

BT Assure Authentication Management Service – Annex to the General Services Schedule

BT Reference No. **_**** _****

1 Definitions

The following definitions apply, in addition to those in the General Terms and Conditions and the General Services Schedule of the Agreement.

“EIS” means External Interface Specification

“Customer” means a customer of the BT Assure Authentication Management Service, i.e., an organisation calling managed authentication to strongly authenticate a User.

“Web Service Interface” means the programmatic interface through which data is passed either by the Customer to the Service or the data that the Service passes to the Customer.

2 Service Description

The BT Assure Authentication Management Service (“the Service”) provides the Customer with the ability to authenticate Users logging on to an application, web portal or online system.

The Service provides multi-factor authentication by supplementing the User’s traditional username and password with another one-time-password (OTP) which can only be generated by a unique algorithm running on a device or item of software issued to that User. One-time passwords expire after a single use and change every few minutes; they are secure and difficult to pfish.

The Service platform architecture is fully resilient, located across two physically separate data centres with mirrored processors and power supplies, and operates twenty-four (24) hours a day, seven (7) days a week. The Customer connects its application to the Service using predefined web service calls.

In addition to supporting OTP, the Service can be configured to support a wide range of additional authentication technologies. Options include, Challenge / Response or Prompted Data Signing in line with the MasterCard Chip Authentication Program (CAP); OATH or proprietary OTP based on a variety of physical format or software tokens.

BT will provide an EIS document which describes how the Customer must format and transmit the data needed to perform each authentication.

The Customer will be given access to a range of management reports via a web portal that will enable it to access details about individual transactions and their status.

2.1 Service Components

The Service comprises of the following service elements:

- 2.1.1 Real Time verification of credentials. The Service will provide a platform that will accept OTPs from the Customer’s web based services and verify that they have been generated from a registered hardware device or software issued to a specific User.
- 2.1.2 Access to a Customer Portal. Logins will be provided for the BT Global Services Portal through which the Customer will be able to access a range of management reports including token usage, token activation, successful authentication and failed authentications.
- 2.1.3 Set up consultancy/technical support. BT will provide technical support to assist the Customer in connecting its application to the Service. The amount of technical support provided will depend on the service band ordered. The Customer will be able to purchase additional technical/consultancy support if the service band so requires.
- 2.1.4 Project Managed Installation. BT project managers will coordinate the Service installation, set up and its commissioning, liaising with the Customer as required.
- 2.1.5 Service Centre and Fault Reporting. If an incident affecting the Service is reported, BT will record and discuss it with the Customer to try to determine the problem. Where BT is unable to resolve the matter immediately it will be logged and passed to the second line technical support team to investigate and initiate a fix as necessary. Faults shall be reported by nominated Customer contacts and not by Users.

BT Assure Authentication Management Service – Annex to the General Services Schedule

BT Reference No. **_**** _*****

2.2 Additional Services (Options)

- 2.2.1 BT can provide, (at an additional charge) a range of second factor credentials, such as keyfob tokens, desktop tokens, soft tokens, which integrate with the Service. The Customer is responsible for the distribution of the tokens.
- 2.2.2 For an additional charge, BT will distribute tokens directly to Users. The Customer will provide details of its Users and their location/address.

3 Service Delivery

BT will:

- 3.1 Configure the Service platform to interface with the Customer's application, to accept and process one time passwords and return a pass/fail response.
- 3.2 Load details of the tokens that have been issued by the Customer that will be authenticated by the Service.
- 3.3 Activate tokens as 'in use' on the platform on request of the Customer.
- 3.4 Deactivate tokens as 'not in use' on the platform on request of the Customer.
- 3.5 Provide the Customer with an EIS document detailing how the Customer's application will interface with the Service.
- 3.6 Provide an agreed number of technical/consultancy support days to assist the Customer's integration of its application with the Service.
- 3.7 Provide logins for the GS Customer Portal so that the Customer can access its BT-held data and management reports.
- 3.8 Provide a user manual for the Service.

4 BT Service Management Boundary (SMB)

If the Customer uses the Internet to access the Service, the SMB is the interface between BT's network and the Internet. BT will not be responsible for web service calls leaving the Customer's network and transporting across the Internet.

If the Customer orders a BT provided dedicated link to access to the Service the SMB is at the point of connection to the BT data centre.

5 The Customer's Responsibilities

- 5.1 The Customer is responsible for ensuring that all information necessary to perform the requested authentication is collected and transported to the advertised BT address via a properly formatted web call as described in the EIS document.
- 5.2 The Customer is responsible for all communication with its Users. Communication between BT and the Customer will be via nominated Customer contacts.
- 5.3 BT can determine that the OTP has come from a specific device, but not that the person using the device is the nominated User, therefore the Customer agrees that it is responsible for examining the results of the Service and for deciding whether to grant or deny access to its systems and/or applications.
- 5.4 The Customer is responsible for ensuring that any token is in the possession of the correct person and is used in accordance with its rules and regulations.
- 5.5 The Customer must notify BT of all tokens that are to be activated or deactivated by the process set out in the user manual.
- 5.6 Tokens are electrical or electronic equipment within the meaning of the European Directive No. 2002/96/EC of 27 January 2003 relating to waste electrical and electronic equipment and its

BT Assure Authentication Management Service – Annex to the General Services Schedule

BT Reference No. **_**** _****

subsequent domestic implementations (“WEEE Regulations”). The Customer shall comply with the WEEE Directive and shall be responsible for arranging the collection, treatment, recycling and disposal of WEEE at its own cost and expense.

6 Charges and Payment Terms

The charges for the Service will comprise some or all of the following components, depending on the option selected on the Order.

Note, the Charges may appear either as BT Assure Authentication Management or BT Managed Fraud Reduction Service on the invoice.

Product	One-time Charge	Recurring Charge	Notes
The Service	Connection and set up charge	Monthly fixed fee per token being managed. Charge dependant on total number of tokens deployed by the Customer.	Connection fee includes standard provisioning activities (including GS portal logins, service set-up, and service commissioning).
Professional services	Yes	N/A	Initial (optional) capture of Customer requirements and extended support in integrating the Customers application with the MA service (charged on a per day basis)
Tokens	Supply of tokens to the Customer. Shipping charges for shipping tokens direct to Users.		The supply Charge is dependent on the number of tokens ordered.

7 Service Levels

The Service is scheduled to be available 24 hours per day, 7 days per week, 365 days per year.

The Service has a target availability of 99.99% within any Month. This target excludes all periods of Planned Maintenance or updates.

The Service has a target that 95% of all web service calls will be answered within 1 second, subject to the availability and performance of the internet or any third party networks.

There are no Service Credits applicable if BT fails to meet these targets, and section 7 of the General Services Schedule does not apply to the Service.