AVAYA CPaaS

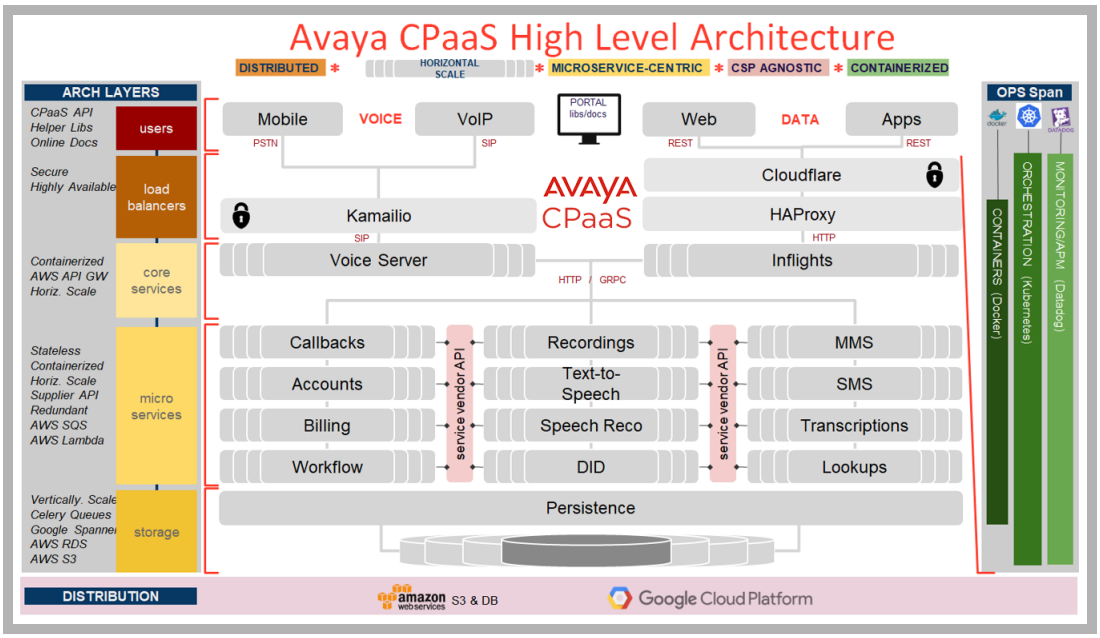
Architecture and Security Guide

ARCHITECTURE & CONNECTIVITY

The CPaaS platform is built using several technologies including Kubernetes, Kamailio, MySQL and others. The platform is hosted on Google's Cloud Platform (GCP).

Architecture

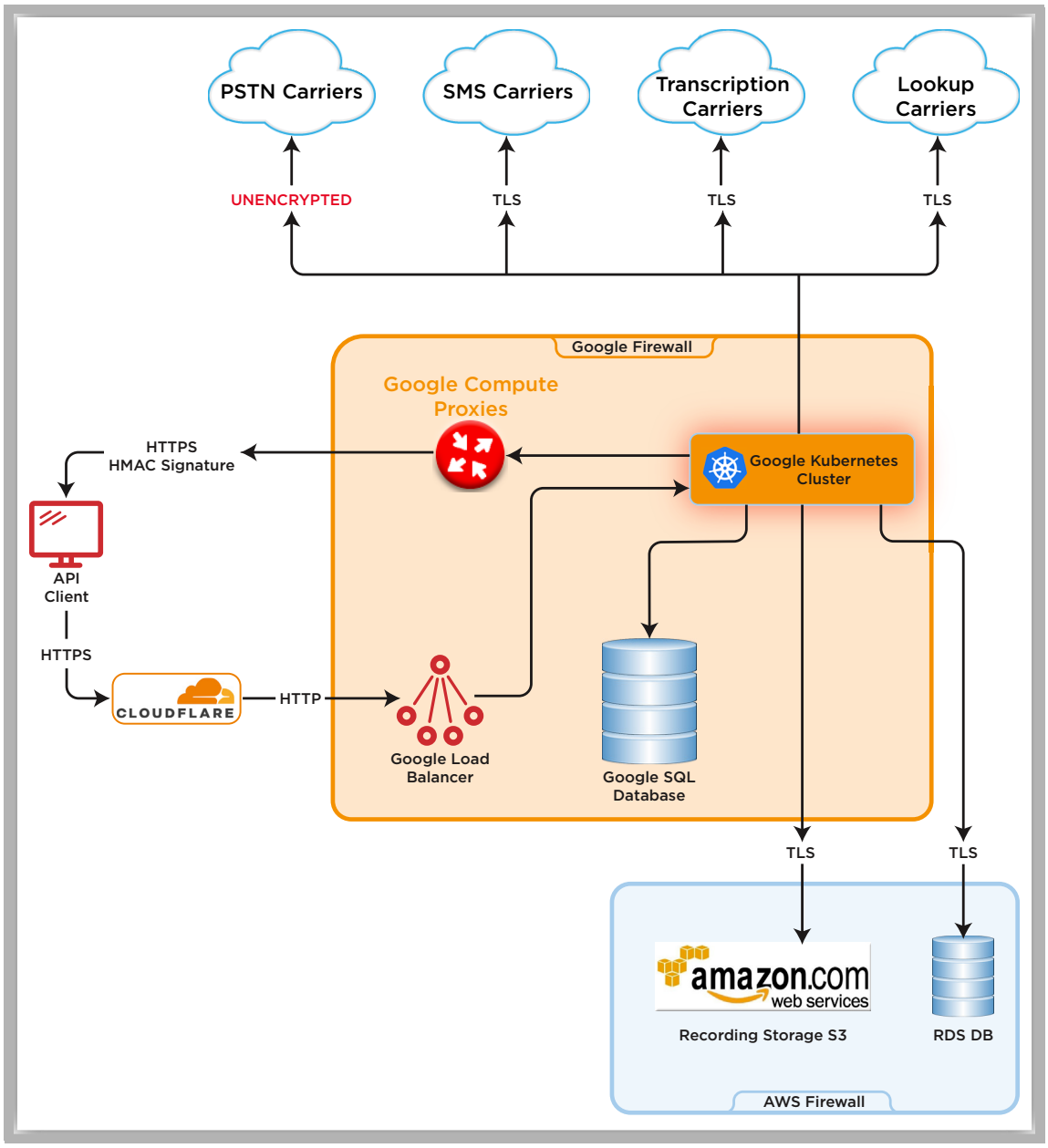
This diagram shows the overall architecture of the platform.



As the documentation shows, the voice communication between the voice providers and Kamailio, and between Kamailio and the voice servers, is entirely SIP based. During regular functions, the voice servers or inflights will connect to the micro services over HTTPS or GPRC depending upon the service.

CPaaS Connectivity

This diagram shows the flow of data and the encryption associated with each step.



SECURITY AND COMPLIANCE

Encryption

Access to the CPaaS platform using the Browser Dashboard or the REST API is encrypted with a SHA256 EC-based algorithm, or RSA2048, depending on the client. Access to these items is available only using TLS 1.2 or TLS 1.3.

Voice Media (RTP) & Signaling (SIP) are not currently encrypted between Avaya CPaaS and its providers, or between CPaaS and customer SIP endpoints.

When sending recordings from the voice servers to S3 for storage, Avaya CPaaS uses HTTPS (not SFTP) to post the recordings.

Un-Subscription Service

Avaya CPaaS has a built-in un-subscription service. Customers are advised to use their own unsubscribe service (configure in the SMS Request URL of a number), but the native service is enabled by default. Recipients who unsubscribe from a message will be unsubscribed from the Avaya CPaaS account that sent the message, but not the "FROM" number.

Example:

1. 905-707-1234 (configured on Avaya CPaaS account SID – AC12323456219834198304) sends a message to John Smith (647-123-4567).
2. John Smith replied back with STOP, CANCEL, OR QUIT.
3. 647-123-4567 will block ALL future messages from Account SID AC12323456219834198304.

Storage

	STORAGE RETENTION PERIOD
Call Logs	18 Months
SMS Logs	6 Months
SMS Body Content	30 Days
MMS Logs	6 Months
MMS Body Content	30 Days
Recording Logs	6 Months
Recordings Content	30 Days
Transcription Logs	6 Months
Transcriptions	30 Days
Server Logs	30 Days

DLRs (Delivery Reports/Receipts)

Level 1 DLRs are currently captured and are accessible via the logging APIs or the Logs dashboard. DLR level 1s provide a summarized status description as shown below:

- **View Call** (queued, ringing, in-progress, completed, failed, busy, no-answer).
- **View SMS** (sent, sending, queued, or failed).

Level 2 DLRs (for SMS) are more granular and can be provided upon request.

CARRIER LEVEL 2 DLR STATUS	AVAYA CPaaS TRANSLATED STATUS
Destination Address is not text enabled	Failed - Destination Number not SMS enabled
Spam Reject	Failed - Content Flagged as SPAM
Message accepted by Carrier	Delivered Successfully
Delivered to handset	Delivered Successfully
Route Denied	Failed - Delivery Not Available to Destination Carrier
Source Not Authorized	Source Number Not SMS Enabled
Temporary Resolution Failure	Failed - Message was Dropped After Reattempts
ESME Receiver reject message error	Failed – Possible Reasons: • A prepaid user whose account is out of money • A subscriber that is provisioned to not receive this type of SMS • SMS was sent to an IoT device • The message is rejected due to AT&T spam analysis
Description Unavailable: Please open a ticket with support for error information.	Failed – Possible Reasons: • Subscriber out of service area • Device off for extended period • Spam Reject
Message rejected	Failed – Possible Reasons: • Subscriber out of service area • Device off for extended period • Spam Reject

PER ACCOUNT LIMITATIONS & NOTIFICATIONS

Account Limitations

By default, an Avaya Cloud account for CPaaS is limited to:

- 1 SMS per second.
- 1 Call per second.

> **Note**: These limitations are based upon the account, and not the phone number(s) assigned to the account.

Account Notifications

By default, Avaya CPaaS will send out a low balance notification to the email associated with the Avaya Cloud account when the account balance reaches $2.00. The threshold amount can be adjusted upon request to support@zang.io.

VOICE SPECIFICATIONS

Compression

- G.711 is supported.
- G.729 is not supported (this feature is planned for a future release).

Bandwidth Requirements

- 87.2 Kbps per call leg.

PORTING & SMS ENABLING OF NUMBERS

1. Service supports the porting over of numbers for voice use. This requires the customer to fill out a **Letter of Authorization**. There is a one-time porting fee that varies based upon number location. There is also a recurring monthly fee (based on the number type and location).
2. Service supports the SMS enablement of numbers for SMS use. This requires the customer to fill out a **Letter of Authorization**. A customer does NOT need to port over the voice portion of their number in order to enable SMS with the CPaaS service. There is no setup fee, just the standard recurring monthly fee (based on number type and location).

ADDITIONAL SECURITY FEATURES

The following security services are provided by the various applications employed by the system.

Server Hardening (Google)

- Google will remediate infrastructure and platform vulnerabilities.
- Avaya will handle configuration vulnerabilities.

Patching (Google)

- All platforms and infrastructure are patched automatically without impacting performance.

System Security (Docker)

- All containers are completely isolated using Docker.
- Docker images protect against unauthorized changes to the file system.

CPaaS Application SDLC (Avaya)

- Any new code is tested in a staging environment, and all code is reviewed before release.

Firewalls (All)

- Google's Cloud Platform (GCP) uses access control groups to provide platform-based firewall protection.
- Access control groups are periodically reviewed by Avaya to ensure that appropriate policies are in place and up-to-date to better protect the environments.
- GCP also performs database monitoring, and alerts are created for all functions.

Data Management (All)

- SQL database and application backups are performed automatically.
- Data is replicated between the Google and Amazon data centers and other cloud regions automatically.

Access & Control (All)

- User rights are limited to the lowest level necessary to satisfy their job requirements.
- Documented approval is required by authorizing parties specifying each user's rights.
- Establish access control based upon a user's need to know. The default setting is to **Deny all** unless otherwise specified.