

SERVICE DESCRIPTION FOR STRONG AUTHENTICATION SERVICES

1. **Definitions.** As used in this Service Description, the following capitalized terms will have the meanings given to such terms in this Clause 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.

"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 Equant access Service used with the Strong Authentication Service, among other factors.

"Authentication Server" means the server, including the hardware and Software, supplied by Equant 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 Equant to Customer to identify and connect the Equant access Service used with the Strong Authentication Service.

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

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

"GCSC" means Equant's Global Customer Support Centers.

"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 Equant 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 Faults.

"Token" means the device provided by Equant for each User that displays single-use token codes, 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.

2. Service Request Form Obligations.

2.1.1. **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 Equant will reasonably assist Customer in completion of the SRFs; however, Customer will ensure that all information contained in the completed SRFs is accurate.

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 Equant 24 hours a day, 7 days a week. All Security Alerts and Faults detected by Equant (collectively, **"Incidents"**) will be reported to the listed contacts, and Equant will respond only to Strong Authentication Services requests and Fault Calls issued by such contacts.

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

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

- All security contact information is maintained and current;
- Equant is notified before and after any planned outages or configuration changes to Customer's 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.

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, Equant 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 Equant facilities, and Equant will manage and monitor the Authentication Servers 24 hours a day, 7 days a week. The Authentication Servers will be shared with other Equant 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.

3.1. **Tokens.** Customer will request all Tokens through CCS, and Equant will provide Tokens to Customer upon Equant's receipt of Customer's requests through CCS. When Equant manages the Token stock, Equant will assign the Token to a User before sending the Token to Customer for shared Authentication Servers. Equant 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, Equant 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 Equant; Customer must request replacement Tokens through CCS.

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.

3.2.1 **Management Methods for Dial Access.** If Customer uses Equant dial access Services with the Strong Authentication Service, then Equant 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 Equant may not support certain aspects of, or may restrict, the relevant dial access Service or the Strong Authentication Service, as identified by Equant 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).

3.2.2 **Failed Authentications.** After a fixed number of failed authentication attempts (which will be determined and may be modified by Equant 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 Equant. When a Token is disabled due to failed authentication attempts, Customer's administrator may re-enable the Token by contacting the GCSC.

3.2.3 **Domains.** Subject to any applicable technical, registration or legal requirements, Equant 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.

3.3 **Configuration.** Equant 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, Equant 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 Equant in accordance with mutually established procedures agreed to in writing by the Parties prior to the commencement of the Strong Authentication Service.

3.4 **CCS.** For Customer's access to CCS, Equant 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.

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.

3.6 **System Upgrades.** Equant 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 effect the operation of the Software. The upgrade to a new operating system level also will be made if Equant deems it necessary for security reasons or for support of the Software. Notwithstanding anything to the contrary contained herein, Equant has no obligation to provide all new releases of Software from the System hardware vendors and Software licensors, and Equant, in its sole discretion, will decide when upgrades take place.

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

3.7 **Remedial Maintenance.** Equant will maintain the Authentication Server in Proper Operational Condition. Equant will repair a Fault caused by a failure in the Authentication Server upon receipt of a Fault Call or detection of the Fault by Equant, which ever occurs first.

The GCSC will classify all Faults 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

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 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.

END OF SERVICE DESCRIPTION FOR STRONG AUTHENTICATION SERVICE

