Mobile Connect Authorisation 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 the Mobile Connect Authorisation product category within the Mobile Connect service portfolio.

The Mobile Connect Authorisation product category includes the Mobile Connect Authorise and Mobile Connect Authorise Plus products that provide the ability to approve authorisations (What You See Is What You Approve - WYSIWYA) at two different assurance levels.

- **Mobile Connect Authorise:** Capturing approval on a mobile device through a binary approval (approve/reject) for a specific transaction as defined by the service provider.
- **Mobile Connect Authorise Plus:** Capturing approval on a mobile device through two factors (possession of the mobile device AND entering a secret); the user either enters their secret and presses approve to authorise the transaction request or simply presses reject to decline the transaction request with or without entering the secret.

1.2 Scope

In Scope	Out of Scope
• Mobile Connect Authorise technical requirements • Mobile Connect Authorise Plus technical requirements	• Mobile Connect Authorise UI (user interface) flows (please refer to PDATA.27 [9])

Table 1: Document scope

1.3 Audience

The target audience of this document is operator's service/technical departments who are considering deploying Mobile Connect Authorisation 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 Mobile Connect Authenticate (1FA) and Mobile Connect Authenticate Plus (2FA) using the mobile device as the authentication device.
Mobile Connect Authorisation	Captures authorisation from a user for a third party application / service to perform an action on the user's behalf. The Mobile Connect Authorisation product category provides two variants: Mobile Connect Authorise and Mobile Connect Authorise Plus, which provide authorisation at two different levels of assurance.
Mobile Connect authorisation device	A mobile device (identified by a 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 a SIM card associated with the Mobile Connect user) used to authenticate the user.
Mobile Connect service user	The individual consuming a service from the Service Provider.
Mobile Connect user	The individual being asked to authorise an action being instigated by the service user with a Service Provider.
First party authorisation	A variant of Mobile Connect authorisation where the service user and the Mobile Connect user are the same.
Third party authorisation	A variant of Mobile Connect Authorisation where the service user and the Mobile Connect user are two separate entities.

1.5 Abbreviations

Term	Description
API	Application Program Interface
B2B	Business- to-Business
B2C	Business-to-Consumer
CPAS	Core Products and Solutions
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transport Protocol
I&A	Identity & Attributes
ID GW	Identity Gateway
IO	Input/output
IoT	Internet Of Things
LoA	Level of Assurance
MSISDN	Mobile Station Integrated Services Digital Network
OIDC	OpenID Connect
PCR	Pseudonymous Customer Reference
RFC	Request for Comments
RQ	Requirement

Term	Description
SP	Service Provider
TTL	Time To Live
UCS	Universal Coded Character Set
UI	User Interface
UTF	Unicode Transformation Format
WYSIWYA	What You See Is What You Approve

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
[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
[19]	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
[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]	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
[3]	RFC 6749	"The OAuth 2.0 Authorization Framework," D. Hard5, Ed. October 2012 available at http://www.ietf.org/rfc/rfc6749.txt

[4]	RFC 4112	A Universally Unique Identifier (UUID) URN Namespace. https://www.ietf.org/rfc/rfc4122.txt
[5]	RFC 2246	Dierks, T. and C. Allen, "The TLS Protocol Version 1.0," RFC 2246, January 1999
[6]	RFC 3339	Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps," RFC 3339, July 2002
[7]	RFC 3986	Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," STD 66, RFC 3986, January 2005
[8]	RFC 4627	Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)," RFC 4627, July 2006
[9]	RFC 5246	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008
[10]	RFC 5322	Resnick, P., Ed., "Internet Message Format," RFC 5322, October 2008
[11]	RFC 5646	Phillips, A. and M. Davis, "Tags for Identifying Languages," BCP 47, RFC 5646, September 2009
[12]	RFC 6750	Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," RFC 6750, October 2012
[13]	RFC 6819	Lodderstedt, T., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations," RFC 6819, January 2013 (TXT).
[14]	RFC 7519	M. Jones, J Bradley, N. Sakimura "JSON Web Token (JWT)", RFC 7519, May 2015
[15]	ISO 29115	International Organization for Standardization, "ISO/IEC 29115:2013 -- Information technology - Security techniques - Entity authentication assurance framework," ISO/IEC 29115, March 2013
[16]	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
[17]	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
[18]	ISO 8601-2004	International Organization for Standardization, "ISO 8601:2004. Data elements and interchange formats - Information interchange - Representation of dates and times," 2004

Table 2 : International standard references

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:

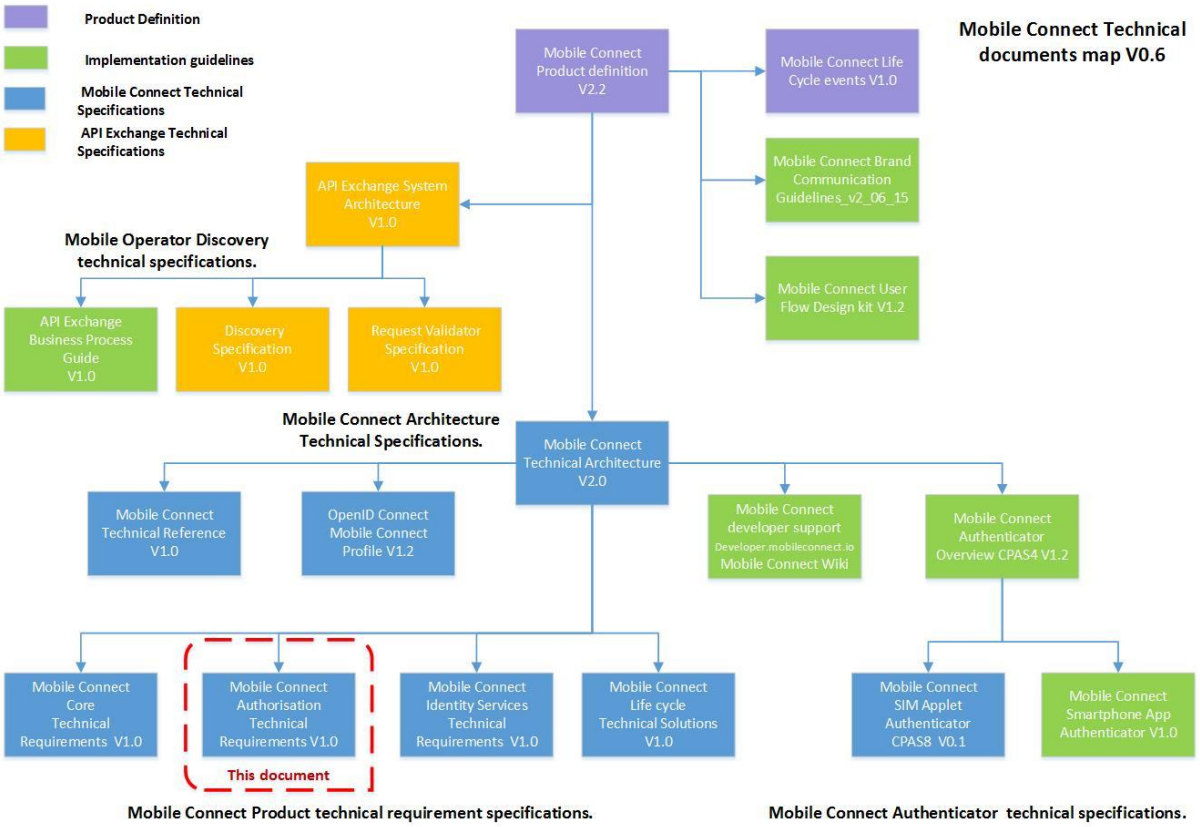

Figure 1: Mobile Connect technical documentation map

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 [1] .

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

Mobile Connect is a global mobile industry solution that provides simple, secure and convenient tools for end users to access online services and to authorise digital transactions by using the end user's unique mobile number to verify and authenticate their identity.

The end users access Mobile Connect via service providers who have integrated one or more of the Mobile Connect portfolio of products. The service providers request these products by using different parameters in an OpenID Connect (OIDC) request. The following diagram illustrates the interactions between different Mobile Connect actors for the Mobile Connect Authorisation products.

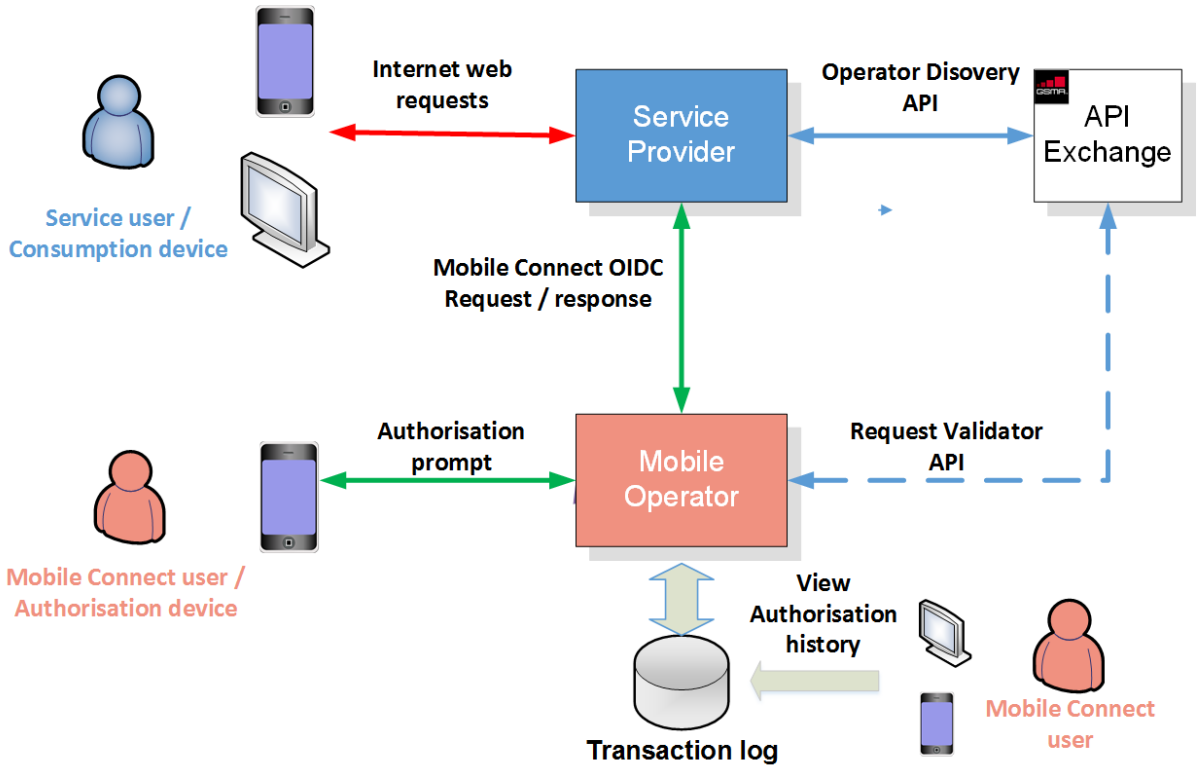

Figure 2: Mobile Connect actors

2.1 Service Provider

A service provider has integrated Mobile Connect and uses the Mobile Connect Authorisation products as part of their service to end users. Their service users use the Mobile Connect products as part of the SP (Service Provider) user flow to authorise an action/transaction.

2.2 Service User

The service user consumes services from the service provider. As part of the user flow for authorising transactions, the service user may need to identify themselves to the Discovery Service so that the SP knows which operator to submit their Authorisation request to.

Note that typically the service user is the individual that needs to provide approval for a specific transaction/action (aka Mobile Connect user – see 2.5). However, in the case of delegated consent (e.g., a parent consenting on behalf of their child), the SP must acquire consent from a third party. Either in the first party or third party authorisation, it is important that the Discovery flow is not 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 a plain MSISDN (Mobile Station Integrated Services Digital Network) or PCR. In both cases, these identifiers would have been acquired during the registration process when the SP set up the approval person for their service.

2.3 Discovery

Discovery is used to identify the operator for a specific Mobile Connect user and the relevant API) Application Program Interface) endpoints supporting the authorisation services. For

security/privacy reasons, Discovery does not disclose any Mobile Connect user personal information to the SP. See [12] for further information on the Mobile Connect Discovery API.

2.4 Operator Identity Gateway (ID GW)

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

The main characteristics of the ID GW are:

1. 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.

2.5 Mobile Connect User

The Mobile Connect user interacts with the operator using the Authorisation/Authentication device (i.e. the mobile device) to authorise transactions/actions requested by the SP. Note that the Mobile Connect user is typically the service user but separating the two roles allows for third party authorisation use cases.

2.6 Authorisation Device

The device authorising an SP-requested transaction is always a mobile device that is addressed via the MSISDN of the user. It receives authorisation requests from the operator and is used by the Mobile Connect user to approve or reject authorisation requests.

2.7 Consumption Device

The device used to consume an 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 Authorisation products for seeking user authorisation for specific transactions/actions.

3 Authorisation Product Design Principles

The Authorisation products offer a mechanism through which a service provider can request an end user to approve or reject a transaction. The Mobile Connect authenticator presents this question to the end user for approval.

Two levels of Assurance are available to the service provider:

- LoA2 = Mobile Connect Authorise
- LoA3 = Mobile Connect Authorise Plus

3.1 Design Principles and Prerequisites

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

A few important differences:

- As an explicit response is required from the user, any form of seamless authentication cannot be used.
- The action which requires authorisation must be constructed by the ID GW from the application short name and the context received in the SP request.
- A complete transaction log must be maintained, archived and accessible to both SPs and end users in order to resolve any disputes.

The following are prerequisites for the service:

- The Mobile Connect user is already registered to Mobile Connect with their operator or capable of creating a Mobile Connect account through on-the-fly registration with the operator.
- The Mobile Connect user must have access to the authorisation device (mobile device) to respond to Mobile Connect Authorisation requests from the Service Provider.

3.2 Authorisation product requirements

The following Authorisation product requirements have been derived based on PDATA.27 [9]:

Requirement	Description
MC_RQ01.3.1 Authorisation request	The Mobile Connect Authorisation products must offer a mechanism through which the SP can request a user to approve or reject a transaction.
MC_RQ01.3.2 Authorisation device	The Mobile Connect Authorisation services must get approval from the Mobile Connect user only on the Authorisation device (i.e. mobile device).
MC_RQ01.3.3 Authorisation Levels	The Mobile Connect Authorisation product category should support single (LoA2) and two factor (LoA3) authorisation. Note that an authentication step is implicit within the authorisation. Product names are: • LoA2 = Mobile Connect Authorise • LoA3 = Mobile Connect Authorise Plus
MC_RQ01.3.4 SP context	The service provider must provide a `context` in the Mobile Connect request that clearly identifies the action/transaction that the user is being asked to authorise.
MC_RQ01.3.5 Authorisation prompt	The Mobile Connect Authorisation product must present a prompt to the user that includes: • Application short name (from the SP, 16 bytes max) • SP provided transaction-specific context

Requirement	Description
	• SP provided binding message (optional)
MC_RQ01.3.6 Authorisation prompt screens	For a better user experience, it is recommended that the prompt is displayed on a single screen (not a sequence of multiple screens) unless local regulation requires otherwise.
MC_RQ01.3.7 Supported authenticators	Explicit responses to the authorisation request must be returned hence seamless authorisation must not be supported. For both Mobile Connect Authorise products valid authenticators include: • SMS + URL (Mobile Connect Authorise only) • USSD (not recommended for Mobile Connect Authorise Plus) • SIM Applet • Smartphone app authenticator
MC_RQ01.3.8 Authorisation requests	Mobile Connect Authorisation should support server-initiated as well as client-initiated authorisation requests.
MC_RQ01.3.9 Mobile Connect Authorisation result	Mobile Connect must return one of the following • a positive result • a negative result with an appropriate error code
MC_RQ01.3.10 First and third party authorisation request.	The Mobile Connect Authorisation products should support both first party and third party authorisation use cases (please refer to PDATA.27 [9] for more details).
MC_RQ01.3.11 User portal for reviewing authorisations	The operator should ideally provide a portal through which the user can review the transactions that they have authorised

Table 3 : Authorisation product requirements

4 Technical Requirements

This section provides a detailed technical walk-through of the Mobile Connect Authorisation products and the requirements for operators for deploying them (e.g., ID GW requirements). Please refer to PDATA.27 for business requirements and product behaviour [9].

4.1 Overview

The service provider (application) must acquire a single set of credentials (client id/secret) for accessing all Mobile Connect services including Mobile Connect Authorisation products. These credentials should be obtained through API Discovery or directly from the ID GW.

The Mobile Connect Authorisation products are requested by SPs via OpenID Connect API requests in alignment with PDATA.01 Mobile Connect Profile v1.2 [1]. These requests must identify the specific Authorisation product that is being requested (i.e., Mobile Connect Authorise or Mobile Connect Authorise Plus) through the combination of <`scope`> and <`acr_values`> as per the following table.

Mobile Connect product	scope	acr_values	LoA
Mobile Connect Authorise	"`openid mc_authz`"	"2"(LoA2)	Single factor authorisation

Mobile Connect Authorise Plus	"openid mc_authz"	"3"(LoA3)	Two-factor authorisation

Table 4: Mobile Connect Authorisation scopes & acr_values

Furthermore, the OIDC request must also include the application short name[1] and transaction context[2] to enable the operator to generate and display the authorisation request. The SP may optionally include a binding message[3] that the operator should also include in the authorisation prompt to mitigate phishing attacks.

The operator can use whichever authenticators it has currently deployed and suitable for presenting the authorisation prompt and capturing user authorisation.

4.2 Core Technical Requirements

The Mobile Connect Authorisation products are built on and extend the core Mobile Connect system capability. As such, implementations of the Mobile Connect Authorisation products must abide by the Mobile Connect core framework requirements as defined in PDATA.13 Mobile Connect Core Technical Requirements [2]. The following table highlights some key areas:

Requirement	Description
MC_RQ03.2.2 Server to server (Core ref)	The ID GW must implement support for server-based invocation[4] as defined in the Core Technical Requirements spec [2].
MC_RQ03.2.3 Trusted/Normal Service provider (Core ref)	The ID GW must support Trusted[5] as well as normal (untrusted) Service Providers as defined in the Core Technical Requirements spec [2].
MC_RQ03.2.4 PCR	The ID GW must issue PCRs as defined in the Core Technical Requirements spec [2]
MC_RQ03.2.5 Account[6] status (Core ref)	The ID GW must take into consideration Account status as defined in the Core Technical Requirements spec [2].
MC_RQ03.2.6 Request processing (Core ref)	The ID GW must implement the request processing requirements as defined in the Core Technical Requirements spec [2].

Table 5: Core technical requirements references

[1] Note that in the OIDC request, application short name must be provided through `client_name`.

[2] Transaction context is provided in the OIDC request through `context` parameter.

[3] Binding message is provided in the OIDC request through `binding_message` parameter.

[4] 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)

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

[6] Due to local regulations and privacy guidelines, the ID GW must not return errors like pin blocked, account is blocked because bill not payed e t c, disclosing the personal data of a Mobile Connect user.

4.3 Identity Gateway Requirements

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

4.3.1 Service Registration

Requirement	Description
MC_RQ03.2.1 Mobile Connect authorisation service variants	The ID GW should enable the service provider (application/service) to register for either of the following services. • Mobile Connect Authorise • Mobile Connect Authorise Plus
MC_RQ03.2.2 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 services, either through the API Exchange or directly; for further information see the Mobile Connect Core Technical Requirements [2].

Table 6: Service registration

4.3.2 Service Invocation

Requirement	Description
MC_RQ03.2.3 Authorisation requests	The service provider must submit Mobile Connect Authorisation OIDC requests to the ID GW using the Mobile Connect API and the ID GW must process these requests if they comply with the Mobile Connect profile v1.2 [1]
MC_RQ03.2.4 Authorisation product type	The service provider must specify the required type of Mobile Connect Authorisation product through the `scope` value and `acr_values` in the OIDC Authorisation request as defined in Table 4.
MC_RQ03.2.5 Server-initiated requests	The ID GW must implement support for server-initiated invocation as defined in the Mobile Connect Core Technical Requirements spec [2].
MC_RQ03.2.6 login hint type	The ID GW must able to serve Mobile Connect Authorisation OIDC requests through supplied encrypted MSISDN[7] or PCR provided vial the `login_hint` parameter (for normal SPs)
MC_RQ03.2.7 Trusted Service Provider	The ID GW must be able to serve identity services OIDC requests through plain MSISDN/encrypted MSISDN[7] and PCR provided via the `login_hint` parameter (for Trusted SPs).
MC_RQ03.2.8 Authorisation requests using encrypted MSISDN through login_hint_token	Any service providers (i.e. Normal or Trusted) must be able to invoke Mobile Connect Authorisation 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.

Table 7: Service invocation

[7] The encryption is done by the API exchange.

4.3.3 Request Processing

Requirement	Description
MC_RQ03.2.9 SP subscription to services	The ID GW must check that the SP is subscribed to the requested Authorisation Service
MC_RQ03.2.10 Pre-registered MC user	The ID GW must check whether the Mobile Connect user is already registered and has a Mobile Connect account. If not, it must provide on-the-fly registration before serving Mobile Connect Authorisation requests.
MC_RQ03.2.11 Mobile Connect account status	The ID GW must maintain various Mobile Connect account states as mentioned in [8].
MC_RQ03.2.12 Account active state	The ID GW must only serve OIDC requests if the corresponding Mobile Connect account is in an "active" state [8].
MC_RQ03.2.13 Error handling if account not active	The ID GW must reject OIDC requests for all other Mobile Connect account states (ex. suspended, deleted, and not available[8]) with appropriate errors as defined in the Mobile Connect Technical Reference [5].
MC_RQ03.2.14 Mobile Connect User Authorisation flow	The ID GW must ensure that the Mobile Connect user is successfully authenticated before or as part of the authorisation process to ensure that the right person is being asked for authorisation.
MC_RQ03.2.15 ID GW policies – LoA	The ID GW should select the authentication method based on the LoA requested by the SP in the OIDC request, operator policy and available authenticators for the user in question.
MC_RQ03.2.16 Authorisation step up	The ID GW may conduct user authentication/authorisation to a higher LoA if the requested authorisation type is not available (e.g., Mobile Connect Authorise Plus is used if Mobile Connect Authorise is not available for any reason)
MC_RQ03.2.17 Authorisation step down	The ID GW may utilise Mobile Connect Authorise if Mobile Connect Authorise Plus is requested but unavailable but this fact must be clearly returned in the OIDC response via the `acr` claim in the ID Token: • 2 (LoA2) • 3 (LoA3)
MC_RQ03.2.18 Minors	The ID GW must reject OIDC requests if it is known that the corresponding Mobile Connect user is a minor[9] (based on local legislation).

Table 8: Request processing

4.3.4 Authorisation Prompt

The Mobile Connect Authorisation products require that the Mobile Connect user is clearly communicated details of the transaction they are being asked to approve or reject. The prompt sent to the user is constructed by the ID GW based on information provided by the SP in the OIDC request.

[8] 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.

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

Requirement	Description
MC_RQ03.2.19 Authenticator neutral	The Mobile Connect Authorisation architecture used by the ID GW must be independent of the selected authenticator technology.
MC_RQ03.2.20 Authorisation prompt	The ID GW must clearly display a prompt detailing the transaction/action the user is being asked to authorise
MC_RQ03.2.21 Authorisation context	The ID GW must support the authorisation context (transaction) details via the `context` parameter in the OIDC request.
MC_RQ03.2.22 Authorisation message	The ID GW must be able to construct the Authorisation prompt to present the following information to the user: • SP short name • Transaction details (i.e., what the user is being asked to authorise) • A binding message (optional)
MC_RQ03.2.23 SP application short name	The service provider must be able to specify application short name in the displayed prompt; the maximum length for the application short name[10] is 16bytes.
MC_RQ03.2.24 Prompt binding message	If a binding message is present in the OIDC request, the ID GW must show this on the consumption device and authorisation device for interlocking purposes (i.e., to mitigate phishing). Note - The maximum length of the binding message is implementation specific, but must be within the limits of the prompt maximum length.
MC_RQ03.2.25 Authorisation prompt length (Interoperability)	For interoperability[11] purposes, the maximum length of the prompt is 93 bytes. This restriction only applies where the operator is using a SIM applet based authenticator. *Formulae* : `length(context) = 93 – length(binding_message) – length(client_name)` The ID GW should truncate the prompt if the underlying authenticator does not support the requested prompt length.
MC_RQ03.2.26 Authorisation locale	The service provider can specify `ui_locales` in the OIDC request. If the ID GW supports the requested locale, it should customise the prompt accordingly.
MC_RQ03.2.27 Authorisation encoding	The ID GW must support the following encoding schemes for the authorisation prompt: • gsm7 • ucs2 • utf-8
MC_RQ03.2.28 Prompt action text	Prompt Action Text (e.g. Click OK to approve), should not be included in the prompt provided to the Authorisation device from the ID GW but generated locally by the Authenticator itself. The Prompt Action Text should be in accordance with the recommendations in the Mobile Connect Product Definition document [9].
MC_RQ03.2.29 Dynamic prompt text	The Authenticator must be able to display Prompt Action Text based on the incoming LoA values

[10] The application short name is provided in the OIDC request through client_name parameter.

[11] 93 bytes is the maximum length supported by the SIM applet authenticator. All other authenticators can support more than 93 bytes. Hence, to work with any authenticator 93 bytes is the maximum.

Table 9: Authorisation prompt

4.3.5 Response to Service Provider

After the Mobile Connect user has approved/denied the authorisation request, the ID GW must return a response to the SP as per the requirements detailed below.

Requirement	Description
MC_RQ03.2.30 Authorisation Token response	Upon successful Mobile Connect Authorisation (Authorise/Authorise Plus), the ID GW must return an Authorisation Code that the SP can exchange at the ID GW token endpoint for an Access Token and an ID Token. If an error occurs, the ID GW must return appropriate error codes as specified in [5]
MC_RQ03.2.31 Token end point	Upon receiving an Authorization Code from the SP, the ID GW Token endpoint must issue an Access Token and an ID Token (with the details of the PCR and relevant claims such as date & time, TTL, displayed data etc.). Upon validation error, the ID GW must return error codes as specified in [5].
MC_RQ03.2.32 Authorisation TTL value	The TTL parameter `expires_in` in the Token response and the `exp` claim in the ID Token must be zero.
MC_RQ03.2.33 Authorisation refresh token	The ID GW must not return a Refresh Token for Mobile Connect Authorisation
MC_RQ03.2.34 Authorisation errors	For timeout, 'action rejected by an end-user' or for any other error, an HTTP error code must be returned with the error description as defined in the Technical reference [5].
MC_RQ03.2.35 Authorisation Token content	The ID Token must return the prompt text as an ID Token claim parameter `displayed_data` (containing `client_name`[12], `context` and `binding_message` if used)
MC_RQ03.2.36 Authorisation events.	The ID GW must support the following events: • **Successful authorisation** – Mobile Connect Authorisation is approved: ID Token and Access Token must be returned. • **Authorisation failure** – User denies the authorisation request (OR) enters the wrong PIN. The ID GW must return an error code. • **Timeout** – user does not respond, ID GW timeouts waiting for the response from the authenticator. This must be considered as "unavailable." • **Any other processing error** – Unknown error must be returned. The ID GW must return appropriate error codes as defined in the Mobile Connect Technical reference [5].
MC_RQ03.2.37 Displayed data	The ID GW must return `displayed_data` in the following format: • <displayed application short name > + "-" < displayed binding message> + "-" +<displayed context> Note that "-" is added to differentiate parameters.

[12] Application short name

Requirement	Description
MC_RQ03.2.38 Authorisation level response	The ID GW must return the achieved authorisation level to the service provider through the `acr` value in the OIDC response: • 2 (LoA2) • 3 (LoA3)

Table 10: Response to SP

4.3.6 Non-functional Requirements

Requirement	Description
MC_RQ03.3.39 logging	The following data should be logged by the ID GW with regard to consent capture. • Date & Time • PCR • Product type requested (i.e. scope parameter + acr_values) • User Response (approve, timeout or authorisation failure) • Status (Complete, In-process, error) • Displayed_data (i.e., prompt that was displayed on Mobile device) • Authenticator type used (as per the returned amr value) • Level of Assurance requested and used • Error codes and error description (as defined in the Mobile Connect Technical Reference [5]).
MC_RQ03.3.40 Response times	The ID GW should respond to the SP request with an Authorization Code (or error message) in a timely manner

Table 11: Non-functional requirements

4.4 Authorisation Device

Requirement	Description
MC_RQ03.3.1 Authorisation device	The Mobile Connect Authorisation device is always a mobile device of a Mobile Connect user.
MC_RQ03.3.2 Prompt action text	Prompt Action Text (e.g. Click OK to approve), should be generated locally by the Authenticator (Authorisation device). The Prompt Action Text should be in accordance with the recommendations in the Mobile Connect Product Definition document [9].
MC_RQ03.3.3 Dynamic prompt text	The Authenticator must be able to display Prompt Action Text based on the incoming LoA values
MC_RQ03.3.4 Authorisation prompt	The Authorisation device must render prompt details correctly i.e. without breaking a word into multiple lines.
MC_RQ03.3.5 Authorisation types support	The Authorisation device must be able to support either single factor or two-factor authorisations.
MC_RQ03.3.6 Internationalization	The Authorisation device must render international language characters correctly wherever applicable.

Table 12: Authorisation device requirements

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	26/5/2016	New document	PDATA/PSMC	Siva (Venkatasivakumar Boyalakuntla) / GSMA
1.1	12/05/2017	Transfer of PRD from Personal Data	TG	Nick Cheung / GSMA

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.