PUBLICATION 1 SERVICE DESCRIPTION FOR FLEXIBLE IDENTITY SERVICE

1.1 Definitions

As used in this Service Description, the following capitalized terms will have the meanings given to such terms in this Clause 1.1. In the event of any conflict between the definitions provided in this Service Description and those provided elsewhere in the Agreement, the definitions in this Service Description will prevail to the extent of any such conflict. All capitalized terms used and not otherwise defined herein will have the meaning ascribed to them elsewhere in the Agreement.

"**Administrator**" means Customer's nominated individual authorized to administer the Service (as notified to Orange).

"**Customer Project Manager**" means the Customer's single point of contact for Orange until the end of the implementation phase of the Service.

"**GCSC**" means an Orange Global Customer Support Center.

"**Hosting Platform**" means the hosting platform used for the provision of the Service and shared between all Customers having subscribed to the Service.

"**Management Portal**" means the web portal for Administrators, allowing them to configure the Service (as further described in this Service Description).

"**Service**" means the Flexible Identity service.

"**User**" means a user of the Service for whom Customer has set up a specific account, using the Management Portal.

"**User Portal**" means the web applications through which the User will be able to manage functions included into his profile (as further described in this Service Description).

1.2 Service Description

1.2.1 Overall description

The "**Service**" is categorized as a Cloud Service and is a managed security service which mitigates the risks of digital identity usurpation by providing Users with a variety of authenticators, each one being more secure than a simple password and share this identity, in a controlled manner, with service providers.

The Service incorporates two service levels:

- The **Flexible Identity Authentication** service level corresponds to the multi-factor authentication function. The related pricing level is called "Bronze".
- The **Flexible Identity Federation** service level corresponds to the identity federation function. The related pricing level is called "Silver" or "Silver Starter Pack". "Starter Pack" is subject to specific price, and is applicable when only one cloud-app is integrated.

The two service levels may be combined. The related pricing level is called "Gold" or "Gold Starter Pack". "Starter Pack" is subject to specific price, and is applicable when only one cloud-app is integrated in **Flexible Identity Federation**.

The two service levels comprise the following features:

- A Management Portal and a User Portal specific for each service level.
- Helpdesk support for designated Administrators.
- Service usage reports as defined by the designated Administrators.
- Maintenance and upgrades of the Service.
- Management and monitoring of the Service on a 24x7 basis.

For the Flexible identity Authentication service level, shipment of hardware authenticators to Administrators is included.

The Service being billed per User, the number of User benefiting from it can be adjusted according to Customer needs.

1.2.2 Flexible Identity Authentication Service Level

The Service is charged on a 'per-created-User' basis, allowing Customer to scale up and down the number of subscribed Users, depending on its requirements throughout the term of the Service.

(a) **Multi-Factor Authentication:** The Service provides a range of authenticators as ordered by Customer. Depending on the security policy put in place by the Administrators using the Management Portal, a User can use one or several of the following authenticators (as ordered by Customer):

- Hardware type: (i) Standard, (ii) Premium, (iii) Platinum, and (iv) Keypad.
- Software type: (i) MobilePass (for desktops/laptops), (ii) MobilePass (for smartphones/tablets), (iii) GrID, and (iv) SMS OTP.

(b) **Multi-Tenanted aspect of Service:** The Service is multi-tenanted to adapt to a Customer's organization by creating independent virtual entities, each of them including: Users, Administrators, a Management Portal and a security policy. Accordingly, it is possible for a customer who has a number of Affiliates to benefit from the advantages of a centrally operated Service without giving up local independence and flexibility.

(c) **Management Portal:** The Service provides a Management Portal allowing designated Administrators to perform day-to-day service management tasks, as follows:

- Creating or deleting Users or groups of Users.
- Managing authenticators and the way they are assigned to Users.
- Managing the Service reports.
- Defining automated messages sent to Users.
- Access to Service logs.

The Management Portal is accessible through a web browser connected to the Internet using a HTTPS connection. The Management Portal is available in English and French. In the context of the multi-tenanted aspect of the Service, each Administrator will only be able to manage their own entity.

(d) **User Portal:** The Service provides a User Portal allowing Users to perform day-to-day actions in an autonomous manner, as follows:

- Resetting hardware or software token PIN code.
- Resetting GrID token PIP code.
- Resynchronizing tokens.
- Triggering a new SMS OTP sending.

The User Portal is accessible through a web browser connected to the Internet using a HTTPS connection. The User Portal is available in several languages that can be personalized by Administrators.

(e) **User Management:** User accounts can be set up and managed using one or all of the following three options (the selection of which will depend on Customer's specific requirements and the size of its organization):

(i) **Manual provisioning:**

Manual provisioning may be appropriate for small businesses without a corporate directory or for businesses not willing to add some of their Users into their corporate directory (e.g. partners, external collaborators, etc.). Manual provisioning allows the manual creation of User accounts using the Management Portal.

To avoid inactive accounts to continue in the Service (even in the case of manual provisioning), it is possible for Administrators to configure a "dormant account lockout" policy using the Management Portal. The "dormant account lockout" policy automatically locks User accounts based on a configurable number of elapsed days since last successful login.

(ii) **Bulk provisioning:**

Bulk provisioning may be appropriate for medium-sized businesses without a corporate directory, but with a significant number of User accounts to create and manage. With bulk provisioning, instead of creating Users manually in the Management Portal, Administrators upload a pre-formatted file including all the required information into the Management Portal.

Bulk provisioning also makes it possible for Administrators to configure a "dormant account lockout" policy in the same way as for manual provisioning.

(iii) **Automated provisioning:**

Automated provisioning may be appropriate when a Customer has implemented a corporate directory and would like to implement a synchronization link between specific corporate directory User groups and the Service. Every User created or deleted from the corporate directory and synchronized groups, are then synchronized with the Service.

This synchronization link is based on a synchronization agent to be installed and operated on one of the Customer's servers. Administration rights are required to install the synchronization agent, but it is not necessary to dedicate a server for the installation. The synchronization agent requires a User account with appropriate privileges to connect to the corporate directory and requires a Microsoft Windows environment, which is able to connect to a Microsoft Active Directory, eDirectory, or Sun One Directory. The installation and management of the synchronization agent are the Customer's responsibility.

The synchronization agent allows Administrators to choose which User groups and User's attributes of the corporate directory will be synchronized with the Service.

The synchronization agent is not a key element of the Service since it is used only for account creation and deletion. If the synchronization agent ceases to operate, the User will still be able to authenticate using the Service. Accordingly, in such scenario, the creation and deletion of Users will not be automated until the synchronization agent restarts.

The above provisioning options can be used indistinctively for each of the Customer's virtual entities.

(f) **User Self-Enrolment:** Following the creation (either manually or automatically) of a User account, an authenticator will be assigned to such User (depending on the policy defined by Administrator) and she/he will receive by email or SMS an enrolment message giving her/him instructions to start the enrolment process. Messages sent to the User during this process can be modified using the Management Portal.

(g) **Connection to the Service:** The Service is accessible, by default, only via an Internet connection. However, as an option, an IPSec tunnel or an Orange MPLS connection can be requested by the Customer to access the Service. These options will be provided by Orange specifically on request and if Orange deems appropriate to the Customer's environment.

(h) **Service Hosting:** The Flexible Identity Authentication service level is hosted in datacenter located in United Kingdom and Canada. The data centers to be used to host the Service may be modified by Orange from time to time. In the event that more than one data center is used, it is mandatory to configure applications to use the all data centers and to allow the hosting of the Service to switch automatically from one data center to the others in case of failure.

(i) **Options to Integration with Customer applications:** Customer's applications can be integrated with the Service using any of the following three options:

(i) Radius connector to connect remote access gateways.

(ii) Agent-based connector to achieve better integration with specific applications.

(iii) SAMLv2 Identity Provider to integrate the Service with cloud service providers.

(j) **Reporting & Access Logs:** Administrators will access to certain sets of reports using the Management Portal. Administrators can specify if they would like to generate reports on a regular basis and obtain access to them using the Management Portal or by email. Such reports will be available on the Management Portal or from Orange for a minimum period of 12 months from the date the report is generated.

In addition to reports, Administrators can access real-time access logs using the Management Portal, including the whole of the Customer's organization or specific Users entries.

1.2.3 Flexible Identity Federation Service Level

The Flexible Identity Federation service level allows the Customer to:

- Share User identity with cloud services providers.
- Provide Users with a direct access to such cloud services via the User Portal (without re-authentication).
- Adapt the list of the allowed cloud services providers depending on User profile and on the security policy defined by the Administrator in the Management Portal.
- Facilitate the integration of new cloud services providers in a simple manner through an application catalogue.

The Service is charged on a 'per-Active-User' basis, allowing Customer to scale up and down the number of subscribed Users, depending on its requirements throughout the term of the Service. An Active User is defined as a User that used the Service at least once during the billing period.

For Customers who wish to use only one cloud application within the identity federation service, Orange Business Services proposes a "Starter Pack" at a reduced price that allows them to benefit from all the features of the Service but for only one cloud application. If Customer wishes to add other cloud applications afterwards, standard price will be applied. To authorize the addition of new cloud applications, Customer must sign a new order form indicating the subscription to "Silver" "No limit" (unlimited number of cloud applications).

On the invoice, "Starter Pack" will be mentioned only when Customer is using the service for only one cloud application within the identity federation service (with the accordingly reduced price of "Starter Pack"). If no mention of "Starter Pack" appears on the invoice, it means the Customer is subscribing to the "No limit" service without any limitation on the cloud applications number (with application of the standard prices).

(a) **Multi-Tenanted aspect of Service:** The Flexible Identity Federation service level is not multitenant.

(b) **Management Portal:** The Service provides a Management Portal allowing designated Administrators to perform day-to-day service management tasks, as follows:

- Creating or deleting Users or groups of Users.
- Allowing the access to Service Providers to Users or groups of Users.
- Creating Service reports
- Access to Service logs.

The Management Portal is accessible through a web browser connected to the Internet using a HTTPS connection. The Management Portal is only available in English. In the context of the multi-tenanted aspect of the Service, each Administrator will only be able to manage their own entity.

(c) **User Portal:** The Service provides a User Portal allowing Users to access to allowed applications and to perform day-to-day actions in an autonomous manner, as follows:

- Resetting their password in the corporate directory.
- Saving the username / password for applications not able to support identity federation.

The User Portal is accessible through a web browser connected to the Internet using a HTTPS connection. The User Portal is available in several languages that can be personalized by Administrators.

(d) **User Management:** User accounts can be set up and managed using one or all of the following two options (the selection of which will depend on Customer's specific requirements and the size of its organization):

(i) Manual User management may be appropriate for small businesses without a corporate directory or for businesses not willing to add some of their Users into their corporate directory (e.g. partners, external collaborators, etc.). It allows the manual creation of User accounts using the Management Portal. Each time a User account is created into the Service, the User receives an enrolment message to connect to the User Portal and to start using the Service.

(ii) Automated User management may be appropriate when a Customer has implemented a corporate directory and would like to provide the Service to corporate directory User depending on their group membership in the corporate directory. The connection between the corporate directory and the Service is based either on a software agent provided with the Service or either by another compatible technical solution not provided by Orange. When the Automated User management is in place, Users can connect to the User Portal using their corporate credentials.

(e) **Connection to the Service:** The Service is accessible only via an Internet connection.

(f) **Service Hosting:** The Flexible Identity Federation service level is hosted in two datacenters located in Germany and Ireland. The data centers to be used to host the Service will be notified by Orange from time to time. In the event that more than one data center is used, it is mandatory to configure applications to use the all data centers and to allow the hosting of the Service to switch automatically from one data center to the others in case of failure.

(g) **Integration with Customer Applications:** Customer can integrate new applications in the Service using the Management Portal.

(h) **Reporting & Access Logs:** Administrators will access to certain sets of reports using the Management Portal. Administrators can specify if they would like to generate reports on a regular basis and obtain access to them using the Management Portal or by email. Such reports will be available on the Management Portal or from Orange for a minimum period of 12 months from the date the report is generated.

In addition to reports, Administrators can access real-time access logs using the Management Portal, including the whole of the Customer’s organization or specific Users entries.

1.2.4 Flexible Identity Authentication and Flexible Identity Federation service levels

The Flexible Identity Authentication and Flexible Identity Federation service levels encompass simultaneously the elements of both service levels.

For Customers who wish to use only one cloud application within the identity federation service, Orange Business Services proposes a "Starter Pack" at a reduced price that allows them to benefit from all the features of the Service but for only one cloud application. If Customer wishes to add other cloud applications afterwards, standard price will be applied. To authorize the addition of new cloud applications, Customer must sign a new order form indicating the subscription to "Gold" (unlimited number of cloud applications).

On the invoice, "Starter Pack" will be mentioned only when Customer is using the service for only one cloud application within the identity federation service (with the accordingly reduced price of "Starter Pack"). If no mention of "Starter Pack" appears on the invoice, it means the Customer is subscribing to the "No limit" service without any limitation on the cloud applications number (with application of the standard prices).

1.2.5 Standard Elements of the Service

The following elements of the Service are standard:

Description	Maximum Value		
	Flexible identity Authentication	Flexible Identity Federation	
		Starter Pack	No Limit
Maximum number of virtual organizations.	5	1	1
Maximum number of Administrators.*	15	5	5
Maximum number of distinct Administrators profiles.	1	1	1
Number of remote training sessions provided to Administrators.	2x 3 hours	2x 3 hours	2x 3 hours
Maximum number of software tokens per Administrator.	2	N/A	N/A
Maximum number of applications to be connected to the Service.	No Limit	1	No Limit
Connectivity to the Service.	Internet	Internet	Internet

Any elements of the Service not stated in the above table will be subject to additional charge.

* Number of Administrators authorized at the Service’s subscription. Any additional Administrator account during the contract term will be subject to extra charges.

1.2.6 Service Implementation

The Service implementation is performed by the Orange technical services based on the information provided by the Customer.

(a) **Information to be provided by the Customer:** In order to start the Service configuration, Customers will be required to provide Orange with certain information ("**Configuration Information**"), such as the list of Administrators and the number of virtual organization, using the electronic form SRF2, which Orange will provide to the Customer with the Order Form. The Configuration Information provided by the Customer must be accurate. In case of delays in Orange's receipt of the Configuration Information, Orange has the right to delay the Target Date proportionally by the length of such delay.

Orange reserves the right not to take any modification of the SRF2, which are delivered by Customer following an undue delay (as determined by Orange in its sole discretion) after the SRF2 was initially received by Orange.

(b) **Target Date:** The Target Date shall be as set out in the Service Level Agreement.

(c) **Service Commencement Notice:** As part of the Service implementation process, Orange will perform the Acceptance Tests and will inform Administrators by email when the Acceptance Tests have been completed. Both Parties shall arrange the applicable training sessions in relation to the Service, such date not to be longer than 4 weeks from the date of the above email confirming completion of Acceptance Tests. At the first training session, Orange will discuss, amongst the provision of applicable training, the Service implementation and Acceptance Tests carried out by Orange. At the end of such first training session, Orange will issue Customer with the Service Commencement Notice (for instance, by confirming the ready for service date).

1.2.7 Service Support

The Service support is provided by the GCSC.

(a) **Incident Opening:** Every incident related to the Service can be reported by Administrator to the GCSC on a 24x7 basis by telephone or email, using the contact information provided by Orange during the Service implementation phase. Administrators will need to provide the GCSC with full details of the problem and their contact details so that they can be contacted for any follow-up. When registering the problem, the GCSC will provide Administrators with an incident number and will carry out a periodic follow-up until the relevant matter has been resolved.

(b) **Incident Diagnostic:** The GCSC will perform an initial diagnosis of the incident to categorize the incident into a Severity Level-1, -2, or -3 as follows:

(i) Severity Level-1 means a problem causing critical impact to the business function(s) or customer(s), which requires immediate management attention and dedicated resources applying all necessary efforts to resolve as soon as possible.

(ii) Severity Level-2 means a problem causing degradation of service resulting in impact to business function of customer, which requires priority attention and application of resources to resolve in a timely manner.

(iii) Severity Level-3 means a problem causing low impact to the business function(s) and customer (which requires timely resolution to minimize future impacts.

For incidents of Severity Level-1 or -2, the GCSC will inform Administrators of an estimated time to repair.

(c) **Incident Report:** When a problem is solved, the GCSC will inform the relevant Administrator of the incident closure. For Severity Level-1 and -2 incidents, the GCSC will send a recovery report detailing:

(i) The incident opening date,

(ii) The root cause analysis, and

(iii) The date of service recovery.

1.2.8 Service Level Agreement

Customer must subscribe to the IT Customer Service Manager Service as a prerequisite to benefit from the SLA.

1.3 Term and Termination

The Service is subject to a minimum term of 3 years commencing on the date of the Service Commencement Notice. The monthly fee for use of the Service is calculated on the basis of the number of Users declared in the Service for the Flexible identity Authentication service level and on the basis of the number of active Users during the billing period for the Flexible identity Federation service level..

The fees for use of the Service are calculated in accordance with the following:

(a) When submitting the Order for subscription of the Service, the Customer shall state the number of Users of the Service ("Initial Users").

(b) Customer shall pay 50% of the fees applicable to the number of Initial Users. Should the Customer not reach that 50% minimum Users commitment for a given month, the applicable minimum monthly service fee will correspond to 50% of the Initial Users declared into the Service.

(c) This minimum commitment will apply after a 6 months ramp-up phase, starting on the date of the Service Commencement Notice.

In case of early Service termination (to the extent permitted under the Agreement), Orange will invoice the Customer for an amount equal to the minimum monthly service fee (as defined above) multiplied by the remaining number of months until the end of the remaining term of the contract.

1.4 Limitations of Use

(a) Customer will not analyze, disassemble, or modify the configuration of the Hosting Platform, its structure or any files therein.

(b) Customer will not perform or attempt to perform (i) any intervention on third-party elements hosted on the Hosting Platform, and/or (ii) any intrusion or attempted intrusion into Orange or its subcontractor(s) information systems. Any such action will be considered a material breach of the Agreement.

(c) Customer agrees that all software used on the Hosting Platform is technically complex and cannot be tested in such a way as to cover every possible use. Customer agrees that the Service will not be error free and may not be available at all times.

(d) Customer will actively cooperate with Orange to maintain its tools at the best possible level of quality. Customer will follow all instructions from Orange and will promptly perform any operation recommended by Orange, including (without limitation) the reinstallation and/or reconfiguration of the Service or installation of updates to software and/or hardware. Customer will be advised of such recommendations by the GCSC or any other means as deemed appropriate by Orange.

(e) Orange reserves the right to interrupt access to the Service to perform repairs, maintenance and/or improvement interventions in order to ensure the proper operation of the Service. Orange will use reasonable endeavors to inform Customer (to the extent possible) about such intervention and its duration; and to limit Service disturbance.

(f) Customer will take all necessary technical precautions for the use of the Service and will ensure the compatibility of its applications with the Service.

(g) Customer will comply with the conditions of use set out in this Service Description and the User Portal guide provided to Customer at the commencement of the Service (as well as any other conditions of use communicated by Orange). Orange will not be responsible for the failure or delay of the Service which is attributable to the non-compliance of such conditions of use.

(h) Customer remains solely responsible for its network's security policy and for its response procedures to security violations.

(i) Orange will not be responsible if the configuration of the Service as selected by Customer is not sufficient to address its business needs.

(j) Orange reserves the right to suspend or terminate the Service in the event of any repeated non-compliance by Customer with the limitations/restrictions specified above or if Customer does not cooperate with Orange as is reasonably required.

1.5 Data Processing

Exhibit A sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and the categories of Data Subjects of the Processing of Personal Data carried out by Orange as part of this Service.

EXHIBIT A DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE BUSINESS SERVICES AS PROCESSOR FOR CUSTOMER - ARTICLE 28 OF GDPR

Name of the Service: Flexible Identity Authentication

ExA.1 Processing Activities

Collection (receiving personal data of employees and users of customer who are natural persons, etc.).	Yes
Recording (capturing personal data in a file or software program, including the generation of metadata like Call Details Records, etc.).	Yes
Organization (organizing personal data in a software program, etc.).	Yes
Storage (keeping the personal data in a software program for a determined period, including for archiving purposes, etc.).	Yes
Modification (modifying the content or the way the personal data are structured, etc.).	Yes
Consultation (looking at personal data that we have stored in our files or software programs, etc.).	Yes
Disclosure or otherwise making available (communicating personal data to another recipient by any means, etc.). Except for disclosure mentioned in the service description or required by law, or otherwise specifically directed by the customer, the categories of potential recipients are only those subcontractors referenced herein or otherwise approved by the customer.	No
Combination (merging two or more databases with personal data, etc.).	No
Restriction (implementing security measures in order to restrict the access to the personal data, etc.).	Yes
Deletion or destruction (deleting or anonymizing the personal data or destroying the hard copies, etc.).	Yes
Other use (if "YES" to be detailed).	No

ExA.2 Categories of Personal Data Processed (Type of Personal Data)

Categories of Personal Data Identifiable by Orange	
Identification data (ID document / number, phone number, email, etc.).	Yes
Traffic / Connection data (IP address, Mac address, CDRs, access and usage data, online tracking and monitoring of services).	Yes
Location Data (geographic location, device location).	No
CRM data (billing information, customer service data, ticketing info, telephone recordings, etc.).	No
Financial data (bank account details, payment information).	No
Sensitive Data (racial/ethnic background, religion, political or philosophical beliefs, trade union membership, biometric data, genetic data, health data, sexual life, and/or orientation).	No
Categories of Personal Data Not Identifiable by Orange	
Any categories of personal data that may be recorded or stored (voicemail, call recording, files) by Customer and which recording is hosted on Orange infrastructure.	No

ExA.3 Subject-Matter and Duration of the Processing

Subject-Matter of Processing		Duration of Processing
Service activation.	Yes	For the period necessary to provide the service to the customer plus 6 months.
User authentication.	Yes	
Incident Management.	Yes	
Quality of Service.	Yes	
Invoice, contract, order (if they show the name and details of the contact person of Customer).	No	
Itemized billing (including traffic / connection data of end-users who are natural persons).	No	
Customer reporting.	Yes	For the duration requested by Customer.
Hosting.	Yes	For the duration of the hosting service ordered by Customer.
Other. [if yes please describe]	No	

ExA.4 Purposes of Processing

Provision of the service to Customer.

ExA.5 Categories of Data Subject

Customer’s employees/self-employed contractors using or managing the service or the contract who are natural persons.	Yes
Customer’s other end-users of the service who are natural persons (client of the Customer, etc.) usable by users other than internal users.	Yes

ExA.6 Sub-Processors

Sub-Processors Approved by Customer	Safety Measures
Orange Business Services entities that are processing information for this Service and that are within the EU/EEA are communicated separately to the customer.	NA
Orange Business Services entities that are processing information for this Service and that are outside of the EU/EEA are communicated separately to the customer	Intra-group agreements with standard model clauses, Binding Corporate Rules approval request filed with CNIL.
Orange Business Services suppliers which are performing one or more processing activities described above in connection with this Service and that are within the EU/EEA are communicated separately to the customer.	NA
Orange Business Services suppliers that are processing information for this Service and that are outside of the EU/EEA are communicated separately to the customer.	Standard Model Clauses in contract with supplier.

END OF SERVICE DESCRIPTION FOR FLEXIBLE IDENTITY SERVICE