PUBLICATION 1 SERVICE DESCRIPTION FOR SSO ON CUSTOMER IDP

1.1 Definitions

All capitalized terms used but not defined in this Service Description will have the meanings given to such terms elsewhere in the Agreement. 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 shall prevail.

"**Access Right Delegation**" or "**ARD**" means the application used by the Customer's administrators to define Users together with their access rights to access the applications of My Service Space.

"**Application**" means an on-line set of functionalities implementing a service accessible via the MSS.

"**ARD Administrator**" means a person who was granted the permission to access the ARD application and manage the permissions of the MSS Users on a given perimeter.

"**ARD Referent Administrator**" means the person mandated by the Customer to be the privileged interlocutor of Orange for MSS permission management on the MSS, on one or many perimeters, who is the primary ARD Administrator and will delegate permissions to the secondary ARD Administrator.

"**Customer Service Manager**" or "**CSM**" supports the run of the solution, managing the Service SLAs, incident escalation and change management, and provides monthly reporting to the Customer.

"**Identity Provider**" or "**IdP**" means the Customer's trusted software service that responds to the Service Provider authentication requests.

"**Multi Factor Authentication**" or "**MFA**" is a way of confirming the identity of a User, with more than one factor. In the MSS the first factor is a password, the second factor is a One Time Password (OTP) send by mail, or an authentication from a SafeNet PKI.

"**My Service Space**" or the "**MSS**" means the self-service portal provided by Orange that allows Customer to manage some of the products and services provided by Orange to the Customer.

"**One Time Password**" or "**OTP**" means a password valid for a unique authentication session. It is usually sent to a device owned by the User who wants to authenticate via the OTP in Multi Factor Authentication.

"**Orange Professional Services**" provides consulting services of experts to support the design, optimization, and deployment of Orange solutions in complex environments.

"**Service**" means the SSO on the IdP service as described in this Service Description.

"**Service Provider**" or "**SP**" means a software service provided by Orange that protects access to the Customer's digital workspace and resources in My Service Space (websites, applications, etc.) by applying a security policy.

"**Single Sign-On**" or "**SSO**" is a session authentication scheme that allows a User to log in with its unique credentials to several applications.

"**Security Operation Center**" or "**SOC**" refers to the Orange teams monitoring the security of Orange's information systems.

"**Users**" means any person with an access to MSS, using the MSS Applications on behalf of the Customer.

1.2 Overview

1.2.1 The Service applies only to the MSS portal.

1.2.2 The Service is a session authentication process based on federated identity management, that allows Users logged in the Customer IT system to access the MSS portal and its Applications directly via SSO, without the need to re-identify themselves. SSO secures credential exchange between (Customer's) IdP and (Orange's) SP, when a User of the Customer domain accesses the MSS and its Applications.

1.2.3 Users' passwords, renewal policies and Multi Factor Authentication, are directly and uniquely defined and managed in the Customer's directory. Some User information must also be defined in the MSS for the management of perimeters permission with the MSS (Applications / resources).

1.2.4 The Service supports IdP or SP initiated access. With IdP initiated access, a User logged on the Customer IT system via the User's usual ID and passwords, uses an internal service setup by the Customer that asks the IdP to establish a connection with the MSS via the SP. With SP initiated access, the User connects to the MSS with a specific URL for SSO, and is asked to enter their email ID, then the SP contacts the IdP to check and validate the authentication credentials of the User.

1.2.5 The credential exchange for Users' authentication between the IdP and SP is secured with certificates. The certificate of Orange is installed on the IdP and the certificate of the Customer on the SP. The certificates are installed during the Service transition. They are updated when the certificates reach their term, as described in Clause 1.7.1 below.

1.3 Prerequisites and Service Transition

1.3.1 The Customer must ensure that its IdP is compatible with SAML v2 and that the Customer login policy makes mandatory Multi Factor Authentication.

1.3.2 The Service is based on SAML v2.0 and has been validated with some of the major IdPs. Orange does not guarantee compatibility with all SAML v2.0 IdP. The compatibility between the IdP and SP will be checked during the tests of the Service transition. In the event a major incompatibility is encountered during the tests, the Service order will be cancelled, free of any charge for the Customer.

1.3.3 The Service requires that the Users' identifier is unique and set to the Users' email address belonging to the Customer's domain name. During the Service transition, any generic account will be allocated to an identified User, duplicated account will be removed and Users' identifier different from the email address will be migrated. Those changes will be done with the support of Orange teams.

1.3.4 The Service transition requires a close collaboration between SSO experts from the Customer and from Orange.

1.3.5 On Orange side the Service transition is managed by Orange Professional Services. Therefore, this Service Description is subject to the Specific Conditions for Orange Professional Services.

1.3.6 The Customer commits to appoint a project manager with expertise in SSO to follow and organize the deployment project on Customer side. The Customer project manager will collaborate with Orange Professional Service to prepare and exchange metadata files with the IdP certificates, configure the IdP with the SP metadata, check and update User accounts list that will use SSO, and make unitary tests.

1.4 Technical Constraints

1.4.1 The SAML v2 exchanges between the IdP and the SP must comply to the following requirements:

(a) all assertions must be signed;

(b) the assertions duration must be limited (3 to 5 minutes); and

(c) SAMLResponse, AuthnRequest, and LogoutRequest must be implemented.

1.4.2 The security certificates must:

(a) be signed by and internal PKI or an external certification authority;

(b) have a maximum validity duration of 2 years; and

(c) be signed by an RSA key of minimum 2048 bits, 3072 recommended, and with a SHA256 hash.

1.4.3 The AES key encryption algorithm must be RSA OAEP.

1.4.4 The assertion encryption algorithm must be AES.

1.5 User Permission Management

1.5.1 The User's permissions are managed by the ARD Administrators with the ARD application of the MSS.

1.5.2 The ARD Referent Administrator:

(a) must be mandated by the Customer for all its perimeters; and

(b) is responsible for the creation of secondary ARD Administrators and allocation of their permissions.

1.5.3 The ARD Administrators are responsible for:

(a) the creation of the Users that need to access MSS; the User login must be set to the User email address;

(b) maintaining the list of active Users accessing MSS;

(c) allocating permissions to the Users; and

(d) removing inactive Users.

1.6 Incident Management

1.6.1 Incidents, others that security ones, are managed by contacting the digital support of Orange from the help menu of the MSS portal.

1.6.2 For security incidents that may endanger the SSO connection between the Customer IT and Orange IT (Users identity compromission, IdP compromission, etc.), the Customer undertakes to warn Orange as quickly as possible and at the latest within 24 hours by sending a mail to the Orange Group CERT: cert@orange.com.

1.7 Change Management

1.7.1 During the run of the Services the Customer will inform Orange 3 months in advance by contacting their CSM or the digital support of Orange as described in Clause 1.6 above:

(a) when the IdP certificate reaches its term. The new certificate must be setup 1 month before expiry of the term; and

(b) if the Customer wants to add or remove perimeter of their domain covered by the Service, for instance in case of company acquisition or carve-out.

1.7.2 Orange will inform the Customer 3 months prior to the term of its certification authority, that determine the Orange certificate term, via the generic mail addresses provided by the Customer during the service transition.

1.8 Security and Audit

1.8.1 Orange will carry out regular intrusion tests and run security audit on a yearly basis.

1.8.2 The Service will be monitored by the Orange SOC. In case of detection of unusual behavior by the Orange SOC, the Service may be suspended without prior notice. The Customer will be informed of the suspension as soon as possible via the generic mail addresses provided by the Customer during the service transition.

1.9 Customer Responsibilities

1.9.1 The Customer is solely responsible for the following on its network:

(a) the identification and authentication of Users;

(b) Its security policy, its response procedures to security violations and for security rule breaches; and

(c) usage of the Service by Users.

1.9.2 The Customer will:

(a) inform Orange as soon as possible of any security breach on its network and/or IdP that may impact the Service or allow unauthorized access or unrightful usage of the Service. In such case Orange will immediately block any access from the compromised IdP;

(b) actively cooperate with Orange to maintain its tools at the best possible level of quality;

(c) follow all reasonable instructions from Orange and will promptly perform any operation recommended by Orange for the continuation and integrity of the Service, including (without limitation) the reinstallation and/or reconfiguration of the Service;

(d) take all necessary technical precautions for the use of the Service and will ensure the compatibility of its applications with the Service; and

(e) comply with the conditions of use set out in this Service Description and the Self-Management Portal User guide provided to Customer at the commencement of the Services (as well as any other conditions of use communicated by Orange).

1.10 Service Duration and Termination

1.10.1 The Service starts once the Customer signs the acceptance form. The Service is maintained as long as the certificate of the IdP and SP remains valid and are renewed.

1.10.2 The Service will automatically be suspended if the IdP certificate reaches its terms without any information from the Customer of its renewal, pursuant to Clause 1.7.1 above.

1.10.3 The Customer may request the termination of the Service at any time, on at least one month’s written notice sent to the CSM.

1.11 Charges

The Charges consist of the following:

(a) a one-time charge invoiced once the Service transition has been fully validated by the Customer by signing the acceptance form (the date of validation being the “**Commencement Date**”); and

(b) monthly recurring charges for Incident and Change Management invoiced monthly in advance from the Commencement Date.

1.12 Limitation of Use

1.12.1 Orange will not be responsible:

(a) for the failure or delay of the Service which is attributable to the non-compliance of Customer with the Customer Responsibilities at Clause 1.9 above; or

(b) if the configuration of the Service as selected by Customer is not sufficient to address its business needs.

1.12.2 Orange reserves the right to:

(a) suspend or terminate the Service to Customer:

(i) if Orange deems it necessary in its reasonable opinion to safeguard the security and integrity of the Service. Orange will endeavor to provide Customer as much notice as is reasonably possible and will, in cooperation with Customer, organize the transfer of Customer’s solution onto the new Service; and

(ii) if Customer does not cooperate with Orange as is reasonably required, until such time Customer’s use of the Service is complying with the terms of this Service Description and the Agreement; or;

(iii) in the event of any repeated non-compliance by Customer with the Customer Responsibilities at Clause 1.9 above; and

(b) 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. Orange will perform maintenance activities at times when the Service is least used by Customer, except in the event of emergency maintenance.

END OF SERVICE DESCRIPTION FOR SSO ON CUSTOMER IDP