1 SERVICE DESCRIPTION FOR STRONG 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 meanings ascribed to them elsewhere in the Agreement.

"**AAP Rules**" means the ordered set of rules against which Customer's requests for and provisioning of the Strong Authentication Service through CCS is checked, which will be configured as part of the System, if Customer receives the Advanced Automatic Provisioning option. The AAP Rules will be determined by Customer, as set forth in the SRF and approved by Orange.

"**Authentication and Domain Parameters**" means the parameters for the Strong Authentication Service that are mutually agreed upon by the Parties and set forth in the SRF. The Authentication and Domain Parameters will be determined by the technical specifications or requirements of Customer's existing network and the configurations of the Orange access Service used with the Strong Authentication Service, among other factors.

"**Authentication Server**" means the server, including the hardware and Software, supplied by Orange as part of the System.

"**CCS**" means the Customer Care Service web portal through which Customer may access reports, order Tokens, manage Users, and make changes to the Strong Authentication Service.

"**CWS**" means the Customer Web Server web portal through which Users may validate their login, PIN or Token; change the PIN code when the Token is in New PIN Mode; or synchronize or reinitialize the Token when the Token is in Next Token Code Mode.

"**Domain**" means the Network Access Identifier (NAI) suffix or other identification provided by Orange to Customer to identify and connect the Orange access Service used with the Strong Authentication Service.

"**FTPS**" means security is provided by the use of FTP over TLS protocols.

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

"**Incident**" means a fault, failure, or malfunction in the Strong Authentication Service.

"**New PIN Mode**" means the Token mode that allows Users to set their PIN code.

"**Next Token Code Mode**" means a Token mode automatically set by the Authentication Server when the Token must be synchronized with the system clock or after several failed authentication attempts.

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

"**Security Alert**" means an event detected by Orange through the Strong Authentication Service indicating a possible attempt to breach Customer's network security.

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

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

"**Token**" means the device provided by Orange for each User that displays single-use tokencodes, which change regularly based on a timecode algorithm.

"**Two-Factor Authentication**" means the identification of a User and authorization of such User to access Customer's network when the User provides 2 required elements of information.

"**User ID**" means the unique identification given to Customer for each User of the Strong Authentication Service. Each User ID must be unique within a Domain.

1.2 Service Request form Obligations

1.2.1 Requirements

Prior to commencement of the Strong Authentication 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; however, Customer will ensure that all information contained in the completed SRFs is accurate.

1.2.2 Customer Security Contacts

Customer will identify a primary security contact and between 1 and 3 secondary 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. All Security Alerts and Incidents detected by Orange will be reported to the listed contacts, and Orange will respond only to Strong Authentication Services requests and calls from Customer regarding Incidents issued by such contacts.

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

The primary security contact identified in the SRF is responsible to ensure that:

- All Security contact information is maintained and current;
- Orange is notified before and after any planned outages or configuration changes to the Customer's internal network or network services; and
- All configuration changes are scheduled at least 5 Business Days in advance.

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

1.3 Scope of Services

The Strong Authentication Service provides Two-Factor Authentication for Users accessing Customer's network. The Strong Authentication Service may be used only with, and will only authenticate, Orange access Services; the Strong Authentication Service is not available for use with any third party services. The Strong Authentication Service is provided through Authentication Servers located at Orange facilities, and Orange will manage and monitor the Authentication Servers 24 hours a day, 7 days a week. The Authentication Servers will be shared with other Orange customers or dedicated exclusively to Customer, as mutually agreed upon by the Parties. The Authentication and Domain parameters will determine the Strong Authentication Service provided. The Strong Authentication Service includes the provision, configuration, and on-going management of the System. The Strong Authentication Service also includes access to the CCS and CWS, as described more fully below. Customer may elect to receive the Automatic Strong Authentication Service Provisioning options described below.

1.3.1 Tokens

Customer will request all Tokens through CCS, and Orange will provide Tokens to Customer upon the receipt by Orange of Customer's requests through CCS. When Orange manages the Token stock, Orange will assign the Token to a User before sending the Token to Customer for shared Authentication Servers. Orange will then send out the Tokens and applicable PINs in 2 separate mailings to Customer, and Customer will distribute the Tokens to Users. When Customer manages the Token stock, Orange will send the Tokens without PINs to Customer, and Customer will assign and distribute the Tokens to Users when required for shared or dedicated Authentication Servers. Tokens will be valid for approximately 3 years, and Customer is responsible for the physical condition of all Tokens. Customer will be responsible for any Tokens damaged due to the acts or omissions of Customer or Users, including damage resulting from extreme temperatures, immersion in water, and cracked LCD panels. Replacement Tokens will not be automatically provided by Orange; Customer must request replacement Tokens through CCS.

1.3.2 Authentication

The Two-Factor Authentication requires the User to provide the login (User ID@Domain) and passcode to access Customer’s network; the passcode is comprised of the User's PIN (Personal Identification Number, which is either system generated or chosen by the User) and the tokencode provided by the Token.

1.3.2.1 Management Methods for Dial Access

If Customer uses Orange dial access Services with the Strong Authentication Service, then Orange will implement a method for managing the Two-Factor Authentication based on the dial access Service used (e.g. the "classic" or "double" method). However, the methods used by Orange may not support certain aspects of, or may restrict, the relevant dial access Service or the Strong Authentication Service, as identified by Orange from time to time (e.g. the double method does not support NAS-specific IP address pools, the classic method does not support CHAP authentication for PPP connections, and the classic method does not support Token resynchronization may by the User or new PIN mode where the PIN is chosen by the User).

1.3.2.2 Failed Authentications

After a fixed number of failed authentication attempts (which will be determined and may be modified by Orange from time to time), the System will automatically disable the Token. For dedicated Authentication Servers, however, Customer may choose the number of failed authentication attempts before a Token is disabled to a number within a range specified by Orange. When a Token is disabled

due to failed authentication attempts, Customer's administrator may re-enable the Token by contacting the GCSC.

1.3.2.3 Domains

Subject to any applicable technical, registration, or legal requirements, Orange will create Domains as mutually agreed upon by the Parties (e.g. one Domain per access Service, one Domain for all access Services, or several Domains based on Customer's requirements). Customer must submit a Domain change order to create a new Domain, to change existing Domain(s) (including a change of a Domain so that it will apply to additional access Services), and to add/change profiles, IP address pools and access server parameters.

1.3.3 Configuration

Orange will configure the System wholly based upon specifications contained in the applicable SRF, including the Authentication and Domain Parameters. 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 the cost of materials

Following commencement of the Strong Authentication Service, Orange will accept requests for changes to the configuration of the System 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 Strong Authentication Service.

1.3.4 CSS

For Customer's access to CCS, Orange will provide Customer with digital certificates to ensure strong authentication for up to 3 Customer administrators, and all transactions using CCS are encrypted using a secure socket layer. Customer must download and validate the certificates. Customer will use CCS to order and assign Tokens, manage User account information, view monthly reports regarding domains and User connections, and request certain changes to or support requests for the Strong Authentication Service (e.g. set a Token to new PIN mode when it is assigned to a User, request a PIN change, request a Token replacement, and add/modify/delete User information). Customer cannot request Domain changes through CCS. If CCS is unavailable, then Customer's administrator may contact the GCSC for urgent requests.

1.3.5 CWS

Users may access the CWS to validate their login, PIN or Token; to change the PIN code when the Token is in New PIN Mode; or to synchronize or reinitialize their Token when the Token is in Next Token Code Mode.

1.3.6 Automatic Strong Authentication Service Provisioning Options

With Automatic Strong Authentication Service Provisioning, Customer can manage its Strong Authentication Service Users database in CCS by uploading Customer information contained in files or by the AAP Rules using FTPS (or such other access mutually agreed upon by the Parties in writing), rather than manually inserting information into CCS. Upon Customer’s request, Orange will provide either the Basic or Advanced Automatic Provisioning, as determined by Customer and as set forth in the applicable Order.

1.3.6.1 Basic Automatic Provisioning

Basic Automatic Provisioning allows Customer to upload files containing Customer information for the Strong Authentication Service in a specified format (which Orange will identify and may modify from time to time) into CCS by using FTPS protocol.

1.3.6.2 Advanced Automatic Provisioning

With Advanced Automatic Provisioning, the System will allow Customer to manage its Users and Tokens for the Strong Authentication Service based on the AAP Rules. The AAP Rules will populate information required, but missing, in Customer’s provisioning of, or requests for, the Strong Authentication Service using CCS.

1.3.7 System Upgrades

Orange will provide version management of the operating system Software for the Authentication Server and the Strong Authentication Software. System upgrades may include the addition of patches to the operating system that are of a security nature and those that would affect the operation of the Software. The upgrade to a new operating system level also will be made if Orange deems it necessary for security reasons or for support of the Software. Notwithstanding anything to the contrary contained herein, Orange has no obligation to provide all new releases of Software from the System hardware vendors and Software licensors, and Orange, in its sole discretion, will decide when upgrades take place.

If Orange needs to take a System off-line to implement Software updates or network enhancements, Orange will provide at least 7 days prior written notice of such events. When possible for dedicated Authentication Servers, Orange will work with Customer to minimize any impact this could have. When possible, Orange will implement System 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 the cost of materials.

1.3.8 **Remedial Maintenance**

Orange will maintain the Authentication Server in Proper Operational Condition. Orange will repair an Incident caused by a failure in the Authentication Server upon receipt of a call regarding an Incident or detection of the Incident by Orange, whichever occurs first.

The GCSC will classify all incidents as follows:

Severity 1	Problems that cause 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.

1.4 Pricing

The Charges for the Strong Authentication Service include one-time and monthly recurring Charges. One-time Charges include Charges for set-up/installation, for Domain creation or change (as described in Clause 1.3.2.3 above), per Token, and for CCS Customer administrator addition or change. Monthly recurring Charges include a fixed Charge per Authentication Server and an incremental Charge per User. Additional Charges may apply to Automatic Strong Authentication Service Provisioning, depending on the option received by Customer.

END OF SERVICE DESCRIPTION FOR STRONG AUTHENTICATION SERVICE