IDY.24 Mobile Connect Account Takeover Protection Definition and Technical Requirements

Version 2.0

06 December 2022

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 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 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 enableMC services, the serving Mobile Operator selecting an appropriate Authenticator (where required) based on Operator policy, regulatory requirements, privacy principles, device capability and the Level of Assurance required by the SP.

This document details the Mobile Connect Account Takeover Protection (ATP) service. Mobile Connect ATP provides a mechanism through which a SP can submit a request to the User's Operator (using the User's mobile phone number (MSISDN)) to obtain information on any recent SIM pairing change related to the User's mobile account.

1.2 Scope

In Scope	Out of Scope
• Mobile Connect Account Takeover Protection (ATP) functional description • Mobile Connect Account Takeover Protection technical specifications • Mobile Connect Account Takeover Protection in Server-Initiated mode.	• Provision of any User information (such as customer category) to complement the ATP result • Detailed Privacy and Trust Principles • UI/UX guidelines • Mobile Connect ATP commercial propositions • Service provider / developer implementation guidelines • Mobile Connect Account Takeover Protect implementation in Device-Initiated mode.

1.3 Abbreviations

Term	Description
API	Application Programming Interface
ATP	Account Takeover Protection
CIBA	Client Initiated Backchannel Authentication
HTTP	Hyper Text Transport Protocol
ID GW	Identity Provider: The entity providing the authentication and Identify services, e.g. the operator
IMSI	International Mobile Subscriber Identity
LoA	Level of Assurance

Term	Description
MSISDN	Mobile Station International Subscriber Directory Number
OIDC	OpenID Connect
PCR	Pseudonymous Customer Reference
RFC	Request For Comments
SIM	Subscriber Identification Module
SP	Service Provider
URL	Uniform Resource Locator

1.4 Audience

The target audience for this document are product managers and service/technical departments and Operators who are considering deploying the Mobile Connect Account Takeover Protection service.

Readers of this document are expected to have familiarity with and a good understanding of the Mobile Connect Technical architecture and Mobile Connect Core requirements [5] and Mobile Connect Resource server specification [8].

1.5 Relationship to Other Mobile Connect Documentation

This document details the Mobile Connect ATP service and its usage. It includes the relevant technical parameters for the service, such as `scope` value and any service specific error codes. It also includes technical requirements that relate to the ATP service. These service-specific elements build upon the Mobile Connect core framework. The ATP service is recommended to be used in Server-Initiated mode using Mobile Connect Server-Initiated OIDC profile [7].

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.

The Mobile Connect Resource Server Specification [8] provides details on how to handle a resource request and the associated response for Mobile Connect attribute services including error codes. It also includes requirements that are common to all Mobile Connect attribute services, which apply to the Mobile Connect ATP service.

The Mobile Connect Technical Overview [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.

GSMA Regulatory requirements for personal data handling is detailed in 'GSMA Regulatory considerations for processing personal data and attributes for Mobile Connect'. Mobile Connect Privacy Principles.

1.6 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]

1.7 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) specification [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[1] (spelled with a 'z') throughout this document.

1.8 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 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

[1] 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 MC Authorisation, hence MC specifications have adopted the term "OIDC Authorization Request" to describe this initial service request in the protocol flow.

2 Mobile Connect Account Takeover Protection (ATP)

Mobile Connect ATP allows SPs to check attributes associated with a User's mobile account to provide a secure method of combatting identity fraud.

Many online banking accounts today are protected using secure online banking credentials (e.g., password and secret customer number), and additionally using the phone number associated with the User's bank account to increase security. This two-factor security helps mitigate fraud if one of the factors is compromised, for example if the User's online banking credentials have been stolen.

Mobile Connect ATP allows SPs to perform additional checks on the User's mobile phone status to determine whether or not this factor may have been compromised. In particular, the service returns an indication of whether there has been a recent SIM swap and may optionally return other information relating to the User's mobile account:

- Recent SIM change (MSISDN - IMSI pairing) - REQUIRED
- Active unconditional call diverts - OPTIONAL
- Device reported lost or stolen - OPTIONAL
- Recent device change (Timestamp of last MSISDN - IMEI pairing change) - OPTIONAL
- Mobile phone account status (active or inactive) – OPTIONAL

2.1 Use Case Examples

Mobile Connect ATP offers a range of practical use cases. Some of the use cases identified for implementation are listed in the table below:

Product	Example Use Cases	Attributes Involved
Mobile Connect Account Takeover Protection	1. Prevention of various types of fraud in banking such as SIM swap fraud 2. Making SMS one-time passwords more secure 3. Secure authentication (authenticate + ATP) 4. Securing add new payee transactions in banking	SIM Swap, Lost / Stolen, Unconditional Call divert status, Device change

Table 1: Use Case Examples

The key aim of the Mobile Connect ATP service is to flag to a SP whether the User's SIM has recently been changed which might indicate fraud where the attacker is attempting to circumvent a SPs second-factor authentication on a mobile device. Depending on Operator implementation, the service may also provide additional information such as whether the device has been reported lost or stolen, or whether the User's SIM has been swapped to a different mobile device.

3 Mobile Connect ATP Service Flow

The Mobile Connect ATP service can be supported in the Server-Initiated mode as a background service.

Note: That Operators within the same market should deploy and operate the Mobile Connect ATP service in the same way.

The SP must register for the Mobile Connect ATP service using Server-Initiated mode.

The SP typically will use the User's mobile number (MSISDN) in order to submit an ATP service request but can also use a PCR. The ATP request will occur in the background without involving the User hence allowing the SP to request an ATP check if the SP suspects fraud (assuming that consent where required is captured separately).

Figure 1 shows a high-level flow for the Mobile Connect ATP service based on the Server-Initiated mode. The Mobile Connect Technical Architecture and Core Requirements [6] provides more detailed sequence diagrams illustrating the flow for the Server-Initiated modes. The Mobile Connect Server-Initiated OIDC Profile [8] define the API calls and responses for each mode.

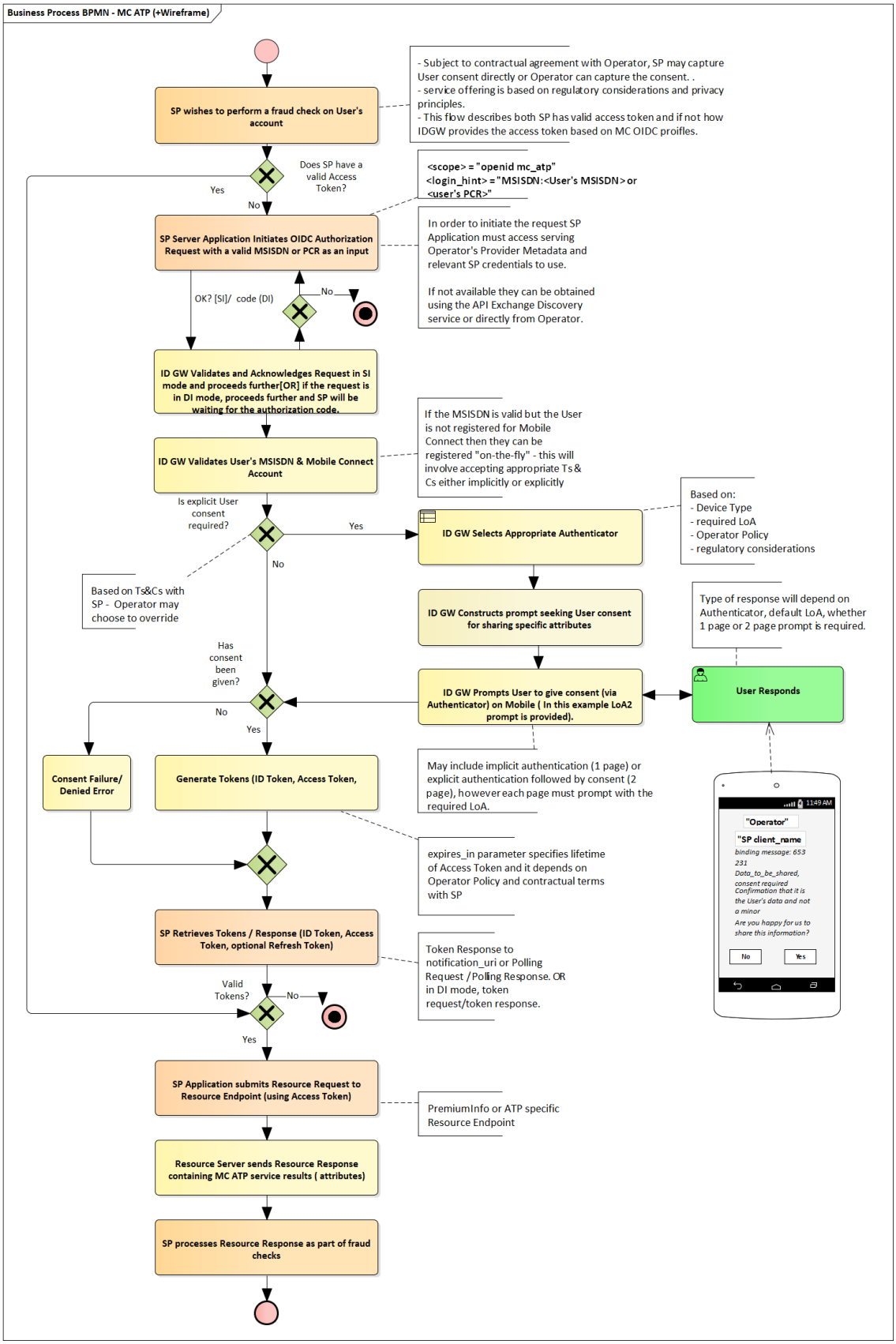

Figure 1: Mobile Connect Account Takeover Protection Service Flow

- The SP wishes to make an ATP service request for this User.
    - If this is the first time that an ATP service request has been made for the User then it may be necessary to obtain the relevant Operator ID GW details (Mobile Connect Provider Metadata [5]5]) for this User using the API Exchange Discovery service. These details can then be stored for future use.
    - If the SP has previously requested the service and has an unused and existing valid Access Token, then a Resource Request can be made directly to the applicable Resource Endpoint specified by the Operator.
    - Otherwise a full Mobile Connect API request (OIDC Authorization Request) is made to the Operator ID GW Authorization Server using the User's MSISDN or PCR as an identifier and specifying the ATP service using the `scope` parameter.
    - If the User has for some reason revoked consent, then the SP should not make the request until the User has given their consent again.

  Note: That the User should have flexibility to block the SP, to revoke the already given consent and to request explicit transaction-based consent to protect the User's personal data.

- The Operator validates the request and confirms if the SP has registered for Mobile Connect ATP in accordance with the Operator's ID GW policy. In the event of an error, the request is terminated, and an error response is returned to the SP Server.
- Assuming the request is valid, the Operator processes the request and returns an ID Token (security token), an Access Token which is used to retrieve the requested attributes (as specified in this document) from the relevant Resource Endpoint.
- Figure 1 for completeness includes a consent flow whereby the ID GW seeks User consent for sharing the ATP information via the User's mobile device (Authentication Device). Note though that such transactional-based consent is not recommended for the Mobile Connect ATP service – more discussion on the legal options for acquiring User consent can be found in section 3.1 and GSMA Regulatory considerations for processing personal data and attributes for Mobile Connect
    - If consent is requested by the ID GW and not given, or the Operator has insufficient proof that User consent has been captured by the SP, then an error message should be generated and returned to the SP instead of the Tokens.
- In Server-Initiated mode, the SP can retrieve the ID Token and Access Token in one of two ways depending on what is supported by the ID GW in the server-initiated mode: using notification where the Tokens are sent to the SP's specified Notification Endpoint or by the SP polling the ID GW Polling Endpoint until a full response is obtained. Further details are provided in the Mobile Connect Server-Initiated OIDC Profile specification [7].
- Assuming the request was successful, the SP receives the ID Token and Access Token and then uses the Access Token to make a Resource Request to the applicable Resource Endpoint in order to obtain the requested information.

3.1 Considerations for Lawful Handling of User Data

Operators may be subject to general data protection laws and telecom specific rules that place conditions and obligations on the use of customer information. Attributes held by Operators may fall into several legal categories of regulated and protected data. SPs will also be subject to some of these obligations and must not use the data obtained from a Mobile Connect service request for anything other than the stated purpose.

Operators are recommended to perform due diligence that a SPs processes are suitable to meet these obligations and that those obligations are clear within the contract between the Operator and the SP. This is discussed in more detail in the Mobile Connect Product Manager's Lifecycle Handbook [9].

Consent from the User for the sharing of the ATP information may be captured either by the SP or the User's Operator, and either as part of a transaction or separately through another business process.

Note: Though that capturing consent within the transaction will alert the fraudster that the SP is using ATP checks thereby reducing the effectiveness of this service in combating fraud – it is therefore recommended that consent is captured from the User as a part of a separate business process.

'GSMA Regulatory considerations for processing personal data and attributes for Mobile Connect' provides more discussion on the legal basis for providing services such as Mobile Connect ATP. The Mobile Connect privacy principles should also be consulted.

4 Account Takeover Protection Service Specification

This section is normative and contains the relevant information required by Operators to implement and support the Mobile Connect Account Takeover Protection service.

4.1 OIDC Authorization Request Parameters - `scope`

The Mobile Connect ATP service is requested by including within the `scope` parameter in the Mobile Connect request (OIDC Authorization Request) the value shown in Table 2.

Mobile Connect Service	Scope
Mobile Connect ATP	`"openid mc_atp"`

Table 2: Mobile Connect ATP `scope` Value

4.2 API Modes Supported

The Mobile Connect ATP service is recommended to be supported in Server-Initiated Mode [[7]; Attribute Set.

Table 3 shows the attribute set returned by the Mobile Connect ATP service.

Attribute Name	Usage Category	Description
`sim_change`	REQUIRED	Timestamp of last MSISDN <-> IMSI pairing change [RFC 3339 absolute timestamp format]

Attribute Name	Usage Category	Description
is_unconditional_call_divert_active	OPTIONAL	Mobile phone account has an unconditional call divert set to a number; Returns true or false
is_lost_stolen	OPTIONAL	Returns true or false
device_change	OPTIONAL	Timestamp of last MSISDN <-> IMEI pairing change [RFC 3339 absolute timestamp format]
account_state	OPTIONAL	Status of the mobile phone account: “active” or “inactive”

Table 3: Mobile Connect ATP attribute set

An Operator ID GW MUST provide the REQUIRED attributes.

An Operator ID GW MAY provide any of the OPTIONAL attributes

Note: That all Operators within a market MUST agree on the final attribute set to ensure consistency within that market.

An Operator ID GW may offer additional attributes to complement the attributes shown in Table 3; this is at their discretion and are not covered by this service definition.

4.3 Service Specific Requirements

Table 4 defines the service-specific requirements relating to the Mobile Connect ATP service. 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.
- Resource Server and Attribute Services Requirements specified in the Mobile Connect Resource Server Specification [8]. Note that these are common to all Mobile Connect attribute services. Service specific requirements may further refine or qualify the more general requirements for attribute services.

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

Requirement No.	Category	Description
MC_ATP_01	Service Registration	The ID GW must be able to allow a SP (client application / service) to register for the Mobile Connect ATP service and be provisioned with the requisite SP-provided parameters dependent on whether the SP intends to use Server-Initiated mode with notification or polling when requesting the service and what modes are supported by the ID GW. See the Mobile Connect Server-Initiated OIDC Profile.
MC_ATP_02	Supported Attributes	The service should support the attributes specified within Table 3. Note that attributes marked as ‘REQUIRED MUST be supported; attributes marked as OPTIONAL MAY be supported (at the Operator’s discretion)

		Note: The Operator may optionally include additional attributes (claims) in the response to provide the SP with further information such as User market segment (pre/post/business/unknown). This is up to the Operator and out of scope of the Mobile Connect ATP specification.
MC_ATP_03	Service Invocation	A SP must be able to request the service through use of the appropriate scope parameter value in the service request as specified in Table 2.
MC_ATP_04	Service Modes	The service can be implemented either SI mode notification only, SI mode polling only or both, depending on the market requirements.
MC_ATP_05	Tokens	The ID GW Authorization Server must issue Access Tokens with 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 based on the regulatory requirements.
MC_ATP_06	Tokens	The ID GW must not issue a refresh token for the Mobile Connect Account Takeover Protection service. If it is issued the value must be set to null.
MC_ATP_07	Consent Capture	Based on the regulatory requirements, contract between SP and Operator, either the Operator or SP must capture consent from the User for the sharing of information within the Mobile Connect ATP service. For more details refer [9].
MC_ATP_08	Revocation	The Operator should ensure that a User is able to revoke their consent.
MC_ATP_09	Consent Failure	In the situation where an Operator needs to capture User consent itself within the transaction, the ID GW must return an error, if it is unable to capture the consent from the User as defined Annex A.
MC_ATP_10	Resource Response	The service should return values for those attributes specified in Table 3 that the Operator is providing in their service to the SP. If the service is unable to provide a value for one of the attributes for a particular User, then the attribute should be returned with an empty value in the Resource Response.
MC_ATP_11	Resource Response	The ID GW must expose either the PremiumInfo Endpoint or an ATP service specific resource endpoint through which the SP can retrieve the attributes. For more information see the Resource Server Specification [8].
MC_ATP_12	Prompt Length	For interoperability purposes the maximum prompt length on the Authentication Device via the selected Authenticator should be <= 220 bytes. This requirement is applicable if Operator prompts the User on their mobile device.

MC_ATP_12	Error Responses	Error Responses may be returned at different stages of the processing of an OIDC Authorization Request as specified in the MC Device-Initiated OIDC Profile and the MC Server-Initiated OIDC Profile and must be supported for the service. Errors may also be generated because of processing of the Resource Request at the Resource Server as specified in the Mobile Connect Resource Server document and must be supported for the service. These errors are generic to Mobile Connect services and Mobile Connect attribute services, respectively. Service Specific Error Responses are specified in Annex A.
MC_ATP_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 this should include: • Phone number (MSISDN) • PCR • Date & Time • Service scope • Consent State (active, revoked) • Status (Complete, in-process, Error) • Error codes and error description • Time of consent capture (if the Operator captures consent) • Evidence of consent (as applicable)

Table 4: Mobile Connect Account Takeover Protection Service Requirements

Annex A Mobile Connect ATP Service Specific Error Codes and Descriptions

This Annex lists the service-specific error codes and associated descriptions that are REQUIRED for the service in addition to the generic error codes and descriptions that are specified in the relevant OIDC Profiles (MC Device-Initiated OIDC Profile [6] and MC Server-Initiated OIDC Profile [7]) and the Resource Server Specification [8].

Note: That error codes relating to transaction consent capture via a Mobile Connect authenticator are only applicable if the Operator captures transactional consent. Where transactional consent capture by the Operator is required, certain error codes are generated depending on whether the implementation of Mobile Connect Account Takeover Protection 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 attributes related information and seeking User consent on the second page.

A.1 Error Responses in Server-Initiated Mode

MC ATP typically operates in Server-Initiated mode. By default, no prompt will be displayed to the User unless the Operator's ID GW policy mandates the capture of User consent.

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

The following tables show the possible error codes and descriptions related to the Mobile Connect Account Takeover Protection service for Server-Initiated requests using either Notification or Polling for token retrieval.

A.1.1 Error Responses: OIDC Authorization Response

Error Scenario	HTTP mode	Error code	Error Description [RECOMMENDED text]
`client_name` parameter does not exist, whereas SP has registered multiple client names.	Bad Request 400	`invalid_request`	REQUIRED parameter `client_name` is missing.
`client_name` exists but is invalid (applicable to both scenarios, where SP has register either single or multiple client names[2].	Bad Request 400	`invalid_request`	REQUIRED parameter client_name value is invalid / not registered.

[2] The SP will register client_names parameter during registration, that can contain either one or multiple client names. The ID GW must maintain this list for verification.

Table 5: Errors – Server-Initiated Authorization Response

A.1.2 Error Responses: Notification

Error Scenario	Error code	Error Description [RECOMMENDED text]
In a single-page environment, the User failed to give consent (or) the ID GW was unable to authenticate the User (authentication failure).	`consent_failure` (or) `access_denied`	User failed to give consent (or) was not authenticated.
In a single-page environment, the User denied the request for consent.	`consent_denied` (or) `consent_failure` (or) `access_denied`	User has not given consent (or) consent failure.
The User was unable to give consent – a timeout occurred.	`consent_failure` (or) `access_denied`	Timeout occurred during consent capture.
In a two-page environment, the ID GW failed to authenticate the User on the first page.	`consent_failure` (or) `access_denied`	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but denied the request for consent	`consent_denied` (or) `consent_failure` (or) `access_denied`	User has not given consent (or) consent failure.

Table 6: Errors - Server-Initiated Token Response using Notification

A.1.3 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 7: Errors - Server-Initiated Notification Acknowledgement

A.1.4 Error Responses: Polling Response

Error Scenario	HTTP Mode	Error code	Error Description [REOMMENDED text]
In a single-page environment, the User failed to give consent (or) the ID GW was unable to authenticate the User (authentication failure).	Forbidden 403	consent_failure (or) access_denied	User failed to give consent (or) was not authenticated.
In a single-page environment, the User denied the request for consent.	Forbidden 403	consent_denied (or) consent_failure (or) access_denied	User has not given consent (or) consent failure.
The User was unable to give consent – a timeout occurred.	Forbidden 403	consent_failure (or) access_denied	Timeout occurred during consent capture.
In a two-page environment, the ID GW failed to authenticate the User on the first page.	Forbidden 403	consent_failure (or) access_denied	User was not authenticated.
In a two-page environment, the User was authenticated in the first step, but denied the request for consent	Forbidden 403	consent_denied (or) consent_failure (or) access_denied	User has not given consent (or) consent failure.

Table 8: Errors - Server-Initiated Polling Responses

Annex B Authenticators

The following table lists the general use authenticators and their suitability to service, if Operator prompts the User on their mobile device.

Mobile Connect Authenticator	Recommended for Consent Capture?	Explanation
SIM Applet	Yes	Supports LoA2 and LoA3 but there is limited space to display information - if the requirement is to list out all the attributes and their values within the consent screen, this may require multiple SIM applet pages.
Smartphone app	Yes	The smartphone app authenticator has plenty of space for displaying the consent prompt
USSD (network initiated USSD)	Yes	MC ATP OK with LoA2.
SMS + embedded link	No	Supports LoA2 – Typically, the URL takes up a lot of space – so limited space is left in the SMS for the consent request, attributes etc. consent can be given in the page which opens after the click on the link, however not recommended[3].
Seamless authenticator (enriched header)	No	Not applicable

Table 9: Authenticator suitability for Mobile Connect ATP

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	23/10/2018	New document created by merging definition and technical requirements documents and updating	David Pollington/ GSMA	Nick Spencer
2.0	07/02/2019	Modified the document to remove DI mode related concepts, consent mangament is condensed now, DQRT comments are incorporated as it is.	David Pollington / GSMA	Venkatasivakumar Boyalakuntla (Siva)/ GSMA
2.0	15/11/2022	Document ready for TG approval	TG	Yolanda Sanz/GSMA

C.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.