Mobile Connect Authentication Definition and Technical Requirements

Version 1.0

26 October 2019

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

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 authentication, authorisation and exchange of attributes, subject to User consent.

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

This document details the Mobile Connect Authenticate service, a solution which offers secure User authentication to SPs.

Mobile Connect Authentication is defined as two service variants:

- Mobile Connect Authenticate, offering a standard-level of assurance (LoA2 – single factor authentication) via a single User-click, and
- Mobile Connect Authenticate Plus, offering a higher level of assurance (LoA3 – two factor authentication) by challenging the User for a PIN or biometric[1]

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

In addition, in situations where the User is accessing the SP over a mobile network, based on Identity Gateway (IDGW) policies the Operator can authenticate the User towards the SP without any User interaction to provide a seamless (zero-click) authentication experience. This special case is considered as single-factor authentication (LoA2[2]).

This document includes a description of the Mobile Connect Authenticate and Authenticate Plus services, applicable use cases and the associated User journeys. It also contains details of 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] 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”)

[2] LoA2 is based on ISO 29115 standard which is used for single-factor Mobile Connect services.

1.2 Scope of the document

In Scope	Out of Scope
• Mobile Connect Authenticate/Plus functionality description • Mobile Connect Authenticate/Plus technical specifications	• Privacy and Trust Principles • UI/UX guidelines • Mobile Connect Authenticate/Plus commercial propositions • SP/developer implementation guidelines • Other Mobile Connect service definitions

1.3 Audience

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

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

1.4 Relationship to Other Mobile Connect Documentation

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

The Mobile Connect Technical Overview document [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 references the relevant documents for the reader to obtain further detail.

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

Detailed specifications for the Mobile Connect APIs (Mobile Connect Device-Initiated OIDC Profile [6] and Mobile Connect Server-Initiated OIDC Profile [7]) provide details for OIDC Authorization Requests & Responses and associated Token retrieval including examples and error codes. The Mobile Connect Server-Initiated OIDC Profile defines two methods for Token retrieval using Notification or using Polling.

1.5 Conventions

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

1.6 Terminology & Definitions

Mobile Connect specifications and related documents make use of terms that are defined by the OpenID Connect Core Specification [1] and supporting specifications and extended in 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 Request[3] (spelled with a 'z') throughout this document.

1.7 References

Ref	Doc Number	Title
[1]	OpenID Connect Core Specification	"An interoperable authentication protocol based on the OAuth 2.0 family of specifications" available at https://openid.net/specs/openid-connect-core-1_0.html
[2]	OIDF CIBA	OpenID Connect MODRNA Client Initiated Backchannel Authentication Flow 1.0 https://openid.net/specs/openid-connect-modrna-client-initiated-backchannel-authentication-1_0.html
[3]	RFC 2119	"Keywords for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at https://tools.ietf.org/html/rfc2119
[4]	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
[9]	IDY.16	Mobile Connect Product Manager's Lifecycle Handbook
[10]	IDY.33	API Exchange Functional Description
[11]	IDY.09	Mobile Connect Authenticator Options
[12]	IDY.10	Mobile Connect SIM Applet Authenticator
[13]	IDY.12	Mobile Connect Smartphone Application Authenticator
[14]	ADD A DOC NO	Mobile Connect Privacy Principles
[15]	IDY.35	API Exchange Discovery Specification

[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.

2 Mobile Connect Authentication

Mobile Connect Authentication relies on the User being in possession of their mobile device and responding to a prompt on that device (the Authentication Device[4]). The prompt itself will depend on the level of assurance (LoA) that the application requires (LoA2 or LoA3) and the type of Authenticator that has been used by the serving Operator's ID Gateway to prompt and authenticate the User.

SPs select which service variant they require by specifying the required LoA in the OIDC Authorization Request using the `acr_values` parameter (see Section 3.1) alongside the `scope` value for the Mobile Connect Authenticate service (see Table 3).

2.1 Use Case Examples

Mobile Connect Authentication supports a range of practical use cases as shown below:

Service	Example Use Cases
Mobile Connect Authenticate	• Simple universal log-in • An additional mechanism to provide a second factor of authentication to an existing authentication mechanism • Forgotten password and account recovery
Mobile Connect Authenticate Plus	• Secure 2-factor authentication without additional hard token • Log in to corporate services requiring a higher level of authentication. • Log in to government services requiring a higher level of authentication

Table 1: Use case examples

2.2 Mobile Connect Authenticate/Authenticate Plus Flow

Mobile Connect Authenticate is an entry-level authentication service which offers a basic level of assurance (LoA2). This requires the Operator, on receiving a Mobile Connect Authenticate request (OIDC Authorization Request) from an SP's application, to confirm that the User is in possession of their mobile device ("Something I have").

Mobile Connect Authenticate Plus combines two factors i.e. "*Something I have*" (device) and "*Something I know*"' (PIN) or "*Something I am*" (Biometric) to offer two-factor authentication (LoA3). This requires the Operator to confirm that the User is in possession of his or her mobile device and has entered a secret that they know (PIN) or have provided a biometric (e.g. a fingerprint) when prompted on their device. The Authenticate Plus service provides the SP with a higher level of assurance ensuring that this is the same individual who registered, rather than someone who has gained access to the User's device (as is the case with LoA2).

[4] Authentication is always conducted on the User's Authentication Device

The PIN/biometric is defined when the User sets up an appropriate Authenticator that supports LoA3 – this may be done at registration for Mobile Connect or as a subsequent step.

 shows a simplified authentication request flow for both Authenticate and Authenticate Plus services illustrating how the services are presented to the User, based on Device-Initiated mode where an SP's application is Mobile Connect enabled and the User accesses or consumes the service via a Consumption Device. Further details on the User Flows are provided in Section 2.5.

A request must be directed to the correct Operator IDGW using the correct SP credentials which may be obtained directly from the Operator or via the Mobile Connect Discovery service [10].

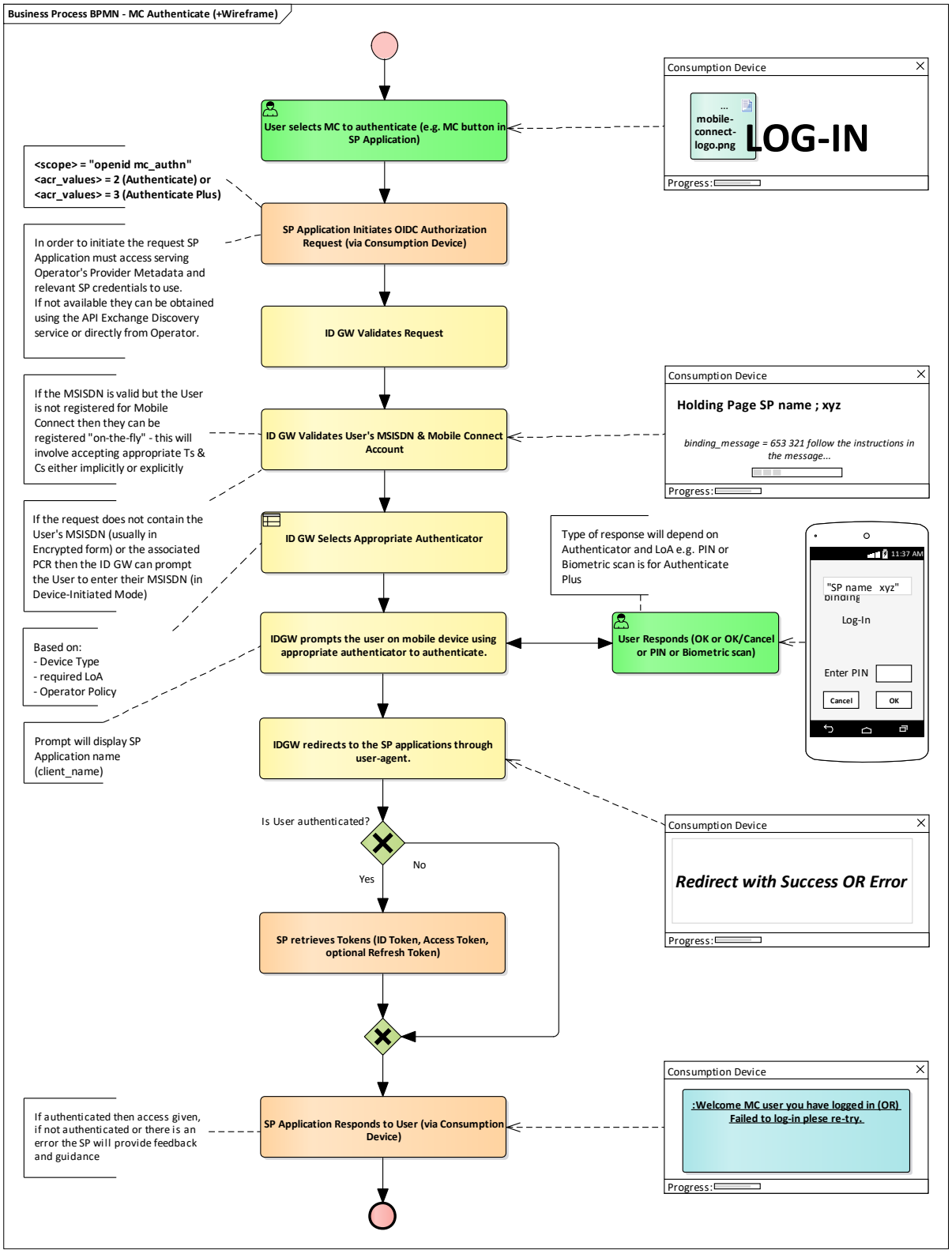
Mobile Connect Authentication services are also supported in Server-Initiated mode where the User is not interacting with the SP via a Mobile Connect enabled application (so there is no Consumption Device) hence the request is initiated directly by the SP – server to server.

One example of where a Server-initiated request might be used is in a call centre where a User is connected to a customer care agent over the phone, and the customer care agent needs to authenticate the User. In this scenario, the call centre can initiate a Mobile Connect service request using a back-end application, providing the phone number in the request that it has on the User's file.

The Mobile Connect Server-Initiated OIDC Profile [7] defines two Server-Initiated mode variants relating to the method that is used for returning tokens to the SP upon successful authentication - using notification or polling. The SP application must register for Mobile Connect Authentication using Device-Initiated mode and/or one of the Server-Initiated modes, depending upon what is supported by the Operator IDGW.

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. The Mobile Connect Device-Initiated OIDC Profile [6], and the Mobile Connect Server-Initiated OIDC Profile [7] define the API calls and responses for each mode.

Table 2 below indicates the suitability of common Authenticators for Mobile Connect Authenticate and Mobile Connect Authenticate 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].



- **: Mobile Connect Authentication Request Flow**

Authenticator	Authenticate	Authenticate Plus	Comments
Seamless Authentication	Yes	No	Using HTTP Header Enrichment or an alternate method of

			obtaining the network-authenticated MSISDN when accessing via the mobile data network, where supported.
USSD (Network Initiated)	Yes	No	Can technically support LoA3 but is not sufficiently secure as the PIN would be transported over the mobile network in plain text
SMS+URL	Yes	No	Recommended for LoA2 only.
SIM-Applet	Yes	Yes	Can support any LoA values.
Smartphone App Authenticator (SAA)	Yes	Yes	Can support biometrics as well as PIN

Table 2: Authenticator suitability for Mobile Connect Authentication

In the case where an SP requests Mobile Connect Authenticate and the serving Operator supports seamless authentication, it is expected that the Operator will typically do the following:

- If the User is on-net, the Operator will perform seamless authentication and return a response to the SP
- If the User is off-net, the Operator will revert to an explicit authentication (such as USSD or SMS+URL)

Note that there may be scenarios in which the SP requires the User to be explicitly authenticated, for instance where Mobile Connect Authenticate is being used for second factor authentication and hence User interaction is key. In such scenarios, the SP can override the seamless authentication through inclusion of `prompt=no_seam` in their OIDC service request.

2.3 Authentication Response

A successful authentication results in the return of an ID Token and an Access Token to the SP Application. An error will be returned if the authentication is not successful.

The ID Token provides confirmation of the successful authentication and includes a Pseudonymous Customer Reference (PCR) identifying the User which can be used in subsequent Mobile Connect service requests. For Authenticate and Authenticate Plus services, the Access Token is generated but is not used. After a User has been authenticated for the first time with Mobile Connect, the SP Application can store the PCR associated with the User, the serving Operator details (issuer ID (`iss`), openid-configuration URL), appropriate credentials (client_id) and sector identifier to be used.

2.4 Mobile Connect Account Setup

If the User has not previously registered, they may 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 this case Operators must follow up with the User to complete registration. The Mobile Connect Product Manager’s Lifecycle

Handbook provides further information of on the Mobile Connect account and “on-the-fly” registration [9].

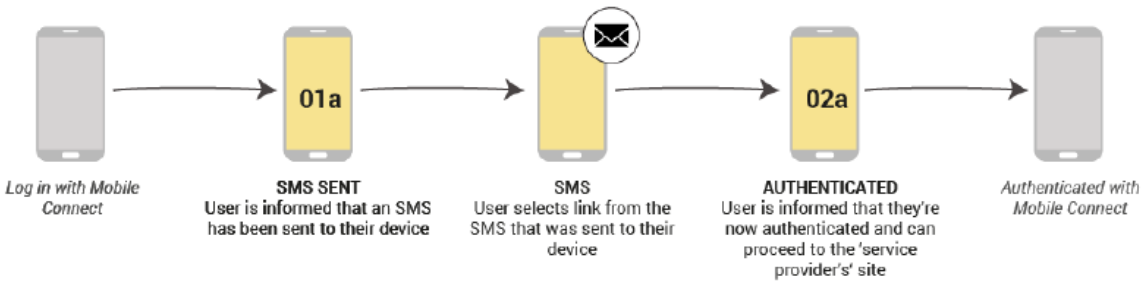
Note: That on-the-fly registration should only be used for Mobile Connect Authenticate service requests (i.e. single-factor authentication) – for Mobile Connect Authenticate Plus (two-factor authentication), it is imperative that the individual is authenticated prior to being allowed to register a PIN hence this process needs to be handled separately by the Operator (e.g., by the User authenticating/logging in to their Operator’s self-care portal and then initiating an LoA3 Mobile Connect registration from there).

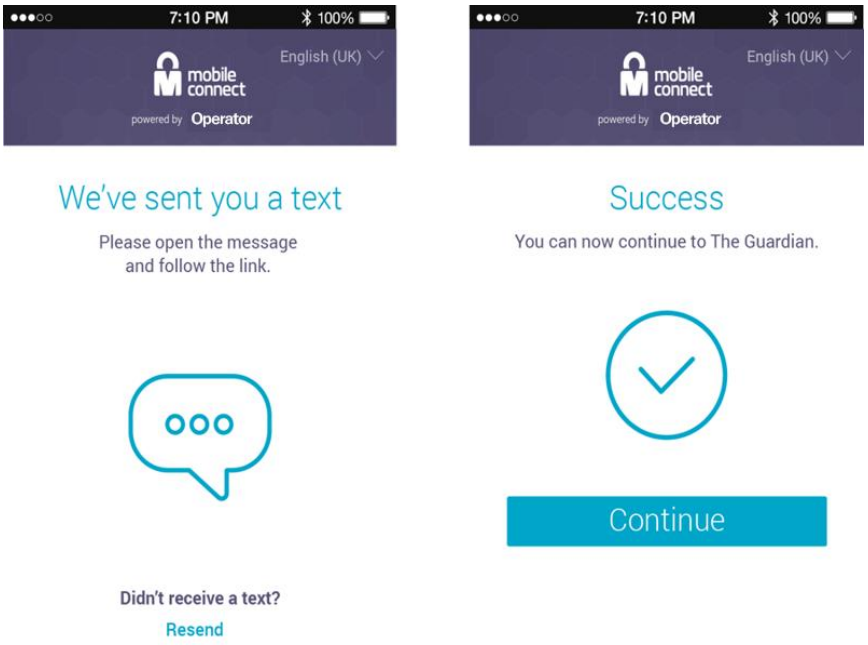
2.5 User Flow Examples

Authentication User journeys depend on many factors including:

- Service type (Authenticate or Authenticate Plus)
- The Mode of Operation – Device-Initiated or Server-Initiated
- The Authenticator that is selected by the Operator
- The device on which the service is consumed (the Consumption Device)
- How the device is connected to the internet (e.g. Mobile Data Connection or Wi-Fi)
- Whether the User is already registered with Mobile Connect
- Whether the SP application is aware of the Mobile Connect API endpoints to be used (and the respective credentials)

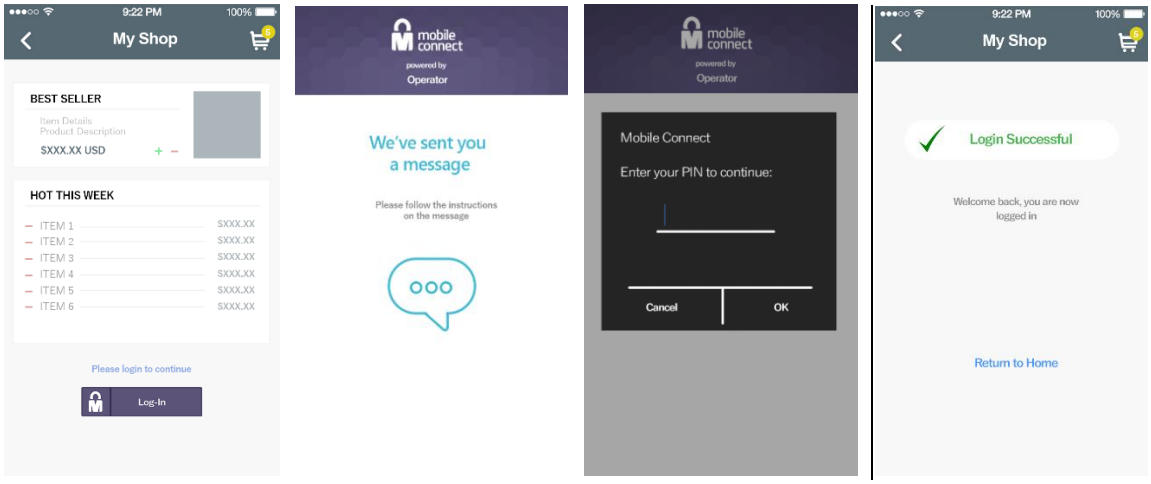
The User journeys will vary depending on a combination of the above factors and therefore it may take many potential paths depending on preconditions. shows an authentication experience on a consumption device for Mobile Connect Authenticate where SMS with embedded URL is used as the Authenticator.





- **: Mobile Connect Authenticate User journey example**

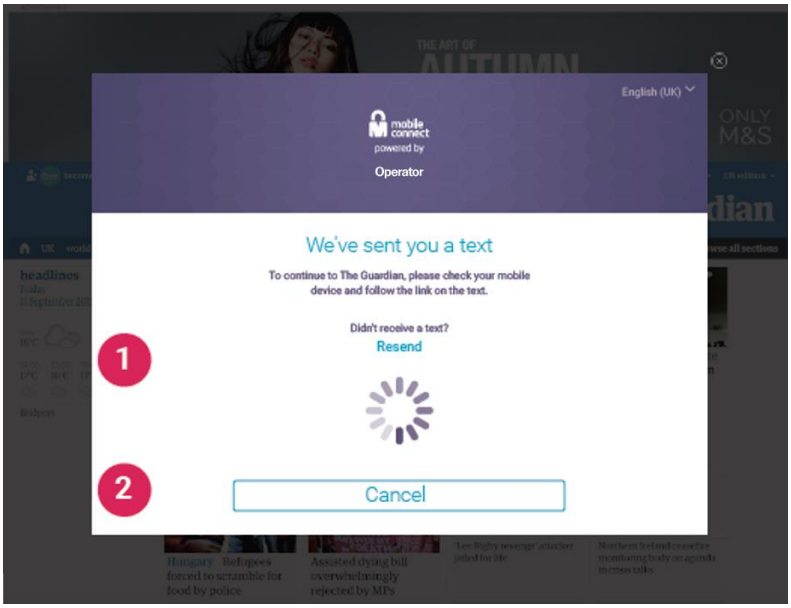
 shows an authentication experience on a consumption device for Authenticate Plus where both the Consumption Device and Authentication Device are the User's mobile device.



- **: Authenticate Plus User journey example**

Note:

- For simplicity, the Discovery screen which the User may need to be presented with to determine their MSISDN (and hence their Operator) after choosing to log into the SP's application with Mobile Connect is not shown in this example.
- The consumption device represented is the mobile phone, i.e. the mobile phone is both the consumption device and authentication device in this example.
- An example of the waiting screen is shown in for scenarios where the consumption device is a personal computer.



- **: An example of a Holding page on a PC or similar**

2.6 Using Mobile Connect with Existing Authentication Systems

SPs may choose to use Mobile Connect either as the primary login mechanism or as a second factor to complement an existing Username/password based approach.

In either case, the SP will need to store the relevant Mobile Connect information in their User's account (associated with the SP's application) (See Section 2.3) This data would be stored alongside existing log-in credentials where Mobile Connect is being used for step-up (second factor) authentication.

In the situation where a User already has an account with the SP (or the intention is to use Mobile Connect as a complement to an existing login mechanism), the SP will need to authenticate the User first (e.g., via Username/password) so that they know which User they're dealing with and then initiate an authentication via Mobile Connect and then store the relevant information against that User's account. Mobile Connect can then be used going forward either as the primary login mechanism, or as a step-up authentication when needed.

3 Authenticate / Plus Service Specification

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

3.1 OIDC Authorization Request Parameters - `scope` and `acr_values`

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

Mobile Connect Service	`scope` value[5]	LoA (`acr_values`)
Mobile Connect Authenticate	"openid mc_authn"	2
Mobile Connect Authenticate Plus	"openid mc_authn"	3

Table 3: Mobile Connect Authentication `scope` and `acr_values`

3.2 API Modes Supported

Mobile Connect Authentication can be used in both Device-Initiated and Server-Initiated Modes. An Operator can support one or the other mode or both, depending on the requirements from target customers (SPs) within their market. Importantly, Operators supporting Mobile Connect within a 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 Authenticate and Authenticate Plus. These should be used in conjunction with the following requirements in the implementation of these Mobile Connect services:

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
MC_AUTHN_01	Support of Service	For Mobile Connect Authenticate, the IDGW must support single factor authentication (LoA2) via a User's mobile device using an appropriate authenticator. Note that Seamless authentication, where supported, can be used for single-factor authentication.
MC_AUTHN_02	Support of Service	For Mobile Connect Authenticate Plus, the IDGW must support two factor authentication (LoA3) via a User's mobile device using an appropriate authenticator. Note that Seamless authentication, where supported, cannot be used for two factor authentication.
MC_AUTHN_03	Service Registration	The IDGW must be able to allow a SP (client application/service) to register for Mobile Connect Authentication services (Mobile Connect Authenticate and Mobile Connect Authenticate Plus) in either Device-Initiated mode or Server-Initiated mode as defined in the Mobile Connect Device-Initiated OIDC Profile and the Mobile Connect Server-Initiated OIDC Profile, depending upon what modes are supported by the IDGW.
MC_AUTHN_04	Service Invocation	For Mobile Connect Authentication services, the IDGW must be able to accept and process an Mobile Connect

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

		Authenticate service request from a registered SP in accordance with the Mobile Connect Device-Initiated Profile or the Mobile Connect Server-Initiated Profile, as appropriate.
MC_AUTHN_05	Service Invocation	The SP will specify the required Mobile Connect Authentication service via the scope parameter and associated acr_values parameter within the OIDC Authorization Request as specified in Section 3 of Mobile Connect Authentication Definition and Technical Requirements. The IDGW must support the use of these scope values for Mobile Connect Authentication services. Where seamless authentication is offered, the IDGW must also support use of the prompt="no-seam" within the OIDC Authorization Request so that an SP can override the use of seamless authentication for specific use cases.
MC_AUTHN_06	Service Request - Validation	The IDGW must validate the submitted Mobile Connect Authentication service request and request parameters as defined in the Mobile Connect Device-Initiated OIDC Profile or the Mobile Connect Server-Initiated OIDC Profile, as appropriate.
MC_AUTHN_07	Service Request SP Validation	The IDGW must check that the SP is registered for the requested Authentication 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.
MC_AUTHN_08	Service Request - User Validation	The IDGW must check whether the Mobile Connect User is already registered and has a Mobile Connect account. If not, it must provide on-the-fly[6] registration before processing the Mobile Connect Authentication request.
MC_AUTHN_09	Service Request - Device-Initiated mode	In the case where the service is being requested in DI-mode, the IDGW should present a holding page to the User on the Consumption Device, referring them to their mobile phone to authenticate.
MC_AUTHN_10	Service Request - Prompt	The Mobile Connect Authentication service must present a prompt to the User via the authenticator that includes the SP's Application's registered Client name. client_name is included within an OIDC Authorization Request but the IDGW must compare this against the client_name submitted by the SP when the Application was registered with Mobile Connect and ensure they match.
MC_AUTHN_11	Token Response	The Mobile Connect Authentication service must return to the initiating SP application: - a positive result, or - a negative result with an appropriate error code and error

[6] Implementations can provide the Mobile Connect registration mechanism differently if on-the-fly registration is not possible, entirely based on their local policies and local regulations. However, before serving the Mobile Connect service the User must accept the Mobile Connect terms and conditions, thus successfully registering for Mobile Connect services

		description. Note that a positive result will provide an ID Token and an Access Token. The ID Token will include a PCR (uniquely identifying that User to the SP's client) and details of the User authentication. 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 Mobile Connect Authentication Definition and Technical Requirements.
MC_AUTHN_12	Error Responses	Error Responses may be returned at different stages of the processing of an OIDC Authorization 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 Authentication services. These errors are generic to all Mobile Connect services. Service Specific Error Responses are specified in Annex A of Mobile Connect Authentication Definition and Technical Requirements and must be supported for Mobile Connect Authentication services.
MC_AUTHN_13	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 Authentication this should include: • Date & Time • MSISDN and PCR • Service type requested (i.e. scope parameter + acr_values) • User Response (approve, timeout or Authentication 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 Authentication Services

Annex A Mobile Connect Authentication Service Specific Error Codes and Descriptions

This Annex specifies the service specific error codes and associated descriptions that are REQUIRED for Mobile Connect Authentication 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 Error Responses for Device-Initiated Mode

Table 5 lists the additional error codes and descriptions for Mobile Connect Authentication that are returned from the Authorize Endpoint for Device-Initiated mode.

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
User failed to authenticate (e.g. invalid pin)	Redirect 302	`authentication_failure` [or] `access_denied`	User failed to authenticate.
User cancelled or rejected the authentication request on their mobile device	Redirect 302	`authentication_denied` (or) `authentication_failure` (or) `access_denied`	User rejected/cancelled the authentication.
User was prompted for authentication, but a timeout occurred.	Redirect 302	`authentication_failure` (or) `access_denied`	Timeout occurred during authentication.

Table 5: Mobile Connect Authentication: Errors - Device-Initiated Authorization Response

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

A.2 Error Responses for 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 (Token) 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 Authentication service.

A.2.1 Error Responses: OIDC Authorization Response

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
The requested authentication service has not been implemented.	Bad Request 400	`invalid_request`	Requested authentication service is not supported.
The requested Authentication service has been implemented, but is not available due to an internal error.	Service Unavailable 503	`server_error`	Requested authentication service is temporarily unavailable.

Table 6: Mobile Connect Authentication: Errors - Server-Initiated Authorization Response

A.2.2 Error Responses: Notification

Error Scenario	Error code	Error Description [RECOMMENDED text]
User failed to authenticate (e.g. invalid pin)	`authentication_failure` (or) `access_denied`	User failed to authenticate.
User cancelled or rejected the authentication request on their mobile device	`authentication_denied` (or) `authentication_failure` (or) `access_denied`	User rejected/cancelled the authentication.
User was prompted for authentication, but a timeout occurred.	`authentication_failure` (or) `access_denied`	Timeout occurred during authentication.

Table 7: Mobile Connect Authentication: Errors - Server-Initiated Notification

A.2.3 Error Responses: Notification Acknowledgement

Error Scenario	HTTP mode	Error Code	Error Description [RECOMMENDED text]
Invalid ID Token	Bad Request 400	`invalid_request`	ID Token is invalid.

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

A.2.4 Error Responses: Polling

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
User failed to authenticate (e.g. invalid pin)	403 Forbidden	`authentication_failure` (or) `access_denied`	User failed to authenticate.

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
User cancelled or rejected the authentication request on their mobile device	403 Forbidden	`authentication_denied` (or) `authentication_failure` (or) `access_denied`	User rejected/cancelled the authentication.
User was prompted for authentication, but a timeout occurred.	403 Forbidden	`authentication_failure` (or) `access_denied`	Timeout occurred during authentication.

Table 9: Mobile Connect Authentication: 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	26/10/2019	New Document Mobile Connect Authentication (Authenticate and Authenticate+) specifications.	TG	Yolanda Sanz/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.