain MSISDN in the OIDC request through a `login_hint` parameter. The ID GW must verify and SP's "trust" status and only allow Trusted Service Providers to send plain text MSISDN in the OIDC request. The ID GW must reject OIDC requests with plain text MSISDN from normal Service Providers and return an `invalid_request` error as per the Mobile Connect Technical Reference [5].
MC_RQ04.2.13 MCIS requests using Encrypted MSISDN through `login_hint`	Any Service Providers (i.e. Normal or Trusted) must be able to invoke Mobile Connect Identity Service requests using encrypted MSISDN in the OIDC request through a `login_hint` parameter[12]. For any processing error, the ID GW must return an `invalid_request` error as per the Mobile Connect Technical Reference [5]. Note that encryption of the MSISDN is done by the API Exchange. The encryption is performed using the public key of the identified operator's ID GW. The Service Provider must not perform any encryption[13] of the MSISDN itself. The TTL (Time To Live) of encrypted MSISDN is infinite.[14]

[11] In rel2, only one application short name per service provider is allowed. In the future releases, multiple application short names are allowed and SP can choose one of the pre-registered application short names, according to its application needs.

[12] In R2, encrypted MSISDN is supported through `login_hint` parameter. This will be deprecated from R3 onwards. Going forward, recommended parameter for encrypted MSISDN is `login_hint_token`.

[13] In Mobile Connect, encryption is done by the API exchange not by the Service Provider. API exchange maintains public keys of all registered operator's ID GW.

[14] In future the TTL of encrypted MSISDNs may be limited (REL3 – TBD).

Requirement	Description
MC_RQ04.2.14 MCIS requests using Encrypted MSISDN through `login_hint_token`	Any Service Providers (i.e. Normal or Trusted) must be able to invoke Mobile Connect Identity Service requests using encrypted MSISDN in the OIDC request through a `login_hint_token` parameter. For any processing error, the ID GW must return an `invalid_request` error as per the Mobile Connect Technical Reference [5]. Note that encryption of the MSISDN is done by the API Exchange. The encryption is performed using the public key of the identified operator's ID GW. The Service Provider must not perform encryption of the MSISDN. TTL of encrypted MSISDN is infinite.
MC_RQ04.2.15 MCIS request using PCR through `login_hint`	Any Service Provider (i.e. normal or Trusted) must be able to invoke Mobile Connect Identity Service requests using PCR through the `login_hint` parameter. The ID GW must keep track of all PCRs generated for a Mobile Connect user per Service Provider. If any submitted PCR is not valid or not available, the ID GW must return an `invalid_request` error.

Table 5: Service Invocation

4.2.3 Request Processing

Requirement	Description
MC_RQ04.2.16 SP subscription to identity services	The ID GW must check that the SP is subscribed to the requested Identity Service
MC_RQ04.2.17 Pre-registered MC user	The ID GW must check that the Mobile Connect user is already registered with their operator and has a Mobile Connect account[15]. If the user is not registered, ID GW must offer on-the-fly registration before serving any MCIS requests.
MC_RQ04.2.18 Mobile Connect accounts status	The ID GW must maintain various Mobile Connect account states as mentioned in [8].
MC_RQ04.2.19 Account active state	The ID GW must only serve Identity Service OIDC requests if the corresponding Mobile Connect account is in an "active" state [8].
MC_RQ04.2.20 Error handling if account not active	The ID GW must reject identity service OIDC requests for all other Mobile Connect account states (ex. suspended, deleted, and not available[16]) with appropriate errors as defined in the Mobile Connect Technical Reference [5].
MC_RQ04.2.21 Mobile Connect user authentication	The ID GW 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 being asked for consent.
MC_RQ04.2.22 Valid authentication session	If an authentication session is still valid (i.e., identity token not yet expired) then the ID GW need not authenticate the user but can simply request user consent.
MC_RQ04.2.23 ID GW policies – LoA	The ID GW should select the authentication method based on the LoA pre-configured for the product being requested.

[15] In Release 2 for Mobile Connect Identity Services, it is mandatory that Mobile Connect User must be registered with their operator.

[16] Not available means the account does not exist, hence authentication for identity services must fail. On fly registration, when an account does not exist is out of scope of this document and REL2.

Requirement	Description
	The ID GW must ignore the `acr_values` parameter in the OIDC authorisation request and select the authentication method based on own policies.
MC_RQ04.2.24 Sign-up/Phone Number – LoA	Mobile Connect Sign-up and Phone-number should use single factor authentication. Two-factor authentication (LoA3) may also be used (operator's discretion or if needed by local legislation).
MC_RQ04.2.25 National ID – LoA	Mobile Connect National ID requires two-factor authentication (e.g., entering a PIN); the ID GW must reject the request if this is not possible.
MC_RQ04.2.26 Minors	The ID GW must reject OIDC requests if it is known that the corresponding Mobile Connect user is a minor[17] (based on local legislation)
MC_RQ04.2.27 Multiple identity services	The ID GW must be able to process multiple identity services scopes in one OIDC request. For example: Scope value = "openid mc_identity_phonenumber mc_identity_signup mc_identity_nationalid" Scope value = "openid mc_identity_phonenumber mc_identity_signup" etc.

Table 6: Request processing

4.2.4 Consent Capture Mechanism

This section provides guidance on the selection of the consent device and consent capture mechanism based on a range of different scenarios as well as the generic requirements for generating and presenting the consent prompt to the Mobile Connect user.

Requirement	Description
MC_RQ04.2.28 Consent device/method selection	The ID GW must implement Identity Services policy management to determine the best method of displaying attributes on the consent device and capturing consent for a given user based on: • the product being requested • the device through which the user is consuming the SP service (and the associated User Agent) • the authenticators available on the authentication device
MC_RQ04.2.29 Scenario 1: consumption device = desktop/tablet	If the authenticator is Smartphone app or NI USSD then the ID GW should either use Consent device = Authentication device (and use the Mobile Connect Authenticator[18]) or Consent device = Consumption device (and use the client user agent). If the authenticator is SIM applet, then the ID GW should use Consent device = Consumption device[19]
MC_RQ04.2.30 Scenario 2: consumption device = mobile device	If the authenticator is Smartphone App or NI USSD then the ID GW should use Consent device = Authentication device (and use the Mobile Connect Authenticator). If the authenticator is SIM applet, then the ID GW should use Consent device = Consumption device (and use the native browser or Web View depending on the client UA as appropriate).

[17] The minor definition depends on the local legislation and regulations, which must be handled by the operator.

[18] NI USSD and Smartphone app authenticators support "paging" so the consent "page" can be included in the Authenticator. NI USSD is a session based protocol and any number of pages can be exchanged and displayed in the active session. Smartphone App is flexible to display additional content.

[19] Assuming that the SIM applet will not have sufficient display real-estate for displaying the attribute labels or values

Requirement	Description
MC_RQ04.2.31 Scenario 3: no consumption device (i.e., server-based invocation)	If the authenticator is Smartphone App or NI USSD, then the ID GW should use the Consent device = Authentication device (and use the Mobile Connect Authenticator). If the authenticator = SIM applet, then the prompt must be displayed by grouping attributes in a single line [within the limit of 93 bytes].
MC_RQ04.2.32 Prompt format	The ID GW must present the attributes list in one of the following formats (in order of preference): • Attribute names + values (e.g., firstname = Marie) • Attribute names only (e.g., firstname, lastname, 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 consent device (i.e., the maximum prompt length based on the target display mechanism; e.g. an SIM applet has a restricted number of characters that can be displayed).
MC_RQ04.2.33 application short name	The ID GW must present the SP application short name in the consent prompt. Note that the maximum length of the application short name is 16 bytes Note that the SP application short name will only consist of alphanumeric characters. No symbols are allowed. The ID GW must ensure that the SP application short name supplied via the `client_name` parameter matches one of the pre-registered SP application short names. If not, the ID GW must return an `invalid request` error.
MC_RQ04.2.34 attribute ownership	If display space permits on the Consent device, the consent prompt should get assurance from the user that the data being shared belongs to them and no one else.
MC_RQ04.2.35 Encoding schemes	gsm7, ucs2, and utf-8 encoding schemes must be supported for generation of the consent prompt
MC_RQ04.2.36 Binary consent	The ID GW must prompt the Mobile Connect user asking whether they give their consent for all the attributes (scopes) requested by the SP (yes/no).
MC_RQ04.2.37 Server-based invocation consent	For server-based invocations, the ID GW should capture authentication and consent using the Mobile Connect authenticator (authentication device) as in such scenarios there is no consumption device.
MC_RQ04.2.38 Authenticator USSD support	If the USSD authenticator is used to capture consent, the ID GW must capture the authentication and consent in a single interaction. The ID GW must not use a 2-stage approach that would result in an additional round-trip interaction.
MC_RQ04.2.39 Authenticator SIM applet support	If the SIM applet authenticator is used to capture consent, the ID GW must restrict the consent message to 93 bytes and group attributes or display only attribute names
MC_RQ04.2.40 Smart phone app authenticator support	If the Smartphone app authenticator is used to capture authentication and consent, the ID GW can choose the consent prompt format based on its policies and the size of the attribute set that needs to be presented to the user for a particular Mobile Connect Identity Service product.

Table 7: Consent capture requirements

4.2.5 Response to Service Provider

Requirement	Description
MC_RQ04.2.41 Returning authorization code	The ID GW must only issue an Authorization Code if the Mobile Connect user successfully authenticates and provides their consent for the requested attributes to be shared

Requirement	Description
MC_RQ04.2.42 Premium Info endpoint	The ID GW must expose all Identity Services through a single PremiumInfo endpoint. It is expected that the operator will source the MSISDN for the Mobile Connect Phone Number product from their ID GW database; the attributes for the other two Identity Services could be provided by the operator's CRM systems. Data quality is on a best-effort basis
MC_RQ04.2.43 Backward compatibility – user info	Mobile Connect deployments should support OIDC UserInfo endpoints for backwards compatibility.
MC_RQ04.2.44 Access token validity	The ID GW must only issue Access Tokens to retrieve attribute values with TTL = zero, (i.e., only one-time use) using the `expires_in` response parameter.
MC_RQ04.2.45 Returning empty values for unavailable attributes	If any mandatory attributes are not available for a particular request (user), the ID GW must return those parameters with empty values.
MC_RQ04.2.46 Logging unavailability	If the ID GW is unable to return all requested mandatory attribute values for a particular Mobile Connect user, this fact should be included in the ID GW logs (e.g., may be needed for billing purposes)
MC_RQ04.2.47 Optional attributes	For attributes marked as [optional] within the Product Definition (see [9]) value may be provided by the ID GW if supported.
MC_RQ04.2.48 Excluding optional attributes	If any optional attributes in the scope are not available, the attribute should be removed from the response, instead of providing empty values.
MC_RQ04.2.49 Customized attribute list through claims	If one or more claims parameters are included in the SP OIDC request, the ID GW must restrict the Access Token to only those attributes requested by the SP (rather than providing all the attributes encompassed by the product scope)
MC_RQ04.2.50 Attribute values supplied via Access Token only	The ID GW must not return any claims through the ID Token[20].
MC_RQ04.2.51 LoA & authenticator type indication	The ID GW should return an indication of the LoA used for authenticating the user through the `acr` parameter. It should also indicate the type of authenticator used via the `amr` parameter.
MC_RQ04.2.52 Refresh token	The ID GW must not issue a refresh token for Identity Services (consent is only granted on a one-time transactional basis).
MC_RQ04.2.53 HTTP error codes	For timeout, action rejected by an End-user and for any other error, an HTTP error code must be returned (as per OIDC best practise and the Mobile Connect Technical Reference [5]).

[20] Although the OpenID Connect specification specifies that either the Access Token or ID Token can be used to retrieve attribute values, Mobile Connect Identity services uses the Access Token/PremiumInfo only.

Requirement	Description
MC_RQ04.2.54 Consent events	The ID GW must support the following events: • **Consent successful** – Mobile Connect authentication and consent capture are successful. • **Consent failur**e – an error code must be returned, if either authentication fails or authentication is successful, but the user declines to give their consent. • **Timeout** – user does not do anything, ID GW timeouts waiting for the response from the authenticator. This must be considered as "unavailable." • **Any other processing error** – consent failure error must be returned. • Standard request processing errors, in line with Mobile Connect Authentication/ Authorisation must be supported.

Table 8: Response to service provider

4.2.6 Non-Functional Requirements

Requirement	Description
MC_RQ04.2.55 logging	The following data should be logged by the ID GW about consent capture. • Date & Time • PCR • Scope parameter • LoA (Level of Assurance) requested and used • User received request(Yes/No) • User response (Consent approved, rejected, timeout) • Status (Complete, in-process, Error) • Authenticator used • Error codes and error description (as defined in the Mobile Connect Technical Reference [5]).
MC_RQ04.2.56 Pre-defined response times	The ID GW should respond to the SP request with an Authorization Code (or error message) in a timely manner
MC_RQ04.2.57 Recommend roundtrip times	The ID GW should return Attribute values to the SP promptly (e.g., <300ms roundtrip) following SP request for the Access Token

Table 9: Non-functional requirements

4.3 Consent Device Requirements

Requirement	Description
MC_RQ04.2.58 Consent prompt rendering	The Consent device must render prompt details correctly i.e. without breaking a word into multiple lines.
MC_RQ04.2.59 Internationalisation	The consent device must render international language characters correctly wherever applicable.
MC_RQ04.2.60 Encoding schemes	gsm7, ucs2, and utf-8 encoding schemes must be supported for presenting the consent prompt

Table 10: Consent device requirements

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	25/05/2016	New document	PDATA/PSMC	Siva (Venkatasivakumar Boyalakuntla) / GSMA
1.1	12/05/2017	Transfer of PRD from Personal Data	TG	Nick Cheung / 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.