



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 standard Service components in accordance with the details as set out in the Order:

1.1 Cloud Contact Biometric Authentication with Pindrop Passport

- 1.1.1 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.
- 1.1.2 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.
- 1.1.3 Cloud Contact Biometric Authentication with Pindrop Passport is set-up as follows:
 - (a) **First Time Caller Authentication.**
For a first-time call with no previous enrolment into the Cloud Contact Biometric Authentication a set of first-time caller authentication policies will be used.
 - (b) **Repeat Caller Authentication**
After first-time caller authentication, policies are further developed 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 enrol call during first-time caller.
 - (c) **Profile Matching and Authentication Score**
The profile match policy function requires that a caller has been previously enrolled. This allows the Cloud Contact Biometric Authentication engines to analyse subsequent calls and authenticate based on a risk result and a minimum authentication score threshold. Authentication scores can consist of carrier signalling, speech, device, behaviour analysis and biometrics features.

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

- 1.2.1 Cloud Contact Biometric Authentication with Pindrop Protect is a real-time fraud detection functionality which allows the Customer to provide risk scores for any call and recalculate account risk based on suspicious behaviour in both the contact centre and for other online channels.
- 1.2.2 This anti-fraud feature works in Customer's interactive voice response (IVR) system to alert on possible reconnaissance activities and raise alerts on "at-risk" accounts using both online and contact centre activity. This feature also alerts agents of high-risk calls by analysing every call for audio and voice anomalies and checking against any previous fraud attempts at Customer's institution.

2. OPTIONAL SERVICE FEATURES

In combination with the Cloud Contact Biometric Authentication with Pindrop Passport, below list of optional features can be implemented as set out on the Order:

2.1 Cloud Contact Biometric Authentication Pulse

This Service option enables contact centre teams to mitigate the risk posed by deepfakes and other synthetic voices in the contact centre by assessing in real time whether a caller is likely a real human speaking live or not. This Service option uses the Pindrop Pulse Module for liveness detection in Pindrop solutions for authentication and fraud detection.

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 enrolment 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 behaviour, 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, enrolments, etc. The following type(s) of information are tracked on the Authentication Dashboard:

- Enrolment 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:

- **Enrolment Report**

For Cloud Contact Biometric Authentication Customers, the Enrolment Report provides information about enrolment 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

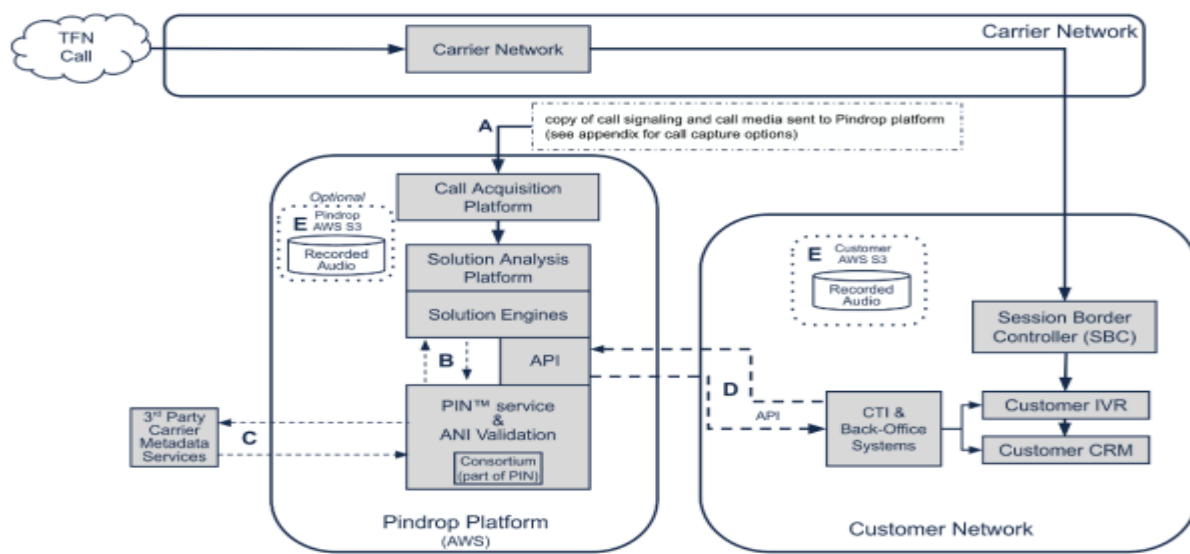
In case of technically the connectivity with Supplier to enable a SaaS is gone through BT Global Management Voice Network (GMV) using standard GSIP and/or ICG BT Services, BT will need to deploy a number of SIPREC channels into BT SBCs according of number of maximum simultaneous calls to be treated by 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 a 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 Centre, for example Audio Hooks application native of Genesys Cloud or other native SIPREC API;
 - 4.1.2 a contact centre service which can process 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 APIs 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



with the notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Supplier Terms

7. EULA

The applicable EULA will be: <https://www.pindrop.com/end-user-terms-cloud-solutions-uk-eu/>

Section B Service Management

8. SERVICE MANAGEMENT

8.1 The Service Management Schedule as referred to in the Order will apply to this Service, except for the following:

8.1.1 Monitoring descriptions, as these do not apply to this Service.

8.1.2 Proactive incident ticket opening, which is also not applicable. For this Service, the Customer must report Incidents to BT's service desk. Once reported, BT's service desk will open a ticket and manage the incident according to the Service Management Schedule.