



Mobile Connect Authorisation Definition and Technical Requirements

Version 1.0

26 November 2019

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

Security Classification: Non-confidential

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

Copyright Notice

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 contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1	Introduction	3
1.1	Overview	3
1.2	Scope of the document	4
1.3	Audience	4
1.4	Relationship to Other Mobile Connect Documentation	4
1.5	Conventions	5
1.1	Terminology & Definitions	5
1.2	References	5
2	Mobile Connect Authorisation.	6
2.1	Use Case Examples	6
2.2	Mobile Connect Authorise/Authorise Plus Flow	6
2.3	Authorisation Prompt	10
2.4	Authorisation Response	11
2.5	Mobile Connect Account Setup	12
2.6	Server-Initiated Invocation	12
3	Mobile Connect Authorisation Service Specification	13
3.1	OIDC Authorization Request Parameters – <code>scope</code> and <code>acr_values</code>	13
3.2	API Modes Supported	13
3.3	Service-Specific Requirements	13
Annex A	Mobile Connect Authorisation Service Specific Error Codes and Descriptions.	17
A.1	Single Page and Two Page Environments	17
A.2	Error Responses – Device-Initiated Mode	17
A.3	Error Responses in Server-Initiated Mode	18
A.3.1	Error Responses: OIDC Authorization Response	19
A.3.2	Error Responses: Notification	20
A.3.3	Error Responses: Notification Acknowledgement	20
A.3.4	Error Responses: Polling Response	21
Annex B	Document Management	22
B.1	Document History	22
B.2	Other Information	22

1 Introduction

1.1 Overview

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

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

The serving Mobile Operator selects an appropriate Authenticator based on Operator policy, device capability and the Level of Assurance required by the SP to present a prompt providing the details of the transaction to the User and seeking their authorisation.

This document details the Mobile Connect Authorise services which offer the ability for a User to authorise or approve transactions presented to them by an SP. The service presents an SP provided context to the User on their mobile device (Authentication Device) in order for them to know what they are authorising or approving.

Mobile Connect Authorisation is defined as two variants:

- Mobile Connect Authorise: captures approval using a standard level of assurance¹ (LoA2 – single factor authorisation) via a single User-click.
- Mobile Connect Authorise Plus: captures approval using a higher level of assurance (LoA3 – two factor authorisation) by challenging the User for a PIN or biometric²

Supporting two different levels of assurance enables SPs to choose the trade-off between User convenience and security to match their intended use case.

This document describes the Mobile Connect Authorisation services, applicable use cases and the associated User journeys. It also contains technical requirements detailing how the service must be implemented and operated (in conjunction with requirements for the Core framework). For further information on the Mobile Connect Core framework please see Mobile Connect Technical Architecture and Core Requirements [5].

¹ In the context of authorisation, the level of assurance relates to the confidence that the User authorising the transaction is the same User that registered for Mobile Connect.

² Two-factor authentication (2FA) is achieved by combining authentication on a mobile device (something I have) with entry of a PIN (something I know) or use of a biometric (e.g. a fingerprint – “something I am”)

1.2 Scope of the document

In Scope	Out of Scope
<ul style="list-style-type: none"> • Mobile Connect Authorise/Plus functional description • Mobile Connect Authorise/Plus technical specifications 	<ul style="list-style-type: none"> • Detailed Privacy and Trust Principles • UI/UX guidelines • Mobile Connect Authorise/Plus commercial propositions • SP/developer implementation guidelines • Other Mobile Connect service definitions

1.3 Audience

The target audience of this document are the product managers and service/technical departments and Operators who are considering deploying Mobile Connect Authorisation/Plus services.

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

1.4 Relationship to Other Mobile Connect Documentation

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

The Mobile Connect Technical Architecture and Core Requirements document [5] describes the Mobile Connect Architecture in more detail and includes the core requirements and the specification of elements for Mobile Connect that are generic to all Mobile Connect services and modes of operation.

The Mobile Connect Device-Initiated OIDC Profile [6] and the Mobile Connect Server-Initiated OIDC Profile [7] specify the Mobile Connect APIs which provide details for OIDC Authorization Requests and Responses, and Token retrieval including examples and error codes.

The Mobile Connect Technical Architecture and Core Requirements document along with the Mobile Connect Device-Initiated OIDC Profile and the Mobile Connect Server-Initiated OIDC Profile together define the Mobile Connect Core framework upon which all services are built.

The Mobile Connect Technical Overview document [4] provides a high-level description of Mobile Connect and how it works. It also includes a master list of abbreviations and terminology used within the Mobile Connect Documentation set and a map of that documentation set. It serves as a starting point for understanding how Mobile Connect works and also references the relevant documents for the reader to obtain further information.

1.5 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [3].

1.1 Terminology & Definitions

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

The Mobile Connect Technical Overview document [4] defines relevant terms that are used within the Mobile Connect Specifications and interprets terminology from source standards in Mobile Connect terms. It also includes a list of abbreviations.

Due to potential confusion with OIDC and OAuth 2.0 terminology, the initial Mobile Connect service request which underpins Mobile Connect Authentication, Authorisation and User consent associated with attribute services, is referred to as an OIDC Authorization Request³ (spelled with a ‘z’) throughout this document.

1.2 References

Ref	Doc Number	Title
[1]	OpenID Connect Core Specification	“An interoperable authentication protocol based on the OAuth 2.0 family of specifications” available at https://openid.net/specs/openid-connect-core-1_0.html
[2]	OIDF CIBA	OpenID Connect MODRMA Client Initiated Backchannel Authentication Flow 1.0 https://openid.net/specs/openid-connect-modrma-client-initiated-backchannel-authentication-1_0.html
[3]	RFC 2119	“Keywords for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at https://tools.ietf.org/html/rfc2119
[4]	IDY.05	Mobile Connect Technical Overview
[5]	IDY.04	Mobile Connect Technical Architecture and Core Requirements
[6]	IDY.01	Mobile Connect Device-Initiated OIDC Profile
[7]	IDY.02	Mobile Connect Server-Initiated OIDC Profile
[8]	IDY.03	Mobile Connect Resource Server Specification
[9]	IDY.16	Mobile Connect Product Manager’s Lifecycle Handbook
[10]	IDY.33	API Exchange Functional Description
[11]	IDY.09	Mobile Connect Authenticator Options

³ In OAuth2.0 the initial request is referred to as an “Authorization Request”, whereas in OIDC it is referred to as an “Authentication Request”. Mobile Connect offers several services including Mobile Connect Authentication and Mobile Connect Authorisation, hence Mobile Connect specifications have adopted the term “OIDC Authorization Request” to describe this initial service request in the protocol flow.

Ref	Doc Number	Title
[12]	IDY.10	Mobile Connect SIM Applet Authenticator
[13]	IDY.12	Mobile Connect Smartphone Application Authenticator
[14]		Mobile Connect Privacy Principles

2 Mobile Connect Authorisation.

Mobile Connect Authorisation⁴ services offer a mechanism through which an SP application can request a User to approve or reject a transaction. The SP provides an “authorisation text” (context) that is presented to the User informing them of what they are being asked to authorise. The SP application provides this context within the Mobile Connect Authorisation service request. For example, a bank might use Mobile Connect Authorise Plus to request a User to approve a funds transfer to a new payee. The nature of the response will depend upon on the level of assurance (LoA) that the SP requires (LoA2 or LoA3) and the type of Authenticator that has been used by the serving Operator’s IDGW to prompt the User. Mobile Connect Authorise offers a standard level of assurance using a single-factor authorisation (LoA2) whereas Mobile Connect Authorise Plus offers a higher level of assurance using two-factor authorisation (LoA3).

It is important to note that Mobile Connect Authorisation is a mechanism for SPs to request a User to respond (to approve) an event or transaction. Mobile Connect will process the request and provide the response to the SP. It is up to the SP to process this response and decide the final outcome of the transaction.

2.1 Use Case Examples

Mobile Connect Authorise/Plus supports a range of practical use cases as shown below:

Product	Example Use Cases
Mobile Connect Authorise	<ul style="list-style-type: none"> • Simple password change verification • Confirming User as human – captcha replacement • Convenient delegated ticket collection
Mobile Connect Authorise Plus	<ul style="list-style-type: none"> • Secure bank transfer to a new payee • Verification of high value or risky card transactions • Secure health record transfer approval

Table 1: Use Case Examples

2.2 Mobile Connect Authorise/Authorise Plus Flow

Mobile Connect Authorise is an authorisation service with a standard-level of authorisation (LoA2). This requires the Operator IDGW, on receiving a Mobile Connect Authorise service request from an SP’s application, to confirm that the User is in possession of their mobile

⁴ Mobile Connect Authorisation is one of the service classes and collectively describes Mobile Connect Authorise and Mobile Connect Authorise Plus

device (“Something I have”) and if that User who has access to the device has approved the authorisation request displayed in the prompt. If the User approves the request, the Operator IDGW will return a successful authorisation response. An appropriate error is returned if the User fails to approve or explicitly denies the request.

Mobile Connect Authorise Plus offers a higher level of assurance (LoA3). This requires the Operator IDGW, on receiving a Mobile Connect Authorise Plus service request from an SP’s application, to confirm that the User who is in possession of their mobile device, has entered a secret that they know (PIN) or has provided a biometric (e.g. a fingerprint) when prompted on their device which approves the request displayed in the prompt. Unlike Authorise, Authorise Plus confirms that the User has approved the authorisation request and not just anyone who has access to that device. If the User approves the request, the Operator will return successful authorisation response. An appropriate error is returned if the User cancels the request.

□ (next page) shows a simplified Mobile Connect Authorise service request flow for both Mobile Connect Authorise and Mobile Connect Authorise Plus services illustrating how the services are presented to the User.

Note: That this illustrates a Device-Initiated request [6], but a Server-Initiated request [7] can also be used. Mobile Connect Technical Architecture and Core Requirements [5] provides more detailed sequence diagrams illustrating the flow for Device-Initiated mode and the Server-Initiated modes.

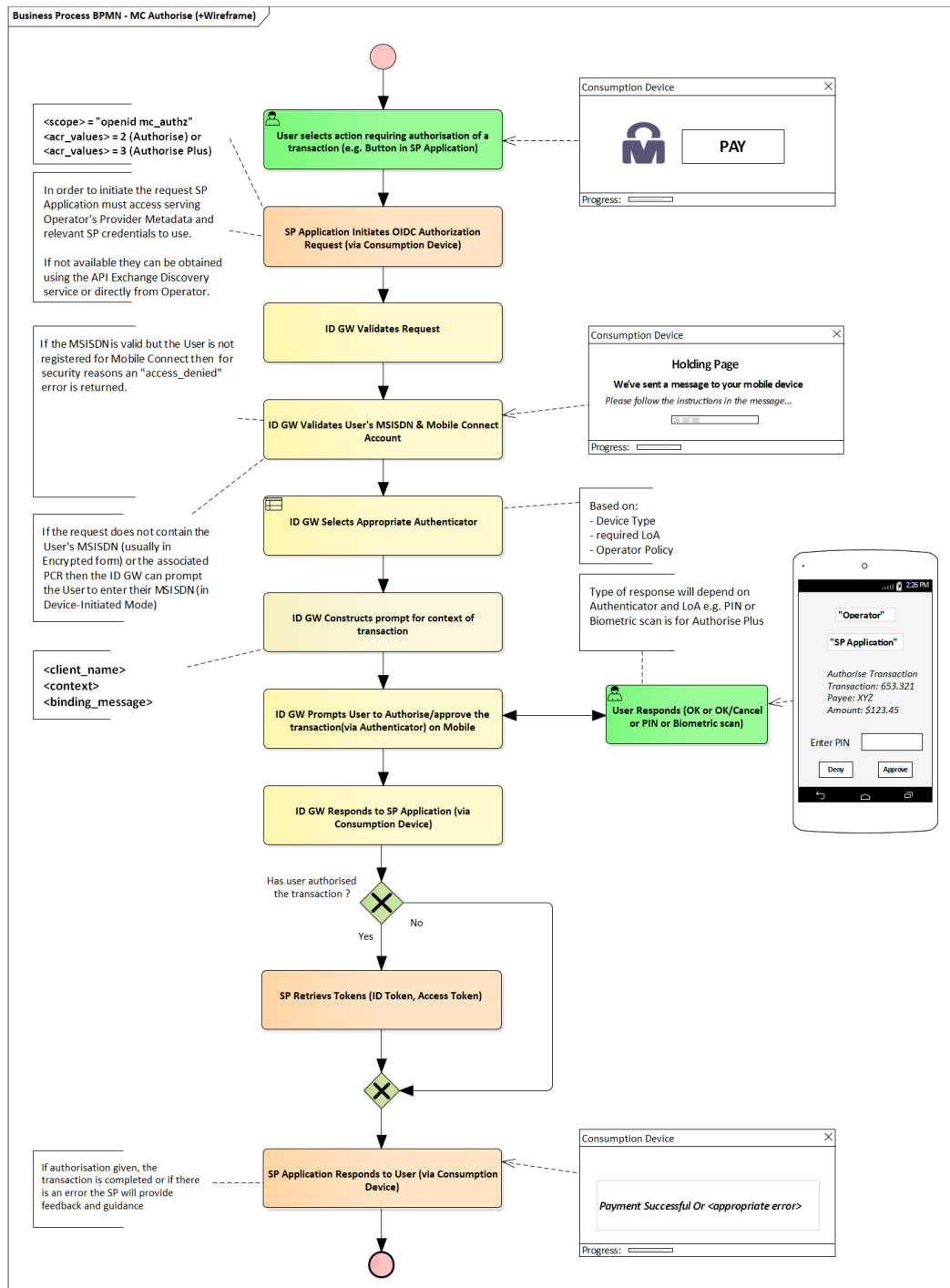
Table 2 indicates the suitability of common Authenticators for Mobile Connect Authorise and Mobile Connect Authorise Plus. More information on each of the authenticators is available [11] along with detailed specifications for SIM Applet [12] and Smartphone App Authenticator (SAA) [13].

Note: That if an Authenticator has been configured for Mobile Connect Authentication services for a User then the same Authenticator would be used for Mobile Connect Authorisation services and the PIN/biometric would be the same.


Authenticator	Authorise	Authorise Plus	Comments
Seamless	No	No	Authorisation requires an explicit approval from the User which is not possible with a seamless authenticator
USSD (network initiated)	Yes	No	Not sufficiently secure for LoA3 as the PIN would be transported over the mobile network in plain text
SMS + URL (embedded link)	Yes	No	Limited space for the authorisation prompt
SIM Applet	Yes	Yes	Limited space for the authorisation prompt

Authenticator	Authorise	Authorise Plus	Comments
Smartphone App Authenticator (SAA)	Yes	Yes	Can support biometrics as well as PIN

Table 2: Authenticator suitability for Mobile Connect Authorisation



• : Mobile Connect Authorisation Service Flow

Based on :


The SP must be registered for Mobile Connect (Device-Initiated mode and/or Server-Initiated mode) and must be registered for Mobile Connect Authorisation.

- The User is accessing a service provided by an SP either through a native app or through a browser on the Consumption Device (e.g. a laptop) and within the SP application there is an option to authorise a payment, for example, using Mobile Connect.
- The SP application initiates the Mobile Connect Authorisation service request (OIDC Authorization Request) to the Operator's IDGW Authorise endpoint. The Authorise and Authorise Plus services are requested by specifying the `scope` parameter and specifying the required LoA using the `acr_values` parameter in the request as specified in Table 3.

The following parameters are also relevant for Mobile Connect Authorisation as they are used to form the authorisation prompt on the User's Authentication Device:

- `client_name` (required) specifies the SP's short name for their application.
 - `context` is required for Mobile Connect Authorisation (optional otherwise) and is used to provide the context for the authorisation (i.e. what is it I am authorising?).
 - `binding_message` is required and allows the same message to be displayed on both the Consumption Device (e.g. on the holding page) and on the Authentication Device so that the User can link what is seen on both devices.
- In Device-Initiated mode, the User is redirected to the IDGW holding page which prompts the User to check their mobile device.
 - The Operator's IDGW validates the request (i.e. that the SP has been registered with the Operator for the Mobile Connect Authorisation service requested and that the required parameters are included in the correct format)
 - The Operator IDGW checks the MSISDN and whether the User is registered for Mobile Connect

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

- The authorisation prompt is then constructed using the `client_name` and `context` and `binding_message`⁵.  illustrates the authorisation prompt.

1.

⁵ Note "prompt action text" relating to the requested action depending upon LoA is inserted into the authorisation prompt by the selected Authenticator

- Assuming the User successfully authorises the transaction on their mobile device, the ID Token and Access Token are retrieved by the SP. The ID Token provides a proof that authorisation has been provided. The method for achieving this differs depending on whether Device-initiated or Server-Initiated requests were made.
- For Device-Initiated mode, the IDGW issues an Authorization Code and control is transferred to the SP server to initiate a token request using that code to retrieve the ID Token and Access Token (Token Response).
- Receipt of the ID Token provides the details of the successful authorisation which allows the SP to proceed with the transaction.

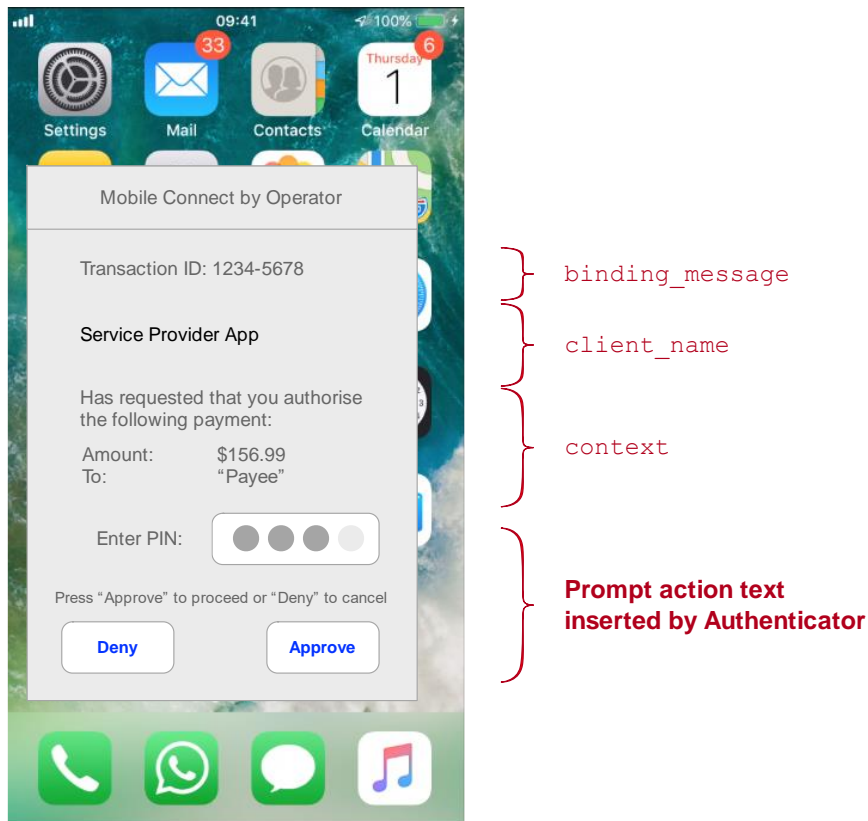
2.3 Authorisation Prompt

□ shows an example authorisation prompt on the User's mobile device (Authentication Device). For interoperability across different markets the maximum length of the prompt should be $\leq 220^6$ bytes which will ensure that the prompt text can work seamlessly across Operators who may be using different authenticators (based upon the use of a SIM-Applet Authenticator).

This means that:

$\text{Length}(\text{client_name}) + \text{Length}(\text{context}) + \text{Length}(\text{binding_message}) \leq 220$ bytes.

⁶ The 220 bytes can be concluded based on the least denominator length (SIM applet authenticator). The existing concatenated SMS feature in the sim applet supports up to 220 bytes. For more information refer to [10]



• : **Example Authorisation prompt**

For the best User experience, it is recommended that the prompt text comprising of both authentication (“enter pin”) and authorisation (“do you authorise...”) are rendered on a single screen. However, it is recognised that this may not always be possible due to limited space on a single screen where local language text may require more space or where, in certain countries, regulations may require explicit confirmation to be displayed with the requested LoA strength to the User on the Authentication Device.

2.4 Authorisation Response

A successful Mobile Connect Authorisation results in the return of an ID Token and an Access Token to the SP application. An error will be returned if the authorisation was not successful.

Note Mobile Connect Authorisation specific errors are defined in Annex A and generic error codes, applicable to all supported services, are defined in the relevant Mobile Connect OIDC Profile (Device-Initiated [6] or Server-Initiated [7]).

The ID Token provides confirmation of the successful authorisation and includes a Pseudonymous Customer Reference (PCR) identifying the User which can be used in subsequent Mobile Connect service requests. For Authorise and Authorise Plus services, the Access Token is not required although it is always generated. After a User has been authenticated or has authorised a transaction for the first-time using Mobile Connect, the SP Application can store the PCR associated with the User, the serving Operator details (issuer

ID (`iss`), openid-configuration URL), appropriate SP credentials (`client_id`) and sector identifier to be used.

The ID Token has a period of validity, defined by the Operator and returned within the `exp` value (expiration time) within the ID Token. This must be kept as short as possible so that the authorisation is only valid for a single transaction.

2.5 Mobile Connect Account Setup

If the User has not previously registered, they could be asked to register “on the fly” to use Mobile Connect, subject to Operator policy. For some SP implementations, the User may not be involved in the User journey to complete registration. In such scenarios, the Mobile Connect account will be created for the User. Operators are encouraged, in this case to follow up with the User to ensure the User is aware of Mobile Connect terms and conditions.

For Mobile Connect Authorisation, depending upon the particular use case, the use of “on-the-fly” registration is not recommended as this may represent a security risk⁷.

Note: That on-the-fly” registration would only be appropriate for Mobile Connect Authorise (LoA2) service requests,.

2.6 Server-Initiated Invocation

An SP can also choose to use a Server-Initiated Mobile Connect Authorisation service request where the request is initiated directly from the SP’s server rather than via the User’s Consumption Device and can be initiated without the User having to be online or initiating a transaction via pressing a button in an application. An example of the use of a Server-Initiated request could be where a bank detects the need to get an explicit approval from the User for a payment request initiated from an unusual location. The bank will use the MSISDN on file for the User to initiate the authorisation request.

This process is broadly the same as described in [6] but with the following differences:

- The format of the request (defined in the Mobile Connect OIDC Server-Initiated OIDC Profile [7]) is different but the same `scope` values are used. The User must be identified using their MSISDN (via the `login_hint` or `login_hint_token` parameter). The mechanism to obtain the ID Token and the Access Token also differs.
- The User is not interacting with the SP application via a Consumption Device so no holding pages can be presented. The User will always be presented with the authorisation prompt and will respond on the Authentication Device.

Mobile Connect Technical Architecture and Core Requirements [5] provides more detailed sequence diagrams illustrating the flow for Device-Initiated mode and the Server-Initiated modes.

⁷ For authorise Plus setting up a PIN on the fly can have a security risk, hence for authorise Plus the User must be pre-registered Mobile Connect User.

3 Mobile Connect Authorisation Service Specification

This Section contains the relevant information required by Operators to implement and support Mobile Connect Authorisation services (Authorise and Authorise Plus).

3.1 OIDC Authorization Request Parameters – scope and acr_values

The SP requests Mobile Connect Authorise or Authorise Plus by specifying the `scope` and `acr_values` parameters in the Mobile Connect OIDC Authorization Request as described in Table 3.

Mobile Connect Service	scope value ⁸	LoA (acr_values)
Mobile Connect Authorise	“openid mc_authz”	2
Mobile Connect Authorise Plus	“openid mc_authz”	3

Table 3: Mobile Connect Authentication scope and acr_values Values

3.2 API Modes Supported

Mobile Connect Authorisation can be used in both Device-Initiated and Server-Initiated Modes. An Operator can support one mode or the other or both, depending on the requirements from their target customers (SPs) within their market. Importantly, Operators supporting Mobile Connect within a particular market must align on deployment approach to ensure a consistent service for all SPs and all Users.

3.3 Service-Specific Requirements

Table 4 provides service-specific requirements relating to Mobile Connect Authorise and Authorise Plus. These should be used in conjunction with the following requirements in the implementation of this Mobile Connect service:

- Core Requirements specified in the Mobile Connect Technical Architecture and Core Requirements [5]. Note that these are common to all Mobile Connect services.

For terminology and associated specifications please refer to the Mobile Connect Technical Overview [4]

No	Relating To	Requirement
Mobile Connect_AUTH Z_01	Support Service of	The Mobile Connect Authorise service must support single factor (LoA2) authorisation via a User’s mobile device using an appropriate authenticator. Note that an authentication step is implicit within the authorisation.
Mobile Connect_AUTH Z_02	Support Service of	The Mobile Connect Authorise Plus service must support two factor (LoA3) authorisation via a User’s mobile device using an appropriate authenticator. Note that an authentication step is implicit within the authorisation.

⁸ “openid” must be included within the `scope` parameter as a string followed by the relevant Mobile Connect service descriptors separate by spaces

Mobile Connect_AUTH Z_03	Service Registration	The IDGW must be able to allow an SP (client application/service) to register for Mobile Connect Authorisation services (Mobile Connect Authorise and Mobile Connect Authorise Plus) and be provisioned with the requisite SP-provided parameters dependent on whether the SP intends to use Device-Initiated mode or Server-Initiated mode when requesting the service and what modes are supported by the IDGW. See the Mobile Connect Device-Initiated OIDC Profile and the Mobile Connect Server-Initiated OIDC Profile
Mobile Connect_AUTH Z_04	Authenticator	Authorisation of a transaction by the User must be via the Authenticator on their Authentication Device (i.e. their mobile device) for Mobile Connect Authorisation services.
Mobile Connect_AUTH Z_05	Authenticator	For Mobile Connect Authorisation services, a Seamless Authenticator cannot be used as explicit authorisation of the transaction must be returned. Table 2 in this document describes suitable Authenticators. The appropriate Authenticator is selected by the IDGW based upon the requested acr_values (LoA), the Authenticators that are supported and the Authenticators provisioned on the User's mobile device.
Mobile Connect_AUTH Z_06	Service Invocation	The SP will specify the required Mobile Connect Authorisation service via the scope parameter and associated acr_values parameter within the OIDC Authorization Request as specified in Section 3.1 of this document. The IDGW must support the use of these scope values for Mobile Connect Authorisation services.
Mobile Connect_AUTH Z_07	Service Request – Validation	The IDGW must validate the submitted Mobile Connect Authorisation service request (OIDC Authorization Request) and request parameters as defined in the Mobile Connect Device-Initiated OIDC Profile or the Mobile Connect Server-Initiated OIDC Profile, as appropriate. For Mobile Connect Authorisation, as well as the REQUIRED parameters, the SP must submit the context for the authorisation in the context parameter. If the context parameter is not submitted an error must be returned.
Mobile Connect_AUTH Z_08	Service Request – SP Validation	The IDGW must check that the SP is registered for the requested Authorisation Service and is registered to use Device-Initiated or Server-Initiated modes as defined in the Mobile Connect Device-Initiated OIDC Profile or the Mobile Connect Server-Initiated OIDC Profile, as appropriate.
Mobile Connect_AUTH Z_09	Service Request – User Validation	The IDGW must check whether the User is already registered and has a Mobile Connect account. Depending upon the use case, if the User has not been registered for Mobile Connect the request may be rejected with an appropriate error code as specified in the Mobile Connect Device-Initiated OIDC Profile or the Mobile Connect Server-Initiated OIDC Profile, as appropriate, subject to Operator Policy.
Mobile Connect_AUTH Z_10	Service Request – Prompt	For the Mobile Connect Authorisation service, the IDGW must present a prompt to the User that includes: - SP provided short application name (client_name parameter in OIDC Authorization Request, 16 bytes max) - SP provided context for the transaction/action to be Authenticated (context parameter in OIDC Authorization Request)

		<p>- SP provided message to link the Authentication Device and Consumption Device (binding_message parameter in OIDC Authorization Request).</p> <p>For the best User experience, it is recommended that the prompt is displayed on a single screen (not across a sequence of screens) unless local regulations dictate otherwise.</p>
Mobile Connect_AUTH Z_11	Service Request – Prompt	<p>For interoperability purposes, the maximum length of the prompt is ≤ 220 bytes (this is based on the SIM-Applet Authenticator). The length of the context message as a result will be determined by: $\text{length}(\text{context}) \leq 220 - \text{length}(\text{binding_message}) - \text{length}(\text{client_name})$</p> <p>The IDGW should be able to support prompts that are $\leq 220^9$ bytes on any Authenticator (excluding a Seamless Authenticator). IDGW Policy may recommend the maximum prompt length that should be used by SPs based on which Authenticators will be used for displaying the prompt and capturing User authorisation. The IDGW should truncate the prompt if the underlying Authenticator does not support the submitted prompt length. Note – The maximum length of the binding message is implementation specific but must be within the limits of the prompt maximum length.</p>
Mobile Connect_AUTH Z_12	Service Response	<p>The Mobile Connect Authorisation service must return to the initiating SP application:</p> <ul style="list-style-type: none"> - a positive result, or - a negative result with an appropriate error code and error description. <p>Note that a positive result will provide an ID Token and an Access Token. The ID Token will include a PCR, which uniquely identifies that User to the SP's client, and details of the User authentication/authorisation as defined in the Mobile Connect Device-Initiated OIDC Profile or the Mobile Connect Server-Initiated OIDC Profile, as appropriate. Error responses are defined in the Mobile Connect Device-Initiated OIDC Profile and the Mobile Connect Server-Initiated OIDC Profile. Service Specific Error Responses are specified in Annex A of this document.</p>
Mobile Connect_AUTH Z_13	Error Responses	<p>Error Responses may be returned at different stages of the processing of a service request as specified in the Mobile Connect Device-Initiated OIDC Profile and the Mobile Connect Server-Initiated OIDC Profile and must be supported for Mobile Connect Authorisation services. These errors are generic to all Mobile Connect services. Service Specific Error Responses are specified in Annex A of this document and must be supported for Mobile Connect Authorisation services.</p>

⁹ 220 bytes is the least denominator length supported by SIM applet authenticator using concatenated SMS for interoperability. For more information refer to [10].

Mobile Connect_AUTH Z_14	Tokens – ID Token	For Mobile Connect Authorisation services, the IDGW must return the displayed_data claim in the ID Token which combines the client_name, context and binding_message. displayed_data uses the following format: client_name + “-“ + binding_message + “-“ + context Note that “-“ is added to differentiate parameters.
Mobile Connect_AUTH Z_15	Tokens	The IDGW must not return a Refresh Token for Mobile Connect Authorisation or if it does it must be with a null value.
Mobile Connect_AUTH Z_16	Tokens	The IDGW Authorization Server must issue Access Tokens with one-time usage for access token OR a zero time-to-live using a very low value for the expires_in parameter in the Token Response or by restricting it to a single-use token and enough time to complete the transaction.
Mobile Connect_AUTH Z_17	Transaction Logs	A complete Mobile Connect transaction log must be maintained, archived and accessible to resolve any disputes in line with local data protection laws and the Operator’s data retention policy. For Mobile Connect Authorisation this should include: <ul style="list-style-type: none"> • Date & Time • MSISDN, PCR • Service requested (i.e. scope + 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 and returned in the ID Token) • Authenticator type used (as per the returned amr value) • Level of Assurance requested and used • Error codes and error description.

Table 4: Requirements for Mobile Connect Authorisation Services

Annex A Mobile Connect Authorisation Service Specific Error Codes and Descriptions.

This Annex is normative.

This Annex specifies the service specific error codes and associated descriptions that are REQUIRED for Mobile Connect Authorisation in addition to the generic error codes and descriptions that are specified in the relevant OIDC Profiles (Mobile Connect Device-Initiated OIDC Profile [6] and Mobile Connect Server-Initiated OIDC Profile [7]).

A.1 Single Page and Two Page Environments

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

A.2 Error Responses – Device-Initiated Mode

Table 5 lists the additional error codes and descriptions for Mobile Connect Authorisation for Device-Initiated mode. These are returned from the Authorization Endpoint.

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
In a single-page environment, the User failed to approve the proposed action/transaction (or) the IDGW was unable to authenticate the User.	Redirect 302	17authorization_failur e (or) access_denied	User failed to authorise the proposed action.
In a single-page environment, the User cancelled or rejected the Mobile Connect authorisation request on their mobile device	Redirect 302	17authorization_denied (or) 17authorization_failur e (or) access_denied	User rejected/cancelled the request for authorisation.
User unable to authorise – a timeout occurred	Redirect 302	17authorization_failur e (or) access_denied	Timeout occurred during authorisation.
In a two-page environment, the IDGW was unable to authenticate the User.	Redirect 302	17authorization_failur e (or) access_denied	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but did not authorise the action/transaction	Redirect 302	17authorization_failur e (or) 17authorization_denied (or) access_denied	User authenticated, but did not authorise the proposed action.
The requested Authorisation service has not been implemented.	Redirect 302	invalid_request	Requested authorisation service is not supported.

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
The requested Authorisation service has been implemented but is not available due to an internal error. (IDGW has capability to return an error through <code>redirect_uri</code>).	Redirect 302	<code>server_error</code>	Requested authorisation service is temporarily unavailable.
The requested Authorisation service has been implemented but is not available due to an internal error. (IDGW does not have capability to return an error through <code>redirect_uri</code>).	500	<code>server_error</code>	Requested authorisation service is temporarily unavailable.
Binding message does not exist (or) is invalid	Redirect 302	<code>invalid_request</code>	REQUIRED parameter <code>binding_message</code> is missing.
Context parameter does not exist (or) is invalid	Redirect 302	<code>invalid_request</code>	REQUIRED parameter <code>context</code> is missing.
<code>Client_name</code> does not exist	Redirect 302	<code>invalid_request</code>	REQUIRED parameter <code>client_name</code> is missing.
<code>Client_name</code> parameter exists, but its value is not registered at the Operator IDGW	Redirect 302	<code>invalid_request</code>	Malformed request. Invalid/unregistered <code>client_name</code> .

Table 5: Mobile Connect Authorisation: Errors – Device-Initiated Authorization Response

Further details on response formats can be found in [6].

A.3 Error Responses in Server-Initiated Mode

For Server-Initiated mode, errors can be returned in the following situations:

- In response to an OIDC Authorization Request (OIDC Authorization Response) from the IDGW Server-Initiated Authorization Endpoint once a request has been received and validated.
- In the Token Response to the SP's Notification Endpoint, where there is an error in processing the request.
- Where the SP is unable to process the Token Response and an error is returned in the Notification Acknowledgement back to the Operator IDGW.
- In the Polling Response, where there is an error in processing the request.

Errors are returned as described in the Mobile Connect Server-Initiated OIDC Profile [7].

Table 6, Table 7, Table 8 and Table 9 show the possible error codes and descriptions related to the Mobile Connect Authorisation services in Server-Initiated Mode.

A.3.1 Error Responses: OIDC Authorization Response

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
Binding message does not exist or is invalid	Bad Request 400	<code>invalid_request</code>	REQUIRED parameter <code>binding_message</code> is missing.
Context parameter does not exist or is invalid	Bad Request 400	<code>invalid_request</code>	REQUIRED parameter <code>context</code> is missing.
<code>Client_name</code> does not exist	Bad Request 400	<code>invalid_request</code>	REQUIRED parameter <code>client_name</code> is missing.
<code>Client_name</code> parameter exists, but its value is not registered at the Operator IDGW	Bad Request 400	<code>invalid_request</code>	Malformed request. Invalid/unregistered <code>client_name</code> .
The requested authorisation service has not been implemented.	Bad Request 400	<code>invalid_request</code>	Requested authorisation service is not supported.
The requested authorisation service has been implemented but is not available due to an internal error.	Service Unavailable 503	<code>server_error</code>	Requested authorisation service is temporarily unavailable.

Table 6: Mobile Connect Authorisation: Errors – Server-Initiated Authorization Response

A.3.2 Error Responses: Notification

Error Scenario	Error code	Error Description [RECOMMENDED text]
In a single-page environment, the User failed to approve the proposed action/transaction (or) the IDGW was unable to authenticate the User.	20uthorization_failur e (or) access_denied	User failed to authorise the proposed action.
In a single-page environment, the User cancelled or rejected the Mobile Connect authorisation request on their mobile device	20uthorization_denied (or) 20uthorization_failur e (or) access_denied	User rejected/cancelled the request for authorisation.
User unable to authorise – a timeout occurred	20uthorization_failur e (or) access_denied	Timeout occurred during authorisation.
Requested Authorisation service has been implemented, but is not available due to an internal error.	Server_error	Requested authorisation service is temporarily unavailable.
In a two-page environment, the IDGW was unable to authenticate the User.	20uthorization_failur e (or) access_denied	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but did not authorise the action/transaction	20uthorization_failur e (or) 20uthorization_denied (or) access_denied	User authenticated, but did not authorise the proposed action.

Table 7: Mobile Connect Authorisation: Errors – Server-Initiated Notification

A.3.3 Error Responses: Notification Acknowledgement

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

Table 8: Mobile Connect Authorisation: Errors – Server-Initiated Notification Acknowledgement

A.3.4 Error Responses: Polling Response

Error Scenario	HTTP Mode	Error code	Error Description [RECOMMENDED text]
In a single-page environment, the User failed to approve the proposed action/transaction (or) the IDGW was unable to authenticate the User.	Forbidden 403	21authorization_failure (or) access_denied	User failed to authorise the proposed action.
In a single-page environment, the User cancelled or rejected the Mobile Connect authorisation request on their mobile device	Forbidden 403	21authorization_denied (or) 21authorization_failure (or) access_denied	User rejected/cancelled the request for authorisation.
User unable to authorise – a timeout occurred	Forbidden 403	21authorization_failure (or) access_denied	Timeout occurred during authorisation.
The requested Authorisation service has been implemented, but is not available due to an internal error.	Forbidden 403	server_error	Requested authorisation service is temporarily unavailable.
In a two-page environment, the IDGW was unable to authenticate the User.	Forbidden 403	21authorization_failure (or) access_denied	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but did not authorise the action/transaction	Forbidden 403	21authorization_failure (or) 21authorization_denied (or) access_denied	User authenticated, but did not authorise the proposed action.

Table 9: Mobile Connect Authorisation: Errors – Server-Initiated Polling Response

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor/Company
1.0	26/11/2019	Major Update, product definition and technical specifications are merged. New document	TG	Gautam Hazari/GSMA

B.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.