Nuance Gatekeeper with BT Service Schedule
Part B – Service Description

The Service

1. STANDARD COMPONENTS OF THE SERVICE

BT will provide the Customer with the following Services in accordance with the details as set out in the Order:

1.1 Audio Authentication via Voice Biometrics

1.1.1 "**Audio Authentication and Fraud Transaction**" means the processing of audio collected from a single User within a single session by the Service.

1.1.2 An Audio Authentication and Fraud Transaction is consumed when audio is processed for the first time from a single User within a single session, independent of the feature used from the list below:

- all audio segments collected within the same session/call, independent of the number of audio segments;
- Real time active authentication;
- Real time passive authentication;
- Real time fraud detection;
- DevicePrint (check whether a device matches a device previously used by the same caller or digital user);
- Intelligent detectors.

1.1.3 Voice biometrics uses acoustic characteristics of an individual's voice to create a voiceprint. This voiceprint can subsequently be compared to an audio sample of someone claiming to be that individual, allowing an authentication match to be performed. In simple terms, it allows a person to be verified by virtue of their voice alone and detect impersonation and fraudsters.

1.1.4 The features that make up a voiceprint fall into two categories, behavioural characteristics and physical characteristics.

(a) Behavioural characteristics arise from what an individual has learnt through their environment or experiences and include accent, pronunciation, rate of speech, etc.

(b) Physical characteristics arise from the physical attributes of the individual's body. Vocal tract length, chest cavity size, lung capacity, etc. are all physical attributes that will impact the features used to create the voiceprint

1.2 ConversationPrint

1.2.1 "**ConversationPrint**" means the processing of audio collected from a single User within a single session by the Service in order to extract conversational profiling to improve authentication and fraud detection.

1.2.2 ConversationalPrints are based on language characteristics such as sentence structure and vocabulary usage.

1.2.3 ConversationPrint alone isn't sufficient to reliably confirm a User's identity, but when used in conjunction with other capabilities it can reduce false accept and false reject errors, as well as highlighting suspicious activity in counter-fraud use cases.

1.2.4 Text security is split into two subcomponents as described below but they are combined into a

single value and referred to as ConversationPrint:

(a) Voice-text security

(i) Voice-text security is comprised of all features that perform analysis on transcribed text. This includes ConversationPrint, fraud pattern detection, topic spotting and all other text security capabilities originating from audio.

(b) Digital-text security

(i) Digital-text security is the set of all features that perform analysis on text from data channels. This includes digital ConversationPrint, digital fraud pattern detection, digital topic spotting and all other text-based security capabilities originating from digital channels.

1.3 Behavioural Biometrics

1.3.1 "**Behavioural Biometrics**" is intended for use in digital channels, creating a print of how a User interacts with a given device. It makes use of keyboard, mouse, trackpad, touchscreen, and mobile accelerometers and gyroscopes to measure how a person interacts with a device.

1.3.2 Interaction Behavioural Biometrics is licensed per concurrent User and is subscribed to annually. The price is calculated using a sliding scale where the price per User is based on the tier minimum quantity. Each User license includes profiles for mobile and web. This feature is invoiced monthly.

1.4 Reprocessing Transactions

1.4.1 "**Reprocessing Transactions**" means processing data that has already been processed at least once by an Audio Authentication and Fraud Transaction.

1.4.2 A Reprocessing Transaction is consumed each time audio that previously consumed an Audio Authentication and Fraud Transaction is reused in a different session.

1.4.3 This applies to operations including clustering, backward searching, smart adaptation, risk-based decision making, reenrolment, data or algorithmic processing and any other operation performed using audio that was previously counted as an Audio Authentication and Fraud Transaction.

1.5 Behavioural Users

1.5.1 "**Behavioural Users**" means the maximum number of concurrent Users that the Customer would use in a given annual period.

1.5.2 Each year of the Subscription Term and any renewal period, if at any time the actual number of Behavioural Users during that term exceeds the number of Behavioural Users per year as described in the Order, the Customer shall pay a fee per additional Behavioural User ("**Additional Behavioural User Fee(s)**").

2. FEATURES OF THE SERVICE

2.1 Web-based Reporting and Tools

2.1.1 BT shall provide to the Customer a secure self-service web portal for access to reporting and administrative tools (the "**Client Portal**") The Client Portal includes the following baseline tools:

(a) Analytic Tools

This tool allows the Customer to access the detailed log viewer where the different actions within the system are recorded. This list of actions includes new User enrolments, authentications, speaker editing or modifications, configuration modifications, etc.

(b) Report and Queries

(i) Detailed information about the currently used number of licenses (transactions) per period of time; allows for generation of reports by a customisable time period (per

day, week, month, etc.)

(ii) Query manager: Allows for generation of customisable reports in order to find and organise different system entities (speakers, voiceprints, authentications, etc.).

(iii) Report(s) allow administrators to view, for the desired time period, the number of calls, the number which resulted in enrolment, the number of verifications, how many matched, how many mis-matched, how many failed, and how many resulted in detection of a fraudster.

(iv) The Customer will have access to reports via the Service. The Customer will be able to monitor the system, view and generate reports and make configuration changes as required.

(v) The underlying data and all other data used by the system will be stored for the Subscription Term.

(c) Authentication and Fraud Management

This tool allows new speakers, fraudster profiles, and groups to be created manually. The status of smart adaptation can also be defined and tracked.

(d) Configuration

This tool allows the Customer to check what the configurations settings defined in the system are and to track what is the current tuning stage that provides information about the level of security that the system can provides in each moment.

(e) Engagements, Fraudster and Watchlists

These tools provide the ability to search and access historical risky sessions, execute backward searches with historical data as well as access results of previously launched clustering tasks.

2.2 Security

2.2.1 BT and the Supplier will implement the following security standards and compliances:

(a) Veracode scan (a vulnerability scanning tool);

(b) Deployment in a PCI certified infrastructure.

2.2.2 BT and Supplier may update security standards and compliances from time to time, but will not reduce the level of security provided.

2.3 Storage

Pricing includes 4 MB per annual transaction included in the Annual Minimum Commitment.

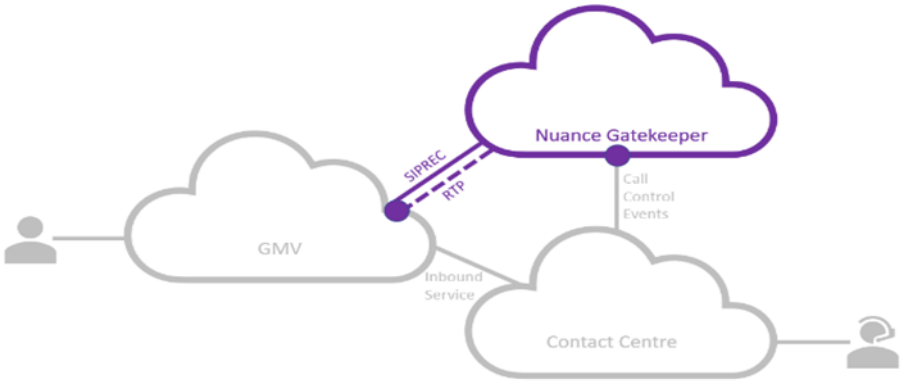
3. SERVICE MANAGEMENT BOUNDARY

3.1 BT's responsibility to provide and manage the Service is physically and logically limited to the following service management boundary:

3.1.1 The scope of monitoring and operational support is limited to the portion of the overall solution that is hosted within facilities utilised by the Supplier to provide the Service ("**SaaS Services Centre**"). Components outside of the SaaS Services Centre e.g. automated call distribution, are not within the scope of monitoring or operational support responsibilities.

3.1.2 To interact with the Service and take advantage of its features, the Customer will need to provide connectivity between their application and/or their call centres and the SaaS Services Centre. That connectivity will typically be an multi-protocol labelling switching network or other private network. The Customer is responsible for the procurement, the sizing, the deployment and the management of such connectivity and all its associated costs and these are outside the Service Management Boundary.

3.1.3 BT will provide and manage the Service up to SIPREC & RTP, as detailed in the diagram below.



3.2 Paragraphs 3.1.1- 3.1.3 together constitute the "**Service Management Boundary**."

3.3 BT will have no responsibility for the Service outside the Service Management Boundary.

3.4 BT does not make any representations, whether express or implied, about whether the Service will operate in combination with any Customer Equipment or other equipment and software.

4. ENABLING SERVICES

4.1 The Customer will have the following services (which may or may not be provided by BT) in place that are necessary for the Service to function:

4.1.1 Inbound SIP voice service (to carry the voice from an end customer to Customer's contact centre);

4.1.2 a contact centre service which is capable of processing Universal Call ID;

4.1.3 Internet access to the contact centre service;

4.1.4 A series of service API's (BT will work with the Customer to ensure that these API's are in place to enable the Customer to consume the Service but BT will not be responsible for any APIs);

(each an **"Enabling Service")**

5. COMMISSIONING OF THE SERVICE

5.1 Before the Operational Service Date, BT will:

5.1.1 deliver and configure the Service as set out in paragraph 1 and 2;

5.1.2 conduct a series of standard tests on the Service to ensure that it is configured correctly;

5.1.3 connect the Service to the Enabling Service;

5.1.4 on the date that BT has completed the activities in this paragraph 5, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

6. ACCEPTANCE TESTS

6.1 The Customer will carry out the Acceptance Tests for the Service within five (5) Business Days after receiving notice from BT ("**Acceptance Test Period**").

6.2 The Service is accepted by the Customer if the Customer confirms acceptance in writing during the

Acceptance Test Period or is treated as being accepted by the Customer if the Customer does not provide BT with notice to the contrary by the end of the Acceptance Test Period.

6.3 Subject to paragraph 6.4, the Operational Service Date will be the earlier of the following:

6.3.1 the date that the Customer confirms or BT deems acceptance of the Service in writing in accordance with paragraph 6.2;

6.3.2 the date of the first day following the Acceptance Test Period; or

6.3.3 the date the Customer starts to use the Service.

6.4 If, during the Acceptance Test Period, the Customer provides BT notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide the Customer notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Section B Service Management

7. SERVICE MANAGEMENT

7.1 The Service Management Schedule as referred to in the Order will apply to this Service.

7.2 In variance to the Service Management Schedule, the Service Care Levels and resolution targets contained in the table below shall apply:

Severity	Initial Response	Updates Frequencey	Resolution Targets
Severity 1 Incident	Within 30 minutes	Every 30 minutes	4 Hours
Severity 2 Incident	Within 1 hour	Every 2 hours	24 hours
Severity 3 Incident	Within 4 hours	Every 4 hours	48 hours

"**Severity 1 Incident"** is as an event in which the Service is down, or not functioning, and no workaround is currently available causing an extremely serious impact. Typically where the Service is completely down or unavailable.

"**Severity 2 Incident**" is an event that results in the Service functioning in a severely reduced capacity, or an important function is not usable which severely restricts operation or use of the Service, resulting in a significantly reduced level of performance causing significant loss, but the impacted business function is not halted.

"**Severity 3 Incident**" is a medium-to-low impact event which involves partial or non-critical functionality loss of the Service. The Service is predominately unaffected, and/or an acceptable work around is available which allows the Service to continue to function causing a small impact. For example, intermittent or occasional disturbance which do not have a major impact; however the Service is not working as expected.