PUBLICATION 1 SERVICE DESCRIPTION FOR FLEXIBLE IDENTITY AUTHENTICATION 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 control for purposes of this Service Description. Capitalized terms used and not otherwise defined in this Service Description 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 within Orange during the Service implementation phase.

"**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 Orange customers of the Service.

"**Management Portal**" means the web portal identified and made available by Orange as part of the Service for use by Administrators, which will allow Administrators to configure the Service.

"**On-Premises**" means an application that is installed and that runs on computers on the premises of Customer's organization.

"**Service**" means the Flexible Identity Authentication Service as described in this Service Description.

"**Service Portal**" means the change request web portal identified and provided by Orange as part of the Service.

"**Standard Catalog**" means the catalog available on the Service Portal which lists the standard optional features (i.e. change requests) with their corresponding price.

"**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 in the User's profile.

1.2 Service Overview

The Specific Conditions for Cloud Services and the Specific Conditions for Security Services apply to the Service. The Service is managed by Orange and aims to mitigate the risks of digital identity usurpation by providing Users with a variety of authenticators. Authenticators (i) are more secure than a simple password, (ii) share digital identity in a controlled manner with service providers outside Customer's network, and (iii) adapt the security level to the authentication context.

Customer will choose one of the following subscribed levels of service: "Essential", "Standard", or "Premium". All levels of service include the following features:

- Management Portal and User Portal specific for the applicable level of service;
- Management and monitoring of the Service on a 24x7 basis;
- Helpdesk support for designated Administrators;
- A secured SaaS infrastructure;
- Service usage reports as made available by the Service and as defined by the Administrators; and
- Shipment of hardware authenticators to Administrators.

The Service is billed per User beginning when the first token is registered. Customer may adjust the number of Users at any time.

1.3 Standard Service Features

1.3.1 **Service Limitations.** The following Service limitations apply:

Description	Service
Maximum number of virtual organizations.	5
Maximum number of authorized Administrators at Service's subscription *	15
Maximum number of distinct Administrators profiles.	1
Number of remote training sessions provided to Administrators.	1
Maximum number of software tokens per Administrator.	2
Maximum number of applications connectable to the Service.	No Limit
Connectivity to the Service.	Internet
* Any additional Administrator account is subject to additional charges.	

1.3.2 Levels of Service

The Service includes the following functionalities based on the level of service provided:

Functionalities	Essential	Standard	Premium
Multi-factor authentication (password, SW token, HW, SMS, etc.).	Y	Y	Y
Integration of On-Premises applications (unlimited number of applications).	Y	Y	Y
Integration of SaaS applications (unlimited number of applications).	Y	Y	Y
Network-based conditional access.	Y	Y	Y
Contextual authentication (localization, session analysis, OS, terminals, etc.).		Y	Y
Advanced scenario-based access policies.		Y	Y
Windows SSO support (Kerberos).		Y	Y
Support of smartcards/PKI.			Y

1.3.3 Multi-Factor Authentication

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:

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

1.3.4 Multi-Tenanted Aspect of Service

The Service is multi-tenanted, meaning that Customer can create independent virtual entities within the Service for its Affiliates, with each virtual entity including Users, Administrators, a Management Portal, and a security policy.

1.3.5 Management Portal

The Management Portal allows Administrators to perform day-to-day service management tasks, which may include:

- creating or deleting Users or groups of Users;
- managing authenticators and their assignment to Users;
- managing the Service reports (i.e. usage statistics);
- defining automated messages sent to Users; and
- access to Service logs.

Modifications made by Administrators on the Management Portal are processed automatically. The Management Portal is accessible through a Customer-provided web browser connected to the Internet using a HTTPS connection. The Management Portal is available in English. Due to the multi-tenanted aspect of the Service, each Administrator will only be authorized to manage the virtual entity for which it is identified by Customer as the Administrator.

1.3.6 User Portal

The User Portal allows Users to perform day-to-day actions in an autonomous manner, which may include:

- resetting hardware or software token PIN code;
- resetting GrID token PIP code;
- resynchronizing tokens; and
- triggering sending of a new SMS OTP.

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

1.3.7 User Account Management

User accounts can be set up and managed using one or all of the following three options, as mutually agreed upon by the Parties: manual provisioning, bulk provisioning, or automated provisioning.

1.3.8 User Self-Enrollment

Following the creation (manually or automatically) of a User account by an Administrator, an authenticator will be assigned to such User (depending on the security policy defined by the relevant Administrator), and the User will receive, by email or SMS, an enrollment message with instructions to start the enrollment process. Messages sent to the User during this process can be personalized using the Management Portal.

1.3.9 Options for Integration with Customer's Applications

Subject to Clause 1.5.3 below, Customer's applications can be integrated with the Service via the Management Portal by using any of the following options:

- Radius connector to connect remote access gateways;
- Agent-based connector to achieve better integration with specific applications; or
- SAMLv2 Identity Provider to integrate the Service with cloud service providers.

1.3.10 Reporting & Access Logs

Administrators can generate and obtain access to reports on the Management Portal or have a copy of the report sent by email. Such reports are available for a minimum period of 12-months from the date the report is generated. In addition, Administrators can access near real-time access logs using the Management Portal.

1.3.11 Connection to the Service

The Service is only accessible via an Internet connection, which will be provided by Customer; except that an IPSEC tunnel will be provided by Orange for Service access if requested by Customer and approved by Orange.

1.3.12 Federation Feature / Single Sign-On (SSO)

The federation feature of the Service allows Customer to:

- Share User identity with its cloud services providers;
- Provide Users with a direct access to such cloud services via the User Portal (without re-authentication);
- Provide smart access policies capable to take the authentication context into account as an additional layer of security;
- 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; and
- Facilitate the integration of new cloud services providers in a simple manner.

1.3.13 Service Hosting

The Service is hosted in data centers located in the European Union. The data centers may be modified by Orange from time to time. In the event more than one data center is used, Customer must (i) configure its applications to use all the data centers and (ii) allow the hosting of the Service to switch automatically from one data center to the others in case of failure. However, in no event will the Service be provided in the following countries: Russia, Brazil, Belarus, Ivory Coast, Democratic People's Republic of Korea (North Korea), Democratic Republic of Congo, Iran, Iraq, Lebanon, Liberia, Myanmar/Burma, Rwanda, Sierra Leone, Sudan.

1.4 Optional Service Features

1.4.1 Optional Features Outside of the Standard Catalog

1.4.1.1 IT Consulting Customer Service

The IT Consulting Customer service offers personalized monitoring of the management and optimization of the Service and is subject to additional charges.

1.4.1.2 Specific Support and Advisory Services

Orange may agree to provide customer-specific support and advisory services as an optional feature of the Service. Any such support and advisory services will be mutually agreed upon by the Parties in writing and will be subject to additional charges.

This optional feature may include:

- An inventory of Customer applications to integrate;
- Assistance to the Administrator in the collection of technical data;
- Preparation for change management by analyzing impacts and expectations by User profile; or
- The methodology to be applied (e.g. communication actions, key messages, format).

1.4.2 Optional Features Available from the Standard Catalog

Customer may order optional features available from the Standard Catalog directly from the Service Portal. The optional features are subject to additional charges.

1.5 Service Implementation

1.5.1 Configuration Information Provided by Customer

Customer must provide all information reasonably requested by Orange to configure the Service (e.g. list of Administrators, number of virtual organizations, etc. (collectively, the "**Configuration Information**")) using the electronic form SRF2 provided by Orange. Customer will ensure that all Configuration Information provided is accurate and complete. In case of delays due to Customer’s failure to provide all or accurate Configuration Information, Orange may adjust any previously agreed target date accordingly.

1.5.2 Service Commencement Notice

Notwithstanding anything to the contrary otherwise contained in the Specific Conditions for Cloud Services or the Specific Conditions for Security Services, Orange will perform its acceptance tests (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 email from Orange confirming completion of Acceptance Tests. At the first training session, Orange will discuss the Service implementation and Acceptance Tests carried out by Orange. At the end of the first training session, Orange will issue a notice confirming the ready for service date (the "**Service Commencement Notice**").

1.5.3 Application Integration

Orange shall support the integration of (i) up to five (5) applications which are (ii) listed in the Standard Catalog of cloud applications (excluding generic SAML/OIDC connector and agent catalog). Customer may autonomously integrate as many applications as it wishes thereafter. Additional integration support requests' of (i) any non-standard applications and/or (ii) of any application beyond the integration of the five listed applications referred to above, is subject to additional charges.

1.6 Service Support - Global Customer Support Center

(a) **Incident Opening:** Any incident or malfunction in the Service can be reported by the Administrator to the GCSC on a 24x7 basis by telephone or email, using the contact information provided by Orange. Administrators must specify the nature of the incident, provide full details of the incident and their contact details. The GCSC will provide Administrators an incident number and will carry out a periodic follow-up until the relevant matter is resolved.

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

(i) **Severity Level 1:** a problem causing high degradation of Service resulting in a critical impact to the Customer's business function(s), which requires immediate management attention and dedicated resources applying all necessary efforts to resolve as soon as possible.

(ii) **Severity Level 2:** a problem causing degradation of Service resulting in an impact to the Customer's business function(s), which requires priority attention and resources application to resolve in a timely manner.

(iii) **Severity Level 3:** a problem causing low degradation of Service and/or low impact to the Customer's business function(s) and which requires timely resolution to minimize future impacts.

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

(c) **Incident Recovery Report:** When an incident is solved, the GCSC informs the Administrator(s) of the incident closure and restoration of the Service. For Severity Level 1 and 2 incidents, the GCSC sends a recovery report detailing (i) the incident opening date, (ii) the root cause analysis, and (iii) the date of service recovery.

1.7 Service Modification

Administrator(s) may formulate modification requests through the Service Portal when requests are not available through the Management Portal, such as ordering new means of authentication or declaring a new client server using the Service.

1.8 Change In Service Level

Customer can only upgrade its level of service to a service level which offers additional functionalities subject to a Change Order.

1.9 Termination of Services

A minimum monthly recurring fee applies to the Service and is calculated on the basis of the number of declared Users of the Service in accordance with the following:

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

(b) The minimum monthly recurring fee is equal to the per User Charge multiplied by 50% of the number of Initial Users.

(c) This minimum monthly recurring fee will apply beginning 6 months after the date of the Service Commencement Notice.

Notwithstanding anything to the contrary otherwise contained in the Specific Conditions for Cloud Services or the Specific Conditions for Security Services, if during the applicable Service Term (1) Customer terminates the Agreement other than pursuant to Clause 7.3.1 of the General Conditions or terminates an Order other than pursuant to Clause 7.3.2, or (2) Orange terminates the Agreement pursuant to Clause 7.3.1 of the General Conditions or terminates an Order pursuant to Clause 7.3.2 or Clause 7.3.3 of the General Conditions, then Customer will pay an amount equal to the minimum monthly recurring fee multiplied by the number of months remaining in the Service Term. The Parties acknowledge and agree that, as of the Effective Date, the Parties cannot estimate with certainty the actual damages that Orange would suffer in the event of a cancellation or termination and that the cancellation and termination liability set forth in this Clause 1.9, (a) represents an attempt by the Parties to approximate Orange's anticipated probable and proportionate loss, and (b) is part of the consideration for this Agreement, is a material and inseparable pricing term for this Agreement, and is reasonable.

1.10 Reversibility

Upon Customer's request three (3) months before the expiry of the Service Term of the applicable Order by registered letter with acknowledgment of receipt, Orange will provide transition services of the Service to Customer or a replacement supplier. The services included in this reversibility service, the price and duration will be agreed separately.

The Service will continue until the end of the reversibility period and will continue to be invoiced. However, if necessary, for the purposes of reversibility services, certain Orange quality of service commitments may be revised downwards. Orange undertakes to provide upon request technical information on the architecture of the Service, provided such information is not assimilated to Orange's know-how.

1.11 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 the information systems of Orange or its subcontractors. Any such action will be 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 in order to maintain Orange's On-Premises software and/or hardware 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 Orange's On-Premises software and/or hardware. Customer will be advised of such recommendations by the GCSC or such other means as deemed appropriate by Orange. Orange will not be responsible for the failure or delay of the Service which is attributable to Customer's non-compliance with the terms of this subsection (d).

(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 terms set out in this Service Description and the User Portal guide provided to Customer (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 Customer's non-compliance with such conditions of use.

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

(i) Orange will not be responsible if the configuration of the Service selected by Customer is not sufficient to address Customer's 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 or restrictions specified in this Service Description or if Customer does not cooperate with Orange as is reasonably required.

1.12 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 contained in the voice, data or internet traffic of Customer carried over Orange network.	Yes
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.
User authentication.	Yes	
Routing configuration.	No	
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.
Answering legal requests from authorities.	Yes	For the duration required by applicable local law in each country in which the service is provided to end-users who are natural persons.
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