PUBLICATION 1 SERVICE DESCRIPTION FOR IOT MANAGED GLOBAL CONNECTIVITY: IOT CONNECT EXPRESS SECURE MOBILE ACCESS INTERNET OPTION

1.1 Definitions

"**Dedicated APN**" means a private APN reserved for the Customer which designates the entry point to the Customer's virtual private mobile network within the Orange Mobile Network.

"**DNS**" (Domain Name System) means a component in the network infrastructure that is responsible for translating domain names into Internet Protocol (IP) addresses, allowing Customer's Terminals to access Internet and other network resources.

"**IP address**" is the 4-byte logical address (IP address version 4; IPv4) or 16-byte logical address (IP address version 6; IPv6) that is permanently or temporarily assigned to each device (mobile phone, PC, modem, server, router, any other type of hardware) connected to the Internet or a computer network.

"**IPSec Tunnel**" means a secure tunnel established between two private networks over a public network that uses a specific implementation of IPSec (Internet Protocol Security) to encrypt data sent between these two private networks.

"**MSISDN**" (Mobile Station International Subscriber Directory Number) is a number that uniquely identifies a subscription in a GSM or a UMTS mobile network. An MSISDN is the number associated with a single SIM Card and used to connect on a mobile network.

"**Private IP addressing Plan**" means a range of IP addresses used in the Customer's internal network.

"**RADIUS**" (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) services for remote users who access and use a network.

"**S/P-GW**" (Serving/PDN-Gateway) is an LTE mobile network equipment that acts as the interface between the LTE mobile network and external packet data networks, serving as a gateway for data traffic between Terminals and external networks.

"**Service**" means the Secure Mobile Access Internet Service described in this Service Description.

"**VPN**" (Virtual Private Network) refers to an extension of local networks ensuring the logical security provided by a local network. It is the interconnection of local networks via a tunneling technique using cryptographic algorithms.

1.2 Purpose

The purpose of this Service Description is to describe the Service and define the conditions under which Orange provides the Customer with secured access between Customer's site and Orange Mobile Core Network through an IPSec Tunnel over the Internet from Customer's Terminals.

The Service is subject to the General Conditions and the Specific Conditions for Managed Global Connectivity: IOT Connect Express Services. The Service is an option to Orange's Managed Global Connectivity: IOT Connect Express Secure Services.

Capitalized terms used and not otherwise defined in this Service Description will have the same meaning as described in the General Conditions and the Specific Conditions for Managed Global Connectivity: IOT Connect Express Services.

1.3 Service Overview

The Service comprises the following elements:

- **Customer Dedicated APN** that Customer's Terminals use for data connectivity.
- **Dynamic IP addressing mode** to temporarily assign an IPv4 Address to each Customer's Terminal on Orange Mobile Network.
- **Orange DNS** to translate the domain names requested by Customer's Terminals.
- **IPSec Tunnel Route-Based** to securely transport data traffic over the Internet between Customer's Terminals and Customer's site.
- interconnection between Customer's Terminals and Customer's site with a dual connection to S/P-GWs (**Redundancy in nominal/standby mode** with automatic failover).

The Customer may select the following optional elements at no additional charges:

- **Static IP addressing mode** to permanently assign an IPv4 Address to each Customer's Terminal on Orange Mobile Network (instead of dynamic IP addressing mode element);
- support of Customer's DNS server (**Customer DNS**) to translate the domain names requested by Customer's Terminals (instead of Orange DNS element);
- **IPSec Tunnel BGP** when the Customer's IPSec gateway is provided by Microsoft Azure or Amazon Web Services and the addition of BGP protocol is required (instead of IPSec Tunnel Route-Based element);
- Radius Server hosted and managed by Orange (**Orange Radius**) or by the Customer (**Customer Radius**);
- **SIM-to-SIM Communications** to allow data exchange between Customer's Terminals using only Orange Mobile Network and without going through the Customer's site via the IPSec Tunnel (by default, SIM-to-SIM communications are disabled).

The Service does not include:

- the provision of the connectivity between the Customer's site and the break-out of Orange Mobile Network (Internet access);
- the provision and maintenance of the Customer's IPSec gateway;
- anything outside of what is expressly stated in this Service Description.

1.4 Conditions of Access To, Supply and Use of the Service

1.4.1 Service Eligibility Requirements - Service Restrictions – Terms of Use

To subscribe to the Service, the Customer must have:

- an IOT Connect Express Service allowing Customer's Terminals to connect to Orange Mobile Network,
- an IPSec gateway compatible with IPSec protocol and Route-Based mode (IPSec Tunnel Route-Based element) or, if it provided by Microsoft Azure or Amazon Web Services, compatible with IPSec and BGP protocols (IPSec Tunnel BGP element), and
- access to the Internet network provided by an Internet access provider of its choice.

1.4.2 Technical Considerations

The optional Static IP addressing element requires the implementation of Orange Business Radius or Customer Radius element.

The Customer must provide the following technical elements:

- Customer Dedicated APN name written in the form "apnname.fr" and in compliance with the following conditions, taking into account the state of current technical knowledge:
  - 2 to 9 characters (lower case letters or numbers, no special or accented characters), starting with a letter ("apnname") and ending with extension ".fr";
  - for security reasons, the Customer is not authorized to use the name of its company;
  - Orange recommends using the Customer's domain name while reserving the right to ask the Customer to choose a Dedicated APN name different from the one initially chosen, if the latter is already in use, is confusing or does not meet the criteria mentioned above or any other criterion resulting from the evolution of technical knowledge;
  - in this context, the Customer guarantees Orange that it has all intellectual property rights over the chosen name and against any third-party recourse whatsoever in this regard.
- the Client ID is written in the form "xxxx.fr.fg" and used to connect the Customer's Dedicated APN to the Customer's BVPN. The Client ID shall be consistent with the Customer Dedicated APN name and must be represented by 2 to 9 characters (lower case letters or numbers, no special or accented characters, starting with a letter) and the extension '.fr.fg';
- the IP Address version of the Customer's Terminals:
  - IPv4: the Terminal must request an IPv4 Address.
  - IPv6: the Terminal must request an IPv6 Address.
  - IPv4 and IPv6: the Terminal can request an IPv4 or IPv6 Address or both (IPv4-IPv6 Addresses).
- one range of IP Addresses belonging to the Customer's Private IP addressing Plan (one range per requested IP Address version to address the Customer's Terminals).

In case of optional elements defined in Clause 1.3 above and/or depending on the Customer's IPSec gateway constructor, the Customer must provide the following technical elements:

- for Customer DNS element, the IP address of the Customer's DNS Server.
- for IPSec Tunnel BGP element, Autonomous System BGP (AS BGP) and BGP Peer IP addresses.
- for Customer Radius element, the IP and NAS-IP addresses of the Customer's Radius server (the shared secret will be exchanged when implementing the Service).
- in the case of an IPSec gateway provided by the constructor Stormshield or Sophos, VTI parameters (Virtual Tunnel Interfaces).

The Customer shall ensure that its Terminals and equipment (hardware and software) comply with market standards and having qualified personnel for the proper functioning of the Service.

1.4.3 Geographical Availability of the Service

The Service is available in the Territory and in the roaming footprint.

1.5 Restrictions and Limitations

The Service does not allow Terminals to connect through fixed networks such as PSTN or xDSL.

The Service does not allow data communications when the Terminal is located in an area covered by 2G or 3G radio technology and requests an IPv6 Address (IPv6 or IPv4-IPv6).

1.6 Build-Implementation-Service Activation

1.6.1 Service Delivery Time

The delivery of the Service will take place within 30 working days from the date of acceptance of the Order, which is a non-contractual period and given for information purposes only, subject to:

- the prior provision by the Customer of all the required technical information.
- compliance with the prerequisites described in Clause 1.4 of this Service Description.
- compliance with the Service acceptance in accordance with Clause 1.6.3 of this Service Description.

1.6.2 Temporary Access to the Customer's Site

In order to validate the delivery of the Service and ensure its technical support, the Customer must provide Orange with temporary access to the Customer's site (for 15 days), and in particular:

- authorize Orange to have access to the Service.
- transmit the MSISDNs which will be used for acceptance of the Service.
- provide at least restricted access to the Customer's site, such as access to a web page containing a file to download.

1.6.3 Service Acceptance

The acceptance tests of the Service will follow the test plan previously sent to the Customer, defining the tests to be carried out by the Customer to determine whether the Service delivered is ready to be activated. At the end of the acceptance tests, the Customer will sign the acceptance report which will confirm the final acceptance of the Service, giving rise to the invoicing of the Service setup fees. In the absence of a signature or any material fault in the Service notified by the Customer within 10 working days, the Service will be deemed accepted by the Customer.

If the Customer notifies Orange of a material fault in the Service within 10 working days, Orange will make reasonable efforts to remedy such fault within 30 working days from the date of receipt of such notice. In such event, the above acceptance process will be repeated.

1.6.4 MSISDN Registration

From the final acceptance of the Service, the Customer may transmit the list of MSISDNs for which access to the Customer Dedicated APN must be activated.

1.6.5 Inability to Implement the Service

In the event that the Service cannot be implemented due to the technical specificities of the Customer's site, the Parties mutually agree that the Service may be terminated automatically at the initiative of either Party. The Parties will then be released from their commitments without any compensation being due from either Party.

1.6.6 Failure to Provide Technical Information

In the event that the Customer failing to meet its duties to provide technical information as defined in Clause 1.4.2, Orange reserves the right to charge the Customer additional fees for implementation of the Service.

1.7 Order-Duration of Service Commitment

The Order Term takes effect from the signature of the Order by the Customer.

Each Order is subscribed for an indefinite period and, therefore, without a minimum commitment period. Any part of a month at the date of termination will be charged as a full month.

1.8 Termination

The request for termination of the Service can only be made by sending Orange's Service termination request form.

Termination of the Service does not result in termination of the IOT Connect Express Service subscribed to by the Customer.

Termination of the Service will take effect one month after the end of the period of the invoice following receipt by Orange of the termination request form.

1.9 Derogations and Additional Conditions to the General Conditions

1.9.1 Obligations of Customer

Under the Service, the Customer shall:

- designate a privileged contact called "Service Manager" whose contact details will be specified in the Order.
- provide Orange, upon request, with access to the Customer's site as specified in Clause 1.6.2 of this Service Description to carry out diagnostic and maintenance operations in the event of a Service failure. In the absence of access to the Customer's site, Orange cannot be held liable for the quality of the restoration of the Service.

The Customer is responsible for:

- providing the resources necessary for the implementation of the Service;
- the implementation of the necessary means (connection, routing, security, address translation, etc.) to enable and ensure secure access to the Customer's site;
- the implementation and integrating of the Service into the Customer's site;

- Service failures related to malfunctions on the Customer’s site (the Customer will carry out corrective interventions at its own expense to remedy Service failures related to malfunctions on the Customer’s site);
- all duties imposed on the Customer under this Service Description. Customer cannot rely on the failure of its subcontractors to exonerate the Customer from its own responsibility.

1.9.2 Orange Obligations

Orange shall:

- designate a privileged contact, called "Project Manager" whose name and contact details will be communicated to the Customer, according to terms determined by mutual agreement.
- use all means at its disposal to implement the Service within the lead-time defined in Clause 1.6.1 of this Service Description, and this within the framework of an obligation of means.

Orange shall implement the necessary means for the quality of the networks and the proper functioning of the Service throughout the duration of the provision of the Service.

In addition to the cases of exclusion provided for in the "General Conditions and the Specific Conditions for Managed Global Connectivity: IOT Connect Express Services", Orange shall not be held liable in the event of:

- misuse of the Service.
- information accessible via the Customer Dedicated APN;
- intrusion by a third party into the Customer’s site (the Customer remains solely responsible for protecting the Customer’s site against such intrusions); or
- incompatibility or malfunctions of network equipment such as the Customer’s IPSec Gateway or Terminals not compliant with market standards.

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 AS PROCESSOR FOR CUSTOMER

This Description of Processing applies to the Processing of Customer Personal Data for the provision of **Secure Mobile Access (SMA)**.

Nature of the Processing Activities	Customer Personal Data are processed to provide the Service in accordance with the Service Description or as further instructed by Customer. Processing operations include collection, consultation, transfer, storage, and deletion of Customer Personal Data, as well as other Processing activities in accordance with the configuration and options of each Service, such as recording, organization, modification, combination, pseudonymization or anonymization.
Subject Matter of the Processing Activities	Duration
Activating and implementing the Services and changes to the Services. Delivering, operating, and managing the Services (including intrusion detection and monitoring the Services if ordered by Customer). Incident management and support.	For the necessary period to provide the Service plus 6 months.
In accordance with the Service Description and the options selected:	
Reporting, i.e. reports on billing, usage, quality of service and other reports if and as required by the Customer.	As per Service Description or Customer instructions.
Portals, i.e. providing access and use of portals, on-line tools and other applications managed by Orange as part of the provision of its Services.	As long as necessary for the provision of the Services.
Types of Customer Personal Data to be Processed	Contact Data: first name, last name, email address, business address and telephone numbers, job role within the Customer. Usage Data: the usage related data to the extent related to natural persons, that Orange collects from Services it provides to its Customers. Support Data: Customer representative or end user service ticket information (including feedback, comments or questions) and if applicable, Customer representative or end user telephone recordings for incident. Identity Data: first name, last name, honorific (e.g. Ms, Mr. Dr., etc.), username or similar identifier, password, ID document/number. Technical Data: Internet Protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, as well as other technology on the devices natural persons use to access areas of Orange portals, or other technical data generated through the use of the service. Traffic/Connection Data: data revealing a communication’s origin, destination, route, format, size, time duration, IP address, time zone setting, MAC address.
Categories of Data Subjects	Employees of Customer and of its Affiliates. If applicable, other individuals using the Service or whose Personal Data are collected via the Service.
Authorized Sub-Processors	Orange Affiliates in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Agreement and communicated separately to Customer.
	Orange suppliers in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Agreement and communicated separately to Customer.

END OF SERVICE DESCRIPTION FOR IOT MANAGED GLOBAL CONNECTIVITY: IOT CONNECT EXPRESS SECURE MOBILE ACCESS INTERNET OPTION