Mobile Connect Product Manager’s Lifecycle Handbook
Version 1.3
06 December 2022

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

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 contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Executive Summary

This Product Manager’s Lifecycle Handbook seeks to provide a top-down view of the business and technical processes associated with the relevant stages of the End-User lifecycle to aid Mobile Network Operators in the deployment and operations of Mobile Connect and to ensure that the full End-User lifecycle is taken into account.

The handbook serves as a high-level description of how Mobile Connect works that can help Operators get the big picture before diving into the detail of the technical specifications. It also serves to highlight the requirements for setting up the Mobile Connect service offering and the User touchpoints at each stage of the Mobile Connect User lifecycle.

This handbook is structured around the elements of the User Lifecycle and seeks to map the business and technical processes against each element within the lifecycle. The lifecycle and business and techncial processes are outlined in Figure 1.

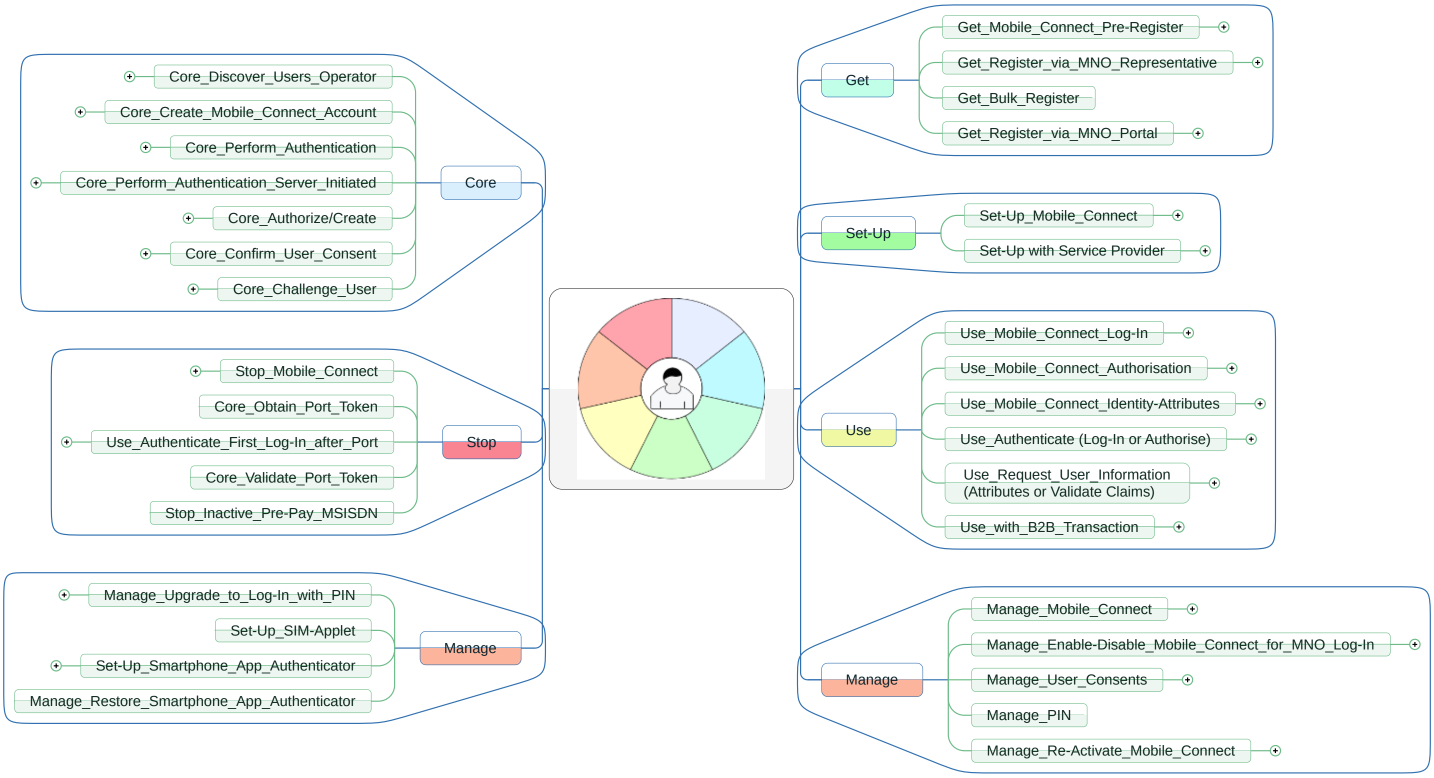

Core_Discover_Users_Operator
Core_Create_Mobile_Connect_Account
Core_Perform_Authentication
Core_Perform_Authentication_Server_Initiated
Core_Authorize/Create
Core_Confirm_User_Consent
Core_Challenge_User
Core
Stop_Mobile_Connect
Core_Obtain_Port_Token
Use_Authenticate_First_Log-In_after_Port
Core_Validate_Port_Token
Stop_Inactive_Pre-Pay_MSISDN
Stop
Manage_Upgrade_to_Log-In_with_PIN
Set-Up_SIM-Applet
Set-Up_Smartphone_App_Authenticator
Manage_Restore_Smartphone_App_Authenticator
Manage
Get
Get_Mobile_Connect_Pre-Register
Get_Register_via_MNO_Representative
Get_Bulk_Register
Get_Register_via_MNO_Portal
Set-Up
Set-Up_Mobile_Connect
Set-Up with Service Provider
Use
Use_Mobile_Connect_Log-In
Use_Mobile_Connect_Authorisation
Use_Mobile_Connect_Identity-Attributes
Use_Authenticate (Log-In or Authorise)
Use_Request_User_Information
(Attributes or Validate Claims)
Use_with_B2B_Transaction
Manage
Manage_Mobile_Connect
Manage_Enable-Disable_Mobile_Connect_for_MNO_Log-In
Manage_User_Consents
Manage_PIN
Manage_Re-Activate_Mobile_Connect

Figure 1: A Summary of Key User Lifecycle Processes Covered in this Handbook

1.2 Objectives

The Product Manager’s Lifecycle Handbook is designed to help Mobile Network Operators work through the requirements for deploying Mobile Connect:

- To understand the end-use lifecycle
- To ensure that all relevant elements for the End-User lifecycle are considered

- To provide a high-level view of the business and technical processes to aid in understanding how to deploy Mobile Connect.
- To understand the User touchpoints and where the User Experience needs to be considered
- To be able to navigate to the relevant technical specifications

This handbook is informative in nature and focuses on the core elements of Mobile Connect and indicates preferred and default options where appropriate. It does not discuss all possible options and variations but seeks to focus on the core elements.

The processes are presented using the Business Process Modelling and Notation syntax (BPMN 2.0) that can be understood by both technical and non-technical people. The processes are consistent with the technical specifications but do not replace the detailed technical specifications. A summary of the BPMN 2.0 syntax is included in Annex B.

1.3 Definitions

Term	Description
API	Application Programming Interface – in case of Mobile Connect the 'protocols' which third party applications will use to interact with the various systems provided by GSMA and Operator to enable Mobile Connect
API Endpoints	The various Internet URLs which applications use to invoke the various API services which make up the Mobile Connect services. API Endpoints are provided by the API Exchange for the Discovery and Logo services, and by the Mobile Network Operator for the Mobile Connect services
API Exchange	The global federation platform for Mobile Operators which enables Service Providers/Developers access to all subscribers of all participating Operators
Authentication Device	This is always the mobile device belonging to a User who is the subscriber of the Mobile Network Operator. It is the device that the User clicks "ok" on or enters a PIN number on within a Mobile Connect Authentication / Authorisation to prove that he/she is in possession of the phone (or more accurately the SIM with registered MSISDN). This is referred to as "*something I have"* in identity terms.
Consumption Device	These are the many devices that the User can use to consume the target service. Including, but not limited to smartphone, feature phone, PC, tablet, Smart TV. The Consumption Device can also be (but does not have to be) the same as the Authentication Device
Developer Portal (Mobile Connect Developer Portal)	A portal either provided by an Mobile Network Operator, GSMA (the Mobile Connect Developer Portal) or a party acting on behalf of the Operator(s) that enables Service Providers/Developers to access technical documents, example code and other developer resources, test an application, access the Mobile Connect Licence and register to discover how to access the API Exchange Discovery and Logo APIs as well the Operators' Mobile Connect APIs.
User	A person or entity who consumes a Service Provider's / Developer's service and who uses Mobile Connect to authenticate to a Service and/or who is requested to authorise a transaction within the service using Mobile Connect
ID GW	The component within an Operator implementation that exposes the Mobile Connect service to the Service Provider/Developer.

Term	Description
Identity Provider	A consumer-facing entity providing the digital identity services. In the case of Mobile Connect this is always the Mobile Network Operator (though the service may be provided on behalf of the Mobile Network Operator by a third party).
nonce	A nonce is an arbitrary number used only once in a cryptographic communication. Authentication protocols may use nonces to ensure that old communications cannot be reused in replay attacks.
OIDC Authorization Request	All Mobile Connect service requests use the same basic call (which differs in format depending on whether Device-Initiated requests or Server-Initiated requests are being made). The Mobile Connect services are specified within the 'scope' parameter. Within Mobile Connect technical specifications this is referred to as an OIDC Authorization Request (spelled with a 'z'). This distinguishes this call from Mobile Connect Authentication or Authorisation services. Note this is equivalent to the "OIDC Authentication Request" used in [5].
Operator On-boarding	The technical and contractual processes that a Operator takes when registering with the GSMA API Exchange or similar Discovery service for federated access by Service Providers to use an Operator's ID Gateway. This is particulalry relevant when multiple Operators support Mobile Connect services in a market or across multiple markets.
Prompt	Question or context displayed to the User on the Authentication Device (or in some cases the Consumption Device) to approve or deny the transaction / action.
REST	REpresentational State Transfer - an architectural style for designing distributed systems on the web, making it easier for systems to communicate with each other.
Service / Application	Digital service or content, consumed by a User.
Service Provider/Developer	A person or legal entity providing digital services and/or content to subscribers (Users).
Service Provider/Developer On-boarding	The technical and contractual processes that a Service Provider/Developer takes when on-boarding / registering with Mobile Operators' ID Gateways to use Mobile Connect services.
Transaction	An operation initiated by the Service to complete a task

1.4 Abbreviations

Term	Description
APIX	API Exchange that provides the Discovery Service for Mobile Connect
JSON	JavaScript Object Notation - an open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types (or any other serializable value). It is a very common data format used for asynchronous browser–server communication
JWT	JSON Web Token is an open standard for creating access tokens that assert some number of claims. The tokens are signed by the server's key, so the client and server are both able to verify that the token is legitimate. JWT claims can be typically used

Term	Description
	to pass identity of authenticated Users between an identity provider and a service provider, or any other type of claims as required by business processes
LoA	Level of Assurance – the degree to which a User is required to assert their identity
MCC	Mobile Country Code – identifies the country in which a mobile service operates
MNC	Mobile Network Code – identifies the mobile network withn a country
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number (mobile phone number)
OIDC	OpenID Connect -
OTA	Over The Air
PAC	Porting Authorization Code – a code provided by the Operator upon request, when a User wishes to port their MSISDN to another Operator within the same country. (local processes may differ by country, and porting is not available in some countries)
PCR	Pseudonymous Customer Reference – a unique reference to an individual User of Mobile Connect which reveals no personal information about the User
PIN	Personal Identification Number – used as the second factor "something I know" in Mobile Connect Authentication / Authorisation. In some countries the PIN is called a Personal Code, but for convenience it will be referred to as the PIN throughout this document.
SDK	Software Development toolKit
SIM	Subscriber Identity Module – the removable smart card inserted into a mobile device which stores User data, together with network and identification data.
SMSC	Short Message Service Centre
TTL	Time to Live
UI	User Interface
UX	User Experience
URI	Universal Resource Identifier

1.5 References

Ref	Doc Number	Title
[1]	IDY.05	Mobile Connect Technical Overview (docx)
[2]	-	Mobile Connect portfolio (Jul 2019).pptx
[3]	-	Mobile Connect Privacy Principles
[4]		Regulatory considerations for processing personal data and attributes for Mobile Connect
[5]	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
[6]	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

Ref	Doc Number	Title
[7]	IDY.33	API Exchange Functional Description v1.0.docx
[8]	Mobile Connect Developer Portal	Mobile Connect Developer Portal: https://developer.mobileconnect.io
[9]	IDY.04	Mobile Connect Technical Architecture and Core Requirements
[10]	IDY.10	Mobile Connect SIM Applet Authentication specification
[11]	IDY.12	Mobile Connect Smartphone App Authenticator Specification
[12]	OIDF Account Porting	OpenID Connect Account Porting, https://openid.net/specs/openid-connect-account-porting-1_0.html
[13]	-	Mobile Connect UX Guidelines
[14]	-	Mobile_Connect_UX_Audit India ThinkDesign 020217.pptx
[15]	-	Hiveworks Mobile Connect User Insights.pdf

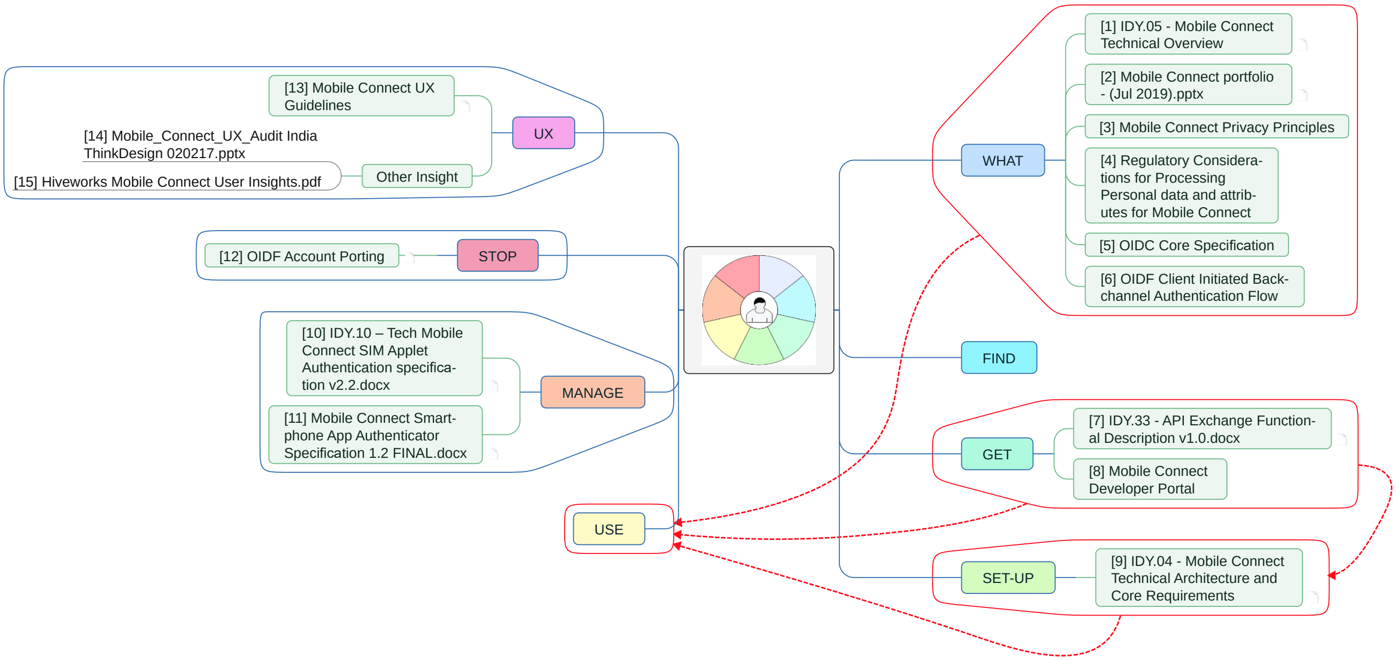

[13] Mobile Connect UX Guidelines
[14] Mobile_Connect_UX_Audit India ThinkDesign 020217.pptx
[15] Hiveworks Mobile Connect User Insights.pdf
Other Insight
UX
[12] OIDF Account Porting
STOP
[10] IDY.10 – Tech Mobile Connect SIM Applet Authentication specification v2.2.docx
[11] Mobile Connect Smartphone App Authenticator Specification 1.2 FINAL.docx
MANAGE
USE
WHAT
[1] IDY.05 - Mobile Connect Technical Overview
[2] Mobile Connect portfolio - (Jul 2019).pptx
[3] Mobile Connect Privacy Principles
[4] Regulatory Considerations for Processing Personal data and attributes for Mobile Connect
[5] OIDC Core Specification
[6] OIDF Client Initiated Backchannel Authentication Flow
FIND
GET
[7] IDY.33 - API Exchange Functional Description v1.0.docx
[8] Mobile Connect Developer Portal
SET-UP
[9] IDY.04 - Mobile Connect Technical Architecture and Core Requirements

Figure 2: References Mapped to User Lifecycle

2 The User Lifecycle

This handbook is structured around the elements of the User Lifecycle and seeks to map the business and technical processes against each element within the lifecycle.

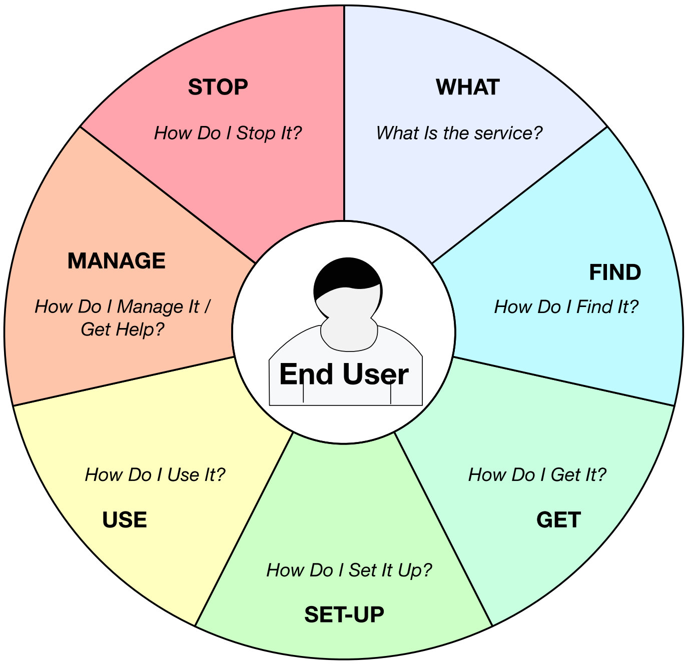


Figure 3: The User Lifecycle

Figure 3 illustrates the different stages within the Lifecycle of a User. This Lifecycle Wheel can be applied to any service from the perspective of any type of customer[1]. This is used to map the key business and technical processes associated with a User finding, getting, setting-up, using, managing and ultimately stopping (cancelling) a service – in this case Mobile Connect. By mapping these business and technical processes, it serves to highlight the elements that need to be put in place to cater for the whole User Lifecycle and also highlights the key customer touch points where the User experience needs to be considered. A similar wheel could be created for a Service Provider that uses Mobile Connect but this is outside of the scope of this handbook.

In understanding the Lifecycle Wheel, it is helpful to consider an example. Take the example of a User who accesses a particular service provided by a Service Provider via an aplication which can be downloaded from an App Store. The lifecycle would then cover:

- WHAT – A description of the service, what is in scope and what is not in scope
- FIND - How the customer would find the service. This would include marketing and sales channels that might be utlisied to make the customer aware of the service
- GET – Where the customer would get access to the service. In this case it would be dowloading an App from the relevant App store (or stores)
- SET-UP – How the customer sets up the App and registers for the service

[1] Note that the full lifecycle includes another segment “Pay – How does the Customer Pay for the service?”. Since the End User does not currently pay for Mobile Connect services, this has been excluded for this handbook.

- USE – How the customer would use the service. Depending upon the Service and the App this might cover a number of Use Cases
- MANAGE – The focus of this is around getting help or self -service around the Service and associated App (in this example) and would cover access to Customer Care or a retail store or a self-help portal or indeed via some form of third party support.
- STOP – looks at how the customer can stop the service. This might involve an explicit cancellation (particularly where some form of subscription is involved) or simply deleting an App from the customer’s smartphone.

By considering these elements, the Service Provider is able to ensure that all elements of the Lifecycle are considered in the design and deployment of the Service including the User experience at each touch-point in the lifecycle. It is worth noting that in the event of an upgrade to the Service as it was originally defined then there would be another iteration around the lifecycle wheel to understand the implications of that upgrade on the customer lifecycle.

When the Lifecycle Wheel is applied to the User in the context of Mobile Connect there are a number of things that need to be considered:

- The Lifecycle relates to the specific service or services that are articulated under “WHAT”. In this case Mobile Connect including Authentication, Authorisation and Attribute Services.
- The entity providing Mobile Connect is the Mobile Network Operator (MNO or Operator); the entity consuming Mobile Connect services (for use within their own services) is referred to as a Service Provider (SP). An SP essentially makes use of Mobile Connect to provide a service to the User where the User is also an Operator’s customer – the service is intimately linked to the User’s MSISDN and Mobile Account.
- It is possible for a User to register for Mobile Connect at the point of access to a service provided by a Service Provider – so called Set-up or Register “On-the-Fly” which covers the Get, Set-Up and Use elements in one process[2].
    - Registration for Mobile Connect with a User’s Operator prior to making use of Mobile Connect with a Service Provider is captured under “GET”.
    - Setting-up Mobile Connect for use with a Service Provider’s service or application is covered under “SET-UP”. This includes “Set-Up On-the Fly”.
    - In turn the process for Set-Up On-the-Fly is identical to the process for Authentication under “USE” but for the information included within the request to the Operator’s Mobile Connect ID GW.

[2] Note that Set-Up “On-the-Fly” is not the preferred method for registering Users on Mobile Connect – this is better achieved by the Operator.

2.1 Process Modelling

2.1.1 Notation

The processes are described using Business Process Model and Notation Version 2 (BPMN 2.0) standard which is maintained by the Object Management Group (OMG). This provides a graphical way to articulate business and technical processes. To make a process easier to digest it may contain sub-processes to hide detail. Some of these sub-processes are expanded in more detail, where appropriate.

Annex B provides a summary of the syntax and outlines some of the specific colour coding used within this document.

Colour coding has been used to highlight:

- Sub-Processes that relate to Mobile Connect and typically are expanded in more detail (Pink). In the interests of brevity not all sub-processes indicated in pink are included within this document
- Sub-Processes that are referenced but not expanded – typically these sub-processes are internal processes to the Operator or Service Provider (Grey)
- User Tasks where interaction is involved (Yellow). Where appropriate a wireframe illustrating the User experience is included within the handbook
- Default flows to indicate the preferred process path or the default process path. Where this relates to a preferred or recommended approach the sequence flow arrow is highlighted with a thicker blue line.

High-level processes outline the basic transaction. These will refer to more detailed processes – shown as sub-processes. The more detailed processes use Pools and Swim-lanes to depict the actors involved in the process – an actor in this context can refer to a person, an organisation, a device, a software component or API that participates in a particular transaction. In some of the process diagrams, pools and swim-lanes are included but don't show any process activities within them – these activities are typically included within a sub-process and the pools and swim-lanes have been retained to show that these actors play a role within the overall transaction.

A number of Sub-Processes are described as "Core Processes" which are re-used a number of times in different contexts. For example "Challenge_User" is utilised for both authentication and User consent in a number of different scenarios. Note that Mobile Connect services are built around the "Mobile Connect Core framework" – the use of the term Core in this handbook is not directly related to the Core Framework although many of these sub-processes fall within the Core framework. Further information on the Core framework can be found in the Mobile Connect Technical Overview [1].

Although the detailed processes are included, the higher level processes should be relatively easy to understand without having to refer to the detail.

2.1.2 Assumptions

The focus of this handbook is around the User's interaction with Service Providers and Operators in the context of Mobile Connect.

It is assumed that Service Providers have already registered their applications with the relevant Operator’s Mobile Connect Identity Gateway. This will include agreement/approval of the specific Mobile Connect services that the Service Provider will use, which are then requested via “scope” values included within a service request

2.2 User Lifecycle Processes

The following structure of this document is based around the Lifecycle Wheel.

Figure 4 provides a summary of the processes that are covered for the GET, SET-UP, USE, MANAGE and STOP Stages as well as the relevant Core Processes. Further detail can be obtained by referring to the associated references.

Note that under the MANAGE and STOP stages, processes are included which are strictly part of GET, SET-UP and USE as they are related to the relevant processes within the MANAGE and STOP stages.

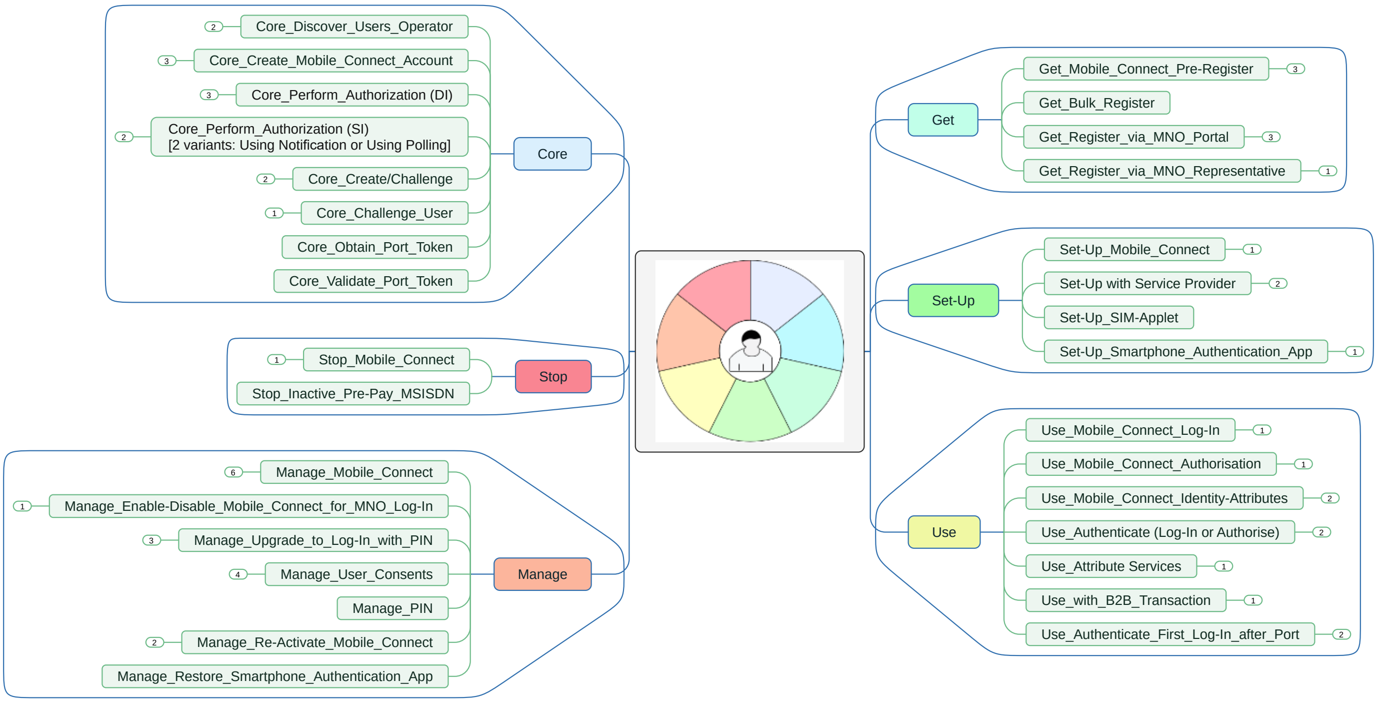

2 Core_Discover_Users_Operator
3 Core_Create_Mobile_Connect_Account
3 Core_Perform_Authorization (DI)
2 Core_Perform_Authorization (SI)
[2 variants: Using Notification or Using Polling]
2 Core_Create/Challenge
1 Core_Challenge_User
Core_Obtain_Port_Token
Core_Validate_Port_Token
Core
1 Stop_Mobile_Connect
Stop_Inactive_Pre-Pay_MSISDN
Stop
6 Manage_Mobile_Connect
1 Manage_Enable-Disable_Mobile_Connect_for_MNO_Log-In
3 Manage_Upgrade_to_Log-In_with_PIN
4 Manage_User_Consents
Manage_PIN
2 Manage_Re-Activate_Mobile_Connect
Manage_Restore_Smartphone_Authentication_App
Manage
Get
Get_Mobile_Connect_Pre-Register 3
Get_Bulk_Register
Get_Register_via_MNO_Portal 3
Get_Register_via_MNO_Representative 1
Set-Up
Set-Up_Mobile_Connect 1
Set-Up with Service Provider 2
Set-Up_SIM-Applet
Set-Up_Smartphone_Authentication_App 1
Use
Use_Mobile_Connect_Log-In 1
Use_Mobile_Connect_Authorisation 1
Use_Mobile_Connect_Identity-Attributes 2
Use_Authenticate (Log-In or Authorise) 2
Use_Attribute Services 1
Use_with_B2B_Transaction 1
Use_Authenticate_First_Log-In_after_Port 2

Figure 4: A Summary of Key User Lifecycle Processes

3 WHAT – Mobile Connect

Mobile Connect is a portfolio of mobile-enabled services that can be integrated into a Service Provider’s application to support access to services provided by the Service Provider. Mobile Connect provides authentication, authorisation, and permissioned access to a User’s attributes. Figure 5 outlines the range of services provided by Mobile Connect. (See also Mobile Connect Technical Overview [1]):

- Mobile Connect Authentication allows Users to log into websites and applications quickly without the need to remember passwords and usernames

- Mobile Connect Authorisation allows Users to approve 3rd party transactions directly from their mobile phones

- Mobile Connect Attribute Services (Identity and Network attributes) allow personal data or attributes relating to the User or their mobile account to be requested by and shared with a Service Provider to support verification of identity or to help mitigate fraud. This will be subject to having a clear legal basis to share the information, as defined within applicable data privacy regulations

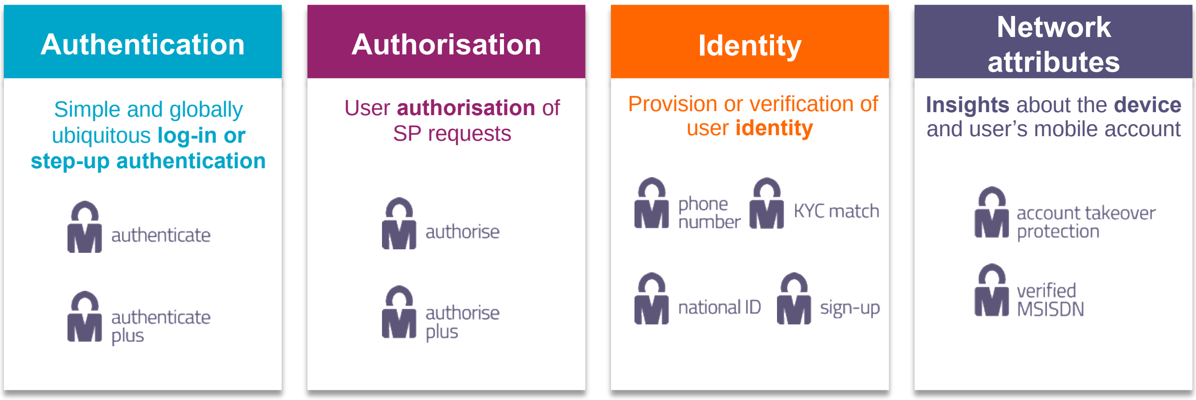

Authentication
Simple and globally ubiquitous log-in or step-up authentication
authenticate
authenticate plus
Authorisation
User authorisation of SP requests
authorise
authorise plus
Identity
Provision or verification of user identity
phone number
KYC match
national ID
sign-up
Network attributes
Insights about the device and user's mobile account
account takeover protection
verified MSISDN

Figure 5: Mobile Connect Portfolio of Services

With Mobile Connect, no personal information is shared with 3rd parties without a clear legal basis to do so, such as obtaining the User's consent; it safeguards online privacy and helps to mitigate the vulnerabilities of online passwords[3]. Mobile Connect Privacy Principles [3] are based on recognised and internationally accepted principles on data protection and privacy. It is mandatory for Operators and Service Providers[4] to commit to these principles before using the Mobile Connect service mark. The Mobile Connect service strategy is to deliver a ubiquitous identity solution federated across Operators, with a consistent User experience, ensuring privacy for Users, and commercial viability for Operators while delivering tangible benefits to Service Providers.

This handbook outlines business and technical process flows that cover the Mobile Connect portfolio across the User Lifecycle. These process flows are illustrative to help Operators work through the necessary processes that need to be put in place as part of a Mobile Connect deployment. Operators are free to select, adapt, or reject the processes illustrated within this handbook or to create different processes more appropriate to their deployment.

3.1 Mobile Connect and OpenID Connect

Mobile Connect is based upon the OpenID Connect (OIDC) protocol [5] which provides an identity layer on top of the OAuth 2.0 protocol. It allows Users to be identified by their MSISDN (or a related Pseudonymous Customer Reference) and to be authenticated via their mobile device.

[3] Note that in some markets MSISDN is not considered personal information while in other markets it is.

[4] Mandatory for any Service Providers using the Mobile Connect mark

Without secure, external authentication and authorization, you'd have to trust that every application, and every developer not only had your best interests and privacy in mind, but also knew how to protect your identity and was willing to keep up with security best practices. With OIDC, you can use a trusted external provider (your Mobile Operator) to prove to a given application that you are who you say you are, without ever having to grant that application access to your credentials.

OIDC enables Clients (applications) to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. OpenID Connect is simple enough to integrate with basic applications, but it also has the features and security options to match demanding enterprise requirements.

Note that OpenID Connect doesn't specify how Users should actually be authenticated, Mobile Connect specifies this and makes use of a User's MSISDN as an initial identifier and then issues a Pseudonymous Customer Reference as a pseudonymous identifier for subsequent Mobile Connect service requests.

Mobile Connect defines two profiles to support Device-Initiated and Server-Initiated requests for authentication, authorisation or permissioned access to User attributes.

3.1.1 Device-Initiated Mode

Within the OIDC specification, a number of different flows are defined. The Authorization code flow is the most commonly used flow which is referred to in Mobile Connect as Device-Initiated mode. It is intended for traditional web applications as well as native / mobile apps. It involves an initial browser redirection to / from the Identity Provider[5] for User authentication and consent, then a second back-channel request (between the Service Provider's Client Application and the ID GW Token endpoint) to retrieve an ID Token and an Access Token. This flow offers optimal security, as tokens are not revealed to the browser and the client application can also be authenticated.

The successful service request will generate a one-time, time-limited Authorization Code that is returned to the Service Provider's Client Application (via the redirection back to the Client Application). The Client Application is then able to request an ID Token and Access Token from the ID GW Token endpoint using this Authorization Code.

3.1.2 Server-Initiated Mode

Whereas Device-Initiated mode supports the use of Mobile Connect for traditional web applications or native apps, where the User is interacting directly with that application, there are a number of cases where it is more appropriate for a Service Provider to initiate a Mobile Connect service request directly as a server to server request which does not involve any re-direction of a web-based application. For example, where a Service Provider is interacting with a User via their customer care centre or retail store and wishes to authenticate the customer or where KYC or fraud checks are required as a background (B2B) check as part

[5] Different terminology is used within OIDC - The Identity Provider is known as an OIDC Provider and in the case of Mobile Connect is the serving Operator's ID GW.

of a registration for a service, then a server-to-server or Server-Initiated request is more appropriate.

Server-Initiated mode is based upon the OIDF Client Initiated Backchannel Authentication Flow (CIBA) [6] which defines a modified service request format and mechanisms for returning tokens suited to secure direct server-to-server interactions. It requires the Service Provider to have the User’s MSISDN in order to identify the User in a service request.

3.1.3 Returned Tokens

OpenID Connect defines a number of tokens that are returned to the Service Provider client application (or server application): the ID Token, the Access Token and an optional Refresh Token.

The ID Token is a security token and resembles the concept of an identity card, in a standard JWT format[6], signed by the Identity Provider (Operator ID GW). The ID Token has the following features:

- Asserts the identity of the User, called *subject* in OIDC (sub).
- Specifies the issuing authority, i.e. the serving Operator ID GW (iss).
- Is generated for a particular *audience*, i.e. Client Application (aud).
- Contains a nonce (nonce) – an arbitrary number that can only be used once and helps to ensures that this ID Token cannot be reused, once it has expired.
- Specifies when (auth_time) and how, in terms of strength (acr), the User was authenticated (i.e. Level of Assurance).
- Has an issue (iat) and expiration time (exp).
- Is digitally signed, so it can be verified by the intended recipients.
- May optionally be encrypted for confidentiality.

The Access Token is issued to the Service Provider for the services it has requested provided that a) the Operator has authorized the Service Provider’s usage of the services (at the ID GW) and b) the User has consented (where required) for the Service Provider to use these services for that particular User.

- The Access Token is an opaque string which has an associated scope and lifetime and may optionally allow refreshing (using a Refresh Token).

3.1.4 Retrieval of Attributes (where requested in the Mobile Connect service request)

Once the Service Provider has obtained the ID Token and Access Token, they can then use the Access Token to retrieve the requested User attributes by submitting a Resource Request to the relevant Operator Resource endpoint. Whoever holds the Access Token is allowed to make a Resource Request to the protected Mobile Connect Resource endpoint, e.g. “PremiumInfo” endpoint. The Access Token must, therefore, be kept secret at all times and only used over HTTPS.

[6] JSON Web Token (JWT) as defined in RFC 7519

The OIDC standard includes a set of identity attributes that can be requested by a Service Provider when authenticating a User; this "UserInfo" set includes attributes such as name, gender, DOB, address, e-mail, phone number etc. Within Mobile Connect this has been extended to include a richer set of information (PremiumInfo). This encompasses the majority of the UserInfo set and extends it further with attributes that Operators can provide, related not only to User information but adding in data categories around the User's account with the Operator, the device they use and their network status. Mobile Connect also allows the specification of service specific Resource Endpoints, where there is a limited service deployment.

3.2 Basic Operation of Mobile Connect and Main Actors

Mobile Connect is delivered through a set of secure application programming interfaces (APIs) based on OpenID Connect [5]. Figure 6 illustrates the basic operation:

Based on Figure 6, the steps are as follows:

- A Mobile Connect service can be invoked by the User (e.g., by clicking on a Mobile Connect button to authenticate) through a browser or via a dedicated application provided by the Service Provider (a Device-Initiated request) or by the SP directly as a Server-Initiated request (e.g., in the case of a B2B attribute service).

- Where the User is accessing a Service Provider's application (Device-Initiated), the User can access it on any device - tablet, laptop, desktop, mobile phone etc. (the Consumption Device) - and across any network (mobile network, WLAN etc.).

    - Each Operator implements an Identity Gateway (ID GW) to enable Mobile Connect; exposing the Mobile Connect API(s) to serve requests from Service Providers' applications. Mobile Connect supports a split architecture where the Resource Server can be implemented separately from the ID GW Authorization Server to provide greater flexibility in implementation.

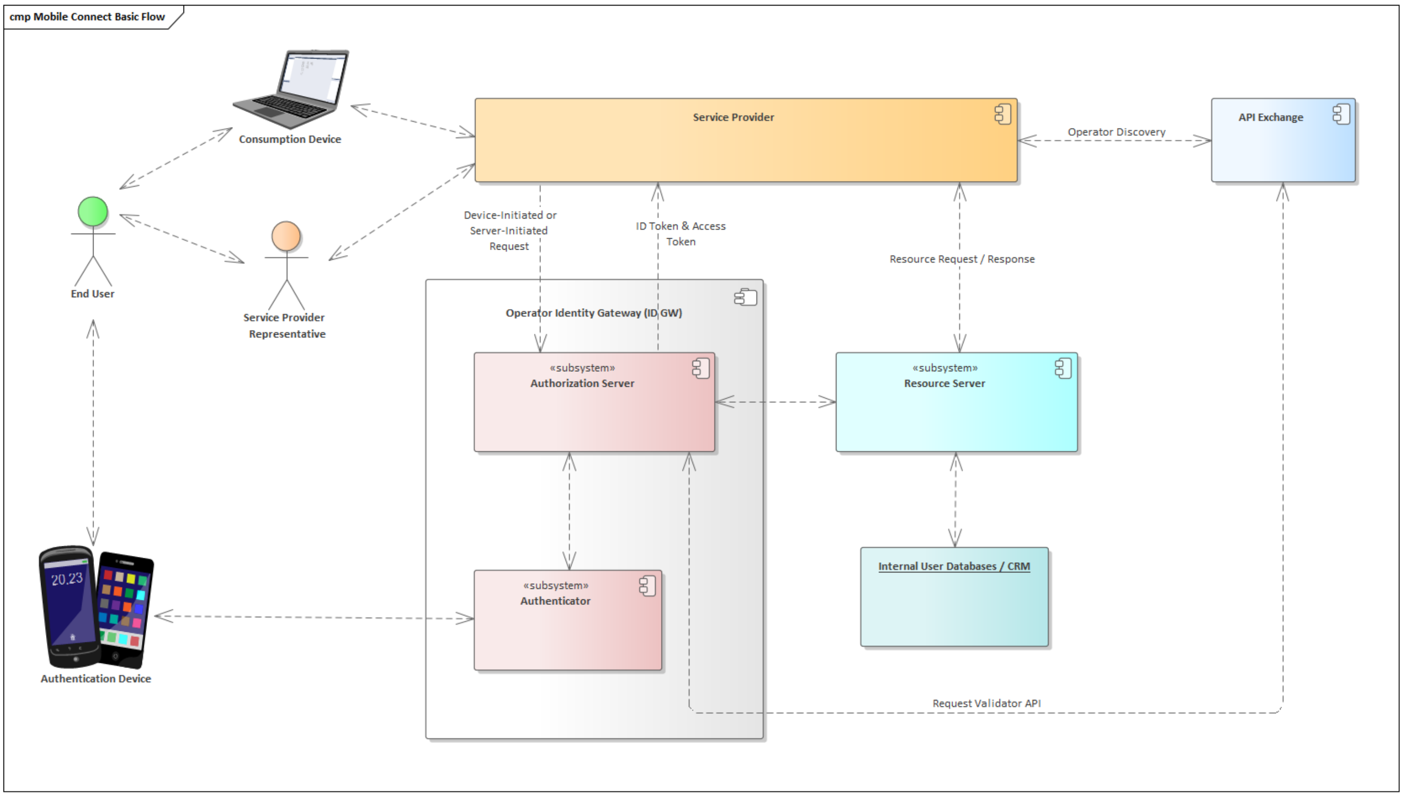

cmp Mobile Connect Basic Flow
Consumption Device
Service Provider
Operator Discovery
API Exchange
End User
Service Provider Representative
Device-Initiated or Server-Initiated Request
ID Token & Access Token
Resource Request / Response
Operator Identity Gateway (ID GW)
«subsystem» Authorization Server
«subsystem» Resource Server
«subsystem» Authenticator
Internal User Databases / CRM
20.23
Authentication Device
Request Validator API

Figure 6: Basic Operation of Mobile Connect and Main Actors

- The Service Provider's client application or server must be able to identify the serving Operator for the End User and obtain the relevant information to be able to submit a Mobile Connect service request to the ID GW. This includes information about the services supported, service endpoints, etc. which are published as part of the Operator's Mobile Connect Provider metadata via their openid-configuration URL. Mobile Connect Provider Metadata is described in more detail in [9]. The SP client also requires the relevant SP credentials for that ID GW. If the SP Client application does not already have this information, then the SP can use the optional Discovery Service (via the API Exchange) to identify the appropriate serving Operator ID GW.
  - The Service Provider submits a Discovery request to the API Exchange supplying the relevant information it has about the User.
  - The primary identifier of a User will be their MSISDN[7] but other information can serve to identify the serving Operator. If the MSISDN is not supplied by the Service Provider and the other information provided is insufficient to allow the User or the serving Operator to be identified, then there is a mechanism to prompt the User to enter their MSISDN within the Discovery process which will not be visible to the Service Provider.

[7] Mobile Connect was originally designed to enable Authentication and Authorisation without having to reveal any personal information unless the User wished to share that information. The MSISDN (mobile number) was considered as personal information - but in some markets this is not regarded in the same way and is freely distributed. Once registered a Pseudonymous Customer Reference (PCR) can be used by the Service Provider as an identifier without needing to use the MSISDN.

    - Once the Service Provider has the relevant serving Operator details for a particular User then there is no need to invoke the Discovery service for subsequent Mobile Connect service requests, so this is typically only carried out at the initial setting up of Mobile Connect for that User.

- The Service Provider submits a Mobile Connect service request to the serving Operator's ID GW.
    - The request can be for Authentication of the User, Authorisation of a transaction or a request for personal information (User attributes) where User consent is required.

- Where required, the ID GW selects an appropriate Authenticator that allows a challenge to be sent to the User's mobile device and allows the User to respond. This could for example, be via a USSD session or via a SIM-Applet loaded on the User's SIM card
    - The ID GW authenticates the User via their mobile device. Authentication or authorisation is always obtained via the Users' mobile device. User consent for sharing or validating User attributes may also be obtained by the ID GW as part of the service flow, this can be via the Authentication Device or the Consumption device depending upon the specific Mobile Connect service and the selected Authenticator. In this case, the User must always be authenticated first via the Authentication Device.
    - Where needed (based on the Mobile Connect service being requested), the ID GW selects an appropriate Authenticator for sending a challenge/prompt to the User's mobile device (the Authentication Device) and acquiring the User's response.
    - The Operator can provide a prompt to help the User to understand whether they are authenticating (Log-In) or what they are authorising, and the Service Provider can provide contextual information about the transaction to be included in this prompt.
    - Note that a User's mobile device can operate as both the consumption device and the authentication device in the case where a User is accessing the SP client application on their mobile device. In this situation the mobile device screen might typically be displaying relevant web pages via the browser or mobile app (as the Consumption device) and then switch to the Authenticator prompt, context and challenge (as the Authentication Device). In this situation, consideration will need to be given to the User Experience, for example where information is presented via the consumption device but then context switches to authentication on that device which may obscure that information. This will be highlighted in the relevant process flows.
    - The User response is processed by the authenticator and the result returned to the ID GW

- The ID GW returns a confirmation to the Service Provider in the form of an Identity Token (ID Token) that provides proof of the authentication of the User. The ID GW also returns an Access Token that allows the Service Provider to obtain User attributes from a Mobile Connect Resource Server[8] if the SP specified one of the Mobile Connect attribute services in their request.

  - In the case of authentication (for example), the Service Provider gives the User access to the service.

- If the Service Provider requested one of the Mobile Connect attribute services, the SP then submits a request to the Resource endpoint on the relevant Resource Server using the Access Token. The request is validated and, if successful, the attributes are returned to the Service Provider.
  - Mobile Connect attribute services can involve the sharing or matching (validation) of User attributes. In the latter case the SP includes the attribute names and values to be matched in the request and the match result is returned.

Further details are provided in the following sections and can also be found [9].

3.3 Authenticators

The User's mobile phone is always the Authentication Device and the Operator may select a number of different mechanisms to prompt the User and to obtain their response to a challenge. Within some of the process flows in this handbook reference is made to an Authenticator associated with the Operator ID GW. This abstracts the different elements that may comprise the Authenticator depending upon the Operator's implementation – for example there would be an Authentication Server associated with an OTA server and SMSC to support a SIM-Applet based Autenticator. Table 1 summarises the Authenticator Types.

3.3.1 Level of Assurance

Authenticator	Advantages	Disadvantages
Seamless	• Single-factor authentication (LoA2) without requiring explicit interaction with the End User (zero friction) • Can be used where Operator supports HTTP Header Enrichment or an alternative method of obtaining the network authenticated MSISDN and where User access is via the mobile data channel	• Limited to LoA2 • Not suitable for Authorisation or User consent as no context can be presented to the User
USSD	• Suitable for LoA2 • Works on all phones. • Doesn't require data connections • Secure channel • Can be used "On-the-Fly"	• Requires User input • Can take time loading • Displays differently on different devices

[8] A Resource Server may be implemented as a separate stand-alone platform or as part of an ID GW. For example, if a common ID GW Hub is implemented to support all Operators within a country or jurisdiction then each Operator may implement separate Resource Servers to support the sharing of User information/attributes for their customers.

SMS/URL	• Suitable for LoA2 • No User input required • Works consistently across enabled devices • Can be used “On-the-Fly”	• Low security • Requires data connection • Data charge may discourage Users
SIM-Applet	• Suitable for LoA2 and LoA3 • Super quick and secure (especially for LoA3)	• Limited text strings for UX display • High investment to roll out • Potentially time consuming to push OTA and therefore not recommended for registering on the fly.
Smartphone App	• Suitable for LoA2 and LoA3 • Very smooth UX as eliminates call times and processes	• Only available for smartphones • Requirement to download may be point of dropout for the registration process and therefore not recommended for registering on the fly.

Table 1: Authenticator Types

Mobile Connect Authenticate Plus and Authorise Plus services provide a higher level of assurance based on the requirement for the User to enter a PIN or biometric[9]. This is classified as Level of Assurance 3 (LoA3) which involves two factors (possession of the mobile device and knowledge of the registered PIN or possessing the correct fingerprint or other biometric) compared with standard Authentication and Authorisation which is LoA2 (a single factor – in possession of the registered device).

The ability to support a higher level of assurance is desireable in Mobile Connect as it provides greater security, is tied to a person rather than just a device and enables its use with a wider range of Service Providers. To achieve a Level of Assurance of LoA3, the appropriate Authenticator application must be installed and configured on the User’s mobile device which will involve a number of additional steps. This will introduce additional friction if the registration process forms part of a service flow to access a Service Provider’s application (“Set-Up On-the-Fly”). One of the benefits of Users registering for Mobile Connect with their Operator is that they can be registered for LoA3 directly and it will not interrupt the process of using Mobile Connect with a Service Provider.

A Service Provider can request a certain Level of Assurance in the API call but this will be dependent upon the Authenticators that are supported by the Operator and the capabilities of a User’s device. For instance, if the SP requires LoA3, an appropriate Authenticator must be installed for the target User and provisioned to be able to support PIN entry or biometric verification. If a Service Provider requests an LoA3 and the User can only be authenticated to LoA2 then it is recommened that the request is rejected. If a Service Provider requests LoA2 and the User is set-up for LoA3 then the the ID GW may authenticate to LoA3 - the achieved LoA is returned to the Service Provider in the ID Token.

[9] Verified locally on the device using the native biometric APIs provided by the underlying device platform

For Mobile Connect registration, particularly registration "On-the-Fly", LoA2 should be provisioned by default. The option to upgrade to LoA3 is then provided via the Operator (Operator Portal or other Operator channels). This allows for the download and set-up of the appropriate authenticator and for additional identity checks (if required) to be completed. It also allows for validation of the personal information that is held by the Operator and may be used for Attribute Services.

The process flows include the set-up of SIM-Applet and Smartphone App Authenticator to support LoA3 at a high level.

3.4 Pseudonymous Customer Reference (PCR)

The privacy principles behind Mobile Connect [3] are aimed at ensuring that personal information is not shared with a Service Provider without a clear legal basis for doing so (e.g. where the User allows such disclosure). A User is initially identified by their MSISDN, which many Users may regard as private information, so during initial set-up of Mobile Connect between a User and a Service Provider, the registration process is geared towards enabling the User to identify themselves to their Mobile Operator using their MSISDN without this information being disclosed to a Service Provider.

After that initial registration a unique Pseudonymous Customer Reference (PCR) is generated by the Operator ID GW that can be used by the Service Provider thereafter for identifying that particular User and for use when requesting Mobile Connect Authentication Authorisation or Attribute Services for that User. Note that if the SP already has the User's MSISDN, they can use this for identifying the target User when issuing a Mobile Connect service request; a PCR will still be generated and returned.

The PCR is a unique identifier that links a User's MSISDN to a Service Provider (SP). PCRs are generated as a Globally Unique Identifier (GUID), which is machine driven code and does not contain any personal information.

A Service Provider may choose to group some of their applications by using specific Sector IDs[10] for the group of Applications which would share the same PCR for a given User. The SP would need to ensure that the Sector ID is used for the group of applications which are closely related to each other. For example, two registered applications may be grouped together because they are actually the same application but consumed on different device platforms (iOS, Android, Windows Desktop etc.). The User would fully expect Mobile Connect to recognise them and to work seamlessly across the different device platforms. This is an acceptable example of one PCR being shared by two grouped applications from a single Service Provider.

A PCR must not be shared by two or more completely different applications from the same Service Provider without End-User permission. And a PCR must never be shared by two applications from two different Service Providers.

[10] A sector ID is the host name part of the sector_identifier_uri that is provided during registration of the SP client application.

The PCR must never be used to track the User for secondary purposes without the User’s explicit consent. Operators will need to implement operational processes to monitor, police, and enforce this approach with Service Providers.

3.5 Mobile Connect Account

When the User registers for and uses Mobile Connect for the first time, a Mobile Connect account will be created by the Operator in compliance with local data laws and regulations. This account will be used by the ID GW to validate User details including account status, Level of Assurance provisioned, Device and Authenticator details and any User consents which may influence whether a Service Provider is able to request a given service or request certain types of information.

The Mobile Connect Account is also intimately related to a User’s existing Mobile Account and, for example, the fact that Mobile Connect is provisioned and that it is to be used for Log-In to the Operator’s services (e.g. self-service portal), including the associated PCR should be reflected in the Mobile Account.

The Mobile Connect Account should include the following information:

- MSISDN (this may change during the Mobile Connect account lifetime)
- LoA Provisioned
- Device and Authenticators that are enabled including identifiers, recovery codes, etc. as appropriate
- Account Status
- Account history (when created / modified / active / suspended / deleted etc.)
- PIN reset history
- PCR for each Service Provider and Service Provider application
    - Service Provider name /Sector ID associated with a PCR
    - Client ID associated with a Service Provider application
- Services for which User consent has been given
    - PCR, Sector ID, Client ID, date consent given, validity period for which User consent has been given and is active
- Transaction History[11] (It is recommended that Operators log all data related to every Mobile Connect transaction.)
    - Timestamp, Transaction type, LoA Requested & Provided, PCR, Service Provider name / Sector ID, Client ID, Transaction details, Outcome

3.5.1 MC Account Status

The Mobile Connect Account should contain a status flag indicating the status of the Mobile Connect Account. The different status conditions are:

[11] Transactions may not be explicitly stored within the Mobile Connect Account but are associated with a specific Mobile Connect Account and can be viewed and filtered based on MSISDN or PCR.

- **Active** - User is able to use Mobile Connect for Authentication, Authorisation with registered Service Providers and the Service Providers also have access to Attribute services in accordance with the Products they have registered for with the Operator.
- **Suspended** - account is restricted and is unavailable for User initiated Mobile Connect transactions subject to the Operator's policy. Typically, if a User's Mobile Account is suspended then their Mobile Connect Account should also be suspended and if the suspension on the Mobile Account is lifted then the Mobile Connect Account should be returned to an Active state[12]. The Mobile Connect Account should be suspended when a lost or stolen SIM / device is reported, when fraud is suspected and where, for example the Mobile Account is suspended due to non-payment of bills or if there is no credit on a pre-pay account.

  The following limitations apply for a Mobile Connect Account in a Suspended state:

  - Mobile Connect cannot be used for any type of authentication or authorisation.
  - All types of authenticator will not be useable. The PIN (if configured) will not be useable and cannot be reset.
  - All tokens, including access tokens and refresh tokens will be revoked immediately. Any attempt to use them will be denied.
  - A User may be able to log in to a self-care portal with a username + password, but their Mobile Connect account should be displayed as Suspended. No admin activities should be possible, and ideally there should be a call to action to contact their Operator.
  - The User cannot reactivate their own Mobile Connect account from a Suspended state - a suspended Mobile Connect account can only be re-activated by the Operator.
- **Closed** - Usually at User's request, the account is closed and so is unavailable for Authentication, Authorisation, Identity or Network Attribute Services. Mobile Connect Account data may be archived in line with local regulations and the Operator's data retention policy. A Closed account can be re-activated. If a Mobile Connect Account is closed:

  - Mobile Connect cannot be used for any type of authentication or authorisation.
  - All types of authenticator will not be useable. The PIN (if configured) will not be useable and cannot be reset.
  - All tokens including access tokens and refresh tokens will be revoked immediately. Any attempt to use them will be denied;
- **Deleted** – A Mobile Connect Account is deleted when the associated Mobile Account has been closed or deleted and the MSISDN has been returned to the pool. Deletion

[12] This is particularly important because if the Mobile Account is suspended and the Mobile Connect Account is not suspended then a User may still be able to use Mobile Connect over a WiFi connection, for example, using a Smartphone App Authenticator.

of the Mobile Connect Account implies that the Account record has been deleted from ID Gateway database and the account cannot be re-activated. Mobile Connect Account data will be retained or archived in line with local regulations and the Operator’s data retention policy.

With Mobile Connect Attribute services, there are scenarios where a request may be made directly to the Operator and where explicit User consent is not required. For example, a Bank typically performs Know Your Customer (KYC) checks when registering a new customer and it could be that Mobile Connect KYC Match forms part of that process. This is often referred to as a Business to Business (B2B) service request. The Service Provider must be approved and trusted by the Operator to use this service and the obligation is on the Service Provider to ensure appropriate User consent is obtained as part of its service and that the Service Provider’s terms and conditions make the context and use of this service clear in order to protect the rights of the User.

If a potential customer of the Service Provider, who is also a customer of a Mobile Operator but is not registered for Mobile Connect, requests a Service Provider service that involves a B2B attribute service request, then a Mobile Connect Account may be created “on-the-fly”, subject to the Operator’s ID GW policy which may vary depending upon specific Mobile Connect services requested. In this case, the User may be unaware that a Mobile Connect account has been created and it would be appropriate for the Operator to follow up with the End User to ensure that they have explicitly accepted the Mobile Connect terms and conditions. It also provides an opportunity to encourage the End User to set-up an appropriate Authenticator for LoA3. In this case the Operator may wish to include an additional flag to indicate that such follow up is pending, for example.

3.6 Terms and Conditions

The acceptance of terms and conditions for Mobile Connect by the User (for those services requiring User interaction) should be part of the registration process for Mobile Connect. The acceptance of terms and conditions can potentially create friction for the User and the optimum approach should be considered by the Operator. Table 2 summarises the options for a User to accept the terms and conditions. The relevant process flows in this Handbook do not (on the whole) dictate a particular approach to how terms and conditions should be presented and accepted by the User – typically the flow will check whether Ts&Cs have been accepted or not.

One variation on the acceptance of terms and conditions occurs with B2B services, where a Service Provider requests attributes or seeks to validate claims asserted by the User (for example, KYC Match) without the User being explicitly requested by their Operator to provide their consent – this is a direct Business to Business (B2B) transaction. In this case it will be the Service Provider’s responsibility to seek the User’s permission to perform such a request or check (either explicitly or through the Service Provider’s Ts&Cs) and to manage the User’s expectations accordingly. In order to perform such a transaction this might, for example, include a request for the User’s mobile number “in order to perform fraud checks”.

It will be important from the Operator’s perspective to ensure that any Service Provider requesting such a B2B service is aware of the obligation on them to seek the User’s permission to request personal information.

It is recommended that careful consideration is given to how terms and conditions are presented and accepted to ensure that Users understand how their information will be used and to ensure that privacy is protected[13] and to comply with local data protection regulations.

For Services Requiring User interaction:

Options for User to accept Ts&Cs	Advantages	Disadvantages
Offline when customer signs or renews contract with their Operator	Frictionless yet transparent process with full explanation of User benefits & MC proposition when contract is purchased on premise.	For contract renewals, the process may be invisible to the User and doesn't guarantee awareness.
IN service flow as extra 1 time only screen for clear acceptance	Full transparency to User. Education that full Ts&Cs are available to be read if required.	1-time only screen/step extends the authentication process as it requires explicit User action to accept. Can therefore be a drop-out point.
IN service flow as boilerplate text hardcoded & pre-checked underneath MC-sign in button	Full transparency to User. Link to full Ts&Cs that can be read if required. Doesn't require explicit User-action for acceptance & proof of acknowledgement.	Unlikely to be accepted on SP sites or requires higher investment of UX design to contextualise on an SP site by site basis.
Ts&Cs handled as part of a pre opted-in process accompanied by an opt-out sms/email/comms campaign	Frictionless yet transparent process with full explanation of User benefits & MC proposition. Can be used as one piece of a wider marketing campaign by Operator / SP on actions to safeguard User digital identity.	No UX disadvantages however there may be legal, regulatory or compliance issues as to why this may not be permissible in specific countries.

For B2B Services:

Options for User to accept Ts&Cs	Advantages	Disadvantages
In service flow (explicit consent sought by Service Provider) as extra 1 time only screen for clear acceptance	Full transparency to User. Education that full Ts&Cs are available to be read if required.	1-time only screen/step extends the authentication process as it requires explicit User action to accept. Can therefore be a drop-out point.

[13] Approaches such as "Privacy by Design" i.e. designing privacy in from the beginning will be important in this regard.

SP includes MC Ts&Cs in their own general contract Ts&Cs	Frictionless, invisible process to User.	No UX disadvantages however Operators may feel they have legal, regulatory or compliance “exposure” and require some audit method.

Table 2: A Comparison of Different Approaches to Managing Terms & Conditions for Mobile Connect

3.7 Attribute Services – Data Handling & Privacy

3.7.1 Considerations for Lawful Handling of User’s 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 a number of legal categories of regulated and protected data. As a broad principle, data should only be provided:

- with the consent of the individual to whom the data pertains, or
- where it is necessary for entering into or for the performance of a contract, or
- to meet legal obligations, or
- for the organisation’s legitimate interests (such as fraud prevention) – but where these do not infringe on the rights of individuals.

If an individual is a minor, many countries impose additional rules when processing data relating to a child. For example, requiring consent from a parent or legal guardian before data can be shared. Local laws will also identify at what age an individual is deemed to be an adult. It is recommended that Mobile Connect attribute services are not made available for minors.

In addition, if a User has a company mobile phone, where the phone is registered to the company, then some Mobile Connect attribute services may be less useful as the Operator is unlikely to hold the relevant personal information about the User

Service Providers 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 to check that a Service Provider’s processes are suitable to meet their obligations and that those obligations are clear within the contract between the Operator and the Service Provider. Further guidance can be found in “Regulatory considerations for processing personal data and attributes for Mobile Connect” [4].

3.7.1.1 Ensuring the Accuracy of User Information (Attributes)

Mobile Connect attribute services are offered on a “best efforts” basis based on what information is held by the User’s Operator .

It will be important for Operators to establish a clear and consistent process of how the data is collected and managed and also how data can be updated to ensure that the User information that is held is accurate, as far as possible.

One aspect may be to enable the User to see the information that is to be shared as part of the service flow - either before or after giving consent to enable the User to identify any inconsistencies, depending upon the use case.

The Operator should consider providing a mechanism to allow the User to update the information held by the Operator, for example, via the Operator self-service portal. Depending upon the sensitivity of the User information, different processes (User checks) may be appropriate, for example, where data is being used for KYC checks.

3.7.2 User Consent

For Mobile Connect Attribute services, User information should be processed in line with the appropriate legal basis for handling that data depending upon the use case before the requested information can be shared with the requesting Service Provider in line with the Mobile Connect Privacy Principles [3]. The principles are not intended to replace or supercede applicable law or company privacy policies.

When this involves User consent, consent may be captured by the Operator or by the Service Provider and may be captured indirectly (e.g. as part of a User accepting the terms and conditions for a service) or explicitly as part of the service flow. How consent is captured is determined by the Operator in line with any applicable local regulations and may vary depending upon specific services and use cases – anti-fraud checks, for example, would typically take place in the background and should not require any explicit User consent as part of the transaction.

For some use cases it is appropriate for consent to be given for a period of time, i.e. for more than a single transaction - referred to as long-lived consent. In this situation it will be important to ensure that the User is able to view and manage the consents that he or she has granted via a dashboard/portal including the ability to revoke that consent. Table 3 summarises the possible options for capturing User consent.

If the Operator allows the Service Provider to capture consent, then this should be reflected in the contractual agreement with the Service Provider including any requirements or constraints on how this is handled.

Who	Service Request Type	Authentication Device	Consumption Device	Comments
Service Provider (offline)	Device-Initiated or Server-Initiated	**N/A**	**N/A**	• Subject to Operator Policy and reflected in SP Contract • Consent captured as part of SP Ts & Cs • Long-lived
Service Provider (as part of SP's service flow)	Device-Initiated or Server-Initiated	✗	✓ (Device-Initiated only)	• Subject to Operator Policy and reflected in SP Contract • Consent captured as part of SP service flow e.g. during registration

Who	Service Request Type	Authentication Device	Consumption Device	Comments
				• Could be within application or verbal acceptance captured by SP, etc. • Can be long-lived
Operator (offline)	Device-Initiated or Server-Initiated	**N/A**	**N/A**	• Consent captured offline – for example, through acceptance by the User of the relevant terms and conditions relating to Mobile Connect • Long-lived
Operator (As part of MC service flow)	Server-Initiated	✓	**N/A**	• 1- step (implicit authentication) or 2-step (depending upon local regulations) • For 2 Step: • Step 1 authenticate User • Step 2: present consent context and seek approval
Operator (As part of MC service flow)	Device-Initiated	✓	✗	• 1- step (implicit authentication) or 2-step (depending upon local regulations) • For 2 Step: • Step 1 authenticate User • Step 2: present consent context and seek approval
Operator (As part of MC service flow)	Device-Initiated	✓	✓	• User authenticated on Authentication Device, Present consent context and seek approval on Consumption Device

Table 3: Options for User Consent Capture for Mobile Connect Attribute Services

3.7.2.1 Capturing User Consent within the service flow by the ID Gateway

If the Operator ID GW captures User consent, as part of the Mobile Connect service flow, the User must always be authenticated before being asked to give consent to ensure that the right person is providing this consent,. The User is authenticated via their Authentication Device and a consent prompt is displayed with a request for approval.

This might consist of a single page where the User is implicitly authenticated (they are in possession of the registered mobile device) by displaying the consent prompt on the Authentication Device or it can be two pages where on the first page the User is asked to authenticate and then on the second page the consent prompt and request for approval is presented. This latter case is a less streamlined user experience (UX) but may be a legal requirement in some jurisdictions.

- Note that for Mobile Connect attribute services, the required Level of Assurance (LoA) is determined by the Operator, typically based upon the sensitivity of the data being shared or validated with the Service Provider

Depending upon the Mobile Connect service requested, the ability to display the consent prompt on the Authentication Device (via the Authenticator) will be a limiting factor in terms of how much information can be displayed (e.g., if the requirement is to list out all the attributes and attribute values for which consent is being sought). Section 3.7.2.2 discusses what information might be presented to the User.

- An alternative is available in Device-Initiated mode, where the User is accessing the service via their laptop or tablet, for example (i.e. the Consumption Device). In this case, the User is authenticated on the Authentication Device and then the consent prompt and request for approval can be presented by the ID GW through the Consumption Device (e.g. via the browser). The Consumption Device has more flexibility in being able to present a richer consent prompt.

- If the User is consuming services via their mobile phone, the situation is similar in that the User can either be authenticated and provide consent via the Authenticator or the User can first authenticate and then be presented with the consent request via the user agent that is being used to consume the service (e.g., the mobile browser or perhaps via a WebView if the User was interacting with an SP’s application).

- Note that for Server-Initiated requests (i.e. B2B services), the only option is to use the Authenticator on the mobile device as in such scenarios the User is not directly accessing the service and therefore there is no Consumption Device associated with the Mobile Connect service request.

3.7.2.2 Contextual Information to Enable Informed User Consent

Table 4 outlines the suggested elements to be included in the consent prompt to the User to ensure that they are able to provide “informed” consent.

The Operator is responsible for choosing the optimal messaging that is appropriate for the use case, the attribute data requested, the device, and the authenticator being used – as well as complying with all relevant laws and regulations. Optimal in this case relates to balancing the requirements for a good user experience (UX) with the appropriate information to allow the User to give informed consent.

Operator Name	The Operator is asking the User for consent to share the data
SP Name	The SP or Application asking for the data
Purpose	Intended use of the data by the SP For example, “So we can proceed with your order”
What Data	A list of the User’s Data to be shared OR A list of the Claim names to be shared OR A description of the type of data from the Operator which will be shared with the SP when the User gives their consent

Period of Consent	Description of the type or length of consent the User is being asked to provide
This is Your Data	The User acknowledge that they are giving consent to share their own data and do not have permission to give consent to share someone else's data
You are Not a Child	The User is legally old enough to give consent

Table 4: Elements of the Consent Request

NOTE: The User is only giving consent for the Service Provider to use the attribute data in the context for which User consent is being requested and it should not be used for any other purposes.

3.7.2.3 Long-Lived Consent

Mobile Connect attribute services can be very useful in supporting identity verification and anti-fraud services by allowing the SP to verify the User's information in the background. In such services, the consent is likely to be captured during the service activation by the Service Provider and can be given for an extended period of time (i.e. "long-lived" consent), rather than being required on a per-transaction basis.

This allows the SP to request the Mobile Connect service for the duration that the consent is valid without having to seek User consent each time. For such use cases, the flow will be:

- When the User registers for or makes a first request to the SP for the SP service that leverages a particular Mobile Connect service, the SP will provide effective notice and capture consent appropriate to the context.
- Whenever the SP detects the need to request that Mobile Connect service, it issues a Mobile Connect attribute service request (assuming the consent is still valid) to the Operator ID GW.
- The Operator's ID GW identifies that the request is for that particular Mobile Connect service.
- The ID GW checks the request to confirm the SP's entitlement to the service including if there is valid consent, based upon the Operator's consent policy
- If the SP is entitled, the Mobile Connect request is executed and the response is provided to the SP.

Whenever the User is asked to grant long-lived consent, the User will need to be made aware of the fact that long-lived consent is being requested, the duration for which consent is being requested and how frequently this will be checked. The User should also be informed about how to revoke consent. The mechanism needs to be clearly set out before offering long-lived consent.

Where the Service Provider manages the consent, the Service Provider and Operator will need to agree a consistent process for handling long-lived consent. For example, the SP must provide evidence of consent to the Operator and also enable an option for Users to revoke this consent.

- The User will always have the choice to give or not give consent for particular information to be shared with the Service Provider

- If consent expires, then the User will need to give their consent again before information can be shared with the Service Provider.
- When consent has been revoked, the SP must not attempt to request the relevant information (until consent is given once again).

3.7.2.3.1 Use of the Access Token for Managing Long-Lived Consent

Depending upon the nature of the Mobile Connect attribute service, long-lived consent can be provided by issuing an Access Token with an extended period of validity (this is specified by the ID GW through the `<expires_in>` parameter returned along with the Access Token to the Service Provider). An alternative is to make use of a Refresh Token that can be used to “refresh” the Access Token which is optional for Mobile Connect[14].

If a valid Access Token exists, then the Service Provider can submit the Access Token directly to the Resource Server to retrieve or validate the specified attributes without the need to submit a full Mobile Connect attribute service request to the ID GW. Once the Access Token has expired, then a new service request is submitted, and a fresh Access Token is issued. If the User revokes consent, then the Access Tokens can be invalidated by the ID GW.

3.7.2.3.2 Notifications for Long-Lived Consent (Optional)

For those scenarios where the User grants long-lived consent to an SP, the Operator may wish to notify the User (e.g. via SMS) when a Mobile Connect attribute service request (for which consent has already been given) has been processed, providing greater transparency for the User.

3.7.2.3.3 Evidence of Granted Long-Lived Consent

Where an SP captures consent from the User, it must be able to demonstrate to the serving Operator and / or the User that such consent has been given. Operators are recommended to collect details such as

- The date and time when the consent is granted,
- The duration that the User agreed to,
- The Service Provider use case (purpose) for which the consent was requested and granted.

This evidence must be available to the Operator or other agreed third parties as defined in the commercial agreement between the Operator and the Service Provider.

3.7.2.3.4 Revocation of Long-Lived Consent

In accordance with the Mobile Connect Privacy Principles [3], a User must be able to revoke permission at any time and in an easy manner via the means provided by the Operator or the Service Provider – doing so prevents the Service Provider from making further Mobile Connect attribute service requests until User consent can be re-established.

Where the User grants long-lived consent to the Service Provider, the Operator will simply know that Service Provider is allowed to request the Mobile Connect service and already has

[14] Note that some Mobile Connect services prohibit the use of a Refresh Token

consent but doesn't know (at the transaction stage) when this consent was obtained. If the User wishes to revoke consent, they need to do so to the Service Provider; the Service Provider must accept this revocation request and stop requesting the Mobile Connect attribute service until they acquire User consent again. The Service Provider must also inform the Operator about revocation through a process which should also include evidence of revocation. Where an Operator grants a Service Provider the responsibility to manage consent, the requirement for a User to revoke permission towards that Service Provider must be asserted through the contract between the serving Operator and the Service Provider.

In order to ensure compliance, Operators are recommended to offer a "fail safe" option for Users to revoke permissions even when the Service Provider is managing the consent.

4 FIND – How Does the User (Mobile Customer) Find Mobile Connect

One of the benefits of adopting the Lifecycle Wheel to describe a proposition is to ensure all the elements required for that proposition are in place which includes the appropriate marketing plan to educate customers, promote the benefits of Mobile Connect and to help customers to understand how they can find or get hold of Mobile Connect.

There are two distinct scenarios for the use of Mobile Connect:

1. Where the User initiates or is involved within the Mobile Connect service flow e.g. is required to authenticate, authorise a transaction or provide user consent.

2. Where the User is not involved within the Mobile Connect service flow, for example, where a background check is to be performed by a Service Provider.

In the first case the requirement for User awareness and take-up of Mobile Connect will be important. In the second case awareness of Mobile Connect will be useful.

There are two primary channels that a User can find out about and get access to Mobile Connect: via their Operator or via a Service Provider that supports Mobile Connect.

The take up of Mobile Connect will be dependent on an understanding of what Mobile Connect can do and a level of trust in the Operator as a provider of this kind of service. As such it makes sense for Operators to be the primary driver in the introduction of Mobile Connect to its customers.

The key messages are that:

- Mobile Connect provides a secure universal identity solution which is based on Mobile Operator facilitated authentication and builds on the trust that people have in their Mobile Operator.
- It provides simple, secure and convenient access to online services. It combines the User's unique mobile number and, depending upon the uses case, a PIN to verify and authenticate the User within the Mobile Connect ecosystem.

- The User no longer needs to remember multiple usernames and passwords, Mobile Connect eliminates User frustration, ensures less abandoned transactions and drives more repeat business.
- In order to avoid setting up multiple usernames and passwords there has been a tendency to use social network log-in details. However, many people are increasingly worried about how much personal information such log-ins need and share, and whether that information will be used without permission. With Mobile Connect, no personal information is made available to the website or app that the User is logging into without their consent.
- News reports are increasingly highlighting online data security breaches that have resulted in people's passwords falling into the wrong hands. With Mobile Connect, your details are more secure because you use your mobile device to first prove your digital identity and then verify it.

As far as possible, Operators should develop a full marketing and communications strategy to effectively inform and educate the User on the benefits of Mobile Connect before their initial use as well as options to upsell (for example to the more secure Log-In with PIN) and to drive usage.

Whilst there is some convenience to Users to register at the point of consumption of a service, the so called Set-Up or Register “On-The-Fly”, they are not necessarily going to be aware of the full range of services and benefits of Mobile Connect as the Service Providers will typically promote Mobile Connect on a much more limited basis around the benefits of using it with the service they provide.

The best approach to drive penetration of Mobile Connect is to pre-register Users; ideally via a bulk registration process initially and then by pre-registering new customers. However, being pre-registered is of little value unless the User is aware of how Mobile Connect can be used, how to set it up for use with Service Providers and which Service Providers support Mobile Connect.

Registration can also be provided via other Operator channels and ideally this should be offered via the Operator ‘s self-care portal rather than via channels requiring staff interaction. The Operator Portal is also the natural place for a User to be able to manage Mobile Connect and as such it represents a natural place to promote Mobile Connect and to provide the appropriate education of what is Mobile Connect and what it can do.

The following are customer touch-points where it would makes sense to be able to promote (and register where appropriate) Mobile Connect and its benefits to customers:

- Through Mobile Connect marketing.
- When logging into an existing self-care portal with username & password.
- When the User or Operator initiates the Upgrade to “Log-In with PIN” based on an initial “Set-Up with Service Provider” registration.
- At the point of a new phone purchase / upgrade.
- At the point of porting a number in to the Operator.
- When there is a general customer service query.

Similarly, there will need to be a co-ordinated Sales and Marketing plan between Operators within the same jurisdiction that are offering Mobile Connect to promote its benefits to Service Providers. This is however, outside the scope of this handbook.

The following channels and initiatives have been found to be useful and are worth considering in order to raise awareness, educate potential Users and as opportunities to convert people to Mobile Connect. Many of these can be relatively simple and straightforward to implement alongside existing marketing channels and collateral:

- Online Channels
  - Emailing and SMS campaigns - Introduction, how to use, where to use, key security and privacy benefits
  - Mobile Connect demo video campaigns on YouTube
  - Social Media campaigns on Facebook and Twitter
  - Reminder + SMS to try Mobile Connect when Users click on "Forgotten Password" links
  - Integrating Mobile Connect onto all Operators Online Portals (internet & extranet)
  - Promote MC Banners on different websites
  - Seed stories in popular consumer / security / news blogs
  - Create own Mobile Connect blog -
- On Mobile Connect Live Sites
  - Branding Mobile Connect button with a call to action alongside MC Logo, e.g. "sign in without passwords; sign in quickly using your mobile"
  - Adding a "try Mobile Connect" link next to the "forgotten password" button
  - Adding Fast Track registration, education and progress bar
- Off-line Channels
  - Include Mobile Connect accounts as part of Operator Ts&Cs for all new subscriber contracts
  - Print posters and promotion material for shop displays
  - Call centre staff to finish all calls asking if the subscriber would like to check their Mobile Connect set-up

5 GET – Where can the User GET Mobile Connect?

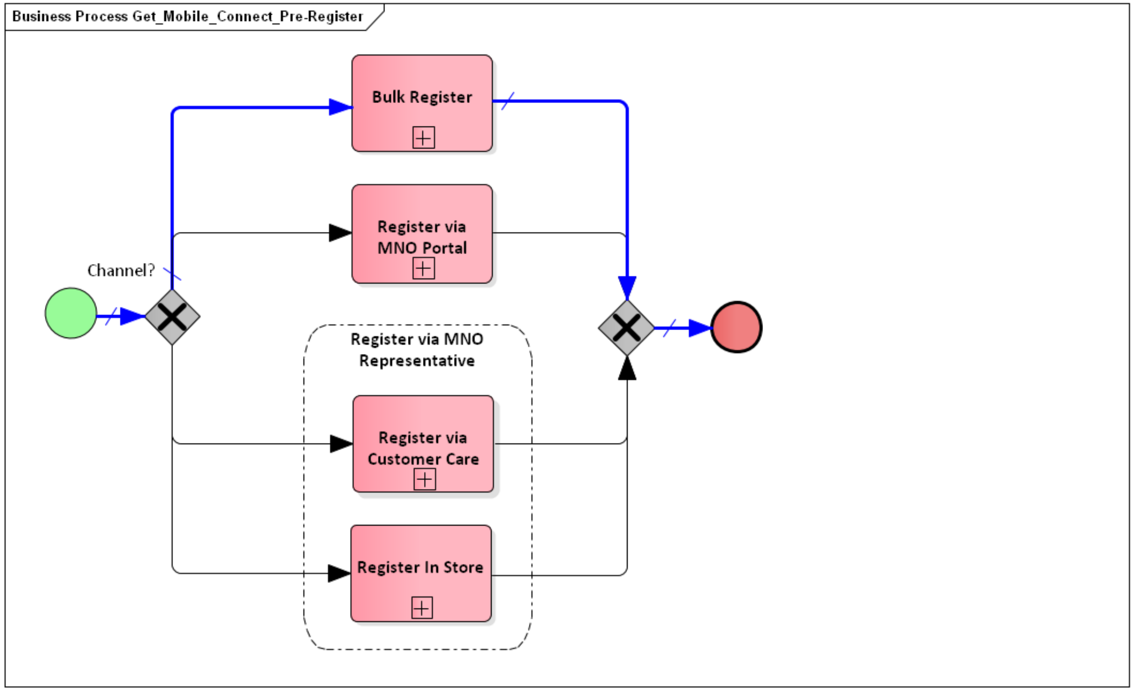

Business Process Get_Mobile_Connect_Pre-Register
Bulk Register
Register via MNO Portal
Channel?
Register via MNO Representative
Register via Customer Care
Register In Store

Figure 7 - Options for Registration for Mobile Connect with the User's Operator

Before a User is able to use Mobile Connect with a Service Provider, they must first register for a Mobile Connect account. Having obtained a Mobile Connect account, the User then needs to request the use of Mobile Connect to access a service provided by a Service Provider. This establishes a link between the User and that Service Provider and this process is repeated for each Service Provider that supports Mobile Connect and with whom the User wishes to use Mobile Connect.

There are three basic methods by which a User can Get Mobile Connect: Pre-registration by their Operator, by direct registration with their Operator or via registration at point of use with a Service Provider. Pre-registration and Direct Registration are covered within this “GET” Section and registration at point of use with a Service Provider is covered within SET-UP (Section 6).

Figure 7 outlines the options for registering for Mobile Connect via a User’s Operator: Register via Customer Care, Register in Store, Bulk Register (pre-registration) or Register via Operator Portal. Registering via Customer Care or in Store is essentially the same process, i.e., registering via an Operator Representative.

Pre-registration or bulk registration is initiated by the Operator, typically when first launching Mobile Connect services. This is the preferred mechanism to register Users for Mobile Connect and should be tied in with a customer education and marketing campaign. The Operator may Bulk Register its existing User base and then subsequently pre-provision Mobile Connect as part of its standard onboarding process (for new customers taking out a mobile contract) or enable Users to directly register via one of their Operator’s customer service touchpoints:

- The Operator’s existing online self-care portal or the Operator’s dedicated Mobile Connect self-care portal or an Operator’s online store (covered by the Register via Operator Portal process)
- The Operator’s retail stores or call centre (covered by the Register via an Operator Representative process)

A key element of registration is ensuring that the User understands the terms and conditions for the Mobile Connect service including the Mobile Connect Privacy Principles [3]. This may be achieved in a number of ways outlined in Section 3.6 but typically a summary of the terms and conditions is presented to the User as part of the registration process to which the User confirms their acceptance.

Where Mobile Connect authentication is to be implemented, it is recommended that Operators deploy Mobile Connect as the preferred log-in method for their own self-care portals. Doing so reinforces the convenience and User value proposition, whilst also delivering the very best working showcase and promotional tool for Service Providers to see the service in action.

In order to be able to register Users, as a minimum, network based authenticators must be enabled, i.e. SMS plus a URL link to confirm or a USSD application to enable Users to confirm acceptance of Ts & Cs and to be able to authenticate or authorise a transaction. This requires that these mechanisms are linked to the Operator ID GW to enable Mobile Connect. SIM-Applet or Smartphone App Authenticators require additional configuration on the User’s mobile (Authentication) device.

As mentioned previously, the ability to support a higher level of assurance is desireable in Mobile Connect as it provides greater security, is tied to a person rather than just a device and enables its use with a wider range of Service Providers. However, this can introduce additional friction in the process of "Setting up with a Service Provider". As a result basic registration only achieves LoA2 and then the User can select to upgrade to LoA3 as a separate process (included under "Manage Mobile Connect").

One of the advantages of direct registration with the User's Operator is that the process for registering to LoA3 can be executed directly. The process flows shown in this handbook have separated the basic registration from the "Upgrade to LoA3" process but this can be streamlined by the Operator.

5.1.1 GET – Bulk Registration of an Operator's Customers

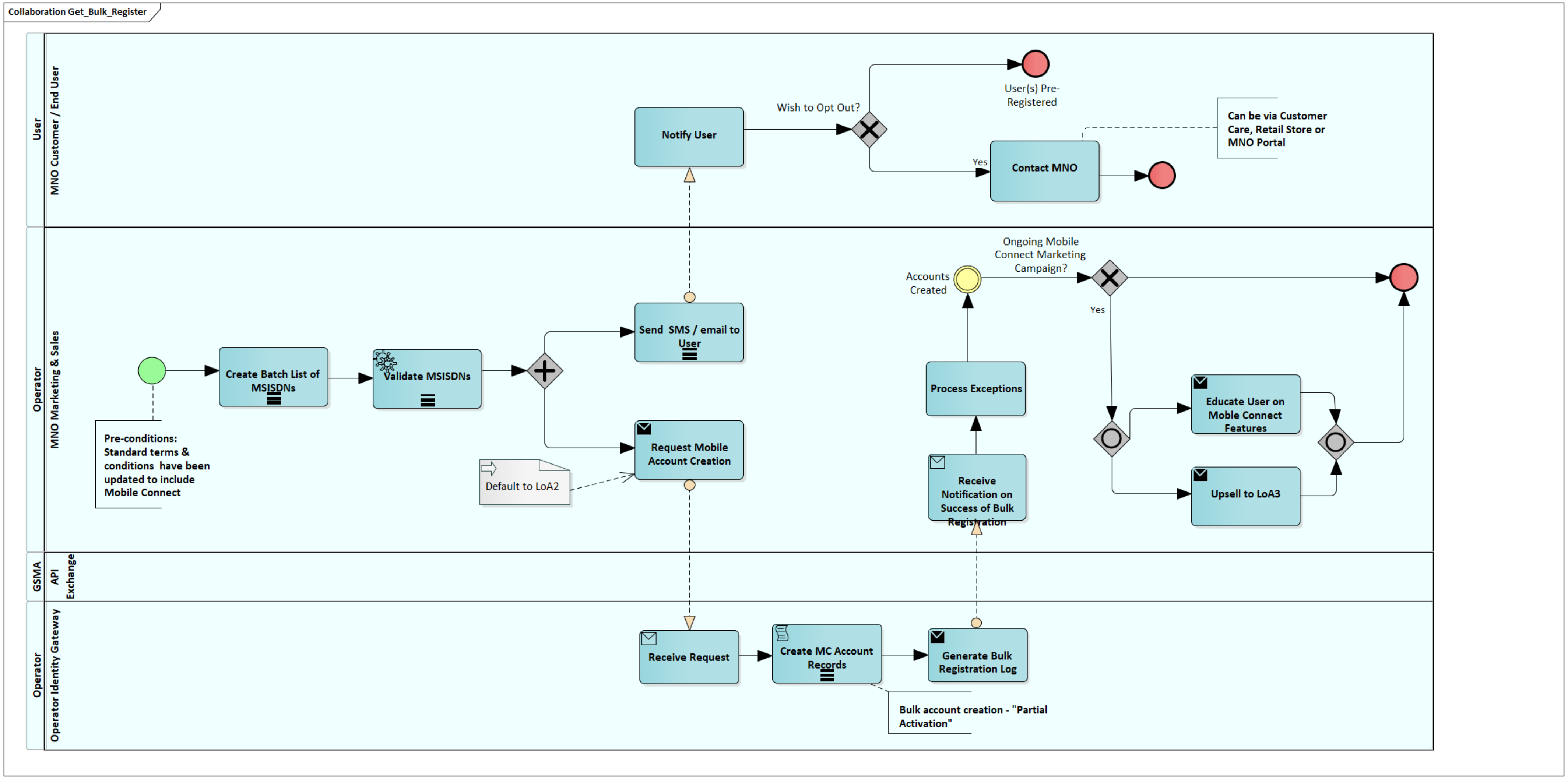

Collaboration Get_Bulk_Register
User
MNO Customer / End User
Operator
MNO Marketing & Sales
GSMA
API Exchange
Operator
Operator Identity Gateway
Notify User
Wish to Opt Out?
User(s) Pre-Registered
Yes
Contact MNO
Can be via Customer Care, Retail Store or MNO Portal
Create Batch List of MSISDNs
Validate MSISDNs
Send SMS / email to User
Request Mobile Account Creation
Default to LoA2
Pre-conditions: Standard terms & conditions have been updated to include Mobile Connect
Accounts Created
Ongoing Mobile Connect Marketing Campaign?
Yes
Process Exceptions
Receive Notification on Success of Bulk Registration
Educate User on Mobile Connect Features
Upsell to LoA3
Receive Request
Create MC Account Records
Generate Bulk Registration Log
Bulk account creation - "Partial Activation"

Figure 8: Bulk Registration of an Operator's Customers (Opt-In)

Figure 8 outlines the process for bulk registration of customers. The bulk registration process is based on a customer opt-in to Mobile Connect.

The actors involved are the User / Mobile Customer, the Operator’s Sales and Marketing Organisation and the Operator ID GW. The API Exchange is shown but does not play a role within Bulk Registration as the Bulk Registration activities take place within each Operator.

The process is as follows:

- The Sales and Marketing Organsiation prepare a Target List of MSISDNs to register for Mobile Connect. The process task has a marker which indicates that this is a process task that operates multiple times in a sequential fashion – the bulk registration will typically be carried out with blocks of Users / MSISDNs. Sales and Marketing will be able to prioritise the roll-out of Mobile Connect to particular segments or sub-segments of customers. For example, prioritising those customers who would benefit most from Mobile Connect due to the types and volumes of digital services that they consume.
- The MSISDNs are validated to check that they are valid and that there are no issues on the related Mobile Account
- An SMS or email is sent to each User. This outlines what is Mobile Connect, its benefits, outlines the terms and conditions and privacy policy. It could include a reference to where the full terms and conditions can be found and also a link for the User to confirm that they wish to proceed.
- The Users’ responses are captured and the Target List is updated accordingly
- A request is then made directly to the ID GW to create Mobile Connect Accounts for each of the Users on the validated list
- The ID GW then creates the Accounts and generates a bulk registration log
- This is passed back to the Sales and Marketing team where any exceptions where the Account was not or could not be created can be handled.
- The Sales and Marketing team could then initiate an SMS or email message to advise the User that the Account has been created, perhaps with instructions about what to do next.
- As part of an ongoing campaign, further communications could be sent to customers (those that opted in) to further educate them on the benefits of Mobile Connect and Mobile Connect Services. This could include encouragement to Upgrade their Account to LoA3.

5.1.2 GET – Register via Operator Portal

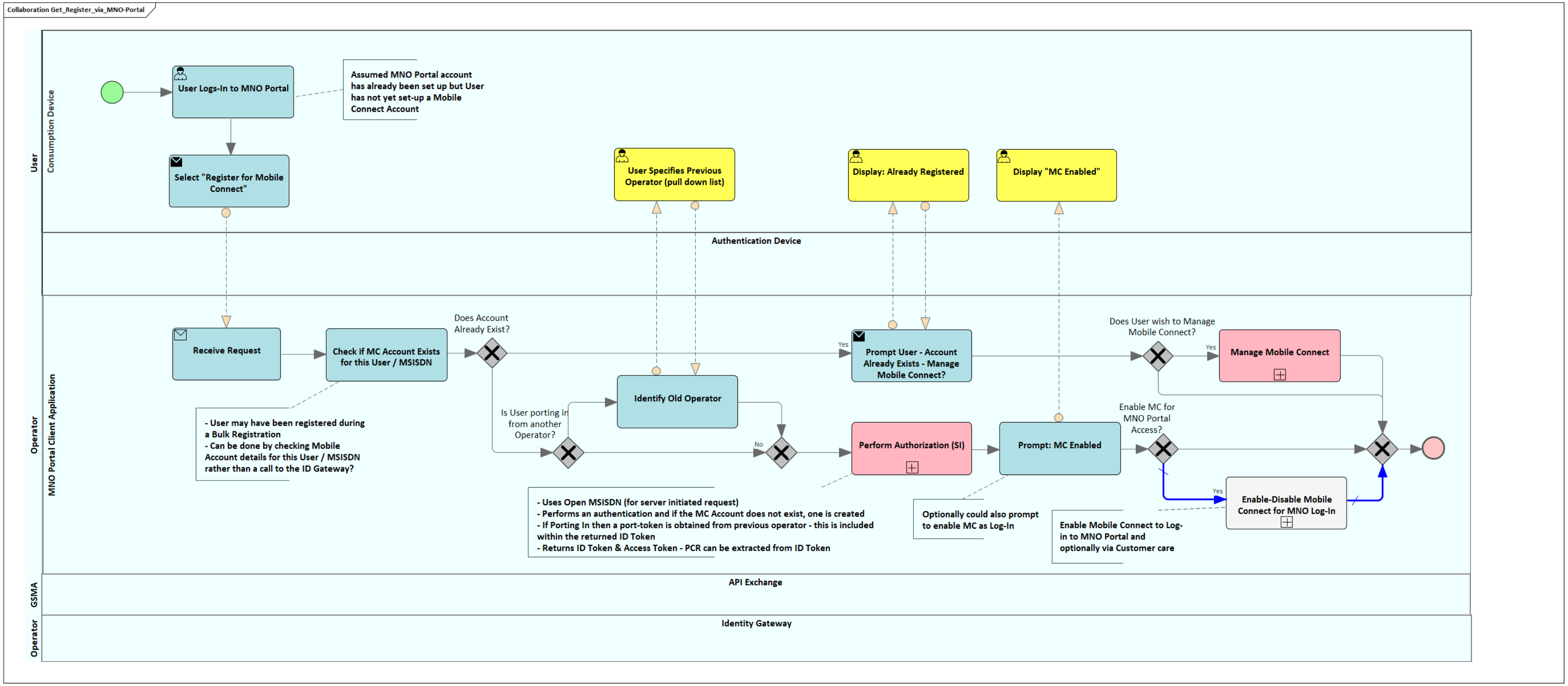

Collaboration Get_Register_via_MNO-Portal
User
Consumption Device
User Logs-In to MNO Portal
Assumed MNO Portal account has already been set up but User has not yet set-up a Mobile Connect Account
Select "Register for Mobile Connect"
User Specifies Previous Operator (pull down list)
Display: Already Registered
Display "MC Enabled"
Authentication Device
Operator
MNO Portal Client Application
Receive Request
Check if MC Account Exists for this User / MSISDN
Does Account Already Exist?
Yes
Prompt User - Account Already Exists - Manage Mobile Connect?
Does User wish to Manage Mobile Connect?
Yes
Manage Mobile Connect
Identify Old Operator
Is User porting in from another Operator?
No
Perform Authorization (SI)
Prompt: MC Enabled
Enable MC for MNO Portal Access?
Yes
Enable-Disable Mobile Connect for MNO Log-In
- User may have been registered during a Bulk Registration
- Can be done by checking Mobile Account details for this User / MSISDN rather than a call to the ID Gateway?
- Uses Open MSISDN (for server initiated request)
- Performs an authentication and if the MC Account does not exist, one is created
- If Porting In then a port-token is obtained from previous operator - this is included within the returned ID Token
- Returns ID Token & Access Token - PCR can be extracted from ID Token
Optionally could also prompt to enable MC as Log-In
Enable Mobile Connect to Log-in to MNO Portal and optionally via Customer care
GSMA
API Exchange
Operator
Identity Gateway

Figure 9: Registration for Mobile Connect via an Operator's Self Service Portal

Figure 9 illustrates the process for registration via the Operator Portal. The User logs into the Operator Portal using an existing username and password or similar, and they are presented with a number of options.Note that "Manage Mobile Connect" is shown as a sub-process – this articulates the Manage stage of the User Lifecycle and is shown in more detail in the MANAGE section of this handbook.

The actors are:

- User: Consumption Device (the device that the User is using to access the Operator Portal) and the Authentication Device. No activity is shown for the Authentication Device as this is included within the sub-process: “Perform_Authorization (SI)”
- Operator Portal Client Application which initiates the registration
- API Exchange - This could, in theory, be called as part of the Perform_Authorization (SI) sub-process but because of this context (Operator Portal Application making an API request to its own ID GW) then this does not necessarily play a role. However, if self-care was provided by a third party across different Operators then this might play a role.
- Operator Identity Gateway - Again activities are hidden within the “Perform_Authorization (SI)” sub-process.

The process is as follows:

- The Mobile Customer / User having logged in to the Operator Portal selects “Register for Mobile Connect” menu option
- Having received the request, the Operator Portal Client Application can then outline Mobile Connect and the associated terms and conditions (including Privacy Policy) to make sure that the Customer understands and to check that the Customer wishes to proceed (i.e. by accepting the terms and conditions). This will typically provide a link for the User to read the full terms and conditions before indictaing acceptance. This is not shown explicitly within Figure 8.
- The Operator Portal Client Application then checks to see if the Mobile Connect Account already exists in case the User is not aware that one has already been created, for example through bulk registration. If the Mobile Connect Account already exists then it may be necessary to check the Account Status to ensure that the account is in an Active state. In this case the User can be re-directed to the “Manage Mobile Connect” option.
    - The process includes an optional step in the case that a User wishes to port their Mobile Connect Account from another Operator – this step allows the User to indicate the Operator that they are porting from and is used subsequently to retrieve a “port_token” to faciltate the process. Mobile Connect Account porting is an optional feature and would require both Operators to support the OIDF Account Porting specification [12]. This is described in more detail in Section 9.3
- If the Mobile Connect Account does not exist then the Perform_Authorization (SI) sub-process is initiated. This goes through a server-initiated authentication. If the Mobile Connect Account does not exist then one is created. The Create_Mobile_Connect_Account Core

Process, which is initiated within the Perform_Authorization (SI) sub-process, includes prompting the User with a summary of the Ts&Cs to confirm their acceptance. On this basis the Mobile Connect Account is created and the status is set to Active.

- The option is provided for the User to use Mobile Connect to authenticate themselves / log-in to the Operator (this could include via Customer Care, Face to Face or via the Operator self-care portal). The thick blue line indicates that it would be the default / preferred option. This simply involves the Customers Mobile Account having the PCR associated with it plus a flag to indicate that the User wishes to use Mobile Connect for Log-in. The User’s username and password should be retained as a recovery mechanism in the event that Mobile Connect is suspended or if authentication via Mobile Connect fails.

Note that, apart from the channel being used, the process is the same as for the “Register via Operator Representative” process described next. In addition, this process (Register via Operator Portal) is essentially the same as the “Set-Up with Service Provider” process described in Section 6, with the Operator also acting as the Service Provider, the only difference being that a server-initiated authentication is performed rather than a device-initiated authentication and that the User in this case selects “Register for Mobile Connect” rather than simply clicking on the Log-In with Mobile Connect icon / option at Log-In. However, that option should also work.

5.1.3 GET – Registering for Mobile Connect via an Operator Representative

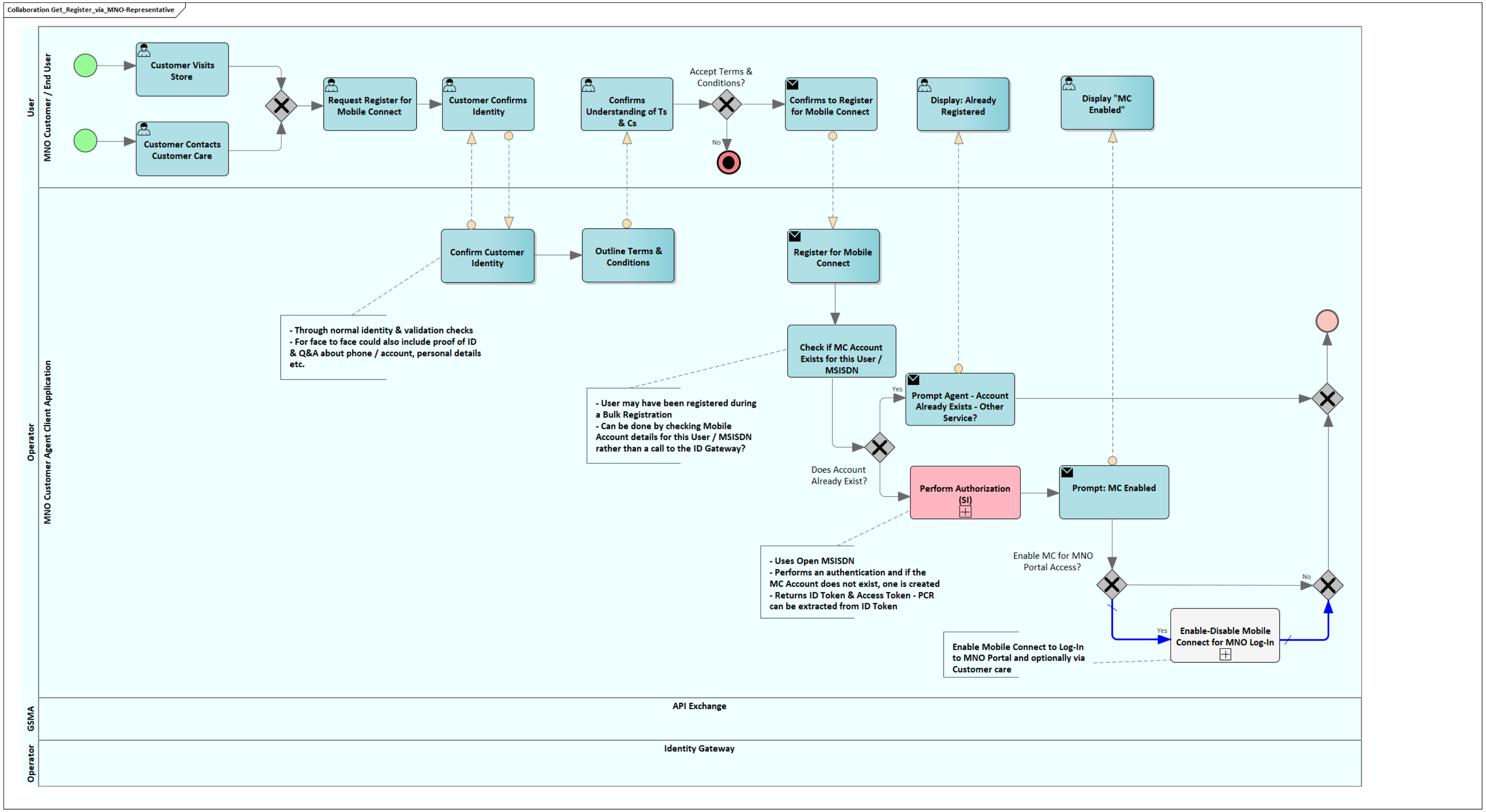

Collaboration Get_Register_via_MNO-Representative
User
MNO Customer / End User
Customer Visits Store
Customer Contacts Customer Care
Request Register for Mobile Connect
Customer Confirms Identity
Confirms Understanding of Ts & Cs
Accept Terms & Conditions?
No
Confirms to Register for Mobile Connect
Display: Already Registered
Display "MC Enabled"
Operator
MNO Customer Agent Client Application
Confirm Customer Identity
Outline Terms & Conditions
Register for Mobile Connect
- Through normal identity & validation checks
- For face to face could also include proof of ID & Q&A about phone / account, personal details etc.
Check if MC Account Exists for this User / MSISDN
- User may have been registered during a Bulk Registration
- Can be done by checking Mobile Account details for this User / MSISDN rather than a call to the ID Gateway?
Yes
Prompt Agent - Account Already Exists - Other Service?
Does Account Already Exist?
Perform Authorization (SI)
Prompt: MC Enabled
- Uses Open MSISDN
- Performs an authentication and if the MC Account does not exist, one is created
- Returns ID Token & Access Token - PCR can be extracted from ID Token
Enable MC for MNO Portal Access?
No
Yes
Enable-Disable Mobile Connect for MNO Log-In
Enable Mobile Connect to Log-In to MNO Portal and optionally via Customer care
GSMA
API Exchange
Operator
Identity Gateway

Figure 10: Get Mobile Connect via an Operator Representative (Customer Care or Retail Store)

Figure 10 illustrates the process for a User to GET (Register for) Mobile Connect via an Operator Representative. This is broadly the same whether the customer is seeking to register for Mobile Connect within an Operator's retail store or via Customer Care. The process could also be initiated by a customer agent contacting the User to promote or upsell Mobile Connect but this is not shown explicitly in the process flow.

The main actors are as follows:

- The Operator's Customer who wishes to be a User of Mobile Connect and associated services
- The Operator's Customer Agent – either a Customer Care Agent or an assistant in a retail store
- The Operator's Customer Agent Client Application – through which the Agent can check account details and also initiate Mobile Connect Registration. Whether this is all integrated into a single application or represents two separate applications is at the discretion of the Operator.
- API Exchange to enable Operator Discovery – There are no activities shown in this process because related activities are included within the sub-process: "Perform_Authorization (SI)" which incorporates the Core Process "Discover User's Operator" (See Annex A for more detail on these Core Processes). In the context of this process flow relating to Registration via an Operator Representative, the Operator Customer Agent Client Application should already know the relevant end-points for the ID GW and also has access to the Customer's / User's MSISDN so Discovery should not be necessary but more generally another Service Provider could also utlise a server initiated authentication when the process would be similar.
- Operator ID GW – Again activities are hidden within the "Perform_Authorization (SI)" sub-process.

The process is as follows:

- The Mobile Customer / User contacts their Operator either by contacting the customer service centre or by visiting a retail store and requests Mobile Connect
- The Operator's Customer Agent checks the User's identity using existing mechanisms - this could include questions and answers about their phone account, personal details, or providing a proof of ID.
- The Customer Agent outlines Mobile Connect and the associated terms and conditions (including Privacy Policy) to make sure that the Customer understands and to check that the Customer wishes to proceed (i.e. by accepting the terms and conditions). This will potentially have to be in two parts – initially a verbal description, and then potentially reinforced with a physical or electronic confirmation

(SMS or email with a link to full Ts & Cs) based on the Operator's existing local policies and processes for soliciting User acceptance of Ts&Cs initially agreed over the phone or face to face

- The Customer Agent then initiates the request to register for Mobile Connect
- The Customer Agent Client Application checks to see if the Mobile Connect Account already exists in case the User is not aware that it has already been created, for example through bulk registration. If the Mobile Connect Account already exists then it may be necessary to check the Account Status to ensure that the account is in an Active state
- If the Mobile Connect Account does not exist then the Perform_Authorization (SI) sub-process is initiated. This goes through a server initiated authentication. If the Mobile Connect Account does not exist then one is created. The Create_Mobile_Connect_Account Core Process, which is initiated within the Perform_Authorization (SI) sub-process, includes prompting the User with a summary of the Ts&Cs to confirm their acceptance. On this basis the Mobile Connect Account is created and the status is set to Active
- The option is provided for the User to use Mobile Connect to authenticate themselves / log-in to the Operator (this could include via Customer Care, Face to Face or via the Operator self-care portal). The thick blue line in Figure 10 indicates that it would be the default / preferred option. This simply involves the Customers Mobile Account having the PCR associated with it plus a flag to indicate that the User wishes to use Mobile Connect for Log-in

6 SET-UP – How Can the User Set-Up Mobile Connect?

In general the Set-Up stage of the User Lifecycle covers the setting-up or configuration of different elements that will enable the User to use Mobile Connect with a specific Service Provider that supports Mobile Connect.

Ideally, the User will already have been registered for Mobile Connect with their Operator and the process of “Set-Up is simply the process of linking a User’s profile with a Service Provider to their Mobile Connect account via the generation of a Pseudonymous Customer Reference (PCR).

This section also includes “Set-Up On-the-Fly” which covers the basic registration and set-up of Mobile Connect as well as associating a Mobile Connect PCR with a specific Service Provider at the point of service access or registration. This can be convenient to Users who have not pre-registered for Mobile Connect with their Operator and who may not be aware of what is Mobile Connect until that point.

The mechanism involves an authentication being performed including checks for an existing Mobile Connect Account and if one does not exist an Account is created and associated with the Service Provider. On-the-Fly Registration should only enable an account for basic authentication and authorisation services (LoA2). The User can at a later time contact their Operator via the Operator Portal to Upgrade to LoA3 (“Log-In with PIN”) and install/configure a relevant authenticator, as appropriate. This process is described in more detail in the “Upgrade to LoA3” process in the MANAGE Section. This approach avoids the complexity of downloading and configuring an Authenticator in the middle of the Set-Up process and allows a more straightforward registration when doing so ‘on-the-fly’, thus reducing the likelihood of drop-out in the registration process.

In order to upgrade to LoA3, the User must obtain and configure an appropriate Authenticator. Since these elements of “Set-Up” are closely tied to the “Upgrade to LoA3” process, the setting up of either a SIM-Applet or Smartphone Authentication App for PIN/Passcode entry are included under “Manage Mobile Connect”

6.1 Setting Up Mobile Connect for Use with a Service Provider

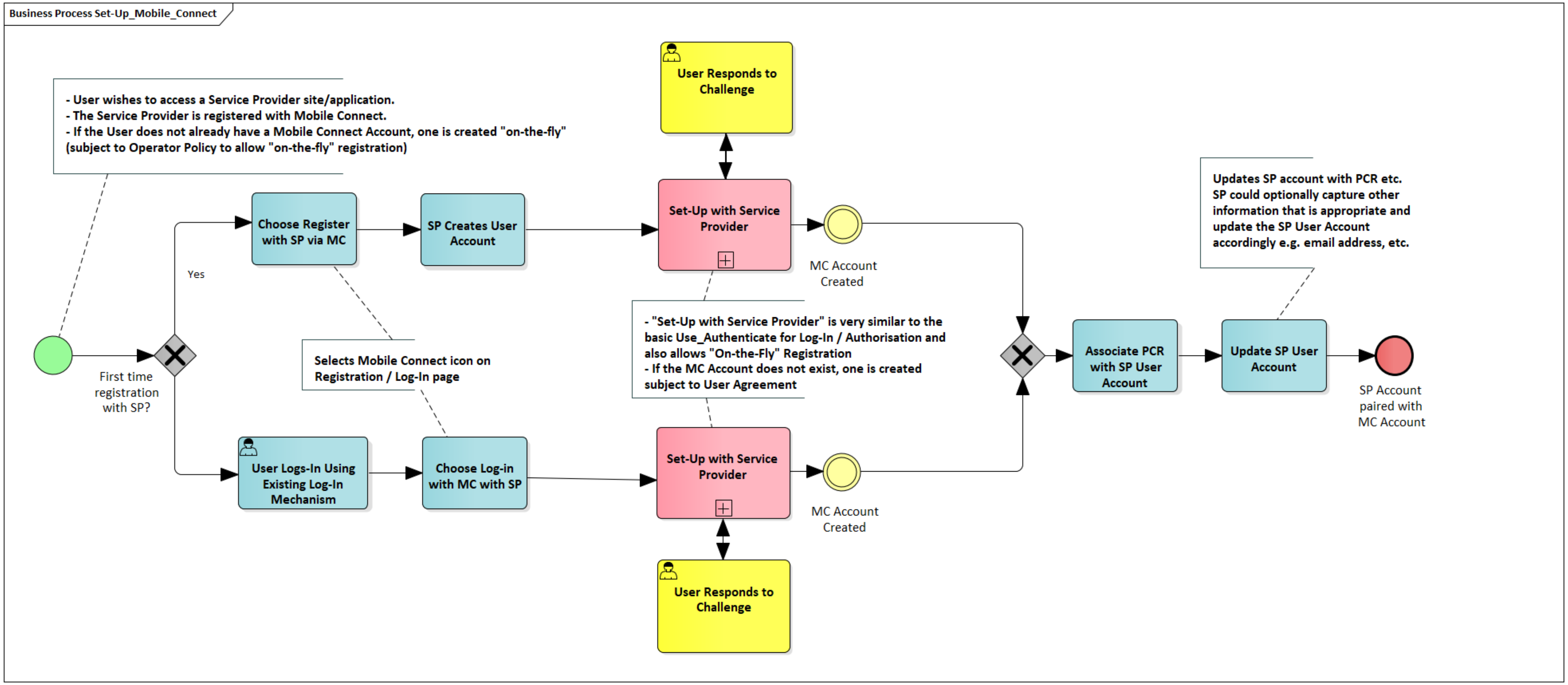

Business Process Set-Up_Mobile_Connect
- User wishes to access a Service Provider site/application.
- The Service Provider is registered with Mobile Connect.
- If the User does not already have a Mobile Connect Account, one is created "on-the-fly" (subject to Operator Policy to allow "on-the-fly" registration)
First time registration with SP?
Yes
Choose Register with SP via MC
SP Creates User Account
Selects Mobile Connect icon on Registration / Log-In page
User Logs-In Using Existing Log-In Mechanism
Choose Log-in with MC with SP
User Responds to Challenge
Set-Up with Service Provider
MC Account Created
- "Set-Up with Service Provider" is very similar to the basic Use_Authenticate for Log-In / Authorisation and also allows "On-the-Fly" Registration
- If the MC Account does not exist, one is created subject to User Agreement
Set-Up with Service Provider
MC Account Created
User Responds to Challenge
Associate PCR with SP User Account
Update SP User Account
Updates SP account with PCR etc. SP could optionally capture other information that is appropriate and update the SP User Account accordingly e.g. email address, etc.
SP Account paired with MC Account

Figure 11 - High Level Flow for Registration and Set-Up of Mobile Connect with a Service Provider

Figure 11 shows a high level process flow for a User who wishes to access a Service Provider’s site or application and wishes to use Mobile Connect. There are four possible scenarios:

- User has not registered for Mobile Connect and has not registered with the Service Provider
- User has registered for Mobile Connect and has not registered with the Service Provider
- User has not registered for Mobile Connect and is an existing customer with the Service Provider
- User has registered for Mobile Connect and is an existing customer with the Service Provider

These 4 scenarios are covered in Figure 11 – the choice to either log-in as an existing customer to the Service Provider’s site or application or to register with the Service Provider for the first time is shown explicitly. By the User selecting Mobile Connect either to Log-In or to Register (for example, by clicking the Mobile Connect icon) the “Set-Up with Service Provider” sub-process is initiated which performs an authentication and if the User’s Mobile Connect Account does not already exist then one is created.

If the User is a new customer to the Service Provider then the Service Provider creates a new User profile or account. The Service Provider would typically request further information such as a name, an email address and other information depending upon the nature of the service. Alternatively the Service Provider could request this information as an Identity or Attribute request via Mobile Connect if it has registered for these services and subject to the User’s consent. This process is shown in the USE Section. One thing to note is that if the User requests to register with the Service Provider via Mobile Connect then the PCR could be the only identifier for that User unless the Service Provider requests further information.

The “Set-Up with Service Provider” sub-process is initiated by the User Agent (e.g., browser or app) on the Consumption Device (i.e. it is device initiated). “Set-Up with Service Provider” will call the “Discover Users Operator” core process to obtain the Operator’s credentials. Set-Up with Service Provider” will also request an authentication. This will prompt the User on their mobile device (Authentication Device) to confirm the request to authenticate and / or create a Mobile Connect Account.

Assuming the authentication is successful an ID Token and Access Token are generated by the Operator ID GW and returned to the Service Provider. The ID Token contains a PCR which links the Mobile Connect User to this Service Provider and can be used by the Service Provider for subsequent Mobile Connect transactions to identify the User. This information would be stored in the User’s profile.

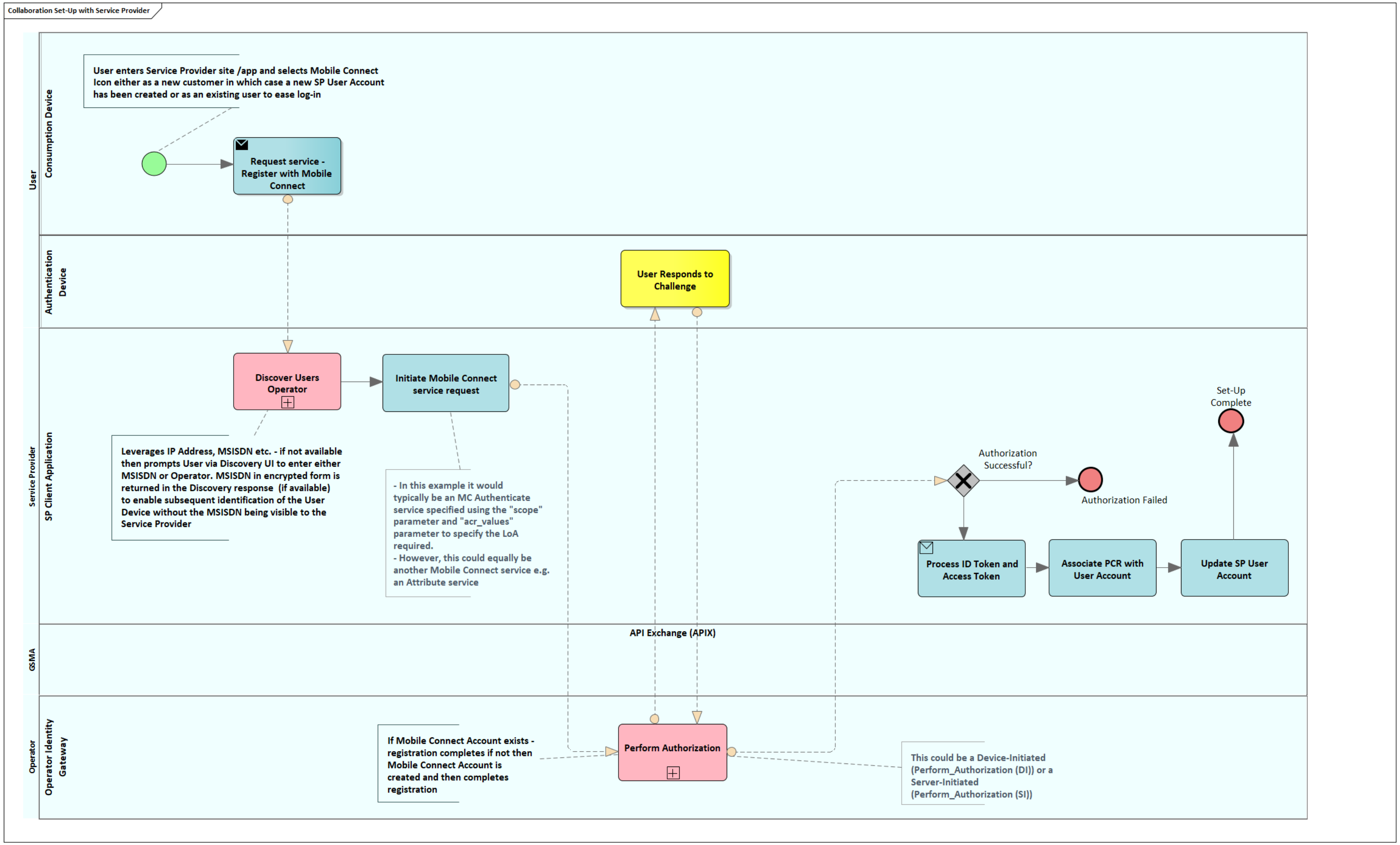

Collaboration Set-Up with Service Provider
User
Consumption Device
Authentication Device
Service Provider
SP Client Application
GSMA
API Exchange (APIX)
Operator
Operator Identity Gateway
User enters Service Provider site /app and selects Mobile Connect Icon either as a new customer in which case a new SP User Account has been created or as an existing user to ease log-in
Request service - Register with Mobile Connect
User Responds to Challenge
Discover Users Operator
Initiate Mobile Connect service request
Leverages IP Address, MSISDN etc. - if not available then prompts User via Discovery UI to enter either MSISDN or Operator. MSISDN in encrypted form is returned in the Discovery response (if available) to enable subsequent identification of the User Device without the MSISDN being visible to the Service Provider
- In this example it would typically be an MC Authenticate service specified using the "scope" parameter and "acr_values" parameter to specify the LoA required.
- However, this could equally be another Mobile Connect service e.g. an Attribute service
Authorization Successful?
Authorization Failed
Set-Up Complete
Process ID Token and Access Token
Associate PCR with User Account
Update SP User Account
If Mobile Connect Account exists - registration completes if not then Mobile Connect Account is created and then completes registration
Perform Authorization
This could be a Device-Initiated (Perform_Authorization (DI)) or a Server-Initiated (Perform_Authorization (SI))

Figure 12: Sub-Process: Set-Up With A Service Provider

Figure 12 shows the "Set-Up with Service Provider" sub-process in more detail.

The actors are:

- User: Consumption Device and Authentication Device
- Service Provider: Client Application
- API Exchange: This does not have any activities explicitly shown but is called during the "Discover User's Operator" sub-process
- Operator: ID GW

"Set-Up with Service Provider" uses a device-initiated process where the request for Authentication is initiated by the User on the Consumption Device. The process allows Operator Discovery by the Service Provider (to recover the appropriate endpoints for the correct Operator ID GW) and User identification by the ID GW without the User having to reveal their MSISDN to the Service Provider. Once a User has set-up Mobile Connect for use with a specific Service Provider then the PCR can be used by the Service Provider thereafter for identifying the User to the ID GW in subsequent Mobile Connect service requests. The device-initiated process includes a number of re-directs to allow the User (via the User Agent – for example their browser) to open an interface with their Operator ID GW to enter relevant information and then return back to the Service Provider's application.

Note that "Set-Up with Service Provider" is a simplified version of the Use_Authenticate Core Process described in the USE Section

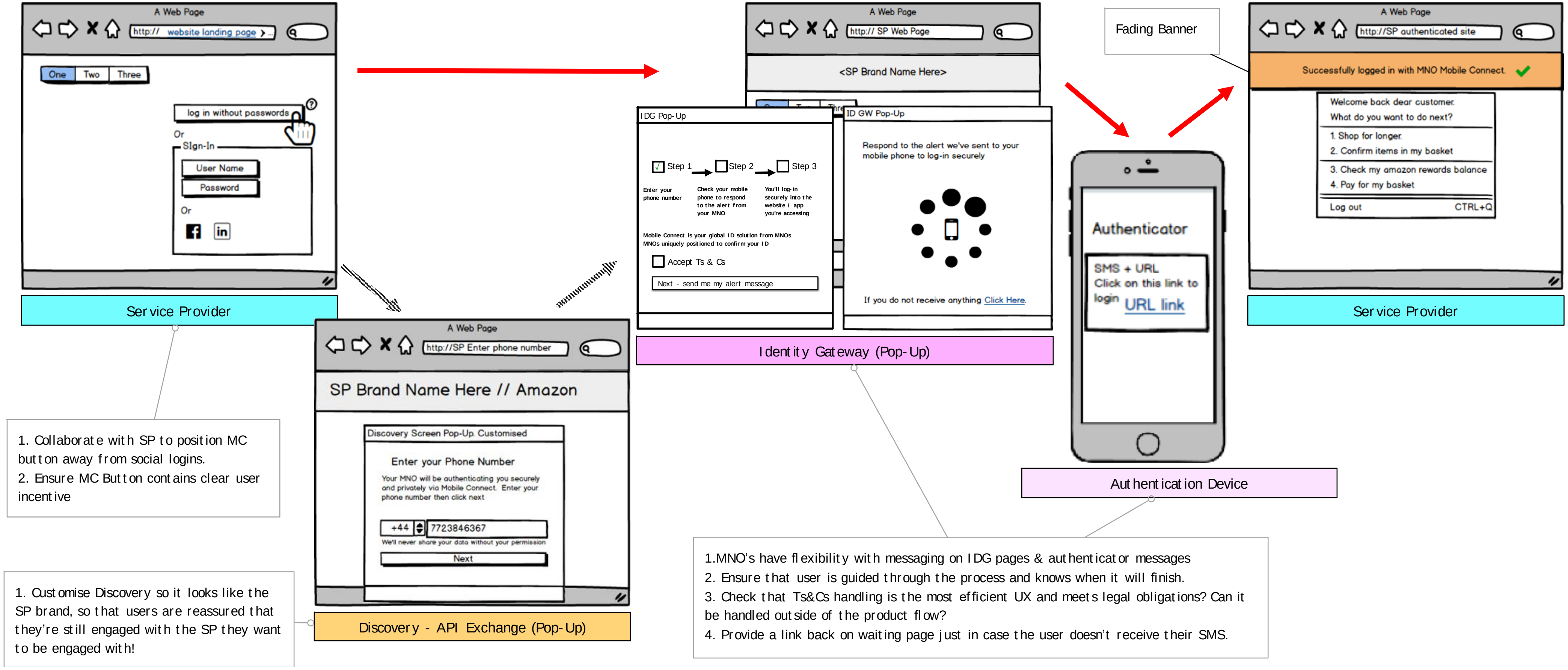
The process is as follows:

- The User requests an authentication by selecting the relevant option within the Service Provider's application – for example by clicking a Mobile Connect 'login' button.
- The Service Provider receives the request and seeks to identify the User's Mobile Operator.
- The "Discover User's Operator" sub-process (See Annex A) seeks to identify the User's Mobile Operator and the end-points to which to direct the relevant API calls. Within the Discovery process the User may be directed to the Discovery UI to provide their MSISDN and possibly to identify the Operator explicitly, to assist in the discovery process in order to provide the correct Operator details back to the Service Provider. Included in the response back to the Service Provider is the User's MSISDN in encrypted form which can then be passed on to the Operator's Identity GW (via a service authorisation request) to identify the User.
- The Service Provider constructs an OIDC Authorization request that is sent via the User agent to the Operator ID GW. The Service Provider can specify within the request the required Level of Assurance (e.g. LoA2 or LoA3) and the type of service required (via

specific scope values) and any appropriate prompt-text that should be presented to the User, if applicable, providing context of what a User is being asked to authorise etc. In practice, for a basic authentication, additional context is not typically required as the Operator ID GW will use a standard prompt (prompt action text) for this.

- The OIDC Authorization request is forwarded to the ID GW via the User Agent, so that the User Agent is looking at the ID GW and can receive the OIDC Authorization response back from the ID GW with a redirect back to their Service Provider's client application. This response is then forwarded back to the client application.
- Within the context of the OIDC Authorization request (using the "Perform_Authorization (DI)" sub-process), a check is made to see if the Mobile Connect Account already exists or not. If it does exist, then the User may be prompted and challenged on their Authentication Device to authenticate. Whilst this is the default behaviour there are some use cases where the service is being accessed via a mobile device (Mobile data flag is set) where seamless authentication can be performed without the User having to explicitly respond. If the Mobile Account does not exist, then one is created, and the User will be prompted to confirm the creation of a Mobile Connect Account.
- Within the OIDC Authorization response that the Client Application ultimately receives there is a time-limited Authorization Code that can then be used by the Service Provider to obtain tokens from the Operator ID GW. These tokens are an ID Token within which is the PCR (and other information on the authentication event) and an Access Token which can be used by the Service Provider for fetching attributes/comparison results (for those MC services involving attributes).
- The SP should store the PCR and Operator's details (endpoints & credentials) in the Service Provider's User Account for future reference. Note that this step is duplicated in Figure 11 to provide clarity for the high-level process.

6.2 SET-UP – What Does the User Experience Look Like?



Enter your Phone Number

Your MNO will be authenticating you securely and privately via Mobile Connect. Enter your phone number then click next

We'll never share your data without your permission

Enter your phone number

Check your mobile phone to respond to the alert from your MNO

You'll log-in securely into the website / app you're accessing

Mobile Connect is your global ID solution from MNOs
MNOs uniquely positioned to confirm your ID

Respond to the alert we've sent to your mobile phone to log-in securely

If you do not receive anything Click Here.

Click on this link to login

Successfully logged in with MNO Mobile Connect. ✓

Welcome back dear customer.
What do you want to do next?
1. Shop for longer.
2. Confirm items in my basket
3. Check my amazon rewards balance
4. Pay for my basket

1. Collaborate with SP to position MC button away from social logins.
2. Ensure MC Button contains clear user incentive

1. Customise Discovery so it looks like the SP brand, so that users are reassured that they're still engaged with the SP they want to be engaged with!

1.MNO's have flexibility with messaging on IDG pages & authenticator messages
2. Ensure that user is guided through the process and knows when it will finish.
3. Check that Ts&Cs handling is the most efficient UX and meets legal obligations? Can it be handled outside of the product flow?
4. Provide a link back on waiting page just in case the user doesn't receive their SMS.

Figure 13: Set-Up with a Service Provider

Figure 13 illustrates what the User will see during the process of setting up to use Mobile Connect with a Service Provider. The figure includes some guidelines on optimising the User Experience (UX).

- In this example, the User accesses the Service Provider's web page via a browser on the Consumption Device (which is not the same as the Authentication Device).

- If the Service Provider has already captured the User’s MSISDN or another identifier and includes this within the Discovery request, then the relevant Operator credentials and endpoints are returned to the Service Provider without the User being prompted to enter their MSISDN; bypassing this step in Figure 13. Further details on the Discovery process can be found in [8].

- The User is guided through the process and (in this example) required to indicate that they accept the terms and conditions for Mobile Connect before a Mobile Connect account is created for the User. Note that if the User has already registered for Mobile Connect directly with their Operator then acceptance of terms and conditions is not required at this stage as they will have already accepted them during registration.

- The User is then advised to check their mobile device (Authentication Device) for a prompt to Authenticate. In this example the Authenticator is SMS+URL.

- A banner displays the outcome of the process in the browser or application on the Consumption Device.

- Note also that Figure 13 would apply where the User is registering for Mobile Connect directly with their Operator via their Operator Portal – the web page would be the Operator Portal pages, as described in Section 5.1.2

Further information on design guidelines can be found in [13]. In addition, various pieces of market insight can be found in [14] and [15].

7 USE – How Does the User USE Mobile Connect?

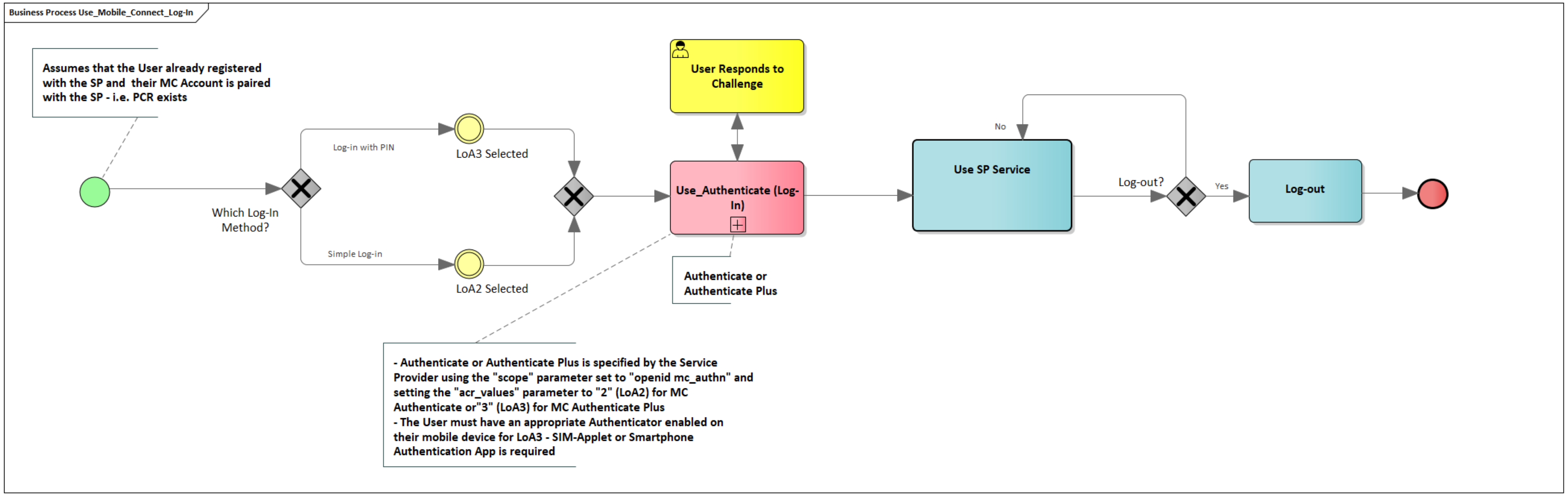
The following process flows illustrate:

- Authentication (Log-In) with a Service Provider
- Authorisation of a transaction such as making a payment using Mobile Connect
- Request for information relating to Identity and Attribute Services typically where a User is logged into a Service Provider and requests an additional service for which certain attributes are required.

These are underpinned by the core processes around “Use_Authenticate” and “Request User Information” which show the process flows at a lower level of detail. For Authorisation of Transactions, Identity and Attribute Services the User is first logged in (Authenticated) before the subsequent transaction takes place.

In addition, the process for a B2B transaction is shown where attributes are requested by a Service Provider directly from an Operator and User consent is not explicitly required by the Operator on the basis that this is managed by the Service Provider. In this situation if the User does not have a Mobile Connect Account then one is created. However, the account is not fully Active and only supports this B2B Attribute service until the User registers for Mobile Connect directly and accepts the T&Cs. As described previously, in this scenario the User’s Mobile Account should be set-up with a “Closed” status and the “Active for B2B Attributes” flag set.

7.1 USE - Authentication


Business Process Use_Mobile_Connect_Log-In
Assumes that the User already registered with the SP and their MC Account is paired with the SP - i.e. PCR exists
Which Log-In Method?
Log-in with PIN
Simple Log-in
LoA3 Selected
LoA2 Selected
User Responds to Challenge
Use_Authenticate (Log-In)
Authenticate or Authenticate Plus
Use SP Service
No
Log-out?
Yes
Log-out

- Authenticate or Authenticate Plus is specified by the Service Provider using the "scope" parameter set to "openid mc_authn" and setting the "acr_values" parameter to "2" (LoA2) for MC Authenticate or"3" (LoA3) for MC Authenticate Plus
- The User must have an appropriate Authenticator enabled on their mobile device for LoA3 - SIM-Applet or Smartphone Authentication App is required

Figure 14 - High Level Flow for Log-In

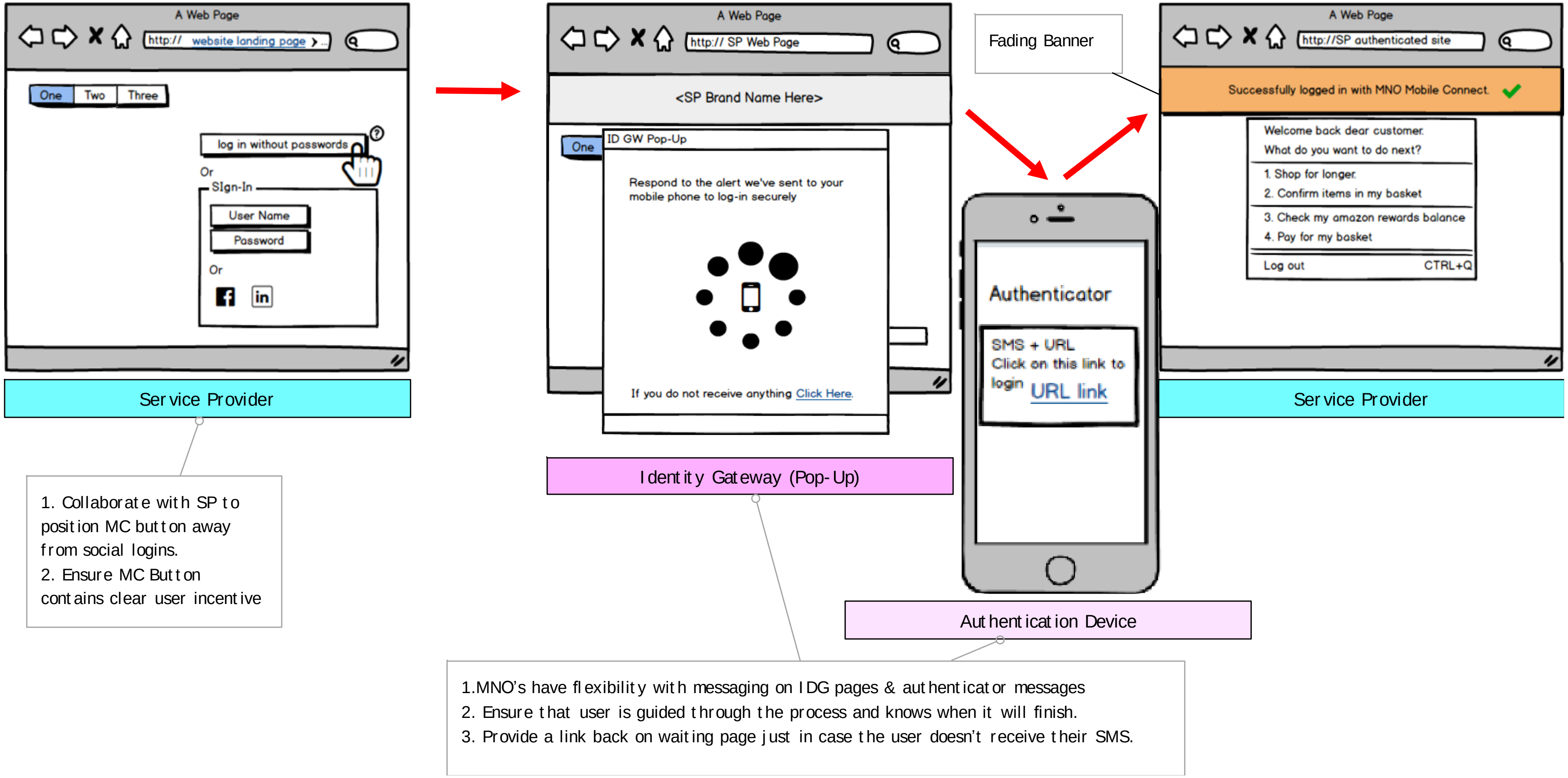
Figure 14 illustrates the high-level process flow for Authentication or Log-In.

- The assumption in this example is that the User has already registered for Mobile Connect and has already Set-Up Mobile Connect with this Service Provider. As a result, the Service Provider has the Pseudonymous Customer Reference (PCR) associated with this User recorded in the User's profile (Service Provider's User Account) and the associated Operator endpoints in order to be able to request a User authentication.
- The Service Provider will determine whether it requires basic Log-In (LoA2) or Log-In with PIN/biometric (LoA3) and includes this within the request for User Authentication.
- The ability to provide basic Log-In or Log-In with PIN/biometric is determined by the Operator's ability to support LoA3 as well as the type of device that the User is using. Log-In with PIN (LoA3) will require either a SIM-Applet Authenticator to be installed and set-up on the User's Mobile Phone SIM/UICC or a Smartphone App Authenticator to have been installed and set-up on the User's phone. The

relative advantages and disadvantages of these approaches are summarised in Section 3.3. It may be that the Operator who wishes to provide LoA3 supports only SIM-Applet or both SIM-Applet for feature phones and an App for Smartphones depending on their customer base and the devices in use within the market.

- Authentication is handled within the Use_Authenticate Core Process (See Figure 18) and will return an ID Token which includes the PCR (that can be cross checked with the PCR submitted in the OIDC Authorization Request) and an Access Token which can be used for requesting attributes (restricted to those MC services that were requested and authorised within the OIDC Authorization Request). The high-level process flow assumes that the Authentication is successful and therefore access to the Service Provider’s service is granted.
    - The User is asked to Authenticate with a challenge being sent to their mobile device (Authentication Device) via the appropriate Authenticator, to which the User responds.
    - If a request is made for LoA3 but the User can only authenticate to LoA2 then this is returned to the Service Provider is the Authentication Response and the Service Provider can then decide how best to act on the achieved level of Authentication
    - Equally if the Authentication is unsuccessful, the Service Provider can then decide on how to proceed, for example they may request an alternative Log-In mechanism or simply terminate the process with an appropriate message.

7.1.1 USE – Authentication - What does the User Experience Look Like?


A Web Page
http:// website landing page
One
Two
Three
log in without passwords
Or
SIgn-In
User Name
Password
Or
Service Provider
A Web Page
http:// SP Web Page
<SP Brand Name Here>
One
ID GW Pop-Up
Respond to the alert we've sent to your mobile phone to log-in securely
If you do not receive anything Click Here
Identity Gateway (Pop-Up)
Fading Banner
Authenticator
SMS + URL
Click on this link to login
URL link
Authentication Device
A Web Page
http://SP authenticated site
Successfully logged in with MNO Mobile Connect
Welcome back dear customer.
What do you want to do next?
1. Shop for longer.
2. Confirm items in my basket
3. Check my amazon rewards balance
4. Pay for my basket
Log out
CTRL+Q
Service Provider

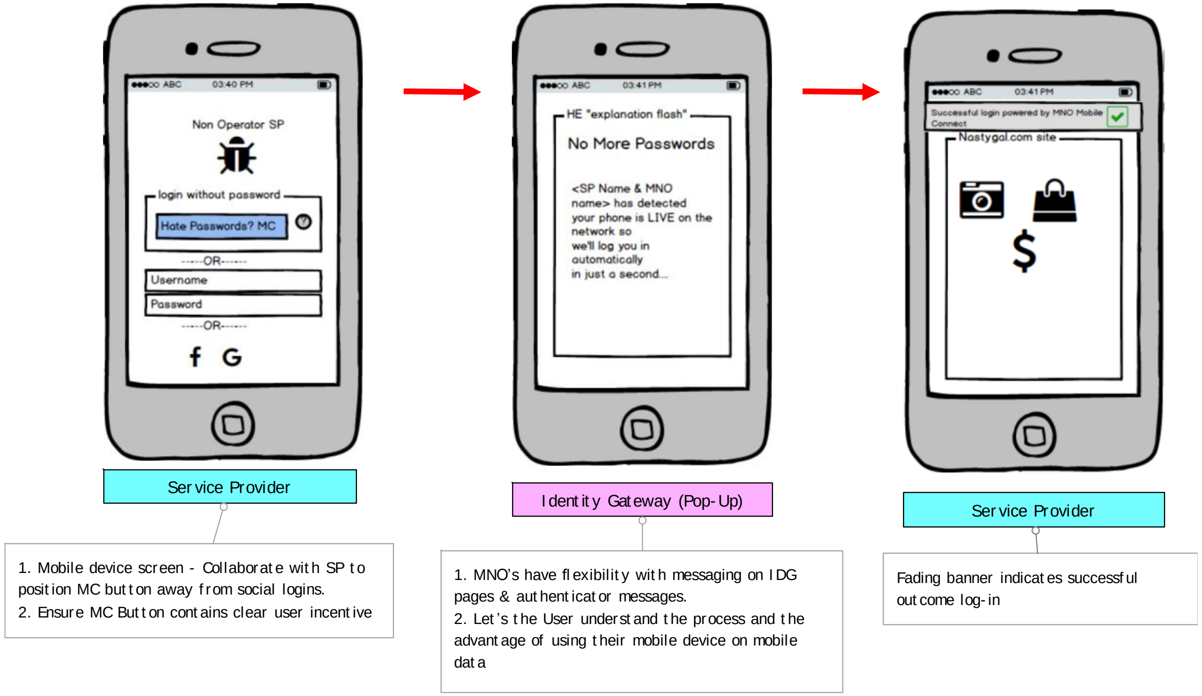
1. Collaborate with SP to position MC button away from social logins.
2. Ensure MC Button contains clear user incentive

1.MNO's have flexibility with messaging on IDG pages & authenticator messages
2. Ensure that user is guided through the process and knows when it will finish.
3. Provide a link back on waiting page just in case the user doesn't receive their SMS.

Figure 15: User Log-In with Separate Consumption and Authentication Devices

Figure 15 illustrates the User Experience where a User has already set-up Mobile Connect for Log-In with a Service Provider. The same considerations apply as discussed under SET-UP. Note that as the SP has already determined the correct serving Operator for the target User, the Discovery step is not required hence normal Log-In is more streamlined than the initial Set-Up.

If access is via the mobile device and the Operator supports Enrichment of the HTTP Header with MSISDN (HHE) then an even more streamlined process can be achieved for basic Log-In as illustrated in Figure 16. This is referred to as "seamless" Log-In where the User's network-authenticated MSISDN can be passed directly to the ID GW within the Enriched Header hence explicit User authentication is not required (i.e., the User's device has already been authenticated to the network and the User is therefore implicitly authenticated through association with that device; if the SP wants confidence that a particular User is responding they will need to step-up the level of assurance to 2-factors = LoA3).



No More Passwords

<SP Name & MNO name> has detected your phone is LIVE on the network so we'll log you in automatically in just a second....

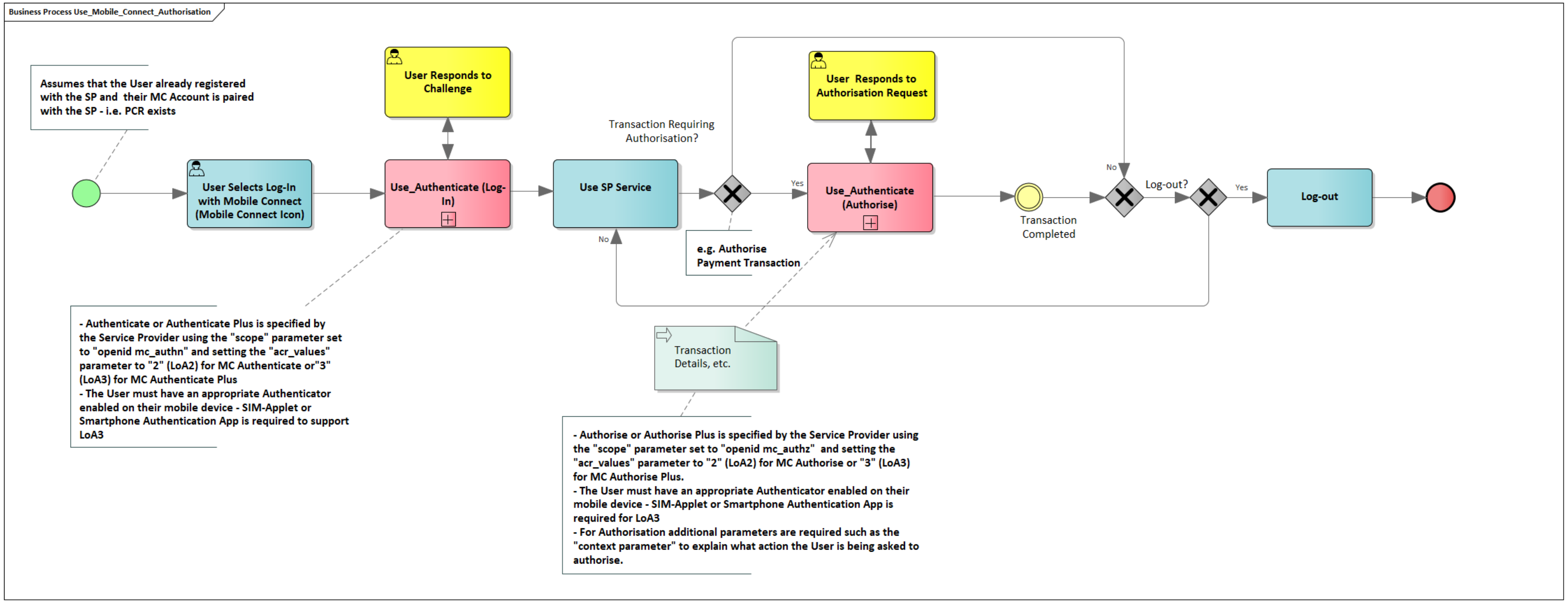
1. Mobile device screen - Collaborate with SP to position MC button away from social logins.
2. Ensure MC Button contains clear user incentive

1. MNO's have flexibility with messaging on IDG pages & authenticator messages.
2. Let's the User understand the process and the advantage of using their mobile device on mobile data

Fading banner indicates successful outcome log-in

Figure 16: Seamless Log-In

7.2 USE - Authorisation


Business Process Use_Mobile_Connect_Authorisation
User Selects Log-In with Mobile Connect (Mobile Connect Icon)
User Responds to Challenge
Use_Authenticate (Log-In)
Use SP Service
Transaction Requiring Authorisation?
No
Yes
User Responds to Authorisation Request
Use_Authenticate (Authorise)
Transaction Completed
No
Log-out?
Yes
Log-out
Transaction Details, etc.

Assumes that the User already registered with the SP and their MC Account is paired with the SP - i.e. PCR exists

e.g. Authorise Payment Transaction

- Authenticate or Authenticate Plus is specified by the Service Provider using the "scope" parameter set to "openid mc_authn" and setting the "acr_values" parameter to "2" (LoA2) for MC Authenticate or"3" (LoA3) for MC Authenticate Plus
- The User must have an appropriate Authenticator enabled on their mobile device - SIM-Applet or Smartphone Authentication App is required to support LoA3

- Authorise or Authorise Plus is specified by the Service Provider using the "scope" parameter set to "openid mc_authz" and setting the "acr_values" parameter to "2" (LoA2) for MC Authorise or "3" (LoA3) for MC Authorise Plus.
- The User must have an appropriate Authenticator enabled on their mobile device - SIM-Applet or Smartphone Authentication App is required for LoA3
- For Authorisation additional parameters are required such as the "context parameter" to explain what action the User is being asked to authorise.

Figure 17 - High Level Flow for Authorisation of a Transaction

Figure 17 illustrates the high-level process for Authorisation which builds on the Authentication flow shown in Figure 14. In this case there is the option for a further transaction to take place within the current session, for example to authorise a payment. The User has already Logged-In either by Authenticating using Mobile Connect or by an alternative mechanism approved by the Service Provider. However, the best User Experience would be obtained by using Mobile Connect to Authenticate and then to Authorise the Transaction.

- As before, the assumption is that the User has already registered for Mobile Connect and has already Set-Up Mobile Connect with this Service Provider. As a result, the Service Provider has the Pseudonymous Customer Reference (PCR) associated with this User recorded in the User’s profile (Service Provider’s User Account) and the associated Operator endpoints in order to be able to request a User authentication.

- The User Logs-In to the online service or application and starts to use that service. Within the service there is the option to authorise a transaction, for example to authorise a payment using stored card details with the Service Provider.
- The Authorisation makes use of the same sub-process, “Use_Authenticate”, as the Authentication. The difference is in the requested service (specified by the <scope> parameter in the service request (OIDC Authorization request) and in providing details of the transaction which can then be presented to the User in the context of the Authorisation, i.e. “this is the transaction that you are authorising”. The User then responds to the challenge to authorise the transaction or not. In Figure 13 the assumption is made that the transaction is successful i.e. authorisation is given and does not show what would happen in the event the authorisation was not successful as this would be down to how the Service Provider wishes to proceed.
- Depending on the nature of the transaction and the information that the Service Provider wishes to display and the capabilities of the User’s device and associated Authenticator, the information can be displayed on the Consumption Device, for example within the browser, or both the information and the challenge are displayed on the Authentication device. For example, there is a limit on the amount of information that can be displayed within a SIM-Applet and so it may be preferable to display the information about the transaction on the Consumption device. Note that if the consumption device is used for this purpose, it is imperative that the User first authenticates via the authentication device and then is asked to review and authorise the transaction via the consumption device, hence ensuring that only the right User (authenticated User) is authorising the transaction.

Figure 18 shows the Use_Authenticate sub-process which is referenced in the high-level authentication and authorisation process flows shown previously. This is a lower level process and illustrates the different actors involved with pools and swim-lanes. It shows the Consumption Device and Authentication Device of the User, the Client Application of the Service Provider, the API Exchange for discovery and the Operator ID GW. Although there are no activities shown within the API Exchange, these are part of the Discover User’s Operator sub-process.

The sub-process uses two other sub-processes: “Discover User’s Operator” and “Perform_Authorization (DI)”. which are shown in Annex A.

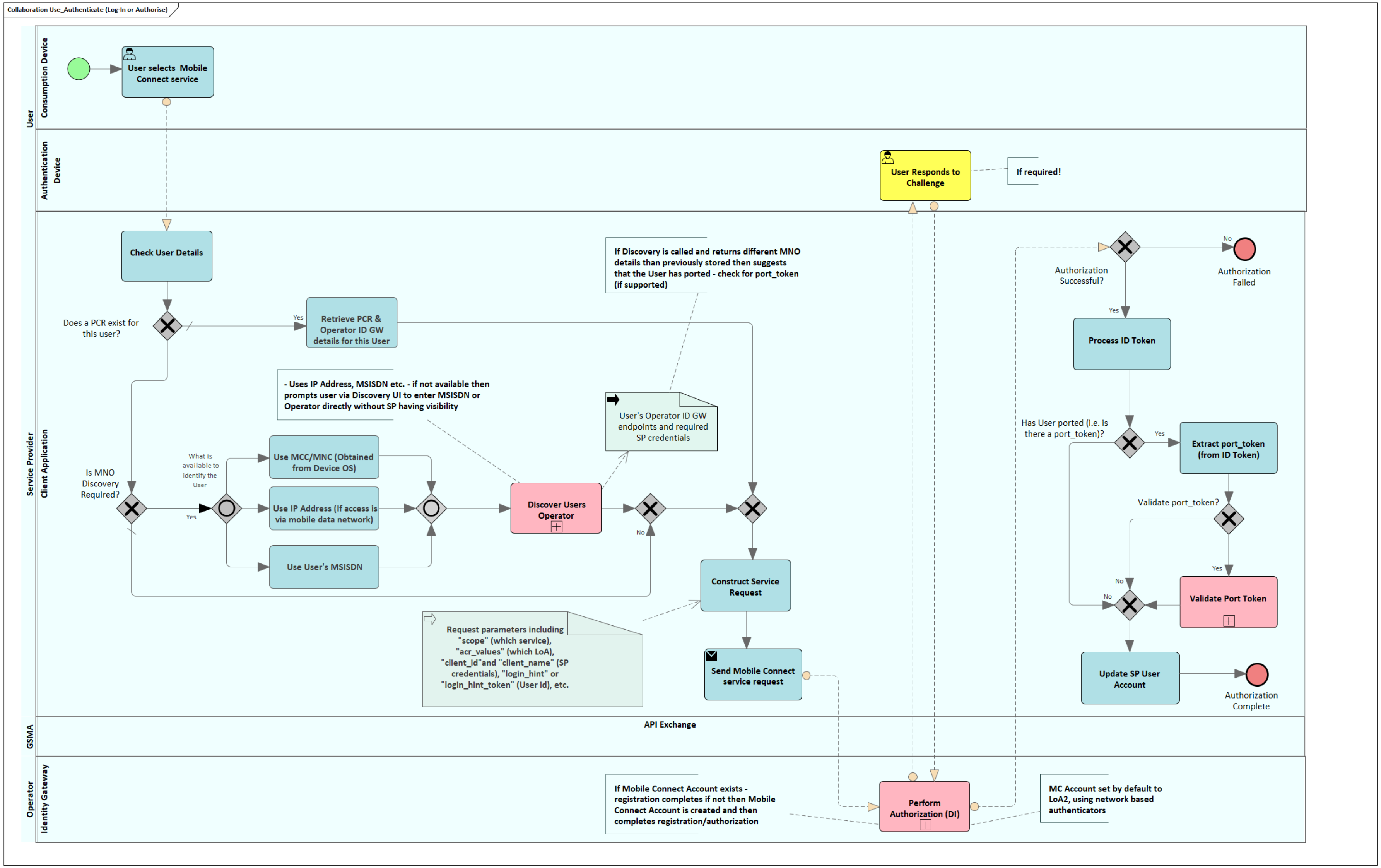

Collaboration Use_Authenticate (Log-In or Authorise)
User
Consumption Device
Authentication Device
Service Provider
Client Application
GSMA
Operator
Identity Gateway
User selects Mobile Connect service
User Responds to Challenge
If required!
Check User Details
Does a PCR exist for this user?
Yes
Retrieve PCR & Operator ID GW details for this User
If Discovery is called and returns different MNO details than previously stored then suggests that the User has ported - check for port_token (if supported)
- Uses IP Address, MSISDN etc. - if not available then prompts user via Discovery UI to enter MSISDN or Operator directly without SP having visibility
User's Operator ID GW endpoints and required SP credentials
Is MNO Discovery Required?
Yes
What is available to identify the User
Use MCC/MNC (Obtained from Device OS)
Use IP Address (If access is via mobile data network)
Use User's MSISDN
Discover Users Operator
No
Construct Service Request
Request parameters including "scope" (which service), "acr_values" (which LoA), "client_id"and "client_name" (SP credentials), "login_hint" or "login_hint_token" (User id), etc.
Send Mobile Connect service request
Authorization Successful?
No
Authorization Failed
Yes
Process ID Token
Has User ported (i.e. is there a port_token)?
Yes
Extract port_token (from ID Token)
Validate port_token?
Yes
No
No
Validate Port Token
Update SP User Account
Authorization Complete
API Exchange
If Mobile Connect Account exists - registration completes if not then Mobile Connect Account is created and then completes registration/authorization
Perform Authorization (DI)
MC Account set by default to LoA2, using network based authenticators

Figure 18 – Sub-Process - Use_Authenticate - Authenticate User or Authorise a Transaction (Device Initiated)

Use_Authenticate shows a device-initiated process where the request for Authentication or Authorisation is initiated by the User on the Consumption Device. The process allows Operator Discovery by the Service Provider (to recover the appropriate endpoints for the correct Operator ID GW) and User identification by the ID GW without the User having to reveal their MSISDN to the Service Provider. Once a User has Set-up Mobile Connect for use with a specific Service Provider then a PCR can be used thereafter to identify the User to the ID GW by the Service Provider. The device-initiated process includes a number of re-directs to allow the User (via the User Agent – for example their browser) to open an interface with their Operator ID GW to enter relevant information and then return back to their Service Provider’s application.

Note that a server-initiated transaction could also be used if the Service Provider has knowledge of the User’s MSISDN directly. This uses a server-initiated authentication core process “Perform_Authorization (SI)” which is shown in Annex A. Note that this server-initiated version was shown in the Direct Registration process flows under the GET stage but can also be used by third-party Service Providers if authorised to do so by the Operator.

The process is as follows:

- The User requests an authentication or authorisation by selecting the relevant option within the Service Provider’s application – for example by clicking the Mobile Connect icon.
- The Service Provider receives the request and constructs a Mobile Connect service request (OIDC Authorization request) that is sent via the user agent on the Consumption Device to the Operator ID GW (this detail is included within the “Perform_Authorization (DI)” sub-process in Figure 38).
- The Service Provider checks the User details. If it is an existing User who has previously set-up Mobile Connect, then a PCR should exist, and the correct Operator endpoints should be known and so by default the PCR will be used and the process to Discover User’s Operator will be bypassed. If a PCR is not available, then another identifier must be used that will assist in identifying the correct Mobile Operator for this User.
- If the Consumption Device is using mobile data, then an IP address might be used to identify the relevant Operator.
- If the PCR does not exist, then the “Discover User’s Operator” sub-process (See Annex A) will be initiated which seeks to identify the User’s Mobile Operator and the end-points to which to direct the relevant API calls. Within the Discovery request the User may be directed to the Discovery UI to provide their MSISDN and possibly to identify the Operator explicitly to assist in the discovery process in order to provide the correct details back to the Service Provider. Included in the response back to the Service Provider is the User’s

MSISDN in encrypted form (if available) which can then be passed on in the OIDC Authorization request to the Operator ID GW to identify the User.

- As indicated previously the Service Provider can include within the request whether they require LoA2 or LoA3 and within the construction of the authorization request the type of service required (via the <scope> parameter) and any appropriate context that is to be presented to the User (to assist, for example, in the authorisation of a transaction) can be provided.
- The request is forwarded to the ID GW via the User Agent. The ID GW responds back to the User Agent which relays the authorization response back to the Service Provider’s client application.
- Within the context of the authorization request (using the “Perform_Authorization (DI)” sub-process), a check is made to see if the Mobile Connect Account already exists or not. If it does exist, then the User may be prompted and challenged on their Authentication Device to authenticate or authorise. Whilst this is the default behaviour there are some use cases where the service is being accessed via a mobile device where seamless authentication[15] can be performed without the User having to explicitly respond.
    - If the Mobile Account does not exist, then one is created, and the User may be prompted to confirm the creation of a Mobile Connect Account, subject to the Operator’s ID GW policies.
- Within the “Perform_Authorization (DI)” sub-process, upon successful authentication or authorisation, the ID GW returns a one-time Authorization code via redirection of the user agent on the Consumption device back to the SP’s Client Application that can then be used by the Service Provider to obtain tokens from the Operator ID GW. These tokens are an ID Token within which is the PCR (and other claims) and an Access Token. In the context of the Use_Authenticate process in Figure 18, the Access Token is not used but it will always be generated.
- The ID Token may also contain an optional port_token to indicate that the User has ported from another Operator. Figure 18 also shows the handling of the port_token if OIDF Account Porting [12] is supported.

[15] If the Operator supports HTTP header enrichment or a similar mechanism that can make the network-verified MSISDN available, the MSISDN can be passed directly to the ID GW. On receiving an incoming request from the User Agent, the ID GW will check the HTTP header for the MSISDN – if it’s there then it can proceed with a seamless authentication (unless Operator/User policy dictates otherwise), if not then it explicitly authenticates the User as normal

7.3 USE - Attribute Services

This section outlines two examples of the use of Mobile Connect Attribute services – one initiated by the User as part of the registration for a new service and one initiated directly by the Service Provider to perform background checks.

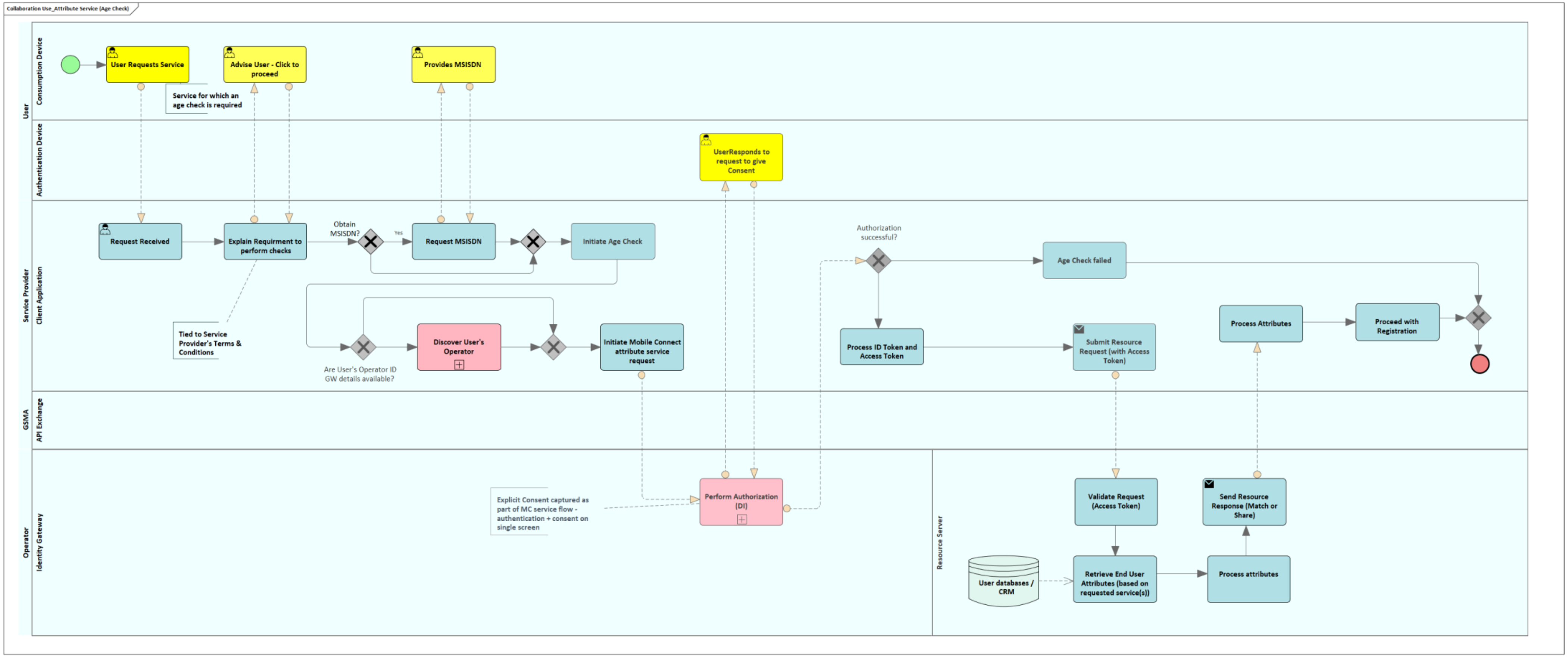

Collaboration Use_Attribute Service (Age Check)
User
Consumption Device
Authentication Device
Service Provider
Client Application
GSMA
API Exchange
Operator
Identity Gateway
Resource Server
User Requests Service
Service for which an age check is required
Advise User - Click to proceed
Provides MSISDN
UserResponds to request to give Consent
Request Received
Explain Requirment to perform checks
Obtain MSISDN?
Yes
Request MSISDN
Initiate Age Check
Tied to Service Provider's Terms & Conditions
Are User's Operator ID GW details available?
Discover User's Operator
Initiate Mobile Connect attribute service request
Authorization successful?
Age Check failed
Process ID Token and Access Token
Submit Resource Request (with Access Token)
Process Attributes
Proceed with Registration
Explicit Consent captured as part of MC service flow - authentication + consent on single screen
Perform Authorization (DI)
Validate Request (Access Token)
Send Resource Response (Match or Share)
User databases / CRM
Retrieve End User Attributes (based on requested service(s))
Process attributes

Figure 19 – Use Attribute Service (Device-Initiated)

As described in Section 3.7, the request for the sharing or validation of User attributes requires User consent which may be captured by the Operator or by the Service Provider, at the Operator’s discretion. For many MC Attribute services consent would typically be captured offline by the Service Provider but depending upon the specific use case may be captured by the Operator as part of the Mobile Connect service flow.

Figure 19 shows the use of a Device-Initiated Mobile Connect Attribute service to validate the User’s date-of-birth as part of the registration for a service provided by the Service Provider. The actors are:

- User: Consumption Device and Authentication Device
- Service Provider Client Application
- The API Exchange is shown as it may be involved in obtaining the serving Operator’s ID GW details
- Operator ID GW (Authorization Server) processes the service request and issues an ID Token and Access Token as a result of the successful processing of the request.
- The Operator’s Resource Server exposes the Resource endpoints[16] and accepts a Resource Request for the sharing or matching of attributes.

The process is as follows:

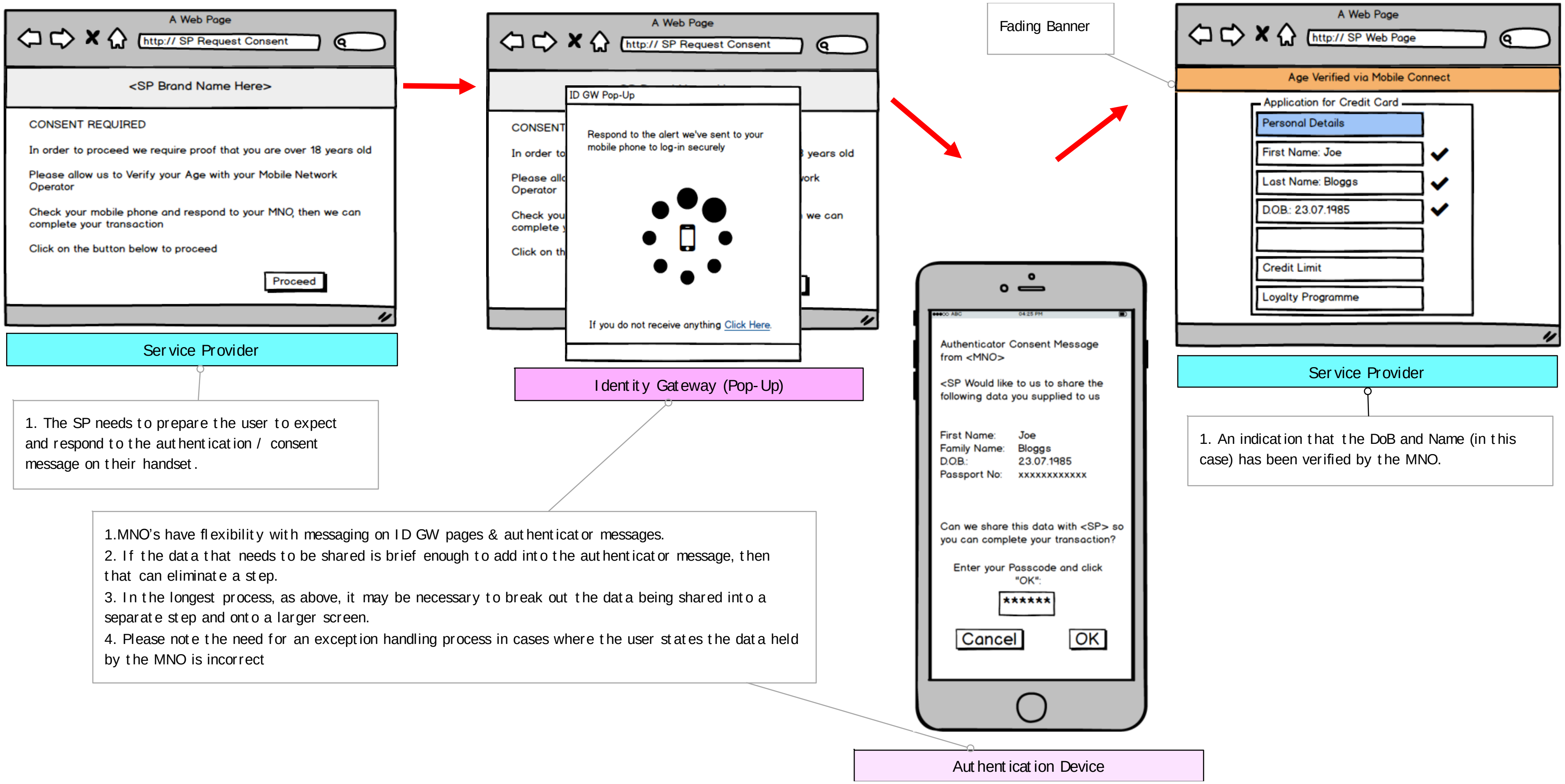
- The User requests a service which requires an age-check to ensure the User is eligible for the service. The Service Provider provides some explanation of the requirements to check the Users data of birth – in this example the User clicks to proceed with the registration.
- There is an option to request the User’s MSISDN, but alternatives could be used to identify the User – for example, using a PCR if the User has previously used Mobile Connect with this Service Provider application.
- If the Service Provider does not have the serving Operator ID GW details then the SP can use the Discovery Service using the User’s MSISDN or by obtaining either the Operator Mobile Country Code (MCC) and Mobile Network Code (MNC) from the User’s mobile device operating system or the IP address if they are accessing via the mobile data network to enable the Discovery Service to identify the Operator (“Discover User’s Operator” sub-process).

[16] Resource endpoints can be a single endpoint for all Attribute services or service specific endpoints depending upon what is supported by the Operator ID GW. Mobile connect defines the general “PremiumInfo” endpoint. The PremiumInfo attribute set is a superset of the UserInfo attribute set referenced within OpenID Connect.

- The Service Provider initiates a Mobile Connect service request to the Operator ID GW (Authorization endpoint). This is a Device-Initiated request in this example - The particular service being requested is indicated via the <scope> value in the service request. For example, the User’s data of birth would be returned as part of the Mobile Connect National ID service (<scope> =”openid mc_nationalid”), if supported by the Operator.
- If the User is not registered for Mobile Connect then a Mobile Connect Account is created for the User as part of the “Perform_Authorization (DI)” sub-process. However, for the example of using the Mobile Connect National ID service the User must be set-up for LoA3 so by implication they would already be registered for Mobile Connect.
- The request is received at the Authorization Server / Authorization endpoint in the ID GW and processed (“Perform_Authorization (DI)” sub-process described in Annex A.2).
    - In this example, the User is prompted to give consent to the sharing of their date of birth. As described in Section 3.7, depending on the type of Authenticator and its capability to display text, the message may be displayed on the User’s Authentication Device (i.e. their mobile device) or the Consumption Device with a prompt for the User to respond (to give consent or not). For the example of a Mobile Connect National ID service request (See Figure 20) then the User is set-up for LoA3 and is required to enter a PIN to provide consent.
    - If the User gives their consent and the request is successful then an ID Token and Access Token are returned to the Service Provider Client application. The ID Token contains the PCR that links the User to this Client application for that ID GW.
- The Access Token is then used within a Resource request to the Operator’s Resource server - Resource endpoint (e.g. PremiumInfo). The Resource server processes the request and returns the requested attributes in a Resource response to the SP Client application. Note that this is a server to server request and does not involve the User’s Consumption Device. The attributes that are returned are specified by the Operator ID GW for that specific requested Mobile Connect service.
    - User consent has a time-limit associated with it and may be given purely for this transaction or to include subsequent requests made by this Service Provider. If the User consent is long-lived in this context, the User can review and revoke consent through the “Manage Mobile Connect” processes.
    - In this context where consent is given as part of the service flow this may be provided by issuing an Access Token with an extended period of validity. If the SP Client application possesses a long-lived Access token then the Perform_Authorization (DI) sub-process would not be required for subsequent requests (for date-of-birth in this example) and simply re-submits the valid Access token to the Resource server to retrieve the date-of-birth.

- If the request was not successful or the User did not give their consent then an error is returned (Error code and description). Errors may occur during the “Perform_Authorization” sub-process or whilst processing the Resource request in the Resource Server.
- Assuming the User gives their consent, the information is shared with the Service Provider and the Service Provider can update their records as appropriate.

7.3.1 USE – Attribute Service (Date of Birth Check) - What does the User Experience Look Like?



CONSENT REQUIRED

In order to proceed we require proof that you are over 18 years old

Please allow us to Verify your Age with your Mobile Network Operator

Check your mobile phone and respond to your MNO, then we can complete your transaction

Click on the button below to proceed

1. The SP needs to prepare the user to expect and respond to the authentication / consent message on their handset.

Respond to the alert we've sent to your mobile phone to log-in securely

If you do not receive anything Click Here

1.MNO’s have flexibility with messaging on ID GW pages & authenticator messages.
2. If the data that needs to be shared is brief enough to add into the authenticator message, then that can eliminate a step.
3. In the longest process, as above, it may be necessary to break out the data being shared into a separate step and onto a larger screen.
4. Please note the need for an exception handling process in cases where the user states the data held by the MNO is incorrect

Authenticator Consent Message from <MNO>

<SP Would like to us to share the following data you supplied to us

First Name:	Joe
Family Name:	Bloggs
D.O.B.:	23.07.1985
Passport No:	xxxxxxxxxxxx

Can we share this data with <SP> so you can complete your transaction?

Enter your Passcode and click "OK":

******

Application for Credit Card
Personal Details
First Name: Joe ✓
Last Name: Bloggs ✓
D.O.B.: 23.07.1985 ✓
Credit Limit
Loyalty Programme

1. An indication that the DoB and Name (in this case) has been verified by the MNO.

Figure 20: Request for Verified Date of Birth as part of MC NationalID service (Requiring User Consent)

Figure 20 Illustrates what the User will see based on a scenario where the Service Provider needs to verify that a User is old enough to be able to register for the service or product (a Credit Card in this example) including comments on optimising the User Experience.

The key element here is that the Service Provider indicates the requirement for obtaining the User information before the request is made to the serving Operator’s Identity Gateway. The details of the information requested are displayed on the Authentication Device (mobile phone). If the information requested cannot easily be displayed on the Authentication Device, then this information can be split and displayed on the Consumption Device (for example in a pop-up within the browser) which would add an extra step / screen in Figure 20.

Note that the Date of Birth is provided as part of the attribute set for the Mobile Connect National ID service in this example – the Service Provider is only using the Date of Birth and Name. The MC National ID service requires 2 factor authentication (LoA3), by default.

7.4 USE - Business to Business Request for User Attributes

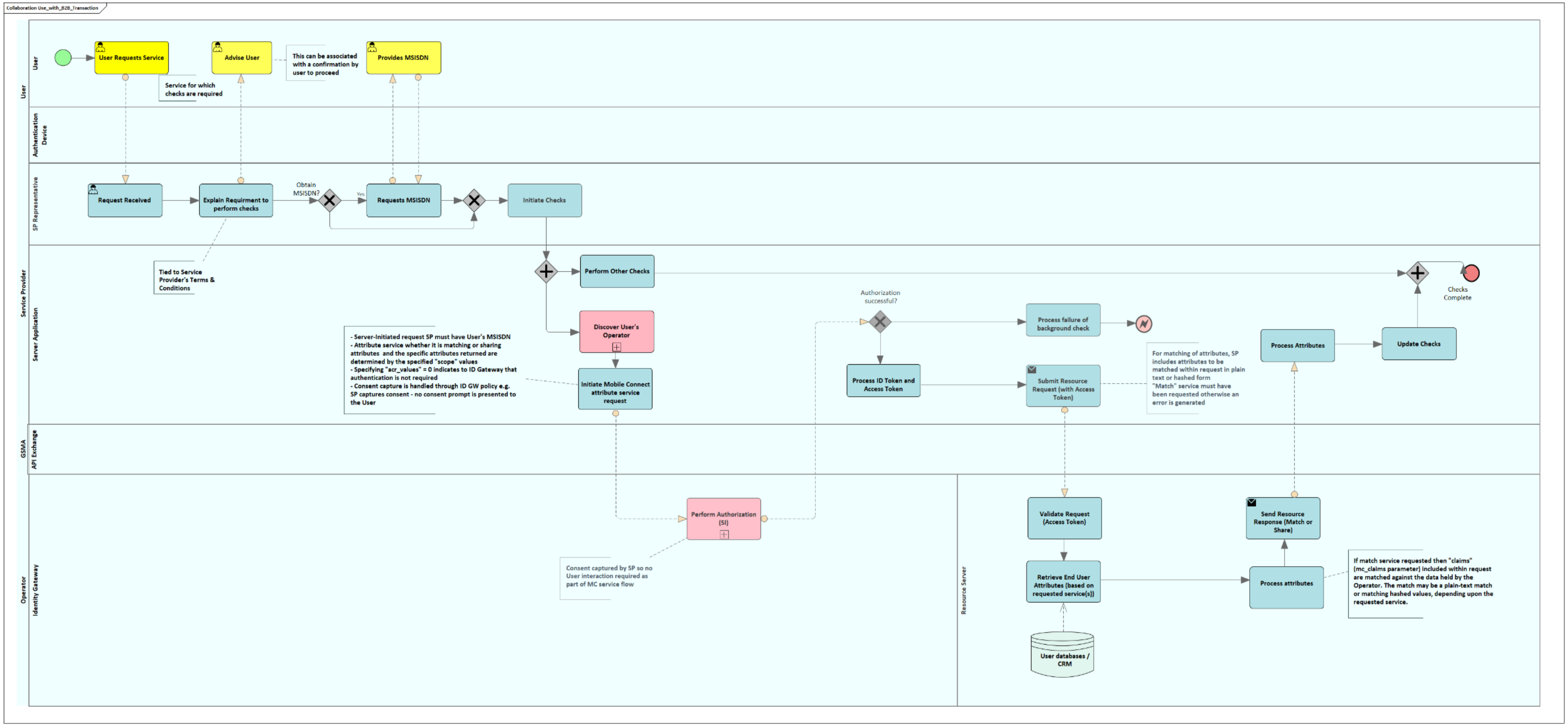

Collaboration Use_with_B2B_Transaction
User
User
Authentication Device
SP Representative
Service Provider
Server Application
GSMA
API Exchange
Operator
Identity Gateway
Resource Server
User Requests Service
Service for which checks are required
Advise User
This can be associated with a confirmation by user to proceed
Provides MSISDN
Request Received
Explain Requirment to perform checks
Obtain MSISDN?
Yes
Requests MSISDN
Initiate Checks
Tied to Service Provider's Terms & Conditions
Perform Other Checks
Discover User's Operator
Initiate Mobile Connect attribute service request
- Server-Initiated request SP must have User's MSISDN
- Attribute service whether it is matching or sharing attributes and the specific attributes returned are determined by the specified "scope" values
- Specifying "acr_values" = 0 indicates to ID Gateway that authentication is not required
- Consent capture is handled through ID GW policy e.g. SP captures consent - no consent prompt is presented to the User
Perform Authorization (SI)
Consent captured by SP so no User interaction required as part of MC service flow
Authorization successful?
Process ID Token and Access Token
Process failure of background check
Submit Resource Request (with Access Token)
For matching of attributes, SP includes attributes to be matched within request in plain text or hashed form "Match" service must have been requested otherwise an error is generated
Validate Request (Access Token)
Retrieve End User Attributes (based on requested service(s))
User databases / CRM
Process attributes
If match service requested then "claims" (mc_claims parameter) included within request are matched against the data held by the Operator. The match may be a plain-text match or matching hashed values, depending upon the requested service.
Send Resource Response (Match or Share)
Process Attributes
Update Checks
Checks Complete

Figure 21 – B2B Request for User Attributes (Service Provider captures consent)

As described previously, there are scenarios where a request may be made by the Service Provider directly to the Operator and where explicit User consent is not required but where the onus is on the Service Provider to directly or indirectly obtain consent from the User (i.e. a B2B request).

Figure 21 illustrates a B2B service request to perform background checks where the User does not interact with the Mobile Connect service – it takes place in the background. In this example the User interacts directly with a Service Provider representative to register for a service. The SP Representative explains the requirements (and obtains consent) and captures the User's MSISDN before initiating checks as part of the registration. The process is as follows:

- The User requests a service from the Service Provider Representative which will involve performing a number of checks.
- The Service Provider explains the requirements for these checks and why, and indicates that as part of the process they will contact the User's Mobile Operator. In order to do this the Service Provider will need to be able to identify the User's Operator and identify the User (or more strictly the User's device) to the Operator. In this case the User's mobile number (MSISDN) is requested.
- If required, the Discovery Service (using the "Discover User's Operator" core process) can be used to determine the User's Operator and obtain the appropriate API endpoints and credentials to make the request (in parallel other checks may be performed).
- An appropriate request is made to the Operator (e.g. Mobile Connect Account Takeover Protection). Note that this is a server-initiated request (using the "Core_Perform_Authorization (SI) sub-process described in Annex A) and the User is not directly involved within the MC transaction.
- Subject to the Operator's contractual agreement with the Service Provider, the Service Provider can indicate that no authentication is required in the request and that consent has already been captured. The "Perform_Authorization (SI)" sub-process, which uses the "Challenge User" sub-process, does not need to request the User to authenticate or give consent via their mobile device (Authentication Device). If the User is not registered for Mobile Connect then a Mobile Connect Account is created for the User as part of the "Perform_Authorization (SI)" sub-process.
    - In this case it may be appropriate for the Operator to follow up with the User at a later date to make them aware that Mobile Connect was used and potentially to promote the wider benefits of Mobile Connect.
- Assuming successful authorization for that User (based on the MSISDN supplied), the SP server application can then submit a Resource request to the relevant Resource endpoint using the Access Token generated as part of the "Perform_Authorization (SI)" sub-process, to retrieve the requested attributes.
    - The Resource Server validates the request and then retrieves the attributes that are specified as part of the requested service. The requested service may be to match the attributes held by the Operator with the information captured or held by the Service Provider in which case a match result is returned or to pass the requested attributes to the Service Provider. Further details can be found in [1] which also references all the technical specifications.

  - In the case of a match service the relevant ‘claims’ are submitted in the Resource Request[17].

.

[17] OpenID Connect provides a mechanism to submit ‘claims’ within the OIDC Authorization request. This is only used with the Mobile Connect KYC Match services and other match services will used the “mc_claims” parameter in the Resource Request.

8 MANAGE – How Does the User MANAGE Mobile Connect or Get Help?

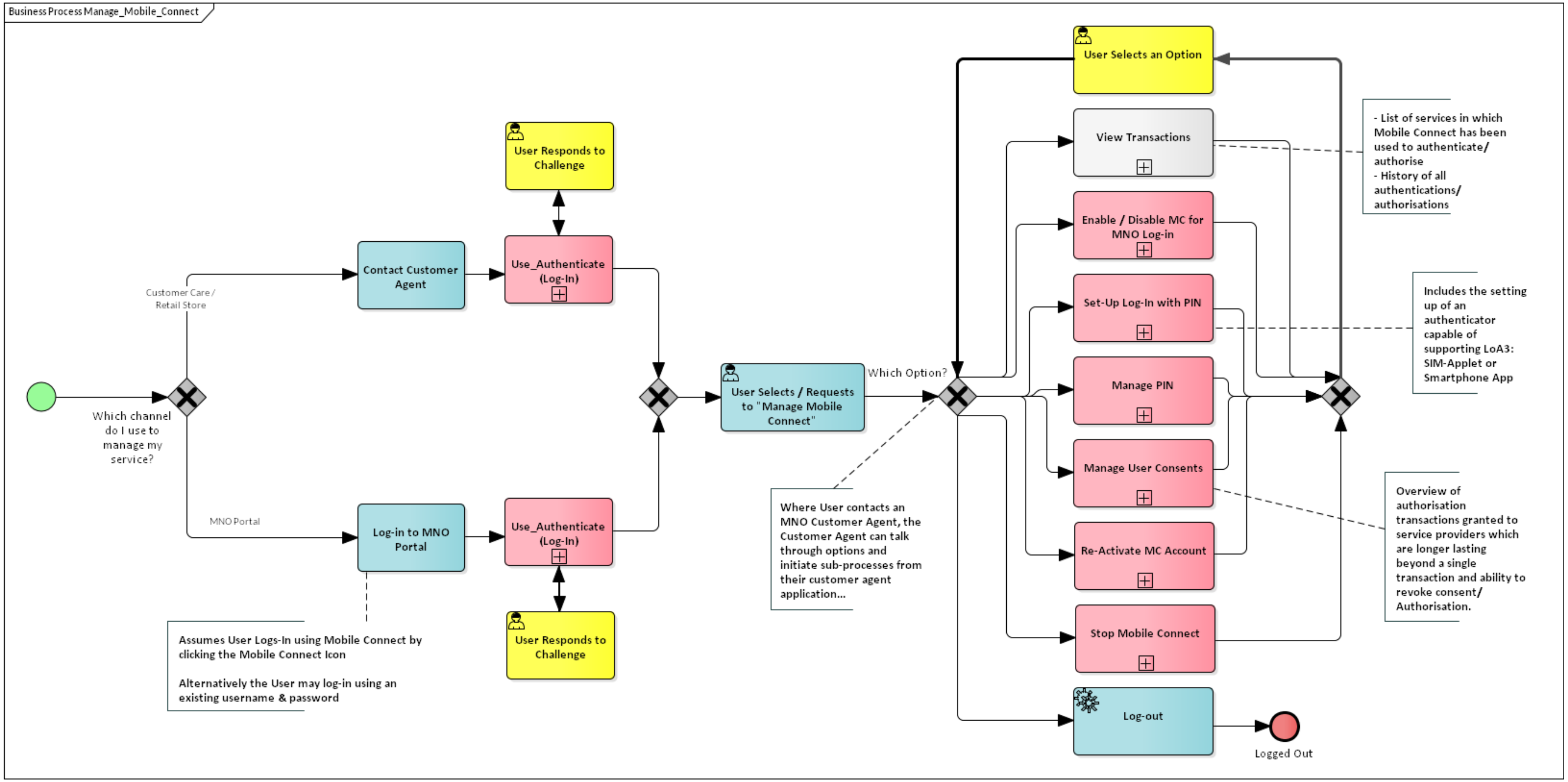

Business Process Manage_Mobile_Connect
Which channel do I use to manage my service?
Customer Care / Retail Store
MNO Portal
Contact Customer Agent
Use_Authenticate (Log-In)
User Responds to Challenge
Log-in to MNO Portal
Use_Authenticate (Log-In)
User Responds to Challenge
Assumes User Logs-In using Mobile Connect by clicking the Mobile Connect Icon
Alternatively the User may log-in using an existing username & password
User Selects / Requests to "Manage Mobile Connect"
Which Option?
Where User contacts an MNO Customer Agent, the Customer Agent can talk through options and initiate sub-processes from their customer agent application...
User Selects an Option
View Transactions
Enable / Disable MC for MNO Log-in
Set-Up Log-In with PIN
Manage PIN
Manage User Consents
Re-Activate MC Account
Stop Mobile Connect
Log-out
Logged Out
- List of services in which Mobile Connect has been used to authenticate/ authorise
- History of all authentications/ authorisations
Includes the setting up of an authenticator capable of supporting LoA3: SIM-Applet or Smartphone App
Overview of authorisation transactions granted to service providers which are longer lasting beyond a single transaction and ability to revoke consent/ Authorisation.

Figure 22 - High Level Flow – Manage Mobile Connect

Figure 22 illustrates the options around a User being able to “Manage Mobile Connect”. The diagram is based around a menu in the Operator Portal, but the same options can be provided via a Customer Agent Client Application when a User contacts a Customer Agent via a retail store or by calling Customer Care. The assumption is made in this diagram that the User logs in using Mobile Connect but equally this could be via an existing username / password. The menu options relate to Mobile Connect only.

- The menu options (shown as pink sub-processes) are explained in more detail in the following pages. Note that the “View Transactions” option is not expanded in this handbook but will be similar to the “Manage User consents” process.
- Note that within the Manage Mobile Connect menu there is an option to Stop Mobile Connect. This links directly to the STOP stage of the User Lifecycle and is covered in Section 9

8.1 Enabling / Disabling Mobile Connect for Log-In

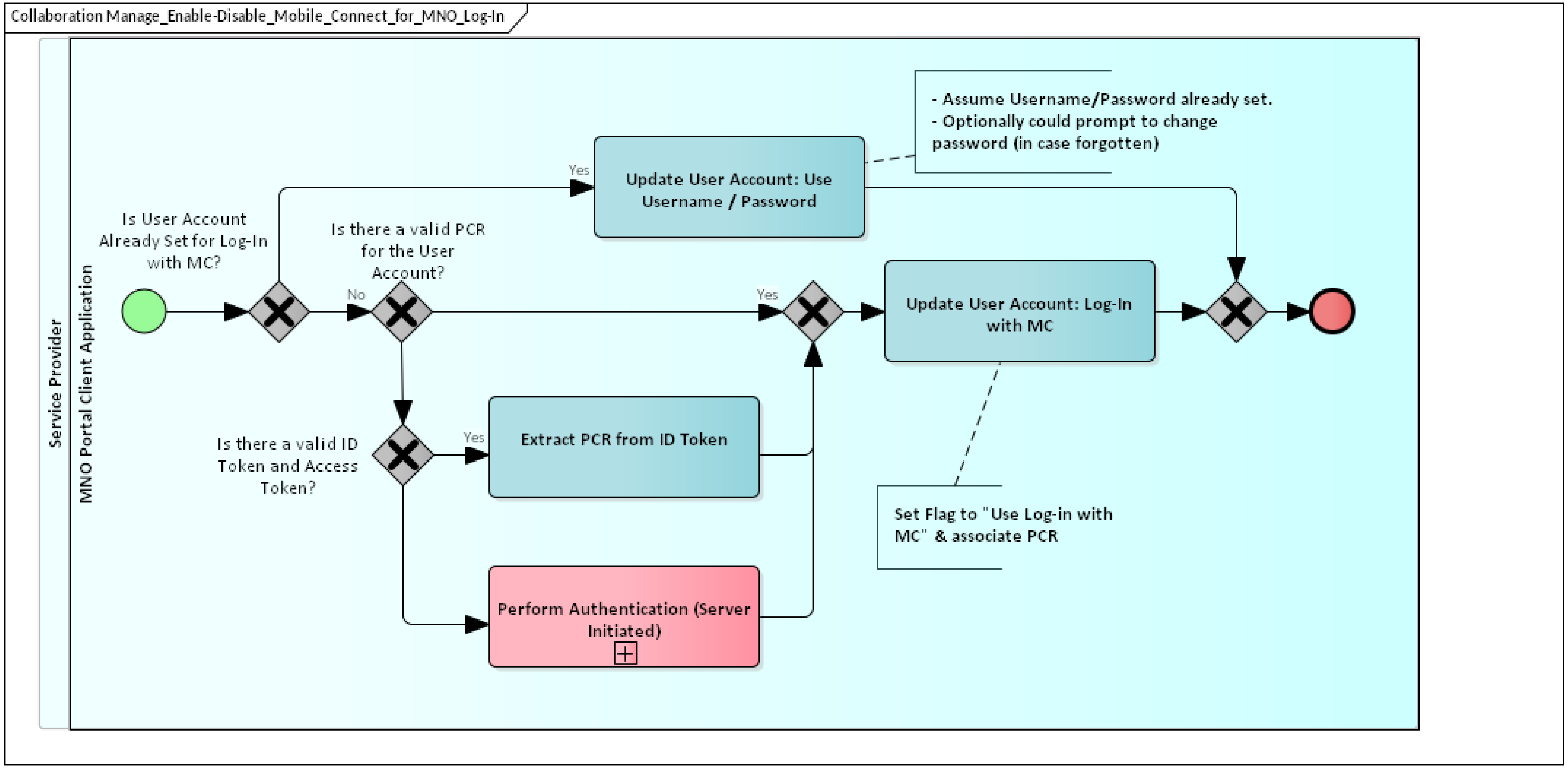
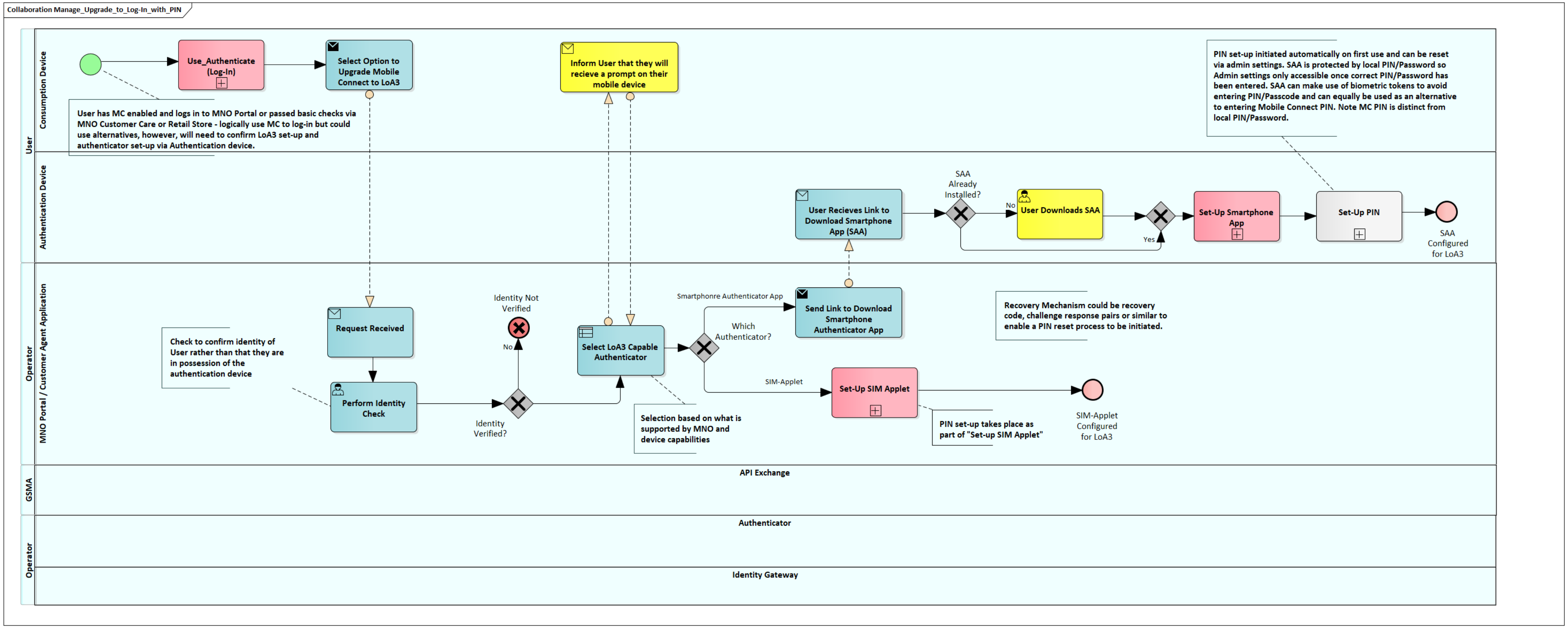

Collaboration Manage_Enable-Disable_Mobile_Connect_for_MNO_Log-In
Service Provider
MNO Portal Client Application
Is User Account Already Set for Log-In with MC?
Yes
Update User Account: Use Username / Password
- Assume Username/Password already set.
- Optionally could prompt to change password (in case forgotten)
Is there a valid PCR for the User Account?
No
Yes
Update User Account: Log-In with MC
Is there a valid ID Token and Access Token?
Yes
Extract PCR from ID Token
Perform Authentication (Server Initiated)
Set Flag to "Use Log-in with MC" & associate PCR

Figure 23 - Enabling / Disabling Mobile Connect for Log-In to the Operator Portal and Customer Care

Within the GET element of the User Lifecycle there is an option to enable Mobile Connect for Operator Log-In for the Direct Registration process flows (this is shown as a sub-process) and is available under the "Manage" menu to allow the User to set their preference. Figure 23 shows that sub-process in more detail. While the context relates to using Mobile Connect for Log-In to Operator services, a similar process could be used by a Service Provider to enable the User to manage their SP Account.

- The User has selected the menu option to Enable / Disable Mobile Connect for Log-In
- If the User already has Log-In with Mobile Connect enabled, then selecting the option will cause the User’s account to be updated to say that they wish to use username and password to log-in. This may optionally trigger a process to renew the User’s password.
- If the User wishes to enable / re-enable Mobile Connect for Log-In, then the Operator Portal Application checks to see if there is a valid PCR associated with the User’s account. If so, then the User’s account will be updated accordingly. If there is not a valid PCR, then an authentication can be performed where the User will respond on their Authentication Device and a fresh ID Token can be generated from which the PCR can be extracted.
    - Note that in this case the account refers to the User account on the Operator portal which is linked to a Mobile Account and (via the PCR and associated flags) is linked to a Mobile Connect Account.

8.2 Upgrading Mobile Connect to Support LoA3


Collaboration Manage_Upgrade_to_Log-In_with_PIN
User
Consumption Device
Authentication Device
Operator
MNO Portal / Customer Agent Application
GSMA
Operator
Use_Authenticate (Log-In)
Select Option to Upgrade Mobile Connect to LoA3
Inform User that they will recieve a prompt on their mobile device
Request Received
Perform Identity Check
Identity Verified?
No
Identity Not Verified
Select LoA3 Capable Authenticator
Which Authenticator?
Smartphonre Authenticator App
SIM-Applet
Send Link to Download Smartphone Authenticator App
Set-Up SIM Applet
SIM-Applet Configured for LoA3
User Recieves Link to Download Smartphone App (SAA)
SAA Already Installed?
No
Yes
User Downloads SAA
Set-Up Smartphone App
Set-Up PIN
SAA Configured for LoA3
API Exchange
Authenticator
Identity Gateway

User has MC enabled and logs in to MNO Portal or passed basic checks via MNO Customer Care or Retail Store - logically use MC to log-in but could use alternatives, however, will need to confirm LoA3 set-up and authenticator set-up via Authentication device.

PIN set-up initiated automatically on first use and can be reset via admin settings. SAA is protected by local PIN/Password so Admin settings only accessible once correct PIN/Password has been entered. SAA can make use of biometric tokens to avoid entering PIN/Passcode and can equally be used as an alternative to entering Mobile Connect PIN. Note MC PIN is distinct from local PIN/Password.

Check to confirm identity of User rather than that they are in possession of the authentication device

Selection based on what is supported by MNO and device capabilities

Recovery Mechanism could be recovery code, challenge response pairs or similar to enable a PIN reset process to be initiated.

PIN set-up takes place as part of "Set-up SIM Applet"

Figure 24 - Upgrade Mobile Connect to Support Log-In with PIN (LoA3)

As discussed previously, by default, a Mobile Connect Account is created with LoA2 enabled and the User must then Log-In to their Operator Portal in order to upgrade the account to LoA3 by installing and configuring an appropriate Authenticator that is capable of supporting a PIN entry in a secure manner. This approach ensures that:

- The User journey for basic Get and Set-Up is not interrupted by the need to download and configure the appropriate Authenticator.
- The process for enabling LoA3 can be better managed to ensure that the process is secure

- An appropriate recovery process can be established (if the User forgets their PIN)
- Optionally, for Identity services, there is an opportunity to review and confirm that the User information held by the Operator is correct.

Figure 24 illustrates the process for Upgrading a User’s Mobile Connect Account to support LoA3.

The Actors are as follows:

- User: Consumption Device and Authentication Device
- Service Provider (in this case the User’s Mobile Operator): Either the Operator Portal Client Application or the Customer Agent Client Application
- API Exchange – is shown but there is no activity associated with the API Exchange in this process.
- Operator: Authenticator and ID GW. While no activity is shown in these swim-lanes, the sub-processes: Set-Up SIM Applet and Set-Up Smartphone App Authenticator encapsulate the activities associated with these entities

The high-level process is as follows:

- The User Logs In to their Operator Portal or passes security checks through Customer Care or a Retail Store. A Mobile Connect authentication could be used in all these situations.
- The User selects or requests the option to Upgrade to Log-In with PIN
- On receiving the request, the Customer Agent or the Operator Portal Client Application can perform additional checks to confirm the identity of the User so that the remainder of the upgrade process can be linked to the User and not just to whoever is using the User’s device. This might involve entering a password, asking the User to answer a series of questions about their Mobile Account and recent usage or bill, the use of a series of questions and personalised answers (knowledge-based authentication) or the checking of identity documents where possible.
- Assuming the identity checks are successful then an appropriate Authenticator to support LoA3 is selected for the User based on the Authenticators that are supported by the Operator (Operator Policy) and by the capabilities of the User’s mobile device. SIM-Applet and Smartphone App Authenticator are currently approved for LoA3.
- The User receives a message on their Consumption Device advising them about the next steps in downloading and / or configuring the selected Authenticator.

  - This could include that they will receive a link on their mobile device to allow them to download an Authenticator – typically only one of these LoA3 Authenticators will be provisioned for each User.
  - A Smartphone App Authenticator would typically be available in an App store either the Apple App Store or Google Play Store or perhaps the Operator’s own App store. It is also possible that it is pre-loaded on the device. The Authenticator App functionality could form part of the Operator’s own self-care / management app which may well have been loaded before Authenticator activation is requested.
  - The SIM-Applet can either be pre-loaded or pushed over-the-air (OTA) to the User’s SIM. The setting up of the Smartphone App is typically User initiated – they have to download the App and then go through the configuration of the App on first use from their mobile device (i.e. Smartphone).

- In the case of using a SIM-Applet, the “Set-Up SIM-Applet” sub-process is initiated which will include loading the applet OTA if required and includes the setting of a PIN.
- With the Smartphone App Authenticator, the setting of a PIN is managed from the App once it has been linked to the User’s Mobile Connect Account.
- The Set-Up of SIM-Applet and Smartphone App Authenticator are explained in more detail below.

8.2.1 Setting Up a SIM Applet

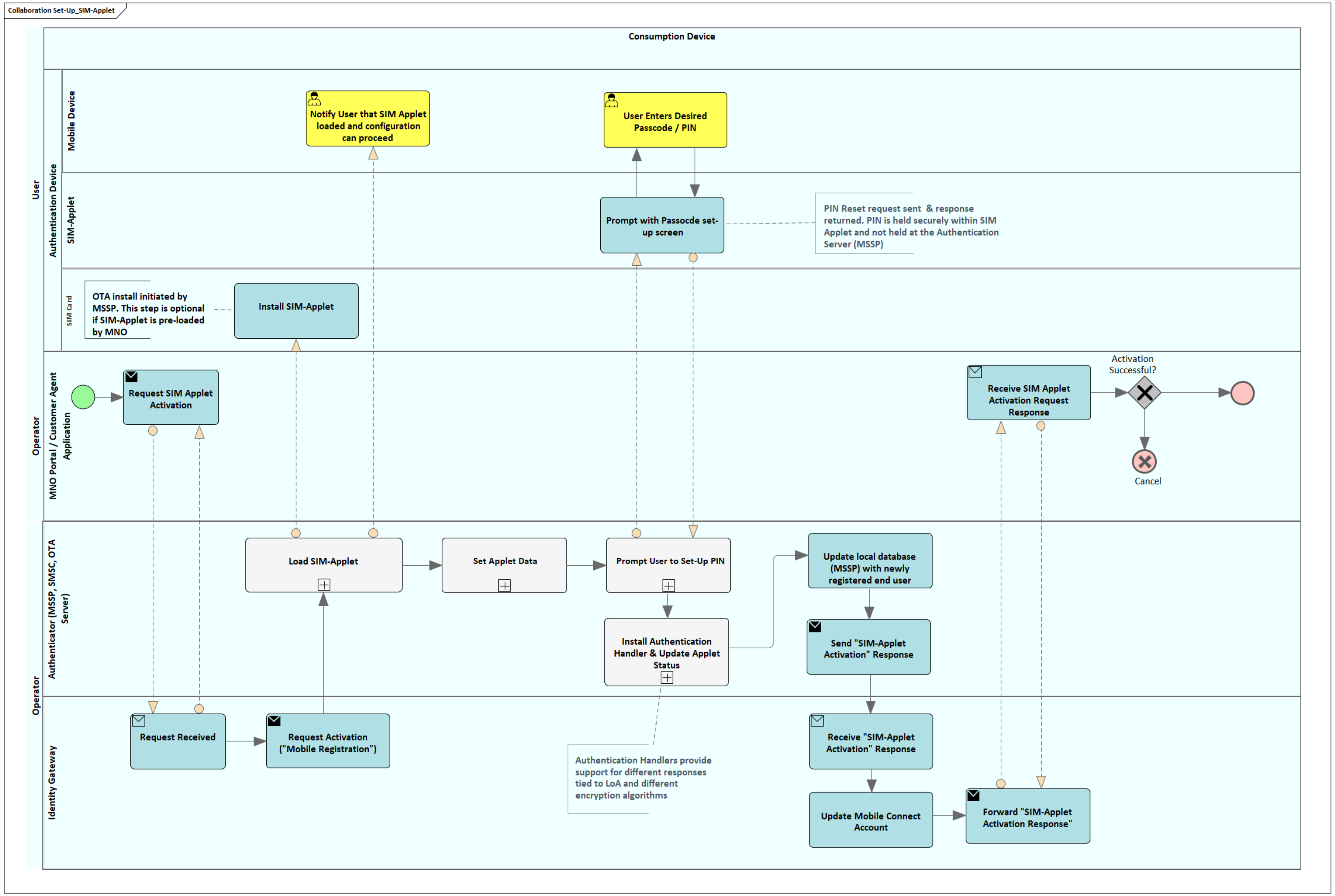

Collaboration Set-Up_SIM-Applet
Consumption Device
User
Authentication Device
Mobile Device
SIM-Applet
SIM Card
Notify User that SIM Applet loaded and configuration can proceed
User Enters Desired Passcode / PIN
Prompt with Passocde set-up screen
PIN Reset request sent & response returned. PIN is held securely within SIM Applet and not held at the Authentication Server (MSSP)
OTA install initiated by MSSP. This step is optional if SIM-Applet is pre-loaded by MNO
Install SIM-Applet
Operator
MNO Portal / Customer Agent Application
Request SIM Applet Activation
Receive SIM Applet Activation Request Response
Activation Successful?
Cancel
Operator
Authenticator (MSSP, SMSC, OTA Server)
Load SIM-Applet
Set Applet Data
Prompt User to Set-Up PIN
Install Authentication Handler & Update Applet Status
Update local database (MSSP) with newly registered end user
Send "SIM-Applet Activation" Response
Identity Gateway
Request Received
Request Activation ("Mobile Registration")
Authentication Handlers provide support for different responses tied to LoA and different encryption algorithms
Receive "SIM-Applet Activation" Response
Update Mobile Connect Account
Forward "SIM-Applet Activation Response"

Figure 25: Set-Up a SIM-Applet

Figure 25 shows a high-level process for setting up a SIM-Applet. The grey sub-processes indicate that these are not expanded in any more detail within this handbook and the reader should refer to the technical specification for the SIM-Applet [10] for more detail.

The main actors are as follows:

- User: Consumption Device and Authentication Device. In this case the Authentication Device consists of the Mobile Device itself and the SIM-Applet that is stored on the SIM card or UICC
- Operator Portal Client Application or the Customer Agent Client Application that initiates the process to Set-Up the SIM-Applet.
- Operator: Authenticator and ID GW. In this case the Authenticator includes an Authenticator server plus OTA Server and SMSC.

The process is as follows:

- The Operator Portal Application or Customer Agent Application initiates a request for activation of a SIM-Applet on the Users mobile device.
- The request is received at the ID GW and validated.
- The ID GW forwards the request to the Authenticator server (Mobile Signature Service Provider) to activate the SIM-Applet (Mobile Registration)
- The Authenticator validates the request and checks whether the SIM-Applet can be loaded onto the Users SIM Card / UICC and whether it is already loaded on the SIM/UICC. This is done either by interrogating the OTA server or interrogating the SIM Card/UICC over the air. If the SIM-Applet is not already loaded, then it is installed over the air.
    - It may be that the Operator has chosen to pre-load the SIM-Applet onto the SIM prior to this process.
    - OTA loading of the SIM-Applet is asynchronous and so the User is notified when the SIM-Applet is loaded, and configuration can proceed.
- Once the SIM-Applet is loaded then the Load Applet Data sub-process is initiated which loads configuration data into the SIM Applet including the address of the Authenticator server.
- The User is then prompted to set-up a PIN via the Authentication device. This would typically require a new PIN to be entered twice to confirm that it has been entered correctly and then clicks enter/OK. This is stored in the SIM-Applet which responds back to the Authenticator server once this is complete.

- The Authenticator server then creates the appropriate authentication handler and loads it into the SIM Applet. The SIM-Applet can support a number of different Authentication Handlers (with different methods of encryption) depending on the Operator’s requirements. An appropriate authentication handler will be installed to handle LoA3 authentication (with a PIN) and LoA2 authentication (“Click OK”). Once the Authentication Handler has been successfully loaded the status of the SIM-Applet is updated (both on the SIM-Applet and in the server).
- The Authenticator server updates its local database and notifies the ID GW that the SIM-Applet has been set-up.
- The ID GW then updates the User’s Mobile Connect Account with the LoA (LoA3) and Authenticator details and responds back to the Operator Portal Application or Customer Agent Application.

8.2.2 Setting-Up A Smartphone App Authenticator

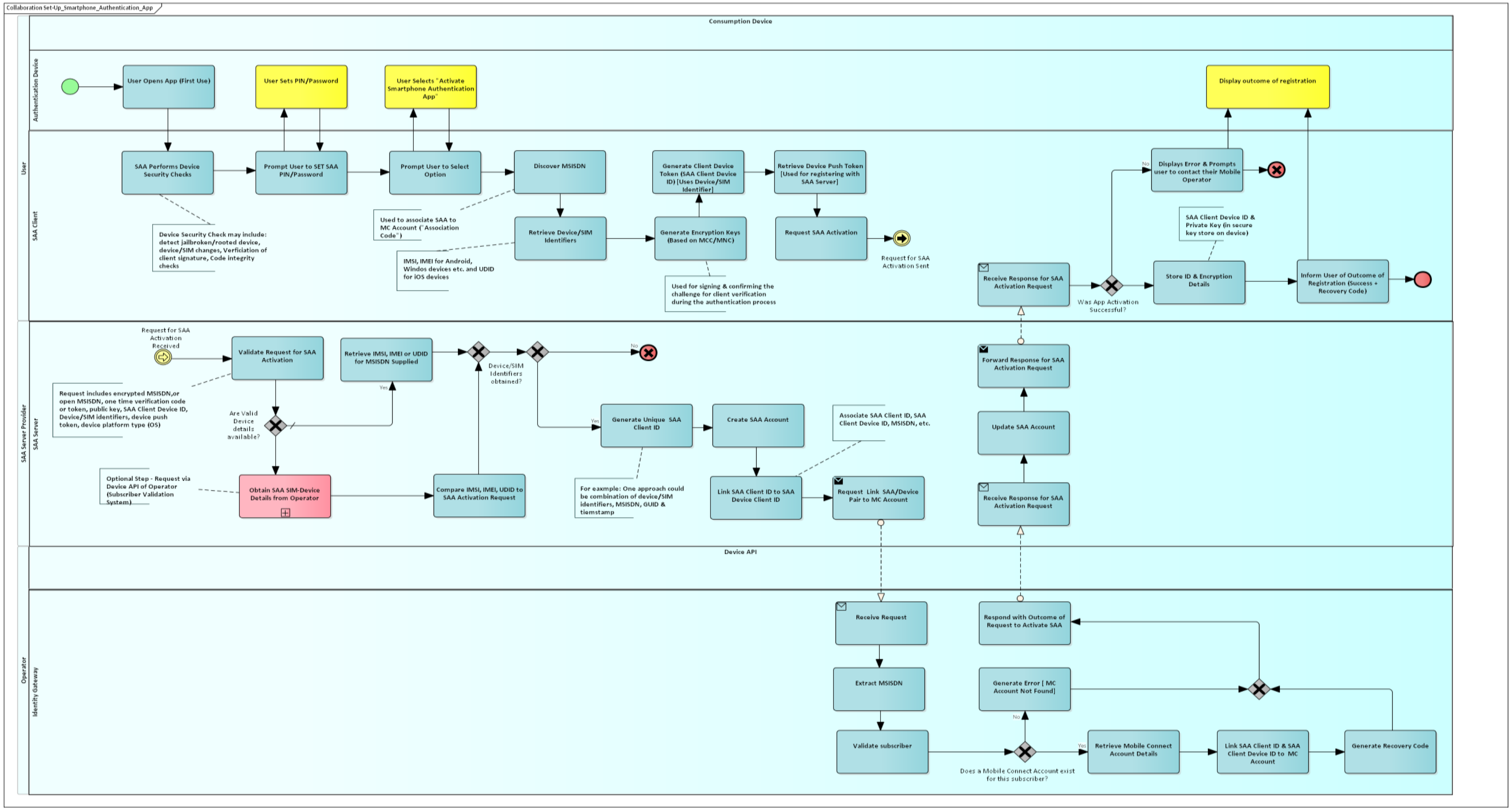

Collaboration Set-Up_Smartphone_Authentication_App
Consumption Device
User
Authentication Device
SAA Client
User Opens App (First Use)
User Sets PIN/Password
User Selects "Activate Smartphone Authentication App"
Display outcome of registration
SAA Performs Device Security Checks
Prompt User to SET SAA PIN/Password
Prompt User to Select Option
Discover MSISDN
Generate Client Device Token (SAA Client Device ID) [Uses Device/SIM Identifier]
Retrieve Device Push Token [Used for registering with SAA Server]
No
Displays Error & Prompts user to contact their Mobile Operator
Device Security Check may include: detect jailbroken/rooted device, device/SIM changes, Verficiation of client signature, Code integrity checks
Used to associate SAA to MC Account ("Association Code")
IMSI, IMEI for Android, Windos devices etc. and UDID for iOS devices
Retrieve Device/SIM Identifiers
Generate Encryption Keys (Based on MCC/MNC)
Request SAA Activation
Request for SAA Activation Sent
Used for signing & confirming the challenge for client verification during the authentication process
SAA Client Device ID & Private Key (in secure key store on device)
Receive Response for SAA Activation Request
Was App Activation Successful?
Store ID & Encryption Details
Inform User of Outcome of Registration (Success + Recovery Code)
SAA Server Provider
SAA Server
Request for SAA Activation Received
Validate Request for SAA Activation
Retrieve IMSI, IMEI or UDID for MSISDN Supplied
Device/SIM Identifiers obtained?
No
Yes
Request includes encrypted MSISDN,or open MSISDN, one time verification code or token, public key, SAA Client Device ID, Device/SIM identifiers, device push token, device platform type (OS)
Are Valid Device details available?
Yes
Generate Unique SAA Client ID
Create SAA Account
Associate SAA Client ID, SAA Client Device ID, MSISDN, etc.
Forward Response for SAA Activation Request
Update SAA Account
Optional Step - Request via Device API of Operator (Subscriber Validation System)
Obtain SAA SIM-Device Details from Operator
Compare IMSI, IMEI, UDID to SAA Activation Request
For eaxmple: One approach could be combination of device/SIM identifiers, MSISDN, GUID & tiemstamp
Link SAA Client ID to SAA Device Client ID
Request Link SAA/Device Pair to MC Account
Receive Response for SAA Activation Request
Device API
Operator
Identity Gateway
Receive Request
Extract MSISDN
Validate subscriber
Respond with Outcome of Request to Activate SAA
Generate Error [MC Account Not Found]
No
Yes
Does a Mobile Connect Account exist for this subscriber?
Retrieve Mobile Connect Account Details
Link SAA Client ID & SAA Client Device ID to MC Account
Generate Recovery Code

Figure 26: Set-Up a Smartphone Authentication App (SAA)

Figure 26 illustrates the process for setting up a Smartphone App Authenticator (SAA). As mentioned previously the Authenticator could be part of a more general Smartphone App provided by the Operator. This process focuses purely on the setting-up of the Authenticator. Further detail can be found in the SAA Specification document [11].

The main actors in this process are:

- User: Authentication Device / Smartphone and the Smartphone App Authenticator (SAA) Client that is running on the Smartphone and which communicates via a data channel with the SAA Server
- SAA Server Provider manages the SAA Server. This may be the Operator or may be a third party which operates the SAA Server on behalf of Operators within a market.
- Operator: ID GW. The ID GW interfaces with the SAA Server

The SAA Set-Up process is as follows:

- The User opens the SAA Client for the first time. In the event that the Set-Up fails then the SAA Client will typically close and be returned to the un-configured (first use) state.
- On first use the SAA Client performs basic security checks to ensure that the smartphone has not been jailbroken, that there have been no SIM/Device changes and that the applications client ID and code are valid.
- The SAA Client then prompts the User to enter a PIN or password for the SAA Client. This is not the same as the PIN that will be set to authenticate and authorise via Mobile Connect but provides an added level of protection against misuse of the Authenticator.
- The SAA Client then extracts the MSISDN and Device/SIM identifiers from the Smartphone OS. For Apple IOS devices this is a unique device ID (UDID). For Android and other smartphone operating systems they make use of the IMSI and IMEI combination.
- The SAA Client then generates an SAA Client Device ID and the encryption keys to support the signing and confirmation of a challenge to support authentication, authorisation and User consent transactions. It also requests a Push token (from the platform service) which will allow the SAA Server to push notifications to the Smartphone.
- Once this information is extracted and keys & tokens generated a request for activation is sent to the SAA Server.
  - *Note that at this point there is a break in the process flow shown by the two yellow intermediate link events: "Request for SAA Activation Sent" and "Request for SAA Activation Received". The latter is on the left-hand side in the SAA Server swim-lane*

- On receipt of the request, the relevant information is extracted from the request – the UDID, IMSI / IMEI are extracted from the SAA Client Device ID token. This can optionally be compared against the Operator’s device database if it is accessible to validate these details.
- This information including the device/SIM identifiers and MSISDN are used to generate an SAA Client ID that can be linked with the SAA Client Device ID to tie the SAA Client to the User’s device.
- The SAA Server creates an account in its local database to store the relevant information and then initiates a request to the Operator ID GW to link the Device/SAA Client combination to the User’s Mobile Connect Account.
- The ID GW will extract the MSISDN from the request, validate the subscriber and check that a Mobile Connect Account exists for this MSISDN. If a Mobile Connect Account does not exist for this MSISDN then an error is generated. Note that within the SAA Specification document, there are use cases where registration for Mobile Connect can be initiated from within the Smartphone App Authenticator [11].
- Assuming the Mobile Account exists then the Mobile Connect Account details will be retrieved, and the SAA Client ID and SAA Client Device ID are linked to the Mobile Connect Account.
- The ID GW will also generate a recovery code which will allow the re-linking of a Smartphone App Authenticator to the Mobile Connect Account. This process is described in Figure 27.
- The outcome of the activation request is passed back to the SAA Server, where the SAA account is updated and then forwarded to the SAA client. If the activation was unsuccessful them an error message is displayed and the App returns to a “first-use state”.
- If activation was successful then the SAA Client stores the IDs, encryption keys and recovery code and prompts the User of the successful outcome displaying the recovery code with an explanation of its use. The recovery code can also be retrieved from within the Smartphone App Authenticator after the User has logged in to the App.

Figure 27 illustrates the process for re-linking the Smartphone App Authenticator with the User’s Mobile Connect Account using a recovery code.

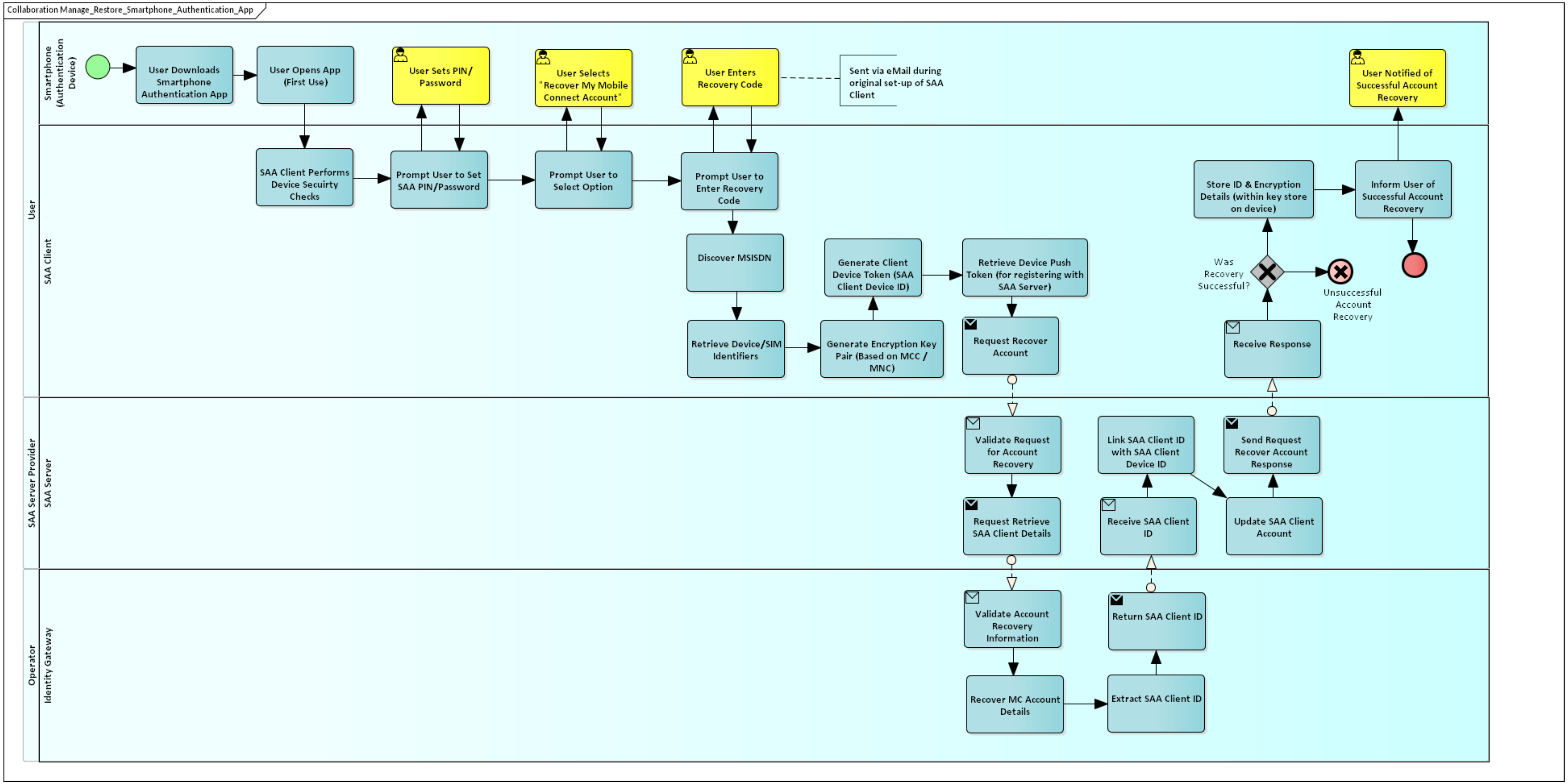

Collaboration Manage_Restore_Smartphone_Authentication_App
User
Smartphone (Authentication Device)
SAA Client
SAA Server Provider
SAA Server
Operator
Identity Gateway
User Downloads Smartphone Authentication App
User Opens App (First Use)
User Sets PIN/ Password
User Selects "Recover My Mobile Connect Account"
User Enters Recovery Code
Sent via eMail during original set-up of SAA Client
User Notified of Successful Account Recovery
SAA Client Performs Device Secuirty Checks
Prompt User to Set SAA PIN/Password
Prompt User to Select Option
Prompt User to Enter Recovery Code
Store ID & Encryption Details (within key store on device)
Inform User of Successful Account Recovery
Discover MSISDN
Generate Client Device Token (SAA Client Device ID)
Retrieve Device Push Token (for registering with SAA Server)
Was Recovery Successful?
Unsuccessful Account Recovery
Retrieve Device/SIM Identifiers
Generate Encryption Key Pair (Based on MCC / MNC)
Request Recover Account
Receive Response
Validate Request for Account Recovery
Link SAA Client ID with SAA Client Device ID
Send Request Recover Account Response
Request Retrieve SAA Client Details
Receive SAA Client ID
Update SAA Client Account
Validate Account Recovery Information
Return SAA Client ID
Recover MC Account Details
Extract SAA Client ID

Figure 27: Re-Linking a Smartphone Authentication App to the User's Mobile Connect Account

During the Set-Up of a Smartphone App Authenticator, a recovery code is generated by the Operator ID GW to enable the SAA Client to be re-linked to a User's Mobile Connect Account should it be deleted (for example). The reason for this process is that the SAA Server will already have an SAA account tied to the Users MSISDN as well as the ID GW having a Mobile Connect Account linked to the same MSISDN. The use of the recovery code enables the SAA Client Device ID and the SAA Client ID to be regenerated and linked to both the existing accounts for that User. This situation could arise as a result of the User having to delete the SAA and then re-installing it or by switching to another Smartphone (for example, as a result of an upgrade) and having to install the SAA on a new device.

Figure 27 illustrates this process. The actors are the same as for the original set-up of the Smartphone App Authenticator. The process is as follows:

- The User downloads the SAA onto their device if they have not done so already and opens the App. This will operate in "first-use" mode.
- On first use the SAA Client performs basic security checks to ensure that the smartphone has not been jailbroken, that there have been no SIM/Device changes and that the applications client ID and code are valid.
- The SAA Client then prompts the User to enter a PIN or password for the Authenticator App. This is not the same as the PIN that will be set to authenticate and authorise via Mobile Connect but provides an added level of protection against misuse of the Authenticator.
- The User selects an option on the SAA menu to "Recover My Mobile Connect Account" or similar
- The User is then prompted to enter the Recovery Code which was generated when they first set-up the Smartphone App Authenticator. Although this would have been accessible via an SAA menu options this will not be the case for a newly downloaded SAA, so they should have made a note of this recovery code. One option is that the recovery code is also issued via an email at generation so that it can be retrieved separately. Although outlined in this handbook, the recovery code could also be made available via the Operator Portal or via an Operator representative.
- The SAA Client then extracts the MSISDN and Device/SIM identifiers from the Smartphone OS. For Apple IOS devices this is a unique device ID (UDID). For Android and other smartphone operating systems they make use of the IMSI and IMEI combination.
- The SAA Client then generates an SAA Client Device ID and the encryption keys to support the signing and confirmation of a challenge to support authentication, authorisation and User consent transactions. It also extracts the Push token which will allow the SAA Server to push notifications to the Smartphone.
- Once this information is extracted and keys & tokens generated a request for recovery is sent to the SAA Server. This will also include the Recovery Code.

- On receipt of the request, the request is validated, the relevant information is extracted from the request – the UDID, IMSI / IMEI are extracted from the SAA Client Device ID Token and Recovery Code. The SAA Account is retrieved.
- The SAA Server then initiates a request to the ID GW to retrieve SAA Client Details, passing the information provided including the Recovery Code.
- The ID GW will extract the MSISDN from the request, validate the subscriber and check that a Mobile Connect Account exists for this MSISDN. If it exists, the ID GW retrieves the account details for this Mobile Connect Account. Note that process flow assumes that these checks are successful.
- The SAA Client ID and new SAA Client Device ID are linked to the Mobile Connect Account.
- The SAA Client ID is recovered from the account details and returned to the SAA Server
- The outcome of the request for Client Details is passed back to the SAA Server, where the SAA account is updated and then forwarded to the SAA client. If the activation was unsuccessful, then an error message is displayed and the App returns to a “first-use state”.
- If activation was successful then the SAA Client stores the IDs, encryption keys and recovery code and prompts the User of the successful outcome displaying the recovery code with an explanation of its use. The recovery code can also be retrieved from within the Smartphone App Authenticator after the User has logged in to the App.

8.3 Manage PIN

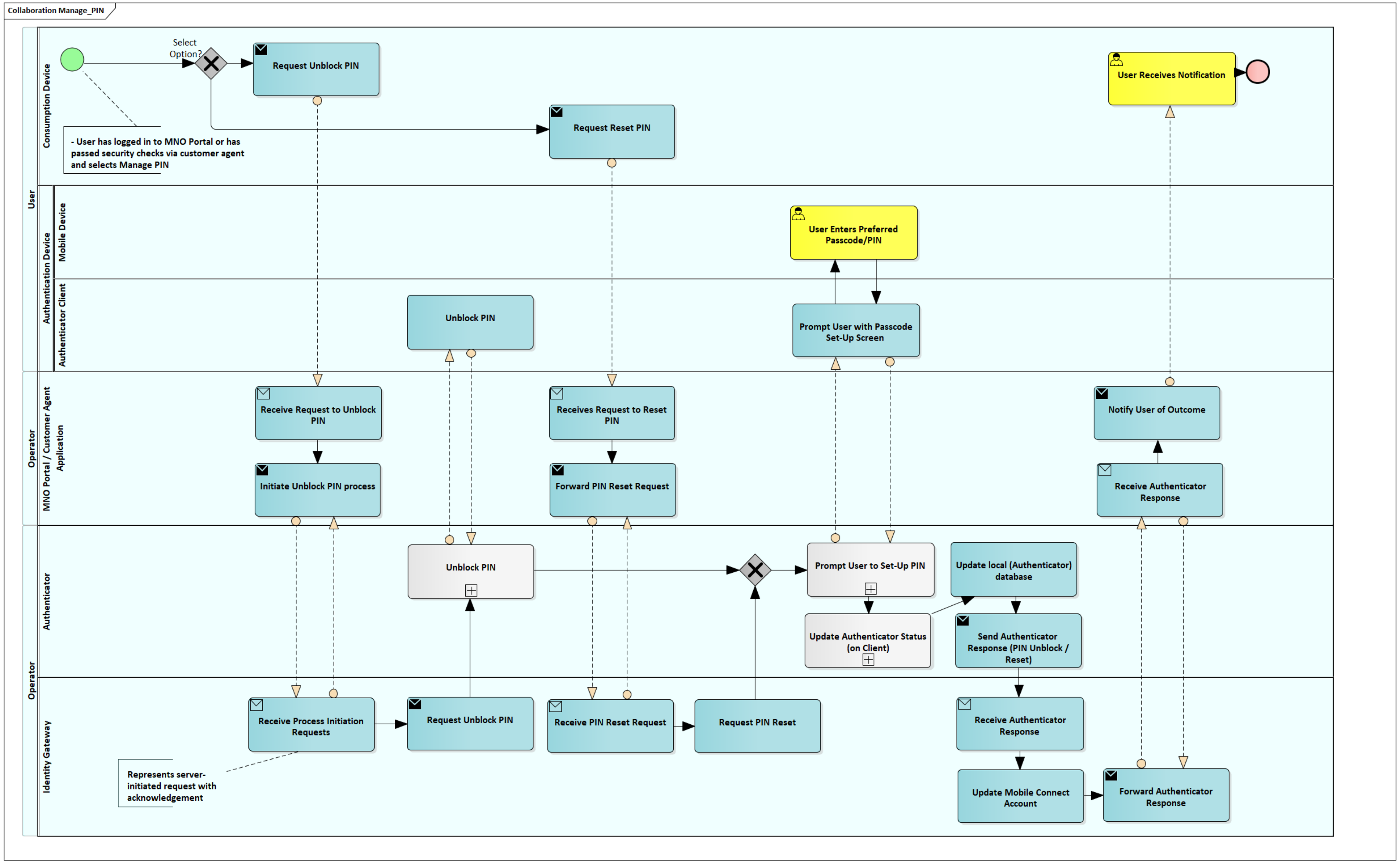

Collaboration Manage_PIN
User
Consumption Device
Authentication Device
Mobile Device
Authenticator Client
Operator
MNO Portal / Customer Agent Application
Authenticator
Identity Gateway
Select Option?
Request Unblock PIN
Request Reset PIN
- User has logged in to MNO Portal or has passed security checks via customer agent and selects Manage PIN
User Receives Notification
User Enters Preferred Passcode/PIN
Unblock PIN
Prompt User with Passcode Set-Up Screen
Receive Request to Unblock PIN
Initiate Unblock PIN process
Receives Request to Reset PIN
Forward PIN Reset Request
Notify User of Outcome
Receive Authenticator Response
Unblock PIN
Prompt User to Set-Up PIN
Update local (Authenticator) database
Update Authenticator Status (on Client)
Send Authenticator Response (PIN Unblock / Reset)
Receive Process Initiation Requests
Request Unblock PIN
Receive PIN Reset Request
Request PIN Reset
Receive Authenticator Response
Update Mobile Connect Account
Forward Authenticator Response
Represents server-initiated request with acknowledgement

Figure 28: Managing (Unblocking) a PIN/Passcode

Figure 28 illustrates the process for unblocking and resetting a PIN or just resetting the PIN. This process applies for any Authenticator that supports LoA3 (two-factor authentication) such as SIM-Applet or Smartphone App Authenticator. The technical mechanism will be different for each type of Authenticator.

The reasons for unblocking or resetting the PIN are, typically:

- The User has entered an incorrect PIN “X” number of times. The PIN is now blocked. The User needs to reset the PIN.
- The User’s PIN is not blocked but the User fears that the PIN may no longer be secret. They want to voluntarily reset their PIN.
- The User is not blocked but has forgotten their PIN and wishes to reset it.

The pre-conditions for this process are that the User has either logged in to their Operator Portal (e.g., via a fall-back username and password) or has passed security checks via an Operator Representative.

The User selects “Manage PIN” and then selects one of two options: “Unblock PIN” or “Reset PIN”. There should, of course, be suitable explanation to manage the User Experience and to help them with this process. Selecting “Unblock PIN will first unblock the PIN and then initiate the PIN reset process. The “Reset PIN” option goes straight to the PIN reset process.

The principles that are operating here are that the process is managed through an Operator channel (Operator Portal Application or Customer Agent Application). A request is passed to the ID GW which then initiates the appropriate requests to the relevant Authenticator for that User. As described previously the Authenticator consists of an Authenticator Server plus appropriate interfaces to communicate with the Authenticator Client that resides on the Authentication Device either on the SIM-Applet on the SIM Card or the SAA Client on the Smartphone. The PIN is stored on the Authentication Device in a secure area and is not accessible to the Operator or a Service Provider.

The process is as follows (following the Unblock process followed by the Reset process):

- The User selects the option to “Request Unblock PIN”. This then triggers a request from the Operator Portal or Customer Agent Application to the Operator ID GW via an internal Operator API/process. The MSISDN is passed in the request.
- The ID GW receives, validates and processes the request – this will involve verifying the MSISDN, checking the Mobile Connect Account and retrieving the relevant information relating to the Authenticator.
- A request to unblock the PIN is sent to the appropriate Authenticator which in turn send a command to unblock the PIN to the Authenticator client. A response is received back to confirm the outcome of the request.

- The User can alternatively select the “Request Reset PIN” option which follows a similar process where a “Request PIN Reset” is sent by the ID GW to the relevant Authenticator. (At this point, if the Unblock PIN sub-process (shown in grey) was successful then the two options come together and there is a common flow going forward)
- The “Prompt User to Reset PIN” sub-process sends a command to the relevant Authenticator Client that then initiates the PIN reset process on the device and the User is prompted to enter a new PIN (twice). A response is sent back to indicate the outcome of the PIN reset process.
- Assuming that the PIN reset process was successful, the “Update Authenticator Status (On Client)” sub-process updates the Authenticator Client status (including updating Authentication Handlers, etc.).
- The Authenticator database is updated (i.e. the Authenticator Account for that MSISDN) and a response sent to the ID GW.
- The ID GW, in turn, updates the Mobile Connect Account and sends a response back to the Operator Portal Application or Customer Agent Application and the User is informed of the outcome.

8.4 Manage User Consents

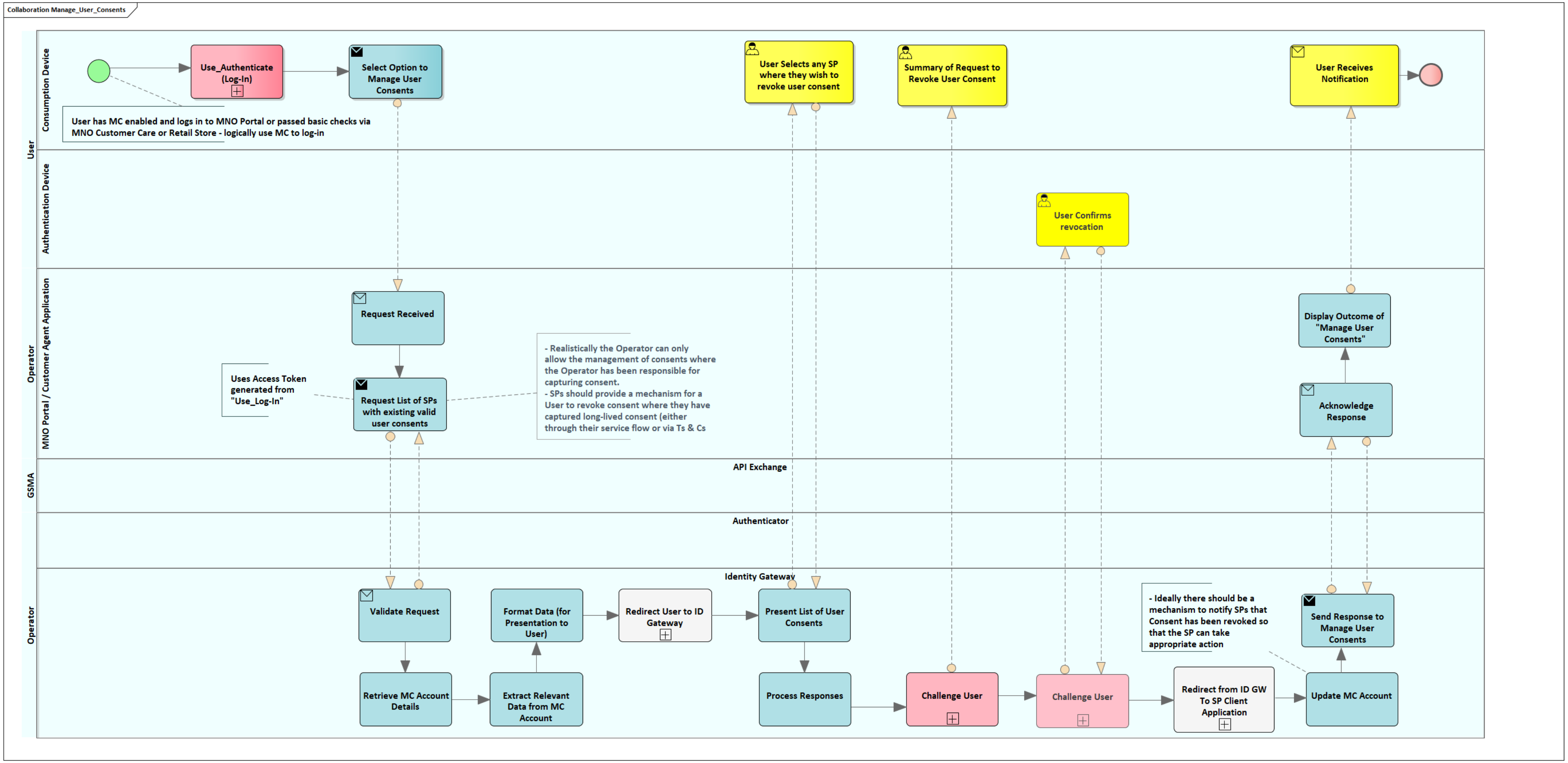

Collaboration Manage_User_Consents
User
Consumption Device
Authentication Device
Operator
MNO Portal / Customer Agent Application
GSMA
API Exchange
Authenticator
Identity Gateway
Operator
Use_Authenticate (Log-In)
Select Option to Manage User Consents
User has MC enabled and logs in to MNO Portal or passed basic checks via MNO Customer Care or Retail Store - logically use MC to log-in
User Selects any SP where they wish to revoke user consent
Summary of Request to Revoke User Consent
User Receives Notification
User Confirms revocation
Request Received
Uses Access Token generated from "Use_Log-In"
Request List of SPs with existing valid user consents
- Realistically the Operator can only allow the management of consents where the Operator has been responsible for capturing consent.
- SPs should provide a mechanism for a User to revoke consent where they have captured long-lived consent (either through their service flow or via Ts &amp; Cs
Display Outcome of "Manage User Consents"
Acknowledge Response
Validate Request
Format Data (for Presentation to User)
Redirect User to ID Gateway
Present List of User Consents
- Ideally there should be a mechanism to notify SPs that Consent has been revoked so that the SP can take appropriate action
Send Response to Manage User Consents
Retrieve MC Account Details
Extract Relevant Data from MC Account
Process Responses
Challenge User
Challenge User
Redirect from ID GW To SP Client Application
Update MC Account

Figure 29 - Managing User Consents

With Mobile Connect Attribute services, a request for User consent can be long-lived (rather than transactional) enabling a Service Provider to request information at different times (within a specified time-limit) without seeking any additional consent from the User. Figure 29 illustrates the process for the User to Manage User consents with their Operator (where the Operator ID gateway is responsible for capturing User consent) allowing existing consents to be reviewed and where required for that consent to be revoked. Note that where a Service Provider is responsible for capturing User consent, it is assumed that the Service Provider will implement the appropriate processes. It may be that the serving Operator places appropriate obligations on a Service Provider to ensure data protection and privacy requirements are met.

The process is as follows:

- The User logs in to the Operator Portal using Mobile Connect or, if this is not enabled, using the existing username and password. Log-In with Mobile connect is assumed to be the normal mechanism. Within the area to Manage Mobile Connect, the User selects the option to Manage User consents.
- On receipt of the request the Operator Portal Application issues a request to the Operator ID GW using the Access Token generated through the initial authentication and the PCR or MSISDN to identify the User.
- The request is validated by the ID GW and if successfully validated, the ID GW will retrieve the Mobile Connect Account details and extract the list of existing User consents. Only the User consents that are current are strictly relevant but there may be value in showing where consents have been given in general and current status.
- The ID GW then formats the data for presentation to the User. This would for example provide the option via a tick box to select a specific Service Provider and the related consents that exist (i.e. the services for which consent has been given) with tools to allow the consent to be revoked. This could equally provide the option to reinstate and extend consents as well, but this can be handled more appropriately through the basic mechanism for granting User consent at the point of request by the Service Provider.
- The User is then re-directed via the Operator Portal Application to the ID GW UI where the list of User consents can be displayed, reviewed and managed. There should be a Confirm or Commit button that will complete the review process and allow the ID GW to process the results.
- The “Challenge_User” sub-process is invoked to display a summary of the SP Client Applications to have consent revoked and then to confirm the request (e.g.seek the User’s confirmation about the changes). Depending upon the Authenticator that is enabled, the summary of changes can be displayed on the User’s Consumption Device with the prompt for User consent/confirmation presented on the Authentication Device.

- The User confirms the changes (revocation)[18] and is redirected back to the Operator Portal Application.
- The User's Mobile Connect Account is updated with the changes and the ID GW provides a response back to the Operator Portal Application (which is acknowledged by the Operator Portal Application).
- The Operator Portal Application then notifies the User that the changes are complete and returns the User back to the Manage Mobile Connect menu options, for example.

[18] Revocation of User consent in this context will force the SP to explicitly request User consent the next time any Identity or Network Attribute services are required.

8.5 Re-Activate Mobile Connect

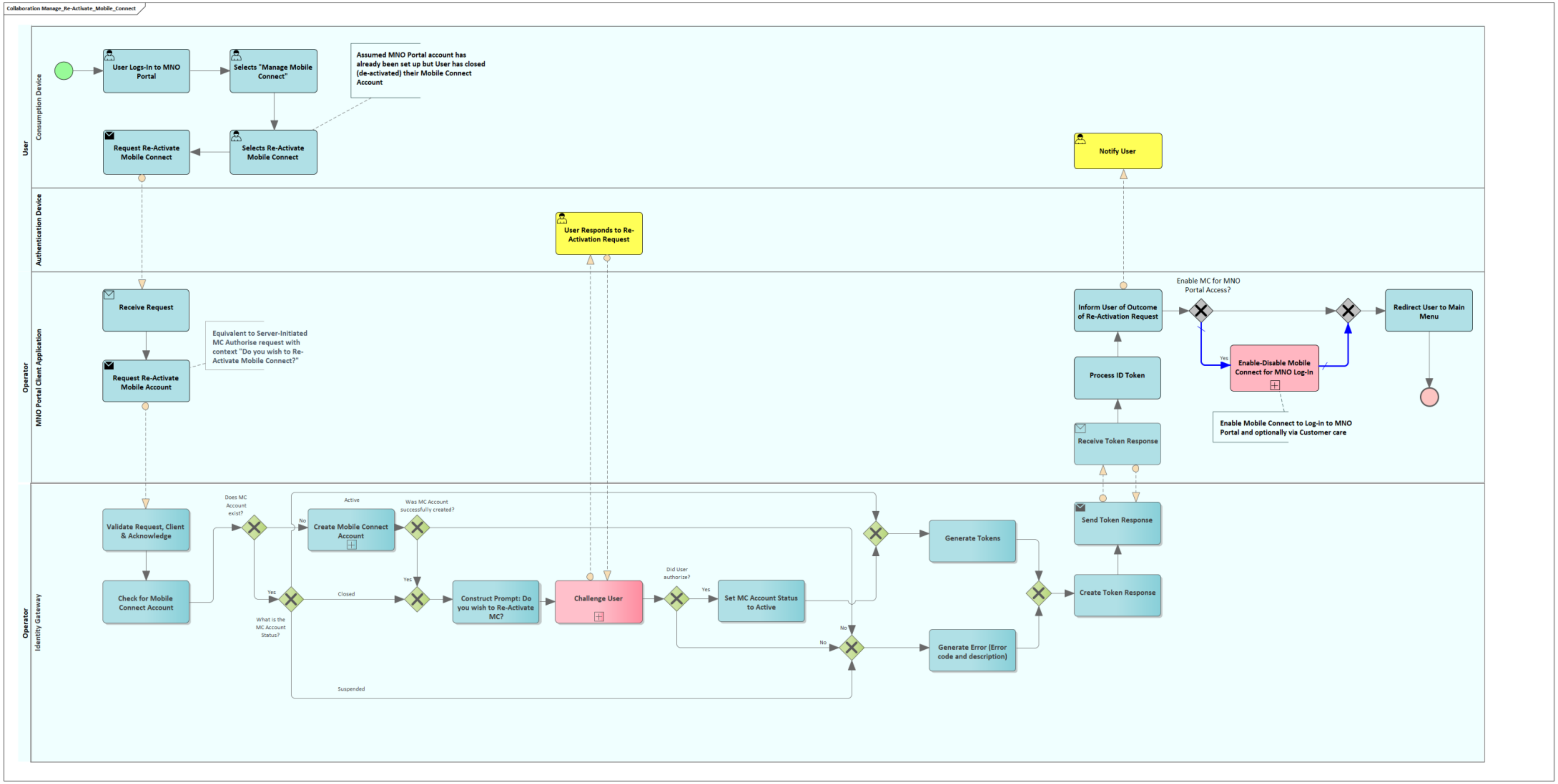

Collaboration Manage_Re-Activate_Mobile_Connect
User
Consumption Device
User Logs-In to MNO Portal
Selects "Manage Mobile Connect"
Assumed MNO Portal account has already been set up but User has closed (de-activated) their Mobile Connect Account
Request Re-Activate Mobile Connect
Selects Re-Activate Mobile Connect
Notify User
Authentication Device
User Responds to Re-Activation Request
Operator
MNO Portal Client Application
Receive Request
Equivalent to Server-Initiated MC Authorise request with context "Do you wish to Re-Activate Mobile Connect?"
Request Re-Activate Mobile Account
Inform User of Outcome of Re-Activation Request
Enable MC for MNO Portal Access?
Redirect User to Main Menu
Yes
Enable-Disable Mobile Connect for MNO Log-In
Enable Mobile Connect to Log-in to MNO Portal and optionally via Customer care
Process ID Token
Receive Token Response
Operator
Identity Gateway
Validate Request, Client & Acknowledge
Check for Mobile Connect Account
Does MC Account exist?
No
Yes
Active
Create Mobile Connect Account
Was MC Account successfully created?
Yes
Closed
What is the MC Account Status?
Construct Prompt: Do you wish to Re-Activate MC?
Challenge User
Did User authorize?
Yes
Set MC Account Status to Active
No
No
Suspended
Generate Tokens
Generate Error (Error code and description)
Send Token Response
Create Token Response

Figure 30 - Re-Activating a User's Mobile Connect Account

If a User has chosen to close their Mobile Connect Account and continue to be a Mobile Customer with the same Operator, then it is possible for them to Re-Activate their Mobile Connect Account at a later date (The Operator may impose a time-limit on this in line with local data handling and data retention policies). If their Mobile Connect Account has been deleted as a result of porting to another Operator or by closing their Mobile Account (cancelling their subscription) then their Mobile Connect Account cannot be re-activated. If a User’s Mobile Connect Account is suspended, normally because their Mobile Account has been suspended, then they will not be allowed to re-activate their Mobile Connect Account. Only the Operator or an approved Operator representative is able to change the account status from Suspended to Active. If a Mobile Connect Account has been suspended because the User’s Mobile Account has been suspended, then the Mobile Connect Account should automatically be returned to an Active state once the suspension has been lifted from the User’s Mobile Account.

Figure 30 illustrates the process of re-activating a Closed Mobile Connect Account.

- The User logs in to their Operator Portal using their normal log-in mechanism (e.g., username/password). The process shows that they select “Manage Mobile Connect” and then select “Re-Activate Mobile Connect”. This is illustrative only and will depend on the menu structure within the Operator Portal. For example, if “Manage Mobile Connect” is only visible if you have an Active Mobile Connect Account then this may appear as a different menu option.
- Selecting “Re-Activate Mobile Connect” initiates a request to the Operator Portal Client Application or the Customer Agent Client Application.
- The Application then initiates a server request to the ID GW (passing the MSISDN) – This is equivalent to a Mobile Connect Authorise request using the “Perform_Authorization (SI) sub-process detailed in Annex A with additional steps to manage the resetting of the Mobile Connect Account status.
- The request will be validated at the ID GW and acknowledged and then a check made for the existence of the Mobile Connect Account
- If the Account exists, then a check is made on the current status of that account:
    - If the Mobile Connect Account is Closed, then the status is changed to Active (and the Mobile Account is updated).
    - If the Mobile Connect Account is already Active there is nothing to do.
    - If the Mobile Connect Account is Suspended, then the process to Re-Activate will fail and an error message will be generated.
- The process shows the option to create a new Mobile Connect Account in the event that one does not exist already. The logic here is that if a User ported from an Operator and then ported back to that Operator at a later stage then they might wish to “Re-Activate”

Mobile Connect and this option would facilitate that situation. In addition, a User might select this when they wish to “Activate” Mobile Connect (depending upon the menu structure).

  - If the Operator does not wish to allow this option within the “Re-Activate Mobile Connect” then if the Mobile Connect Account does not exist, then an error is generated and returned to the Operator Portal / Customer Agent Client Application.

- The response will be received and acknowledged by the Operator Portal / Customer Agent Client Application, who can then process the ID Token and Access Token, update the User’s Mobile Account with the PCR and set Mobile Connect as the preferred Log-In, if required.
- The User is notified of the outcome of the Re-Activation request.

9 STOP - How Does the User STOP their Mobile Connect Service?

There are 4 scenarios for stopping Mobile Connect. The first three are User initiated (via the Operator Portal or via an Operator Representative) and the last is Operator initiated:

- Request to Close a Mobile Connect Account (User Initiated)
- Request to Cancel a Mobile Subscription, which will implicitly cancel the Mobile Connect Account (User Initiated)
- Request to Port to another Operator including Mobile Connect (User Initiated)
- Suspension and Closure of a Mobile Account e.g. a Pre-Pay account by the Operator

These are described in more detail in this section. The most complex of these processes is where a User wishes to port their mobile number to another Operator which is discussed in greater detail.

A request to Cancel a mobile subscription also includes the situation where the User has died and the Executor / Lawyer / 3rd party managing their estate needs to cancel the Users’ mobile phone contract and Mobile Connect account.

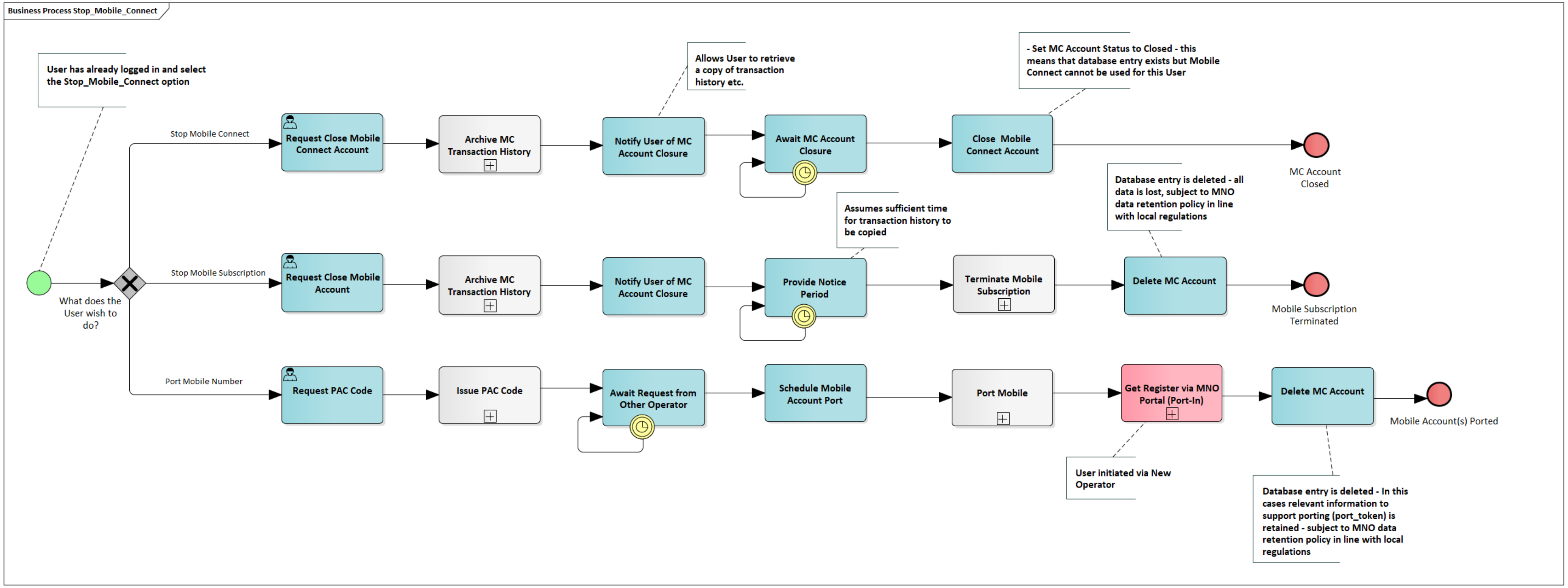

Business Process Stop_Mobile_Connect
User has already logged in and select the Stop_Mobile_Connect option
What does the User wish to do?
Stop Mobile Connect
Request Close Mobile Connect Account
Archive MC Transaction History
Notify User of MC Account Closure
Allows User to retrieve a copy of transaction history etc.
Await MC Account Closure
Close Mobile Connect Account
- Set MC Account Status to Closed - this means that database entry exists but Mobile Connect cannot be used for this User
MC Account Closed
Stop Mobile Subscription
Request Close Mobile Account
Archive MC Transaction History
Notify User of MC Account Closure
Provide Notice Period
Assumes sufficient time for transaction history to be copied
Terminate Mobile Subscription
Delete MC Account
Database entry is deleted - all data is lost, subject to MNO data retention policy in line with local regulations
Mobile Subscription Terminated
Port Mobile Number
Request PAC Code
Issue PAC Code
Await Request from Other Operator
Schedule Mobile Account Port
Port Mobile
Get Register via MNO Portal (Port-In)
User initiated via New Operator
Delete MC Account
Database entry is deleted - In this cases relevant information to support porting (port_token) is retained - subject to MNO data retention policy in line with local regulations
Mobile Account(s) Ported

Figure 31 - Stopping Mobile Connect – User Initiated

Figure 31 illustrates three potential ways that a User can request to Stop or cancel Mobile Connect:

- Requesting to Close Mobile Connect but continue as a mobile subscriber with the same Operator
- Requesting to close their mobile account, i.e. cancelling their mobile subscription with their current Operator
- Requesting a porting authority code (PAC Code) to enable them to transfer their MSISDN to another Operator and also to "Port Mobile Connect"

It is assumed that the User has logged into their Operator Portal and selected "Manage Mobile Connect" and then selected "Stop Mobile Connect". Although not explicitly shown in this flow for any of the requests, the Operator Portal Application or Customer Agent Application could initiate a Mobile Connect Authorise request for the User to authorise the requested transaction to Stop or Port.

9.1 Closing Mobile Connect

Closing Mobile Connect is perhaps the simplest case, where the request is made; Mobile Connect Account details may be archived (based upon the Operator's data management and data retention policy) and a notice period provided to enable the User to change their mind if they wish and to retrieve any data such as transaction history from their Mobile Connect Account.

Once this period is over the Mobile Connect Account status is changed to Closed. The account is not deleted, and it is possible for the User to re-activate the account at some point in the future. As well as changing the account status to Closed, all ID Tokens and Access Tokens will be revoked and cannot be used, and all Authenticators will be disabled and cannot be used for authentication or authorisation by the User.

9.2 Cancelling Mobile Subscription

Cancelling a Mobile Subscription should follow the same process that the Operator currently uses. In the case shown there is a "cooling off period" to enable the User to change their minds and to retrieve any data before the internal Operator process to cancel the subscription is initiated. If the Mobile Account is closed, then the Mobile Connect Account is deleted after the Mobile Connect Account data has been archived in line with data retention policies. Deletion of the account will remove any Access Token and disable authenticators. In line with the Operator's internal policies, the MSISDN will be returned to the number pool.

9.3 Porting Mobile Number and Mobile Connect

A request to port to another Operator would follow the Operator's standard process and the porting rules that operate within a jurisdiction. Figure 31 illustrates the use of a PAC Code which is given to the new Operator to allow the MSISDN to be ported. Once the MSISDN has been ported to a new Operator then the User must register for Mobile Connect with the new Operator. As part of this process they must indicate that they have ported in from another Operator. The porting process consists of two stages:

- The User registers for Mobile Connect with their new Operator and indicates that they have ported in – this is outlined in Figure 9
- Once registered for Mobile Connect, for each Service Provider that the User has previously registered with to use Mobile Connect and for the first time they log-in, a process occurs to identify that the User has ported and to enable the Service Provider to update the appropriate PCR[19] and Operator credentials to allow Mobile Connect to continue to be used by the User (See Figure 33 and Figure 34).

Further detail can be found in [12].

[19] Note that the PCR may remain the same but the issuer (iss) will be different

9.3.1 Porting a Mobile Connect Account

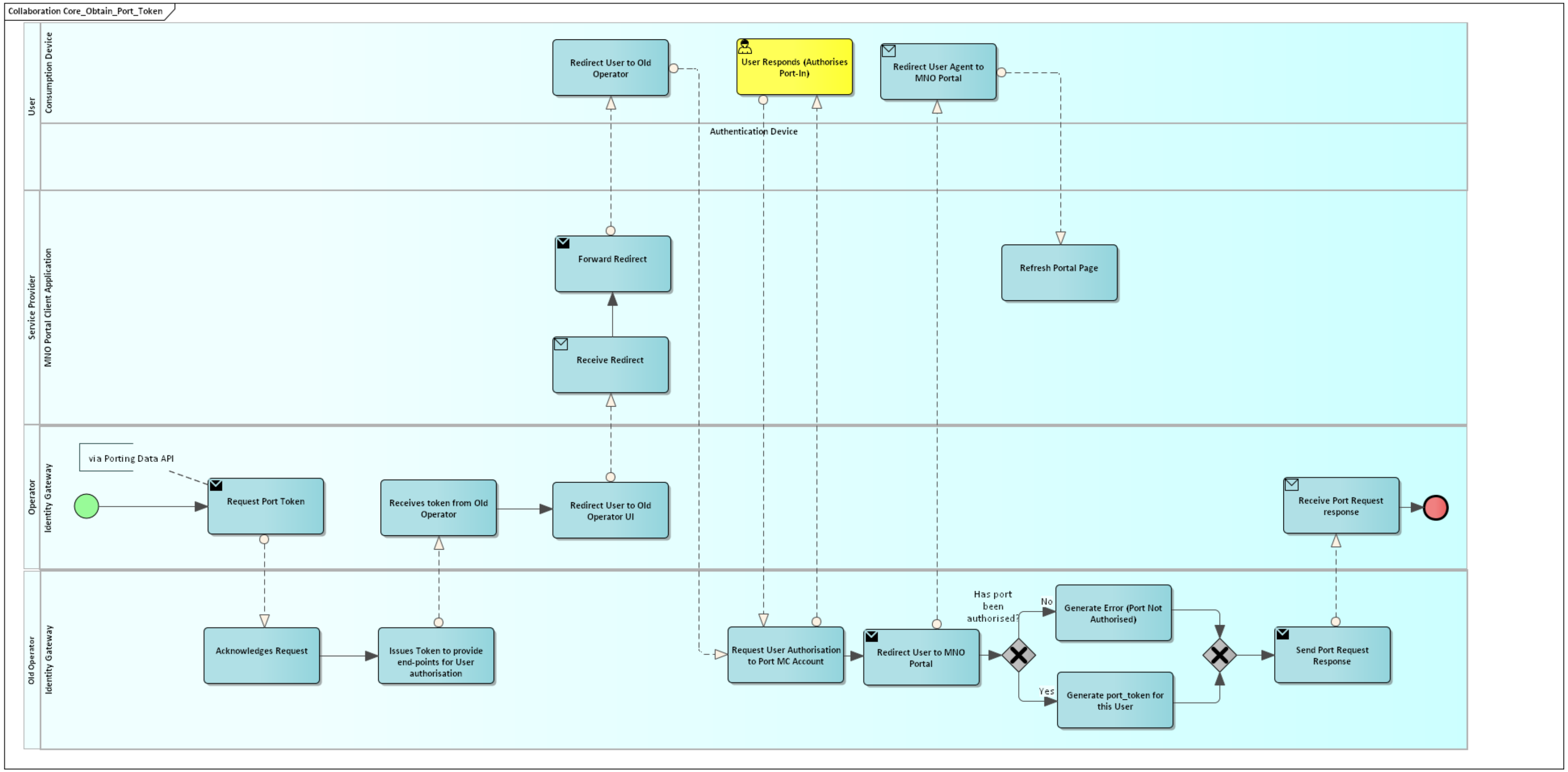

Collaboration Core_Obtain_Port_Token
User
Consumption Device
Authentication Device
Service Provider
MNO Portal Client Application
Operator
Identity Gateway
Old Operator
Identity Gateway
Redirect User to Old Operator
User Responds (Authorises Port-In)
Redirect User Agent to MNO Portal
Forward Redirect
Refresh Portal Page
Receive Redirect
via Porting Data API
Request Port Token
Receives token from Old Operator
Redirect User to Old Operator UI
Receive Port Request response
Acknowledges Request
Issues Token to provide end-points for User authorisation
Request User Authorisation to Port MC Account
Redirect User to MNO Portal
Has port been authorised?
No
Yes
Generate Error (Port Not Authorised)
Generate port_token for this User
Send Port Request Response

Figure 32: Core Process – Obtain Port Token

Error! Reference source not found. illustrates the process for creating a Mobile Connect Account. Within this process, if the Operator detects that a User wishes to port in a Mobile Connect Account from another Operator then the new Operator is able to contact the old Operator in order to obtain a port token which will allow a Service Provider to associate a User with the two Mobile Connect Accounts (new and old) thus avoiding account duplication and enabling the Service Provider's User Account to be updated accordingly.

The port token is obtained by the “Core Obtain Port Token” sub-process, which is illustrated in Figure 32, and includes a redirection of the User to the old Operator’s UI to enable them to authorize the issue of a port-token before re-directing them back to the new Operator Portal to complete the registration process. The port_token is issued to the new Operator who then incorporates the port_token into the ID Token that is issued to a Service Provider in response to a successful authentication.

9.3.2 Logging-In to A Service Provider for The First Time Since Porting

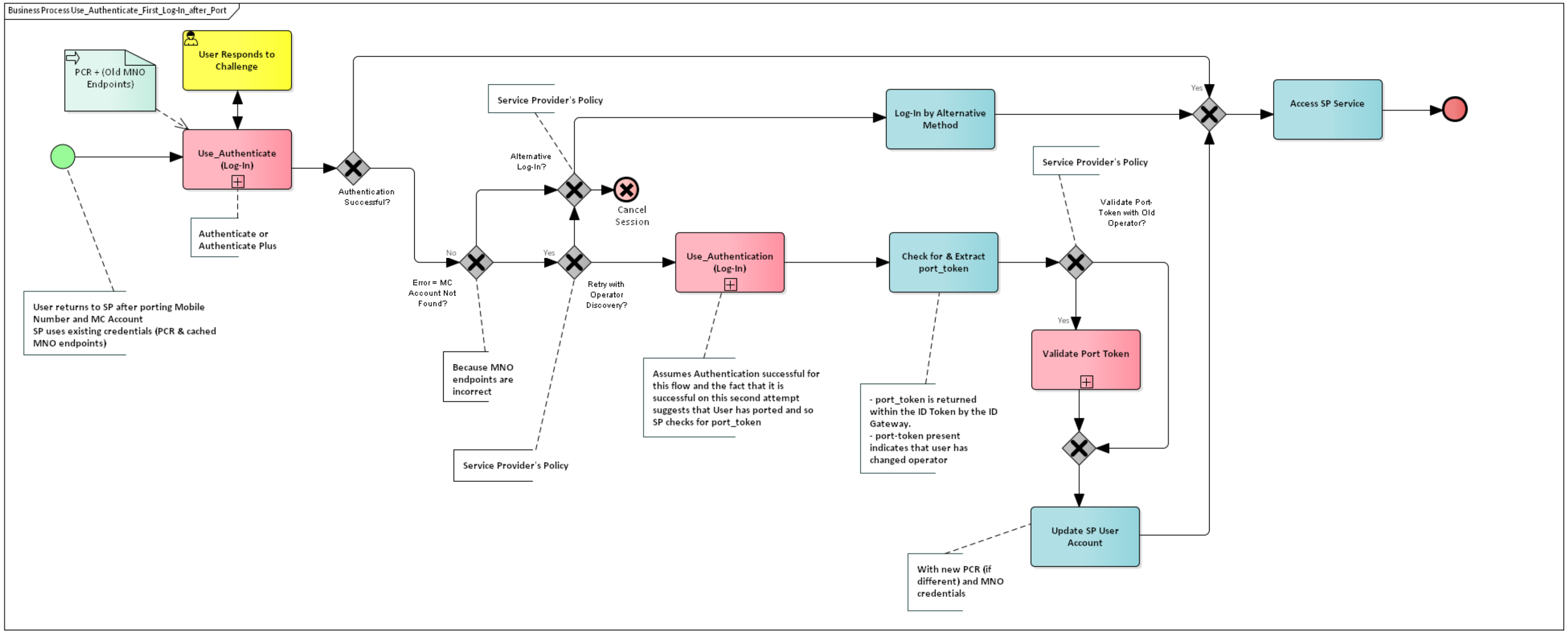

Business Process Use_Authenticate_First_Log-In_after_Port
PCR + (Old MNO Endpoints)
User Responds to Challenge
Use_Authenticate (Log-In)
Authenticate or Authenticate Plus
User returns to SP after porting Mobile Number and MC Account
SP uses existing credentials (PCR & cached MNO endpoints)
Authentication Successful?
No
Error = MC Account Not Found?
Because MNO endpoints are incorrect
Yes
Retry with Operator Discovery?
Service Provider's Policy
Alternative Log-In?
Service Provider's Policy
Cancel Session
Log-In by Alternative Method
Use_Authentication (Log-In)
Assumes Authentication successful for this flow and the fact that it is successful on this second attempt suggests that User has ported and so SP checks for port_token
Check for & Extract port_token
- port_token is returned within the ID Token by the ID Gateway.
- port-token present indicates that user has changed operator
Service Provider's Policy
Validate Port-Token with Old Operator?
Yes
Validate Port Token
Update SP User Account
With new PCR (if different) and MNO credentials
Yes
Access SP Service

Figure 33 - Logging into a Service Provider’s Site / App for the First Time After Porting

Figure 33 illustrates the high-level process that takes place when a User chooses to Log-In to a Service Provider for the first time after porting their mobile number to another Operator. This would occur for each Service Provider where the User has previously enabled Mobile Connect for Log-In. The assumption here is that the User already has an account with the Service Provider and has previously used Mobile Connect to Log-In. As a consequence, the Service Provider has a PCR and (old) Operator credentials to allow the User to Log-In.

The User attempts to Log-In as normal at the Service Provider and an Authentication Request is directed to the old Operator endpoints and because the Mobile Account has been ported (no longer exists with that Operator), the authentication will fail. The Service Provider should then use Operator Discovery to obtain the correct Operator credentials and endpoints and resubmit the Authentication Request to the new Operator;

the User should then be prompted to respond on their Authentication Device (i.e. their mobile device) and the Authentication should be successful.

The Service Provider will have identified that the Operator has changed during this process and can check the returned ID Token to extract the PCR and port_token. The Service Provider can then validate the port_token at the old Operator (shown as the “Validate Port Token” sub-process) to confirm that the User has indeed ported and can then update the Service Provider’s User Account accordingly. Note that the “Validate Port Token” sub-process is also shown as part of the “Use_Authenticate” process (See Figure 18) which is where it would logically be executed – it is shown within Figure 33 for illustrative purposes.

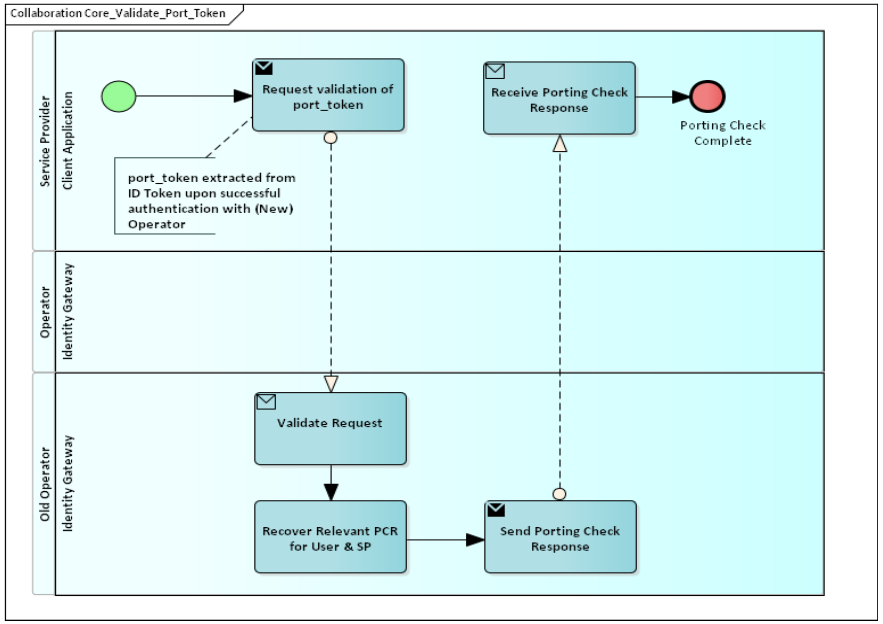
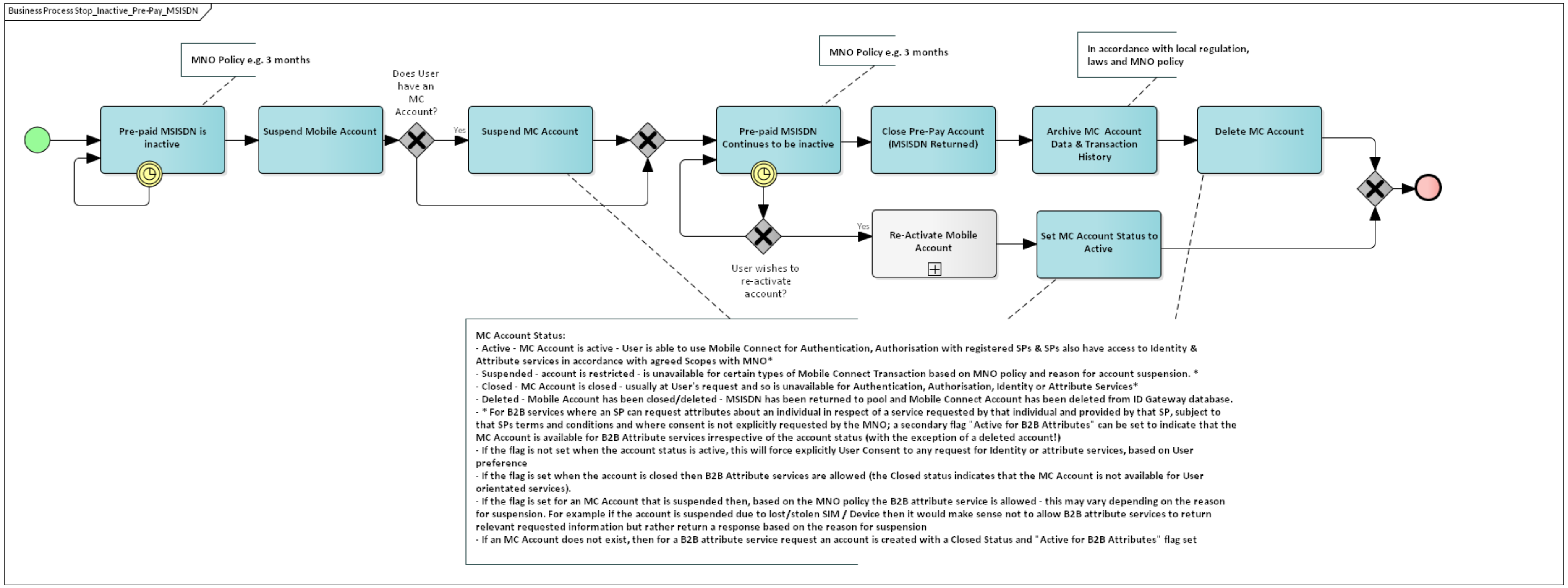

Collaboration Core_Validate_Port_Token
Service Provider
Client Application
Request validation of port_token
Receive Porting Check Response
Porting Check Complete
port_token extracted from ID Token upon successful authentication with (New) Operator
Operator
Identity Gateway
Old Operator
Identity Gateway
Validate Request
Recover Relevant PCR for User & SP
Send Porting Check Response

Figure 34 – Core Process – Validate Port Token

Figure 34 shows the “Validate Port Token” sub-process which can be optionally invoked by a Service Provider if the Service Provider does not recognise the User from the new Operator’s PCR. The port_token which was issued by the User’s previous Operator is extracted from the ID Token upon a successful authentication and can then be included within a request to the old Operator’s Mobile Connect Account Porting Check API. The port_token, which is encrypted, is decrypted by the old Operator and used to identify the User’s (old) PCR associated with that

Service Provider. The Service Provider is then able to update the User Account (Service Provider’s User Account) and associate the two identifiers (PCRs), as appropriate.

9.4 STOP – Operator Initiated


Business Process Stop_Inactive_Pre-Pay_MSISDN
MNO Policy e.g. 3 months
Pre-paid MSISDN is inactive
Suspend Mobile Account
Does User have an MC Account?
Yes
Suspend MC Account
MNO Policy e.g. 3 months
Pre-paid MSISDN Continues to be inactive
User wishes to re-activate account?
Yes
Re-Activate Mobile Account
Set MC Account Status to Active
Close Pre-Pay Account (MSISDN Returned)
In accordance with local regulation, laws and MNO policy
Archive MC Account Data & Transaction History
Delete MC Account

MC Account Status:
- Active - MC Account is active - User is able to use Mobile Connect for Authentication, Authorisation with registered SPs & SPs also have access to Identity & Attribute services in accordance with agreed Scopes with MNO*
- Suspended - account is restricted - is unavailable for certain types of Mobile Connect Transaction based on MNO policy and reason for account suspension. *
- Closed - MC Account is closed - usually at User's request and so is unavailable for Authentication, Authorisation, Identity or Attribute Services*
- Deleted - Mobile Account has been closed/deleted - MSISDN has been returned to pool and Mobile Connect Account has been deleted from ID Gateway database.
- * For B2B services where an SP can request attributes about an individual in respect of a service requested by that individual and provided by that SP, subject to that SPs terms and conditions and where consent is not explicitly requested by the MNO; a secondary flag "Active for B2B Attributes" can be set to indicate that the MC Account is available for B2B Attribute services irrespective of the account status (with the exception of a deleted account!)
- If the flag is not set when the account status is active, this will force explicitly User Consent to any request for Identity or attribute services, based on User preference
- If the flag is set when the account is closed then B2B Attribute services are allowed (the Closed status indicates that the MC Account is not available for User orientated services).
- If the flag is set for an MC Account that is suspended then, based on the MNO policy the B2B attribute service is allowed - this may vary depending on the reason for suspension. For example if the account is suspended due to lost/stolen SIM / Device then it would make sense not to allow B2B attribute services to return relevant requested information but rather return a response based on the reason for suspension
- If an MC Account does not exist, then for a B2B attribute service request an account is created with a Closed Status and "Active for B2B Attributes" flag set

Figure 35 - Closing a Mobile Account and Associated Mobile Connect Account for a Pre-Pay User

Figure 35 illustrates a typical process for the situation where a pre-pay mobile has not been used for a period of time and, in line with the Operator's internal policy, the mobile account is first suspended after a specified period of inactivity. This remains in a suspended state for a period of time during which the User may contact the Operator to re-activate the mobile. At the end of this period, if there has been no further activity then the mobile account is closed and the MSISDN is returned to the number pool. If the User has registered for Mobile Connect, then the Mobile Connect Account should be suspended automatically at the point the Mobile Account is suspended. In this situation, it would also be prudent to prohibit any B2B Attribute service. If the User re-activates their Mobile Account, then similarly the Mobile Connect Account should be returned to an Active state. If, however, the Mobile Account is closed then the Mobile Connect Account should be Deleted with any associated data being archived in line with local regulations and the Operator's data retention policy.

A similar approach would apply to other Operator initiated cancellation, for example where a bill has not been paid with the account first being suspended and then after a period closed.

Annex A Core Processes

This section outlines a number of core processes that underpin the GET, SETUP and USE phases of the User Lifecycle. The core processes are more detailed process flows illustrating lower level business and technical processes and these processes are re-used for a variety of different transactions. Some core processes have been included within the main body of the handbook where it seemed appropriate to illustrate what is happening in that context.

Figure 36 shows the processes documented in this handbook including the sub-processes that are referenced. Note that sub-processes shown in grey text are not expanded within this handbook in order not to overburden the reader with too much detail. Typically, these sub-processes are self-explanatory in the context of the processes shown and further details can be obtained within the relevant technical documents that are referenced within this handbook. The remaining core processes included within this Annex are:

- Core Discover User’s Operator – use of the Discovery API to identify the serving Operator for a User and to obtain the relevant service endpoints for Mobile Connect
- Core Perform_Authorization (DI)
- Core Perform_Authorization (SI) – this is used within the Operator related processes but can equally be used by third-party Service Providers for B2B services.
- Core Create/Challenge – used within “Perform_Authorization (DI)” and “Perform_Authorization (SI)” core processes
- Core Create Mobile Connect Account – used within “Core Create/Challenge
- Core Challenge User – used within “Core Create/Challenge” and Core Create Mobile Connect Account”

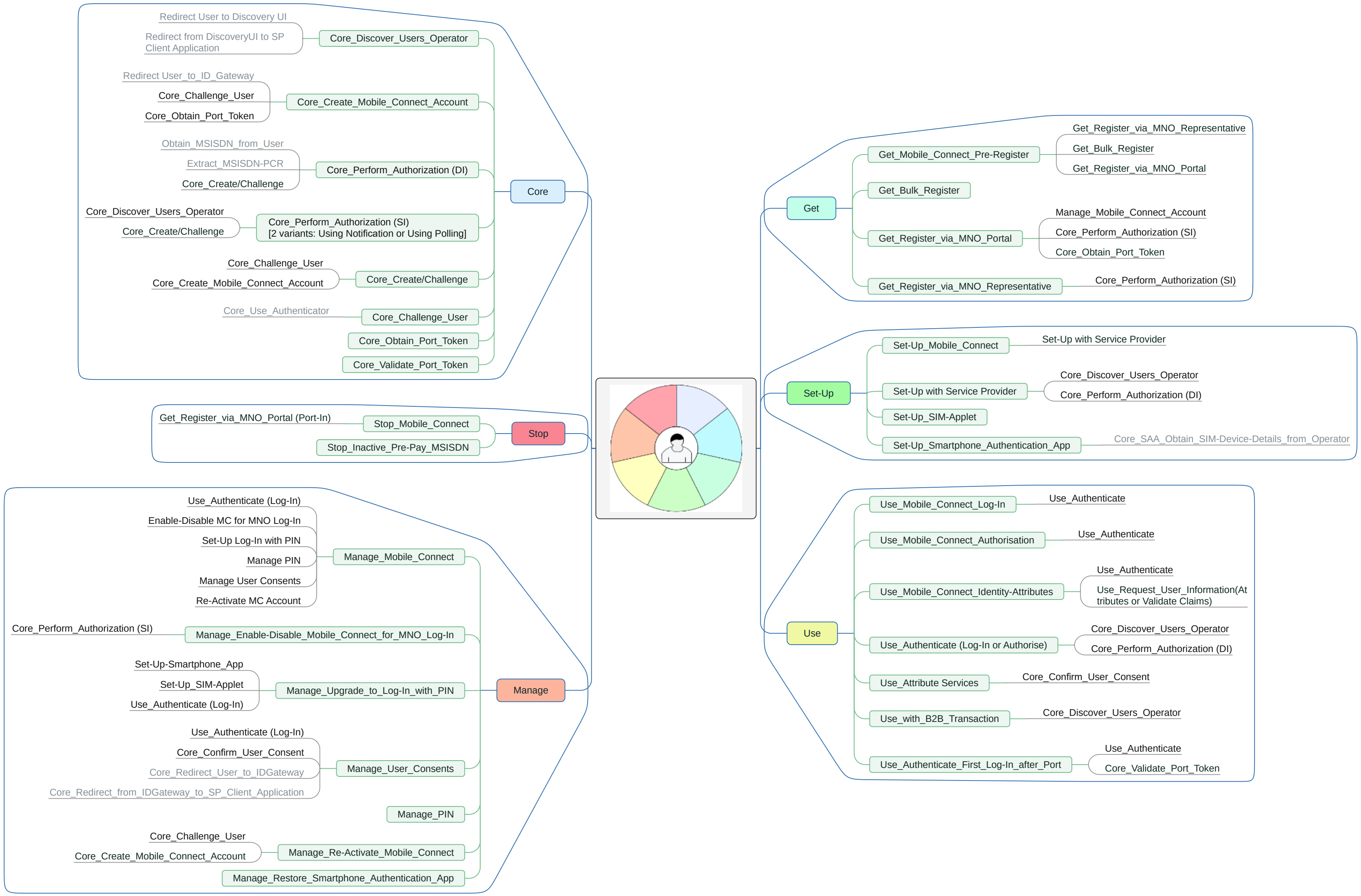
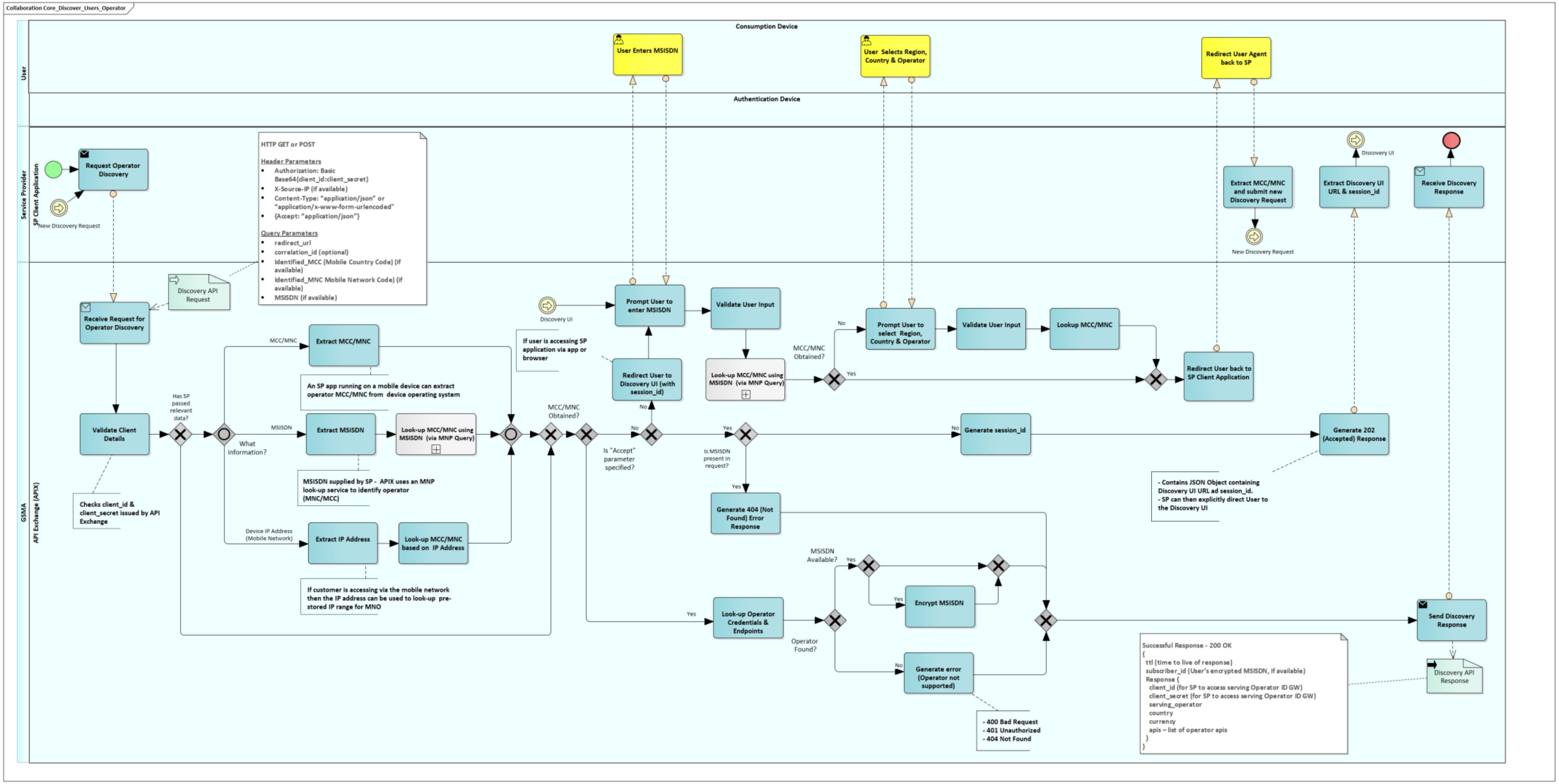

Core
Core_Discover_Users_Operator
Redirect User to Discovery UI
Redirect from DiscoveryUI to SP Client Application
Core_Create_Mobile_Connect_Account
Redirect_User_to_ID_Gateway
Core_Challenge_User
Core_Obtain_Port_Token
Core_Perform_Authorization (DI)
Obtain_MSISDN_from_User
Extract_MSISDN-PCR
Core_Create/Challenge
Core_Perform_Authorization (SI)
[2 variants: Using Notification or Using Polling]
Core_Discover_Users_Operator
Core_Create/Challenge
Core_Create/Challenge
Core_Challenge_User
Core_Create_Mobile_Connect_Account
Core_Challenge_User
Core_Use_Authenticator
Core_Obtain_Port_Token
Core_Validate_Port_Token
Stop
Stop_Mobile_Connect
Get_Register_via_MNO_Portal (Port-In)
Stop_Inactive_Pre-Pay_MSISDN
Manage
Manage_Mobile_Connect
Use_Authenticate (Log-In)
Enable-Disable MC for MNO Log-In
Set-Up Log-In with PIN
Manage PIN
Manage User Consents
Re-Activate MC Account
Manage_Enable-Disable_Mobile_Connect_for_MNO_Log-In
Core_Perform_Authorization (SI)
Manage_Upgrade_to_Log-In_with_PIN
Set-Up-Smartphone_App
Set-Up_SIM-Applet
Use_Authenticate (Log-In)
Manage_User_Consents
Use_Authenticate (Log-In)
Core_Confirm_User_Consent
Core_Redirect_User_to_IDGateway
Core_Redirect_from_IDGateway_to_SP_Client_Application
Manage_PIN
Manage_Re-Activate_Mobile_Connect
Core_Challenge_User
Core_Create_Mobile_Connect_Account
Manage_Restore_Smartphone_Authentication_App
Get
Get_Mobile_Connect_Pre-Register
Get_Register_via_MNO_Representative
Get_Bulk_Register
Get_Register_via_MNO_Portal
Get_Bulk_Register
Get_Register_via_MNO_Portal
Manage_Mobile_Connect_Account
Core_Perform_Authorization (SI)
Core_Obtain_Port_Token
Get_Register_via_MNO_Representative
Core_Perform_Authorization (SI)
Set-Up
Set-Up_Mobile_Connect
Set-Up with Service Provider
Set-Up with Service Provider
Core_Discover_Users_Operator
Core_Perform_Authorization (DI)
Set-Up_SIM-Applet
Set-Up_Smartphone_Authentication_App
Core_SAA_Obtain_SIM-Device-Details_from_Operator
Use
Use_Mobile_Connect_Log-In
Use_Authenticate
Use_Mobile_Connect_Authorisation
Use_Authenticate
Use_Mobile_Connect_Identity-Attributes
Use_Authenticate
Use_Request_User_Information(Attributes or Validate Claims)
Use_Authenticate (Log-In or Authorise)
Core_Discover_Users_Operator
Core_Perform_Authorization (DI)
Use_Attribute Services
Core_Confirm_User_Consent
Use_with_B2B_Transaction
Core_Discover_Users_Operator
Use_Authenticate_First_Log-In_after_Port
Use_Authenticate
Core_Validate_Port_Token

Figure 36: Summary of Processes and Relationships

A.1 Discovery – Discovering a User’s Operator


Collaboration Core_Discover_Users_Operator
User
Consumption Device
Authentication Device
Service Provider
SP Client Application
GSMA
API Exchange (APIX)
User Enters MSISDN
User Selects Region, Country & Operator
Redirect User Agent back to SP
Request Operator Discovery
New Discovery Request
Discovery API Request
Receive Request for Operator Discovery
Validate Client Details
Has SP passed relevant data?
What information?
MCC/MNC
Extract MCC/MNC
MSISDN
Extract MSISDN
Look-up MCC/MNC using MSISDN (via MNP Query)
Device IP Address (Mobile Network)
Extract IP Address
Look-up MCC/MNC based on IP Address
MCC/MNC Obtained?
Is "Accept" parameter specified?
No
Redirect User to Discovery UI (with session_id)
Discovery UI
Prompt User to enter MSISDN
Validate User Input
Look-up MCC/MNC using MSISDN (via MNP Query)
MCC/MNC Obtained?
No
Yes
Prompt User to select Region, Country & Operator
Validate User Input
Lookup MCC/MNC
Redirect User back to SP Client Application
Yes
Is MSISDN present in request?
Yes
Generate 404 (Not Found) Error Response
No
Generate session_id
Generate 202 (Accepted) Response
Yes
Look-up Operator Credentials & Endpoints
Operator Found?
MSISDN Available?
Yes
Encrypt MSISDN
No
Generate error (Operator not supported)
Send Discovery Response
Discovery API Response
Extract MCC/MNC and submit new Discovery Request
New Discovery Request
Extract Discovery UI URL & session_id
Discovery UI
Receive Discovery Response

HTTP GET or POST

Header Parameters
- Authorization: Basic Base64(client_id:client_secret)
- X-Source-IP (if available)
- Content-Type: “application/json” or “application/x-www-form-urlencoded”
- {Accept: “application/json”}

Query Parameters
- redirect_url
- correlation_id (optional)
- Identified_MCC (Mobile Country Code) (if available)
- Identified_MNC Mobile Network Code) (if available)
- MSISDN (if available)

Checks client_id & client_secret issued by API Exchange

An SP app running on a mobile device can extract operator MCC/MNC from device operating system

MSISDN supplied by SP - APIX uses an MNP look-up service to identify operator (MNC/MCC)

If customer is accessing via the mobile network then the IP address can be used to look-up pre-stored IP range for MNO

If user is accessing SP application via app or browser

- Contains JSON Object containing Discovery UI URL ad session_id.
- SP can then explicitly direct User to the Discovery UI

- 400 Bad Request
- 401 Unauthorized
- 404 Not Found

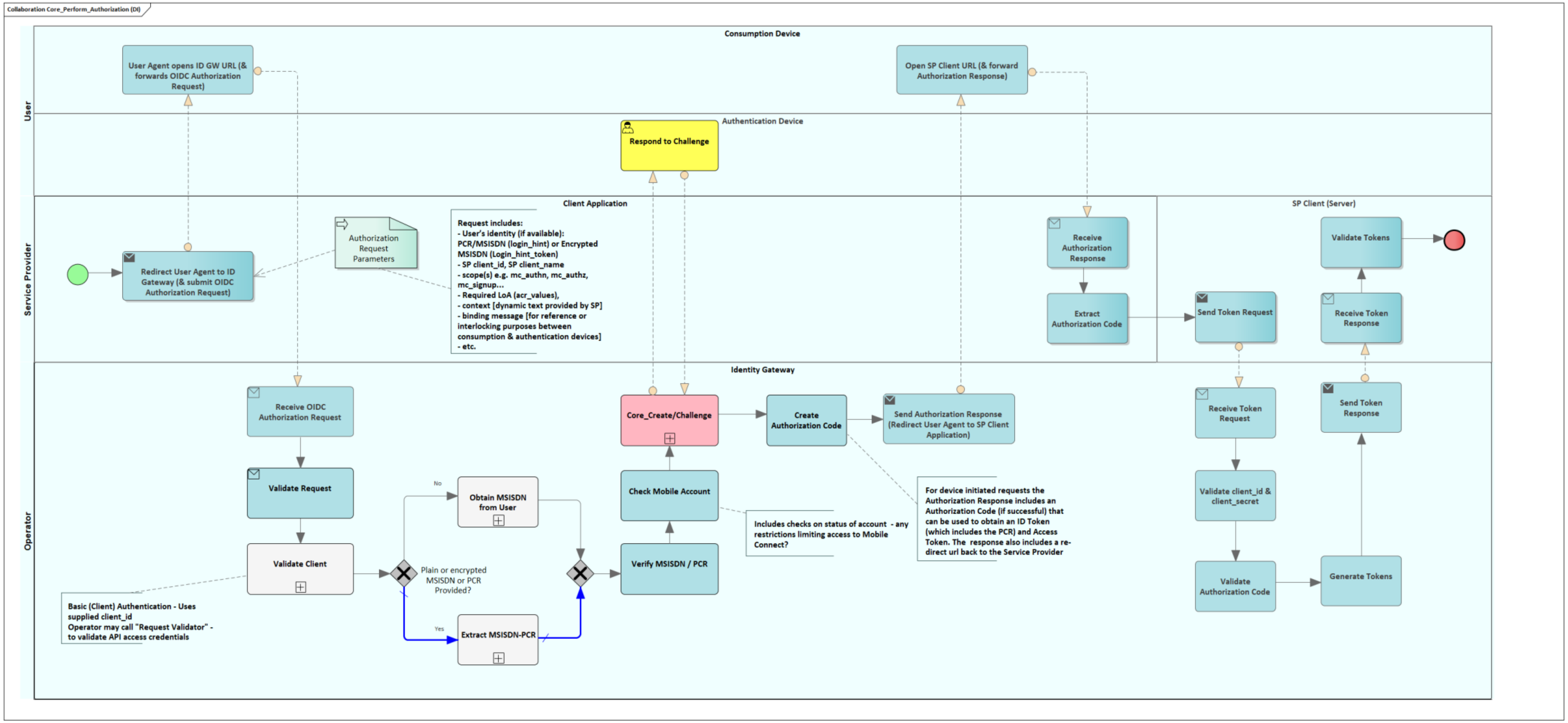
```
Successful Response - 200 OK
{
 ttl (time to live of response)
 subscriber_id (User’s encrypted MSISDN, if available)
 Response {
  client_id (for SP to access serving Operator ID GW)
  client_secret (for SP to access serving Operator ID GW)
  serving_operator
  country
  currency
  apis – list of operator apis
 }
}
```

Figure 37: Core Process - Discovery

Figure 37 illustrates the process to discover a User’s Operator and to return the relevant credentials and endpoints to allow the Mobile Connect transaction to be performed. Further detail can be found in [8]. The process flows in this handbook reference the Discovery Service provided by the API Exchange. The Discovery Service can also be deployed and operated locally, where required for security, regulatory or commercial reasons.

- The process is initiated by a Service Provider, typically when a User wishes to use Mobile Connect for Log-In for the first time. The Service Provider can repeat the process as required, however, once the Operator credentials and the PCR have been obtained by the Service Provider then this process does not have to be repeated under normal circumstances.
- When a request is made to the API Exchange, the request can contain a number of parameters that can be used to discover the correct Operator (specified in terms of Mobile Country Code and Mobile Network Code – MCC/MNC). This can include MSISDN of the User, the MCC/MNC of the Operator derived from the mobile device operating system or explicitly provided by the User or via the IP address (if the User is accessing via a mobile channel). One or more of these are used to identify the MCC/MNC.
- When the request is made, the first step is to validate the client details (Application client_id, and client_secret).
- The discovery process should not require any User interaction in normal circumstances. However, if the information provided in the request is insufficient to identify the Operator, then the User (on their Consumption Device) is redirected to the Discovery User Interface (UI) where they are first prompted to enter their MSISDN. On this basis a look-up can be performed within a porting database to obtain the relevant MCC/MNC details.
    - If for some reason this doesn't provide the required details, the User can also be prompted to select the Region, Country and Operator explicitly.
    - Once the User has input the relevant details, the User Agent, for example the browser, on the Consumption Device will be re-directed back to the Service Provider’s redirect_uri (e.g. the SP Client Application) with the Operator’s MCC and MNC returned.
    - The Service Provider can then submit a fresh Discovery Request using the supplied MCC/MNC in order to obtain the Operator ID GW details and associated credentials to be used for Mobile Connect service requests.
- As part of the processing of the Discovery Request, once the Operator has been identified (MCC/MNC) then the API Exchange looks up the Operator service endpoints and applicable credentials and a response is returned. A successful response includes serving Operator details, client id, client secret, and API endpoints. If an MSISDN is available this is encrypted and returned as “subscriber_id”.
    - Otherwise an error is returned.

A.2 Perform_Authorization (DI)


Collaboration Core_Perform_Authorization (DI)
User
Service Provider
Operator
Consumption Device
User Agent opens ID GW URL (& forwards OIDC Authorization Request)
Open SP Client URL (& forward Authorization Response)
Authentication Device
Respond to Challenge
Client Application
Authorization Request Parameters
Redirect User Agent to ID Gateway (& submit OIDC Authorization Request)
Receive Authorization Response
Extract Authorization Code
SP Client (Server)
Send Token Request
Receive Token Response
Validate Tokens
Identity Gateway
Receive OIDC Authorization Request
Validate Request
Validate Client
No
Obtain MSISDN from User
Plain or encrypted MSISDN or PCR Provided?
Yes
Extract MSISDN-PCR
Verify MSISDN / PCR
Check Mobile Account
Core_Create/Challenge
Create Authorization Code
Send Authorization Response (Redirect User Agent to SP Client Application)
Receive Token Request
Validate client_id & client_secret
Validate Authorization Code
Generate Tokens
Send Token Response

Request includes:
- User’s identity (if available): PCR/MSISDN (login_hint) or Encrypted MSISDN (Login_hint_token)
- SP client_id, SP client_name
- scope(s) e.g. mc_authn, mc_authz, mc_signup...
- Required LoA (acr_values),
- context [dynamic text provided by SP]
- binding message [for reference or interlocking purposes between consumption & authentication devices]
- etc.

Includes checks on status of account - any restrictions limiting access to Mobile Connect?

For device initiated requests the Authorization Response includes an Authorization Code (if successful) that can be used to obtain an ID Token (which includes the PCR) and Access Token. The response also includes a re-direct url back to the Service Provider

Basic (Client) Authentication - Uses supplied client_id
Operator may call "Request Validator" - to validate API access credentials

Figure 38 - Core Process – Perform_Authorization (DI)

Figure 38 illustrates the “Perform_Authorization (DI)” sub-process which describes the processing of a Device-Initiated service request. This was referenced in the Use_Authenticate sub-process in Figure 18. While Figure 18 illustrates the “Use_Authenticate” sub-process in the context of a Mobile Connect authentication or authorisation, the Perform_Authorization (DI) can equally apply to Mobile Connect Attribute services where a successful OIDC Authorization results in the issuing of an ID Token and Access Token, which can then be used as part of a Resource request to obtain the requested attributes (See **Error! Reference source not found.**).

The process in Figure 38 is as follows:

- The Service Provider initiates a Mobile Connect service request by specifying the relevant service codes in the “scope” parameter of the OIDC Authorization request and specifying the required LoA. The request will also include the User’s Identity if available (PCR, MSISDN or Encrypted MSISDN), Service Provider’s client details, optional context, etc.The user agent on the Consumption device is re-directed to the ID GW URL by the SP Client application forwarding the OIDC Authorization request to the ID GW.
- The request is received at the ID GW.
    - The request is checked to ensure it is in the correct format and that it contains all mandatory parameters, etc.)
    - The requesting SP Client Application is checked to ensure that the client_id and client_name submitted in the request correspond to a registered client and that the client is registered for the requested Mobile Connect service. The SP Client application credentials (client_id and client_name) are generated as part of the registration of an SP application with the ID GW. The ID GW may implement a process to capture and store the credentials as part of the SP Client application registration.
    - Alternatively, the ID GW can make use of the optional Request Validator service provided by the API Exchange to retrieve the relevant client details. In order to use this both the SP Client application and the Operator ID GW must be registered with the API Exchange and the ID GW must have subscribed to this service (Further details can be found in [7]).
- If the PCR, MSISDN or encrypted MSISDN have been provided (the default) then these are verified and used to check the Mobile Account and Mobile Connect Account. If not, then the User can be prompted via the Consumption Device to enter their MSISDN. This is not visible to the Service Provider.
- The “Core_Create/Challenge” sub-process (See Figure 41) then checks the User’s Mobile Account and Mobile Connect Account (if it exists) for eligibility for the service and then generates a challenge to the User to authenticate, authorise a transaction or, if appropriate, to give consent for sharing the User’s attributes with the Service Provider (See Section 3.7 for details on options to capture User consent). If the Mobile Connect Account does not exist, then one is created, subject to ID GW policy. Note that the task to “Check Mobile Account” is duplicated within the “Perform_Authorization (DI)” sub-process and “Core_Create/Challenge” sub-process to aid readability.

- If the Authentication or Authorisation was successful, then an Authorization Code is generated. This is a one-time, time-limited code that is passed to the Service Provider through redirection of the user agent on the Consumption Device back to the SP Client application.
- The SP Client application then makes a direct server to server request to the ID GW Token endpoint to retrieve the relevant ID Token and Access Token from the ID GW. The ID Token contains the PCR that can be used for subsequent transactions.
- If a Mobile Connect Attribute service was requested, then the Access Token, returned with the ID Token, can be used to validate or share the relevant User attributes (that are specified by the specific service requested).

A.3 Perform_Authorization (SI)

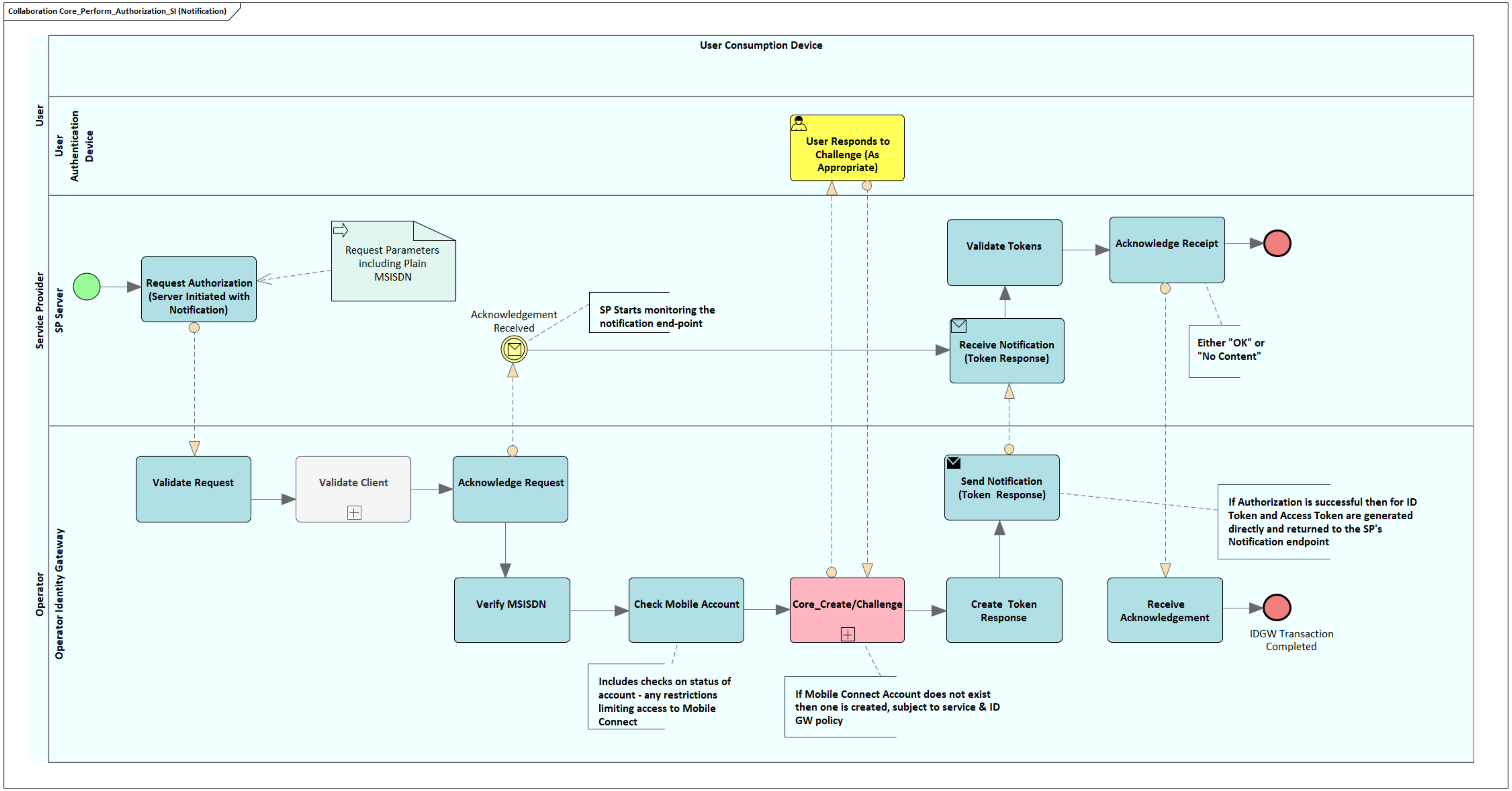
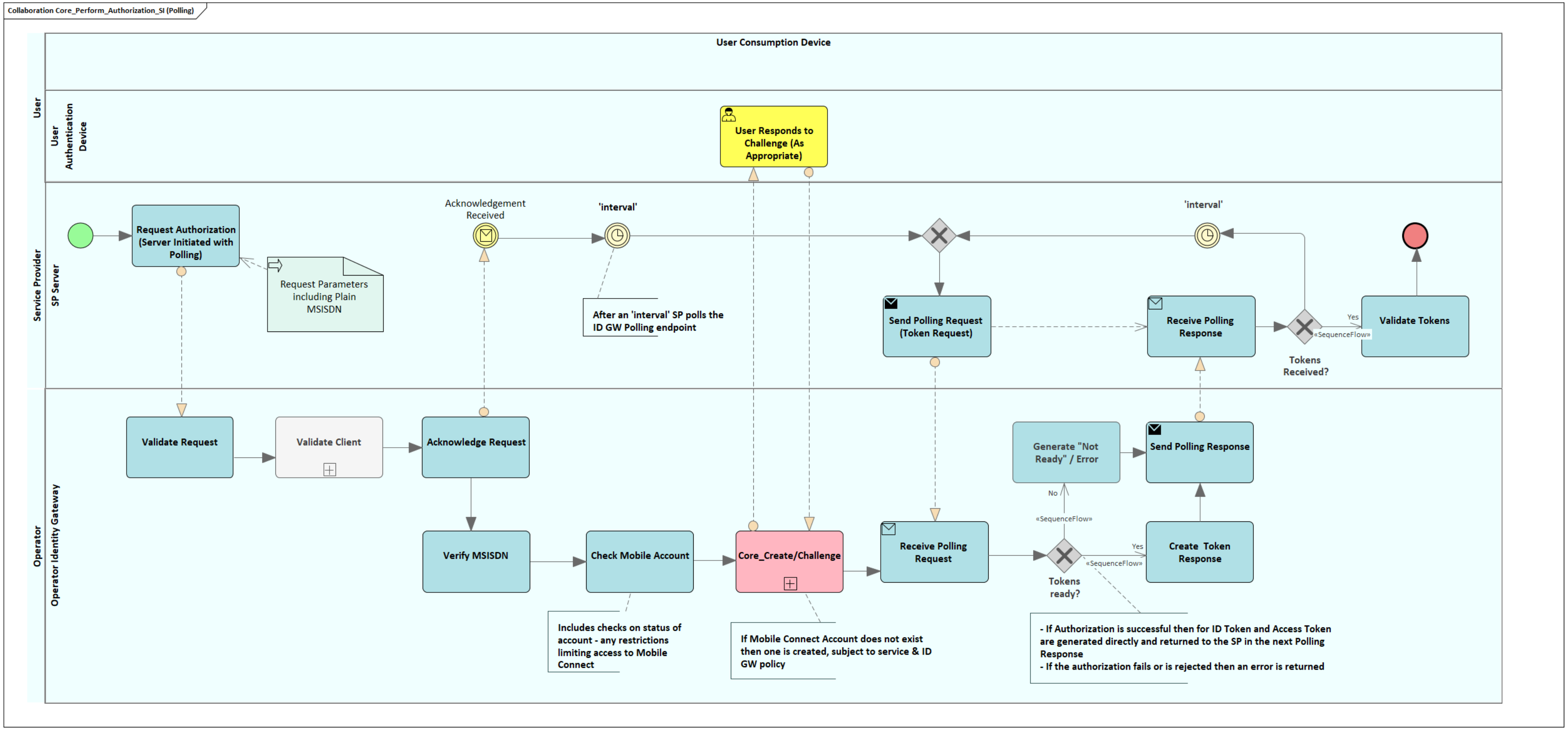

Collaboration Core_Perform_Authorization_SI (Notification)
User
User Consumption Device
User Authentication Device
User Responds to Challenge (As Appropriate)
Service Provider
SP Server
Request Authorization (Server Initiated with Notification)
Request Parameters including Plain MSISDN
Acknowledgement Received
SP Starts monitoring the notification end-point
Validate Tokens
Acknowledge Receipt
Receive Notification (Token Response)
Either "OK" or "No Content"
Operator
Operator Identity Gateway
Validate Request
Validate Client
Acknowledge Request
Send Notification (Token Response)
If Authorization is successful then for ID Token and Access Token are generated directly and returned to the SP's Notification endpoint
Verify MSISDN
Check Mobile Account
Core_Create/Challenge
Create Token Response
Receive Acknowledgement
IDGW Transaction Completed
Includes checks on status of account - any restrictions limiting access to Mobile Connect
If Mobile Connect Account does not exist then one is created, subject to service & ID GW policy

Figure 39 - Core Process – Perform_Authorization (Server Initiated using Notification)



After an 'interval' SP polls the ID GW Polling endpoint

Includes checks on status of account - any restrictions limiting access to Mobile Connect

If Mobile Connect Account does not exist then one is created, subject to service & ID GW policy

- If Authorization is successful then for ID Token and Access Token are generated directly and returned to the SP in the next Polling Response
- If the authorization fails or is rejected then an error is returned

Figure 40 - Core Process – Perform_Authorization (Server Initiated using Polling)

Figure 39 and Figure 40 show two variants of Server-Initiated sub-process flows. Both variants use the same request format; the difference between them is in the mechanism used to retrieve the ID Token and Access Token from the ID GW – using notification or a polling mechanism. Within this handbook “Perform_Authorization (SI)” can refer to either of these Server-Initiated process flows depending on what has been implemented within the Operator’s ID GW.

Perform_Authorization (SI) illustrates the basic OIDC Authorization request and token retrieval that is the basis for all Server-Initiated Mobile Connect service requests. This is equivalent to the Device_Initiated request flow, Perform_Authorization (DI) sub-process illustrated in Figure 38

As mentioned previously the Perform_Authentication (SI) sub-process is used as the basis for Direct Registration for Mobile Connect with the User’s Operator but it can also be used by 3rd Party Service Providers where they have a trusted status and have access to the User’s MSISDN. The key requirement here is that the Service Provider has access to the MSISDN and has configured their Client Application Server to make direct API calls to the ID GW.

It is assumed that the Service Provider (or Operator self-care portal, etc.) has the relevant ID Gateway details including the relevant SP credentials that they should use with the ID Gateway. If not then a Discovery request (Discover_User’s_Operator sub-process) will need to be performed prior to this request.

The process is as follows:

- As part of an interaction with a customer, a Service Provider may wish to initiate a Mobile Connect service directly as a server to server transaction. This may be authenticating the customer who has called customer care before accessing their account or it may be performing background checks as part of registration for a new service.
- A Mobile Connect service request is made to the Operator ID GW directly from the Service Provider’s Client Application, passing the User’s MSISDN (in open format).
    - As indicated previously the Service Provider can include within the request whether they require LoA2 or LoA3 and within the construction of the authorization request the type of service required (“scope” values).
- The ID GW then validates that the request is well-formed and in the right format and validates the Client credentials. Once this has been performed then an acknowledgement is returned to the SP server application.

- Once the acknowledgement has been received (assuming successful initial validation then the SP server application then starts to either monitor the Notification endpoint it had previously specified during registration or after an interval starts to poll the published ID GW Polling endpoint in order to retrieve the ID Token and Access Token.
- The ID GW verifies the MSISDN and checks the Mobile Account, for example to see if there are any restrictions on the Mobile Connect Account that would prevent the transaction taking place.
- The “Core_Create/Challenge sub-process then checks the User’s Mobile Account and Mobile Connect Account (if it exists) for eligibility for the service. If the Mobile Connect Account does not already exist, then one is created.
- If the service request was successful, then an ID Token and Access Token are generated directly and passed back to the Service Provider. If not, then an error is returned (Error Code and Description).
    - There are also some use cases where explicit Authentication or Authorisation by the User are not required. If this is the case, then ID Token and Access Token are generated directly and returned.
- The Token response is received, validated and acknowledged by the Service Provider (in the notification variant) and the ID Token and Access Token can then be processed as normal.

A.4 Core_Create/Challenge

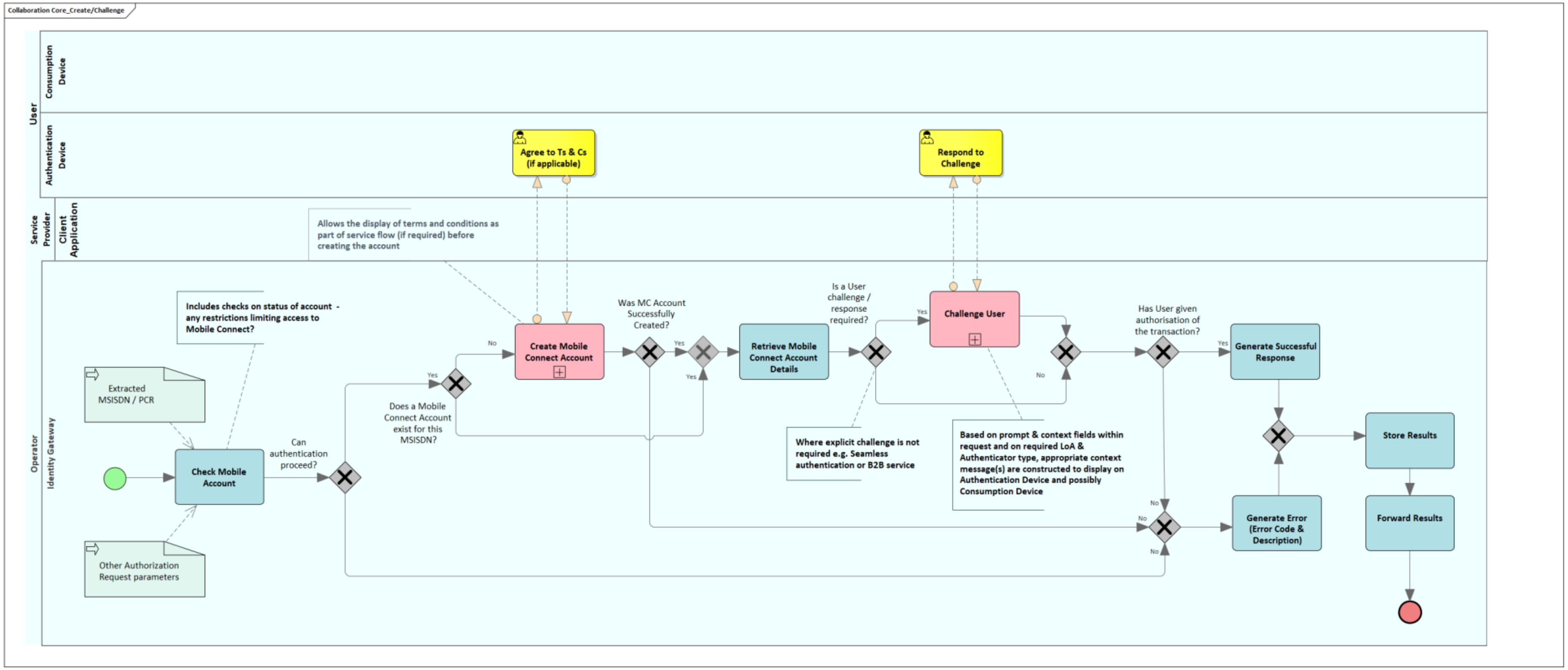

Collaboration Core_Create/Challenge
User
Consumption Device
Authentication Device
Service Provider
Client Application
Operator
Identity Gateway
Agree to Ts & Cs (if applicable)
Respond to Challenge
Allows the display of terms and conditions as part of service flow (if required) before creating the account
Includes checks on status of account - any restrictions limiting access to Mobile Connect?
Extracted MSISDN / PCR
Other Authorization Request parameters
Check Mobile Account
Can authentication proceed?
Does a Mobile Connect Account exist for this MSISDN?
Yes
No
Create Mobile Connect Account
Was MC Account Successfully Created?
Yes
Yes
Retrieve Mobile Connect Account Details
Is a User challenge / response required?
Yes
Challenge User
No
Where explicit challenge is not required e.g. Seamless authentication or B2B service
Based on prompt & context fields within request and on required LoA & Authenticator type, appropriate context message(s) are constructed to display on Authentication Device and possibly Consumption Device
Has User given authorisation of the transaction?
Yes
Generate Successful Response
No
No
No
Generate Error (Error Code & Description)
Store Results
Forward Results

Figure 41: Core Process – Create/Challenge

Figure 41 shows the "Core_Create/Challenge" sub-process which is used in "Perform_Authorization (DI)" and in "Perform_Authorization (SI)" sub-processes. It takes the PCR or MSISDN to look up the relevant Mobile Account and Mobile Connect Account for the User.

- The ID GW verifies the MSISDN or PCR and checks the Mobile Account to see if there are any restrictions on the Mobile Account that would prevent the transaction taking place. For example, if the account was suspended due to a lost or stolen SIM or Device then this would prevent an authentication proceeding and would generate an error response that is returned to the Service Provider.
    - If there are any restrictions on the Mobile Account that prevents access to Mobile Connect, then an error is generated.

- If there are no such restrictions then there is a check to see if a Mobile Connect Account exists – this, of course, would typically be done at the same time as any checks on the Mobile Account.
    - If a Mobile Connect Account does not exist, then one is created (using the “Create Mobile Connect Account” sub-process)
- The Mobile Connect Account Details are retrieved. If the User is required to respond to a challenge (i.e. authenticate, authorise or provide consent, as appropriate), then an appropriate prompt is prepared for the User Challenge depending upon the requested service(s) using standard prompt action text for that type of transaction generated by the ID GW and optionally including context information provided by the Service Provider Client application.
- The User is then challenged (“Challenge_User” sub-process) via the appropriate Authenticator.
    - If access is via the mobile channel using the mobile device that is also the Authentication Device and the Operator supports Enriched Headers then the MSISDN can be passed directly in the Enriched Header which allows seamless authentication, where explicit authentication by the User is not required. In this case the authentication step is bypassed as shown.
    - Where the User is required to respond (authenticate, authorise or give consent), and they do not do so[20] then an error is generated
- The outcome of the process is then forwarded to the calling process (“Perform_Authorization (DI)” or “Perform_Authorization (SI)” sub-processes)

[20] Either by clicking “Cancel” or “Deny”, as appropriate, or if the request times-out

A.5 Create a Mobile Connect Account

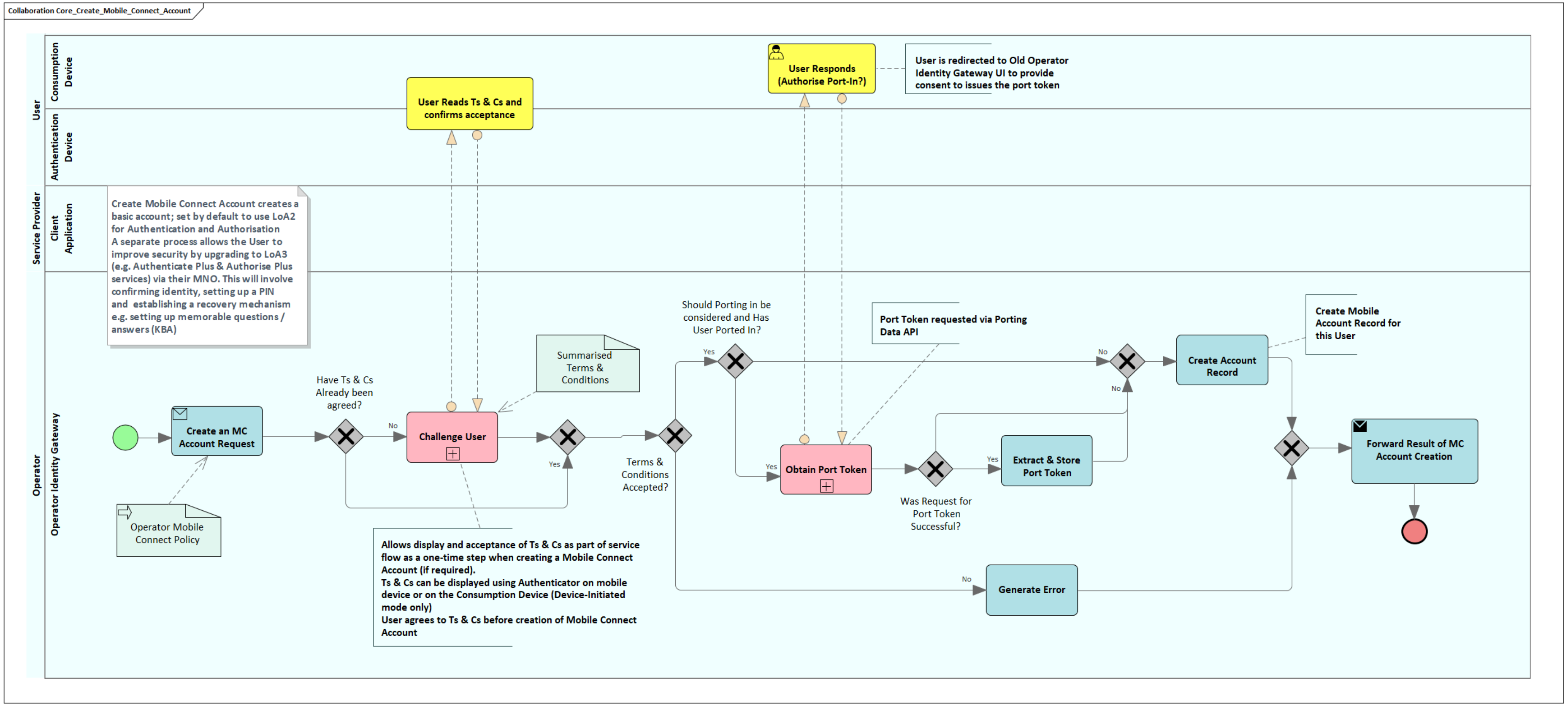

Collaboration Core_Create_Mobile_Connect_Account
User
Consumption Device
Authentication Device
Service Provider
Client Application
Operator
Operator Identity Gateway
User Reads Ts & Cs and confirms acceptance
User Responds (Authorise Port-In?)
User is redirected to Old Operator Identity Gateway UI to provide consent to issues the port token
Create Mobile Connect Account creates a basic account; set by default to use LoA2 for Authentication and Authorisation
A separate process allows the User to improve security by upgrading to LoA3 (e.g. Authenticate Plus & Authorise Plus services) via their MNO. This will involve confirming identity, setting up a PIN and establishing a recovery mechanism e.g. setting up memorable questions / answers (KBA)
Should Porting in be considered and Has User Ported In?
Port Token requested via Porting Data API
Create Mobile Account Record for this User
Summarised Terms & Conditions
Have Ts & Cs Already been agreed?
Create an MC Account Request
No
Challenge User
Yes
Terms & Conditions Accepted?
Yes
No
Create Account Record
No
Obtain Port Token
Yes
Extract & Store Port Token
Was Request for Port Token Successful?
Forward Result of MC Account Creation
Operator Mobile Connect Policy
Allows display and acceptance of Ts & Cs as part of service flow as a one-time step when creating a Mobile Connect Account (if required).
Ts & Cs can be displayed using Authenticator on mobile device or on the Consumption Device (Device-Initiated mode only)
User agrees to Ts & Cs before creation of Mobile Connect Account
No
Generate Error

Figure 42 - Core Process – Creating a Mobile Connect Account

Error! Reference source not found. illustrates the “Create Mobile Connect Account” sub-process that is used to create an account as part of the processing of a Mobile Connect service request, if one does not already exist. The sub-process is referenced within “Core_Create/Challenge” and therefore potentially plays a role within “Set-Up with Service Provider”, “Use_Authenticate”, “Perform_Authorization (DI)”, “Perform_Authorization (SI)” processes. The “Create Mobile Connect Account” sub-process is executed within the Operator ID GW and may involve prompting the User with a summary of Terms and Conditions and seeking their agreement to those terms and conditions. Note that by default the Mobile Connect Account will be set at LoA2 and a network-based Authenticator (USSD, SMS + URL) would be used. If supported by the ID GW, these are available to all mobile devices.

The process is as follows:

- The request is received, and a check is made to determine if terms and conditions (including privacy policy) have been accepted by the User. This may be as a result of the terms and conditions having been accepted implicitly because they are included within the Operator’s standard mobile contract terms and conditions or through interaction with a Customer Agent the terms and conditions have been explained and accepted – either verbally or via a tick box (or similar) on the Operator Portal. If this is the case, then it may not be appropriate to seek explicit acceptance again or it may be that a modified message and prompt is presented. It is good practice to ensure that the User is aware of those terms and conditions by providing a link to or a copy of the terms and conditions via SMS or email.
- If explicit acceptance of terms and conditions is required, then the appropriate message for display on the Consumption Device or on the Authentication device is constructed. This is shown within the “Challenge_User” sub-process in Figure 43. The User is prompted to respond to the challenge or request i.e. to accept the terms and conditions.
- If the terms and conditions have been accepted confirming that the User wishes to register for Mobile Connect, then a Mobile Connect Account record for that User is created within the ID GW User database.
- In the case where a User has indicated to their Operator that they wish to port in a Mobile Connect Account then the “Core Obtain Port Token” sub-process is executed, where the Operator contacts the User’s previous Operator to obtain a port_token (via the Mobile Connect Account Porting Data API) – this is then ultimately included within the ID Token issued to a Service Provider to enable the SP to check the Mobile Connect Account details with the previous Operator to allow the SP’s User account to be updated. Further information is provided in [12].
- Note that the “Create_Mobile_Connect_Account sub-process includes the option to bypass this part of the process (“Should porting in be considered?”). Clearly if the porting in mechanism is not supported then this part of the sub-process is not applicable. If it is supported then, depending upon the specific use case (e.g. for registration on-the-fly), it may be inappropriate to invoke this flow as it will interrupt the normal service flow and potentially introduce a number of additional steps that would increase friction and the likelihood for drop-out by the User. However, it may be appropriate when registering for Mobile Connect via the Operator’s customer care, retail store or self-care portal. The decision to invoke this is down to Operator policy

A.6 Challenging the User via an Authenticator

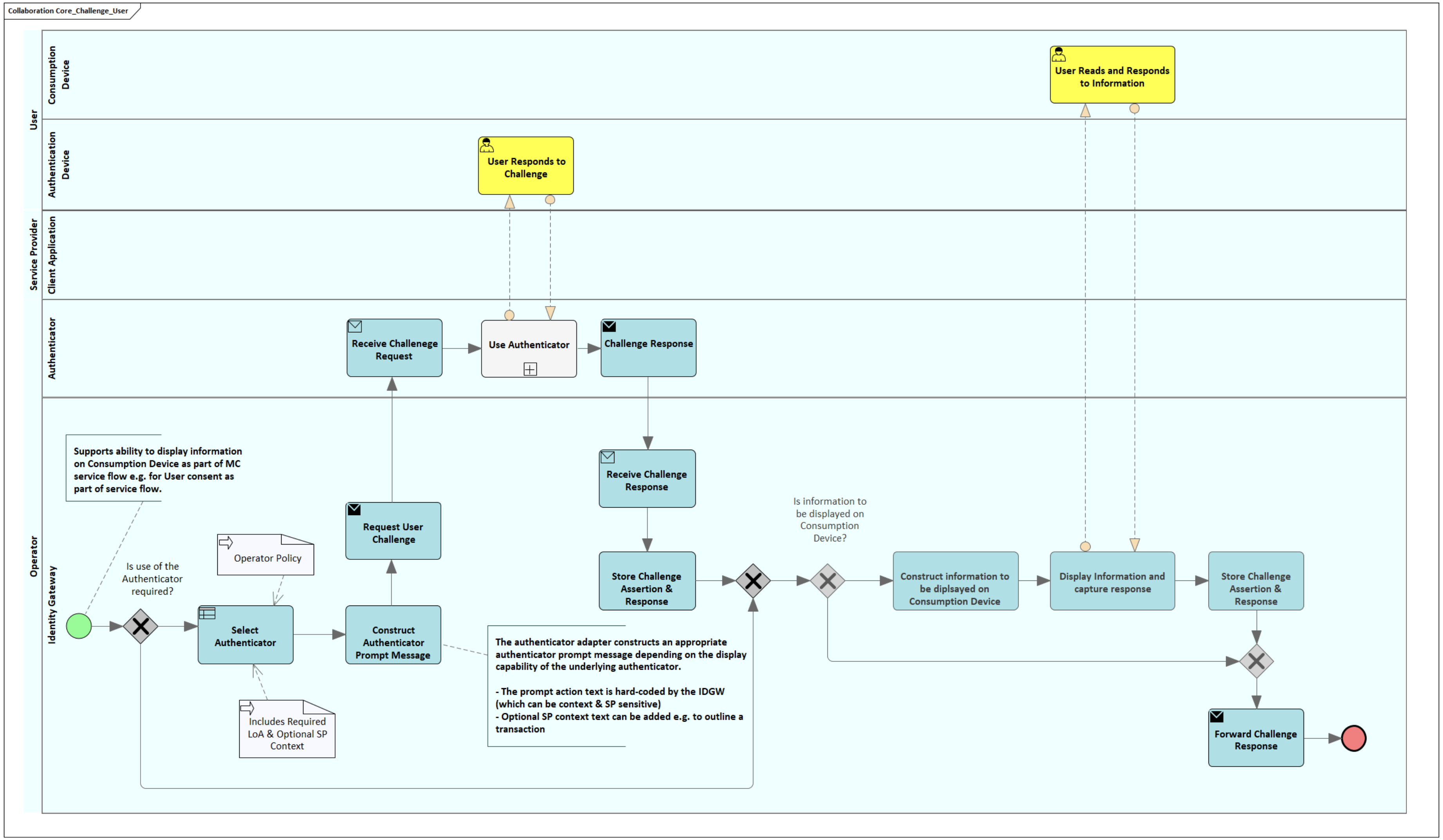

Collaboration Core_Challenge_User
User
Consumption Device
Authentication Device
Service Provider
Client Application
Operator
Authenticator
Identity Gateway
User Reads and Responds to Information
User Responds to Challenge
Receive Challenege Request
Use Authenticator
Challenge Response
Supports ability to display information on Consumption Device as part of MC service flow e.g. for User consent as part of service flow.
Receive Challenge Response
Is information to be displayed on Consumption Device?
Request User Challenge
Operator Policy
Is use of the Authenticator required?
Select Authenticator
Construct Authenticator Prompt Message
Store Challenge Assertion & Response
Construct information to be diplsayed on Consumption Device
Display Information and capture response
Store Challenge Assertion & Response
The authenticator adapter constructs an appropriate authenticator prompt message depending on the display capability of the underlying authenticator.
- The prompt action text is hard-coded by the IDGW (which can be context & SP sensitive)
- Optional SP context text can be added e.g. to outline a transaction
Includes Required LoA & Optional SP Context
Forward Challenge Response

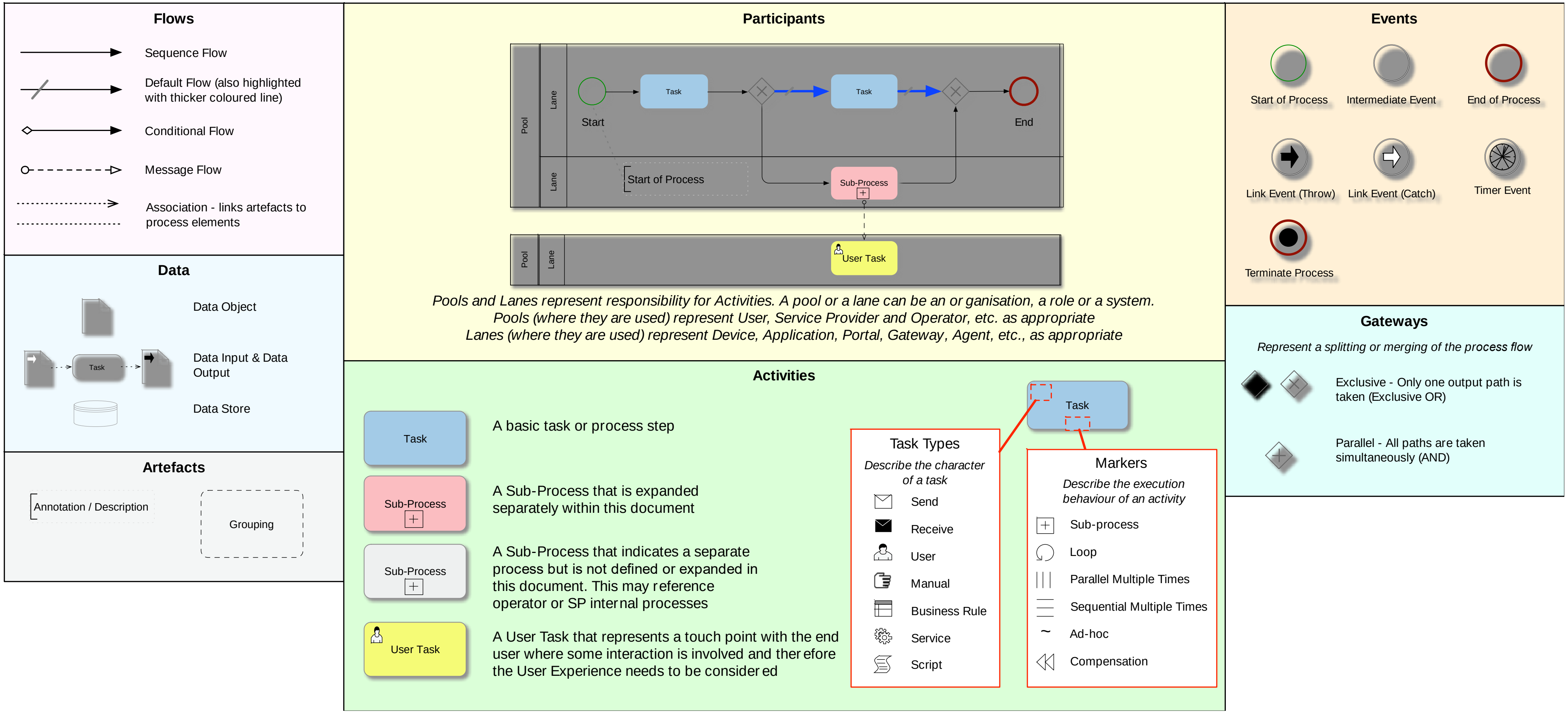
Figure 43 - Core Process – Challenge User

Figure 43 outlines the "Challenge User" sub-process that is used within "Create Mobile Connect Account", "Perform_Authorization (DI)", "Perform_Authorization (SI)" and "Confirm User Consent".

- It receives a prompt message which may be specified by the Service Provider and passed within the request or depending upon the context (Requested Scope(s)) can be constructed by the Operator ID GW.
- The first step is the selection of an appropriate authenticator by the Operator based on what is supported by the Operator, the requested LoA and User's mobile device capabilities.
- Depending on the selected Authenticator it may be necessary to display information on the Consumption Device rather than on the Authentication Device where the screen size and Authenticator capabilities may limit what can be displayed. Clearly the User experience (UX) is important in this regard.
- If the Consumption Device is the same as the Authentication Device then this arrangement could result in a prompt message being displayed on the Consumption Device, for example in the browser on the mobile device and then replaced by the Authentication prompt and challenge on the Authentication Device for example a USSD screen which overwrites the display. On this basis a delay has been introduced to enable the User to read the context message before the challenge appears.
- A request is passed to the relevant Authenticator that then initiates the prompt and challenge on the Authentication device and returns the result. The "Use Authenticator" sub-process is not expanded within this handbook but takes into account the different Authenticator mechanisms – for example using SMS + URL will mean that a positive confirmation is obtained by the User clicking on the embedded URL but a negative response arises from the User not doing so such that the process times-out whereas using USSD allows an explicit yes or no response.
- The response is received back at the ID GW and the transaction, assertion and response are stored in the User's Mobile Connect Account to allow transaction history to be monitored.
- The response is then forwarded to the call process.

Annex B BPMN 2.0 Syntax

B.1 Quick Reference and Colour Coding Used within this Handbook



Pools and Lanes represent responsibility for Activities. A pool or a lane can be an or ganisation, a role or a system.
Pools (where they are used) represent User, Service Provider and Operator, etc. as appropriate
Lanes (where they are used) represent Device, Application, Portal, Gateway, Agent, etc., as appropriate

A basic task or process step

A Sub-Process that is expanded separately within this document

A Sub-Process that indicates a separate process but is not defined or expanded in this document. This may reference operator or SP internal processes

A User Task that represents a touch point with the end user where some interaction is involved and ther efore the User Experience needs to be consider ed

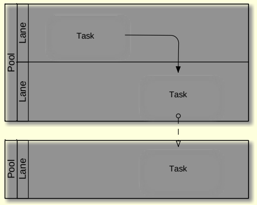
Describe the character of a task

Describe the execution behaviour of an activity

Represent a splitting or merging of the process flow

B.2 Summary of BPMN 2.0 Syntax

Participants



Pools and Lanes represent responsibility for Activities. A pool or a lane can be an organisation, a role or a system.

Flows

——→ Sequence Flow defines the succession of execution

-/-→ Default Flow defines the flow that is followed by default if all other conditions are not met

◇——→ Conditional Flow contains a condition which defines when this flow will be followed and when not

○- - - -▷ Message Flow represents information exchange, typically between pools. Message flows can be attached to pools, activities, and message events

Artefacts

Grouping — Allows process elements to be grouped

[Annotation / Description — Allows annotations, qualifications, explanations to be added to process elements

·········> Association - links artefacts to process elements

Note that other (different) symbols can also be used as artefacts

Activities

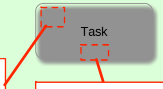
Task — A Task represents a basic process step or task. With the sub-process marker it represents a collapsed sub-process

Transaction — A Transaction is a group of activities which belong together logically e.g. represents a critical process where all activities must be completed successfully (or not at all) before progressing.

Call Activity — A Call Activity represents a globally defined sub-process or a globally defined task which is used (called) in the current process

Event Sub-Process — An Event Sub-Process is placed within another sub-process. It is triggered by a start event and can interrupt the surrounding sub-process or it can be executed in parallel depending on the type of start event e.g. to trigger some remedial action

Activities can be qualified using task types and markers



Task Types

Describe the character of a task

- ✉ Send
- ✉ Receive
- 👤 User
- ✋ Manual
- ▦ Business Rule
- ⚙ Service
- 📜 Script

Markers

Describe the execution behaviour of an activity

- ⊞ Sub-process
- ↻ Loop
- ||| Parallel Multiple Times
- ☰ Sequential Multiple Times
- ~ Ad-hoc
- ⏪ Compensation

Gateways

Represent a splitting or merging of the process flow

◆ ⊗ Exclusive - The process follows only one outgoing sequence flow based on the result of a query or decision. When merging, the process waits for one incoming path to activate the outgoing sequence flow

✚ Parallel - All outgoing paths are activated simultaneously. When merging , the process waits for all incoming paths to complete before activating the outgoing sequence flow

○ Inclusive - One or more outgoing paths are activated. When merging incoming paths are synchronised.

⬠ Event Based - The gateway is always followed by catching events or receive tasks - the outgoing path that receives the event first is used.

✱ Complex - Splitting and merging behaviour that is not handled by any other type of gateway (Normally qualified through annotation)

⬠ Exclusive Event Based (instantiating) - As soon as one of the following events occurs, the process is started

✚ Parallel Event Based (instantiating) - Only if all the preceding events occur will the process be stated

Data

Data Object - represents data or information that flows through the process e.g. token, documents, e-mails, letters, etc.

Data Input is an external input for the whole process. Data Output is similarly the result or output of a whole process

A List Data Object represents a group of information e.g. a list with order positions

A Data Store is where a process can read or write information e.g. a database or a filing cabinet. It exists independently of the process .

✉ Throw ✉ Catch

A Message depicts the content of a communication between two participants

Events

Event Type	Start			Intermediate				End
		Event Sub-Process		Catching	Boundary		Throwing	
		Interrupting	Non Interrupting		Interrupting	Non Interrupting		
None	○			○				○
Message	✉	✉	✉	✉	✉	✉	✉	✉
Timer	⏲	⏲	⏲	⏲	⏲	⏲		
Error		ϟ			ϟ			ϟ
Escalation		⌃	⌃		⌃	⌃	⌃	⌃
Cancel					✖			✖
Compensation		⏪			⏪		⏪	⏪
Conditional	☰	☰	☰	☰	☰	☰		
Link				➡			➡	
Signal	△	△	△	△	△	△	▲	▲
Terminate								●
Multiple	⬠	⬠	⬠	⬠	⬠	⬠	⬟	⬟
Multiple-Parallel	⊕	⊕	⊕	⊕	⊕	⊕		

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	12/02/2018	Initial Draft of the handbook based around a finalised set of process flows	D Pollington	N Spencer
0.2	12/03/2018	Updated based on reviews by D Pollington & J Gore	D Pollington	N Spencer
0.3	13/03/2018	Minor updates following second review	D Pollington	N Spencer
0.4	23/03/2018	Correction of a few remaining typographical erros	D Pollington	N Spencer
1.0	30/03/2018	Draft 0.5 upgraded to v1.0 and issued	D Pollington	N Spencer
1.1	24/11/2018	Updated sections on Mobile Connect Account and Attribute Services (User consent)	D Pollington	N Spencer
1.2	08/07/2019	Updated as part of developing MNO Deployment Guidelines	D Pollington	N Spencer
1.3	27/09/2019	Tidy up of discussion around user consent and ‘legal basis for sharing attributes’	D Pollington	N Spencer
1.3	06/12/2022	Go throught TG approval	TG	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 mobileconnect@gsma.com

C.1 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.