## PUBLICATION 1 SERVICE DESCRIPTION FOR MOBILE SSL SERVICE

### 1.1 Definitions

All capitalized terms used but not defined herein 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 will control for purposes of this Service Description.

"**Customer Information**" means the Customer information to which Users will have access through the Mobile SSL Service.

"**Device**" means the unit (e.g. PDAs/laptops/kiosks) from which a User may connect to the SSL Gateway to access the Customer Information. Orange will identify and may modify from time to time the Devices that may be used with the Mobile SSL Service.

"**Fault**" means a fault, failure, or malfunction in the Mobile SSL Service.

"**Fault Call**" means the notification made by Customer to the GCSC to report a Fault.

"**Firewall**" means a method to enhance network security.

"**GCSC**" means the Orange Global Customer Support Centers.

"**Incident**" means a security event, alert, or problem regarding the Mobile SSL Service detected by Orange.

"**Proper Operational Condition**" means that the SSL Gateway is functioning in accordance with the parameters of the Mobile SSL Service, as set forth in this Service Description and in the SRFs.

"**Security Rules Base**" means the ordered set of rules against which each connection is checked, which is configured in the SSL Gateway. The Security Rules Base will be determined by Customer's security policy, as set forth in the SRF.

"**Service Request Form**" or "**SRF**" means the form that details Customer's specific Mobile SSL Service requirements.

"**Severity Level**" means the category assigned by the GCSC for Incidents and Faults.

"**SSL Gateway**" means the centrally managed server, including Software, provided by Orange as part of the Mobile SSL Service, on which the Security Rules Base is configured and to which Users connect to access the Customer Information.

### 1.2 Description of the Mobile SSL Service

The Mobile SSL Service provides Users with secure access to Customer Information from a Device using a web browser supported by the service. The Service will be delivered by Orange in accordance with the Service Level Agreement for Mobile SSL Service. Users remotely connect to the SSL Gateway either through an Orange managed Firewall or through a Customer managed firewall. The Security Rules Base implemented on the SSL Gateway allows different Users to access specific Customer Information. Depending on the Security Rules defined jointly between the Customer and Orange, the Users may experience either a clientless access and may be asked to use dedicated connectivity software provided by the SSL Gateway. If due to technical constraints, it's not possible to publish Customer Information according to what has been defined in the Security Rules Bases, Orange reserves the right to amend the publication mean and to implement "**client based**" connectivity instead of a clientless connectivity. If the Customer chooses to benefit from an Orange managed firewall, he also must receive the Orange Managed Firewall Service, as described in a separate Service Description attached to this Agreement and to which separate Charges will apply. Except as otherwise expressly provided in this Agreement, Orange will have no responsibility or liability for, or related to, the Customer Information, Devices, Internet browsers, authentication services, or other services not provided by Orange, but that may be used or accessed by Customer or Users in connection with the Mobile SSL Service. By default, the service is considered hosted in customer premises but upon customer's request, it can be hosted in Orange premises. If the Customer chooses to benefit from the Orange hosting service, he also must receive the Orange Hosting Service, as described in a separate Service Description attached to this Agreement and to which separate Charges will apply.

### 1.3 Service Request Form

1.3.1 **Customer Requirements.** Prior to commencement of the Mobile SSL Service, the Parties will complete the applicable SRFs. Customer will provide all relevant technical specifications and documentation regarding its existing network, and Orange will reasonably assist Customer in completion of the SRFs. Customer will ensure that all information contained in the completed SRFs is accurate.

1.3.2 **Customer Security Contacts.** Customer will identify a primary security contact and between 2 and 4 secondary security contacts in each SRF. Customer will ensure that all primary and secondary contacts are available and can be contacted by Orange 24 hours a day, 7 days a week. Orange will respond only to Mobile SSL Service requests and Fault Calls issued by such contacts. All communications between the Parties will be in English, unless otherwise agreed to by the Parties.

For Severity Level-1 and Severity Level-2 Incidents, Orange will notify Customer's security contacts of the Incident using all contact details provided in the SRF. For Severity Level-3 Incidents, Orange will send a message to the email addresses set forth in the SRF. All contacts by Orange will be made in English, unless otherwise agreed to by the Parties.

The primary security contact identified in the SRF will ensure that:

(a) All security contact information is maintained and current;

(b) Orange is notified before and after any planned outages or configuration changes to Customer's network or network services; and

(c) All configuration changes are scheduled at least 5 Business Days in advance.

(d) All changes to Customer's primary security contact must be made in writing, on Customer's letterhead, and be signed by a senior manager in Customer's organization.

**1.4 Service Deployment**

1.4.1 **Site Survey.** Promptly upon completion of the SRF, Customer will perform a survey of the physical premises where the SSL Gateway will be installed (a "**Site Survey**"). Customer must gather the information requested in the Site Survey form provided by Orange for Orange to determine if the Location meets the necessary requirements for the proper installation and functioning of the Mobile SSL Service and to identify the specific tasks, if any, that Customer must complete to provide the Location with the proper infrastructure to support the SSL Gateway. Upon Customer's request and for an additional charge, Orange will perform the Site Survey. If Orange performs the Site Survey, a Customer representative must provide Orange access to the Location and accompany the Orange personnel at all times during the Site Survey.

1.4.2 **Physical Environment Requirements.** Upon completion of the Site Survey, Orange will advise Customer of all Location preparation requirements that Customer must complete prior to the scheduled date for commencing installation of the SSL Gateway. If Customer fails to complete all such required preparations, Orange is relieved of its Mobile SSL Service responsibilities at that Location until such time as it has been adequately prepared.

The Location must provide appropriate space, conditioned power, environmental controls, and a direct access PSTN line for remote access into the SSL Gateway. The hardware components of the SSL Gateway have been designed to operate as a single unit and must be located within 3 feet of each other. Customer also must provide:

(a) A secure location in which to install the SSL Gateway, accessible on a 24 x 7 basis.

(b) Appropriate space within a standard 19" rack.

(c) Appropriate environmental controls.

(d) 5 power outlets per single SSL Gateway or 8 power outlets for the resilient SSL Gateway, which are 110V/60Hz conditioned power outlets (or 220V/50Hz as appropriate for the applicable country) and installed within 3 feet of the SSL Gateway.

(e) If the Customer did not subscribed to the Orange Secure Gateway service, a dedicated physical or virtual interface on a customer managed firewall to connect the DMZ switch included into the service.

(f) If the Customer did not subscribed to the Orange Secure Gateway service, an unfiltered Ethernet interface with internet connectivity to connect the management firewall included into the service.

Alternatively, the SSL Gateway can be housed in an Orange facility, where the requirements set forth above can be provided for an additional monthly charge.

1.4.3 **Lead Time Requirements.** The average time observed to deploy the service from the date on which the service order is signed by the customer is:

(a) 10 weeks for a deployment in Europe.

(b) 11 weeks for a deployment in North America.

(c) and may vary for other geographical locations.

The completed SRF must be received from the customer in the two weeks following the signature of the order form. The deployment will be delayed if Customer doesn't conform to this exigency or if he requires changes to the specifications listed in the completed and accepted SRF.

1.4.4 **Configuration.** Orange will configure each SSL Gateway wholly based upon specifications contained in the applicable SRF. Any configuration changes required due to inaccurate or revised specifications will be charged to and paid by Customer at the Hourly Labor Rate for such services, plus Expenses.

Upon completion of the configuration, the SSL Gateway will be delivered to the Location specified in the SRF. Customer will visibly inspect the exterior condition of the SSL Gateway packaging prior to accepting delivery. After accepting delivery, Customer will store the SSL Gateway in a secure location until Orange commences installation. Customer will bear the risk of loss while the SSL Gateway remains at the Location.

Following installation and acceptance testing, Orange will accept requests for changes to the configuration of the SSL Gateway only from the security contacts identified in the SRF. All such changes will be subject to verification by Orange in accordance with mutually established procedures agreed to in writing by the Parties prior to commencement of the Mobile SSL Service.

1.4.5 **Installation.** Before Orange will install the SSL Gateway, Customer must provide written confirmation that the following tasks have been completed:

(a) Satisfactory delivery of the SSL Gateway to the Location;

(b) All data circuits are installed and operational; and

(c) The Location has been properly prepared in accordance with the terms of this Service Description.

Orange will install the SSL Gateway upon its receipt of Customer's confirmation. Unless otherwise agreed to by the Parties, SSL Gateway installation will be conducted during Business Hours. If Customer requests Orange to install the SSL Gateway outside of Business Hours, Orange will advise Customer of any increased charges prior to commencement of the installation.

Orange will not be responsible for any delay in the installation of the SSL Gateway if such failure is due to any cause beyond its reasonable control, including the inability by Orange to gain access as scheduled to the Location or Customer's failure to properly prepare the Location.

Orange will contact Customer at least one day prior to the scheduled installation date to confirm the installation appointment and will confirm with Customer that the Location has been properly prepared. If Orange determines that the Location has not been properly prepared, and that Orange cannot install the SSL Gateway, then Orange will notify Customer promptly, and Orange will have no responsibility to continue the installation. However, if the designated Customer contact disagrees with the Orange assessment that the Location has not been properly prepared, the Parties will escalate the issue promptly. Customer will advise Orange when the Location has been properly prepared, and the installation will be rescheduled depending upon the preparation activities required. If, as a result of rescheduling, Orange must make more than one trip to the Location or remain at the Location and wait for the Location to be properly prepared, then the additional time required will be billed at the Hourly Labor Rate, plus Expenses.

As part of the installation, Orange will interconnect the SSL Gateway to the demarcation and Customer's network and will notify Customer promptly if any problems occur during installation that adversely affect the installation process.

1.4.6 **Server Upgrades.** Orange will provide version management of the operating system and various elements of the SSL Gateway Software, which may include patches to the operating system or upgrades to a new operating system level. Notwithstanding anything to the contrary contained herein, Orange has no obligation to provide all new releases of Software from the SSL Gateway hardware vendors and Software licensors, and Orange, in its sole discretion, will decide when upgrades take place.

If Orange needs to take a SSL Gateway off-line to implement Software updates or network enhancements, Orange will provide at least 7 days prior written notice of such events. When possible, Orange will work with Customer to minimize any impact this could have. When possible, Orange will implement SSL Gateway upgrades remotely during Business Hours. If Orange is required to install an upgrade at the Location or outside of Business Hours, Customer will be charged at the Hourly Labor Rates for such services, plus Expenses.

1.4.7 **Acceptance Testing.** Upon completion of the installation of the SSL Gateway, Orange will commence acceptance testing, which will confirm that all aspects of the SSL Gateway and the Mobile SSL Service are operational in accordance with the terms of this Service Description and the parameters set forth in the SRF. Upon completion of the acceptance testing, Orange will provide to Customer a "**Mobile SSL Service Acceptance Form**" for Customer's execution, which form will identify the acceptance tests performed by Orange. Customer will be deemed to have accepted the Mobile SSL Service on the date on which Orange issues the Mobile SSL Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Service within 5 Business Days of receipt of the Mobile SSL Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.4.8 **Security Policy Changes Procedure.** Following installation and acceptance testing, Orange will accept requests for changes to the Security Rules Base only from the security contacts identified in the SRF. All such changes will be subject to verification by Orange in accordance with mutually established procedures agreed to in writing by the Parties prior to the commencement of the Mobile SSL Service. Orange will contact the primary security contact to agree to the appropriate actions, timeframes, and charges, if applicable. Any potential conflict in the Security Rules Base or any inadvertent reduction in the security effectiveness perceived by Orange will be brought to Customer's attention, and Orange will recommend alternative strategies.

Orange will require the following information for any changes to the Security Rules Base:

(a) Completed change control form on the Mobile SSL Care Service web portal ("**Portal**");

(b) Date by which Customer requests the change to be completed; which will be no earlier than 5 Business Days after Orange receives the change request;

(c) Supporting details relevant to the specific change action; and

(d) Contingency plans and contact details of Customer personnel performing acceptance testing for the changes to the Security Rules Base.

### 1.5 Standard Service Features

When using the Mobile SSL Service, Users will access a Web portal sign-in page, where they will be required to identify the information requested for authentication (e.g. username and password). Different Users will be allowed to access, or will be denied access to, specific Customer Information based on the Security Rules Base implemented on the SSL Gateway. The Mobile SSL Service also will encrypt the traffic between the Device and the SSL Gateway and will support basic security features and authentication services that may be provided by Customer, as identified and as may be modified by Orange from time to time. Customer may download periodic reporting for the Mobile SSL Service from the Portal.

Depending on the complexity of the configuration asked by the Customer, Orange will identify the maximum number of profiles that may be supported on the same SSL Gateway and the maximum number of user groups per profile. Orange also will provide up to three administrator certificates with the standard Mobile SSL Service.

### 1.6 Optional Service Features

Orange may provide the following optional features, subject to additional Charges.

1.6.1 **Dual Gateway.** Two SSL Gateways are deployed as a cluster pair in active/passive mode.

1.6.2 **Additional Profiles.** If the Customer is expecting to implement a high number of profiles (superior to 20), on the same Mobile SSL gateway, Orange will charge additional management fees to reflect the complexity of this configuration and the related management charges.

1.6.3 **Secure Virtual Workspace.** A protected workspace is created on a Device, requiring the User to perform all interactions within a completely protected environment.

1.6.4 **Emergency License (ICE) Option.** Customer may activate on request the Emergency license option, providing the option has been previously subscribed to. The option consists in extending on a temporary basis the number of concurrent end-users to the maximum potential of the gateway (respectively 1,000 and 10,000 simultaneous users for SA 4500 and SA 6500 but these numbers may vary depending on Customer Security Base Rule). This option is not available for the smallest SSL Gateway (the SA 2500). The option can last up to a cumulative 8 week period. The remaining time is displayed on an on-line portal. During the activation of the Emergency license option, any SLA and SLO are waived.

1.6.5 **Extended Features.** Customer may receive any of the following:

(a) External Native ACE Authentication Server, for which Customer must provide Orange with a configuration file.

(b) Public Key Infrastructure ("**PKI**") Authentication.

(c) Successive Authentication (i.e. two external authentication servers are used).

(d) Additional administrator certificates.

### 1.7 Maintenance of the SSL Gateway

1.7.1 **Remedial Maintenance.** Orange will maintain the hardware portion of the SSL Gateway in Proper Operational Condition. If a Fault is caused by a failure in the SSL Gateway hardware, Orange will repair the Fault following receipt of a Fault Call or detection of the Fault by Orange, whichever occurs first. If Orange is unable to restore the SSL Gateway hardware to Proper Operational Condition remotely, an Orange field engineer will be dispatched to the Location.

The GCSC will classify all Fault Calls and Incidents as follows:

**Table 1: Orange Mobile SSL – Fault Calls & Incident Classifications**

| | |
|---|---|
| **Severity 1** | Problems causing critical impact to the business function(s) or customer(s). Justifies immediate management attention and dedicated resources applying continuous efforts to resolve as soon as possible. |
| **Severity 2** | Problems causing degradation of service resulting in impact to business function of customer. Impact justifies priority attention and application of resources to resolve in a timely manner. |
| **Severity 3** | Problems causing low impact to the business function(s) and customer(s). Requires timely resolution to minimize future impacts. Resources should be allocated in accordance with normal managerial planning prioritization. |

1.7.2 **Remedial Maintenance Exclusions.** Orange will have no obligation to furnish Remedial Maintenance Services for, nor will Orange be liable to Customer for damages for loss of the Mobile SSL Service or the SSL Gateway caused by any of the following (collectively "**Limitations**"):

(a) Damage to the SSL Gateway caused by temperature or electrical current fluctuation, or any Force Majeure Event, or any other casualty or loss;

(b) Damage caused by adjustments and repairs made by persons other than Orange own representatives, its Subcontractors, or personnel approved in writing by Orange; or

(c) Any instabilities in the operation of the SSL Gateway that are caused by or related to the use of certain software, or by any other software provided by Customer or its designees, or by combinations of the SSL Gateway and software, even if such combination is specified on a duly accepted SRF, or by any hardware connected to the SSL Gateway.

(d) Fault calls and Remedial Maintenance Services rendered necessary by the above causes may be performed by Orange at Customer's request, and will be charged to and paid by Customer at the Hourly Labor Rate, plus Expenses.

Remedial Maintenance Services do not include:

(e) Electrical work external to the SSL Gateway, except as otherwise set forth in this Service Description;

(f) Maintenance of attachments or other devices not specified in the SRFs;

(g) Correction of software databases and/or programming errors or any errors or damages caused by or arising out of input or error, except as otherwise set forth in this Service Description; or

(h) Failure by Customer to meet the physical and environmental specifications for the SSL Gateway.

(i) Any visits to a Location or repairs to the SSL Gateway made necessary by the preceding causes will be charged to and paid by Customer at the Hourly Labor Rate, plus Expenses.

### 1.8 Pricing

One-time and monthly recurring Charges apply to the Mobile SSL Gateway Service and to each optional feature. The monthly recurring Charges will vary depending on the number of concurrent Users of the Mobile SSL Gateway Service.

### 1.9 Geographical and Legal Service Availability

Being based on SSL/TLS standards, this service is embedding cryptographic materials. Depending on the country, the use or import of such materials is subject to specific conditions. The list of countries into which it is possible to import the device is available, upon request, to the Customer. The Customer will verify whether he is legally allowed to use the service in his country.

The Orange capacity to physically install the equipment's out of Europe or North America will be subject to verification on a case-by-case basis.

### 1.10 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: Mobile SSL**

### 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.). | No |
| 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. | Customer = the only addressee. |
| 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). | Yes, IP address. |
| Customer Relationship Management 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). | Yes | For the period required by applicable law. |
| 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 MOBILE SSL SERVICE**