Cloud Contact Biometric Authentication 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 Voice Authentication and Fraud Transactions.

1.1.1 The Voice 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 from the list below:

(a) all audio segments collected within the same session/call, independent of the number of audio segments;

- 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)

(b) Reporting and analysis tools

1.1.2 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.

1.1.3 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, Dual Tone Multi Frequency ("DTFM") pattern recognition etc.; and

(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 Cloud Contact Biometric Authentication with Pindrop Passport

1.2.1 Cloud Contact Biometric Authentication with Pindrop Passport means the processing of audio collected from a single User within a single session by the Service to extract conversational profiling to improve authentication and fraud detection. Based on language characteristics such as sentence structure, vocabulary usage.

1.2.2 Cloud Contact Biometric Authentication with Pindrop Passport is intended for use in voice, creating a print of how a User interacts with a given device. It makes use of networks, device type, keyboard, mouse, trackpad, touchscreen, and mobile accelerometers and gyroscopes to measure how a person interacts with a device.

1.3 Momentum of Authentication:

1.3.1 First Time Caller Authentication.

For a first-time call with no previous enrollment into the Cloud Contact Biometric Authentication it can be achieved by using a set of first-time caller authentication policies that Cloud Contact Biometric Authentication is based upon.

1.3.2 Repeat Caller Authentication

After first-time caller authentication, policies are used to verify the identity of a caller. These policies are the rules which govern the authentication process. Policies are evaluated in real time, matching or not with a prior enroll call during first-time caller.

1.3.3 Profile Matching and Authentication Score

The profile match policy function requires that a caller has been previously enrolled. This allows Cloud Contact Biometric Authentication engines to analyze subsequent calls and authenticate based on a risk result and a minimum authentication score threshold. Authentication scores can consist of carrier signaling, speech, device, behavior analysis and biometrics features.

2. OPTIONAL FEATURES OF THE SERVICE

In combination with the Cloud Contact Biometric Authentication with Pindrop Passport can be implemented a below list of optional features:

2.1 Cloud Contact Biometric Authentication with Pindrop Protect (Anti-fraud)

A Real-time fraud detection functionality which allows the Customer to provide risk scores for any call and recalculate account risk based on suspicious behavior in both the contact center and for other online channels. Anti-fraud feature works in your IVR to alert on possible reconnaissance activities and raise alerts on "at-risk" accounts using both online and contact center activity. This feature also alerts agents of high-risk calls by analyzing every call for audio and voice anomalies and checking against any previous fraud attempts at Customer's institution.

2.2 Cloud Contact Biometric Authentication Web-based Reporting and Tools

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 tools:

2.2.1 Calls - management and analysis tools for calls

The calls portal provides extensive management and analysis tools for calls and the enrollment and authentication status for each caller. The calls page lists all incoming and historical calls and provides a breakdown of Cloud Contact Biometric Authentication and risk analysis on a per call basis. It provides the ability to e.g.:

- search for specific call activity,
- review the authentication and risk analysis for a specific call,
- view Caller ID status,
- view Blocklist status and listen to the recording of a call,
- create a case,
- manually create enrollment decisions,
- review the authenticate request history for a call.

2.2.2 Cloud Contact Biometric Authentication Risk Analysis

The risk analysis lists the risk factor from the call for device, voice and behavior, with the below features described:

(a) Cases Reports

Through Cases Report tool the cases portal is the primary screen used in resolving fraud investigation cases. These cases require further review to determine whether the selected call was a genuine Customer call or attempted fraud.

(b) Authentication Dashboard

The Authentication Dashboard provides real time telemetry and trends into each Customer's authentication funnel, enrollments, etc. The following type(s) of information are tracked on the

Authentication Dashboard:

- Enrollment Rates,
- Authentication Rates,

(c) Custom Reports

The Customer will have access to reports via the Service. The Customer will be able to monitor the system, view and generate following reports:

- **Enrollment Report**

  For Cloud Contact Biometric Authentication Customers, the Enrollment Report provides information about enrollment for Customers' accounts.

- **Voice Removal Report**

  For Cloud Contact Biometric Authentication Customers, the Voice Removal Report provides information about Voice Removal for Customers' accounts.

- **Blocklist Report**

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

2.3 Voice recording Storage

Storage will only be used in situations where the Customer would require a post call Fraud Investigation Tool. Store does not need apply, only in case high risk fraud detected voice storage could be needed for after call analysis, this recording will be made on Customer premise as first instance. Retained audio for fraud analysis will be stored securely within the Customer's network, that recorded audio is used to create fraud cases within Cloud Contact Biometric Authentication Case Report tool. The audio is typically stored and controlled by the Customer, with final control over retention and access.

2.4 SIPREC Channels

In case of technically the connectivity with Supplier to enable a SaaS is gone through BT Global Management Voice Network (GMV) using standard GSIP and/or ICG BT Services , BT will need to deploy a number of SIPREC channels into BT SBCs according of number of maximum simultaneous calls to be treated by Cloud Contact Biometric Authentication solution with Pindrop Passport or Pindrop Passport and Protect.

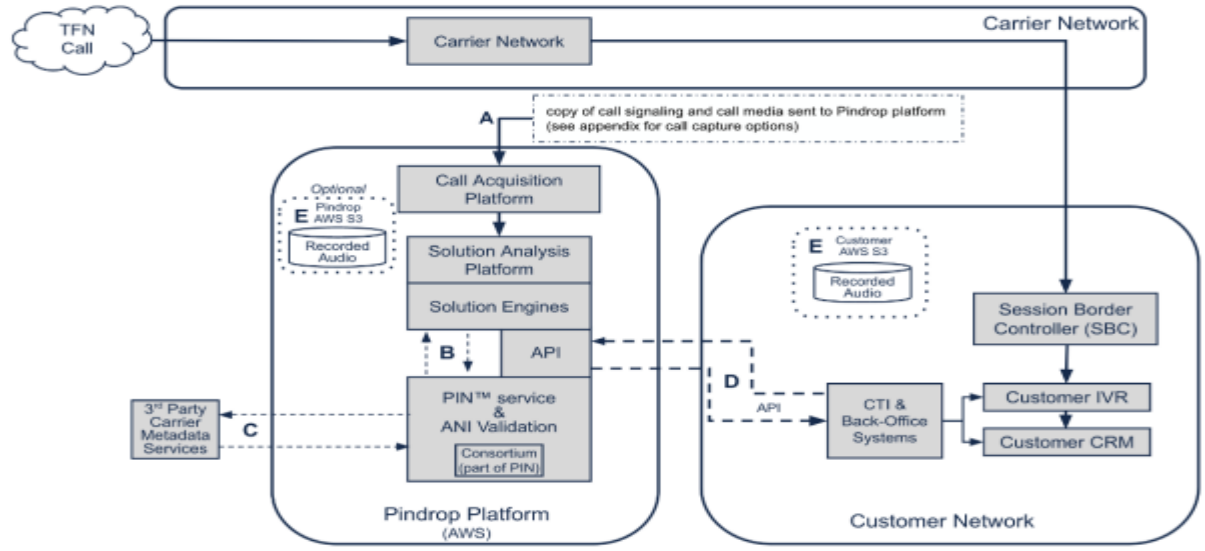
3. SERVICE MANAGEMENT BOUNDARY

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.

Data Flow Example (Carrier Integration)



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

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

3.1.5 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 /outbound SIP voice service (to carry the voice from an end customer to Customer's contact centre) supporting SIPREC protocol or other native application to allow third-party connectivity into Contact Center, for example Audio Hooks application native of Genesys Cloud or other native SIPREC API;

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

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 implement (with the Supplier) the following security standards and compliances:

- Veracode scan (a vulnerability scanning tool;
- Deployment in a PCI certified infrastructure.

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

5.1.4 connect the Service to the Enabling Service;

5.1.5 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.

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

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	8 Hours
Severity 2 Incident	Within 1 hour	Every 2 hours	12 hours
Severity 3 Incident	Within 4 hours	Every 4 hours	1 Business day

"**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. An error that renders the Service inoperable or unable to enroll or authenticate calls received by the Service.

"**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. A major Service functionality is impacted or Service performance is significantly degraded; issue is persistent and affects many of BT customers using the Service and/or major functionality of the Service. No reasonable workaround is available.

"**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.