Genesys Interaction Recording Solution Guide

Security and Encryption

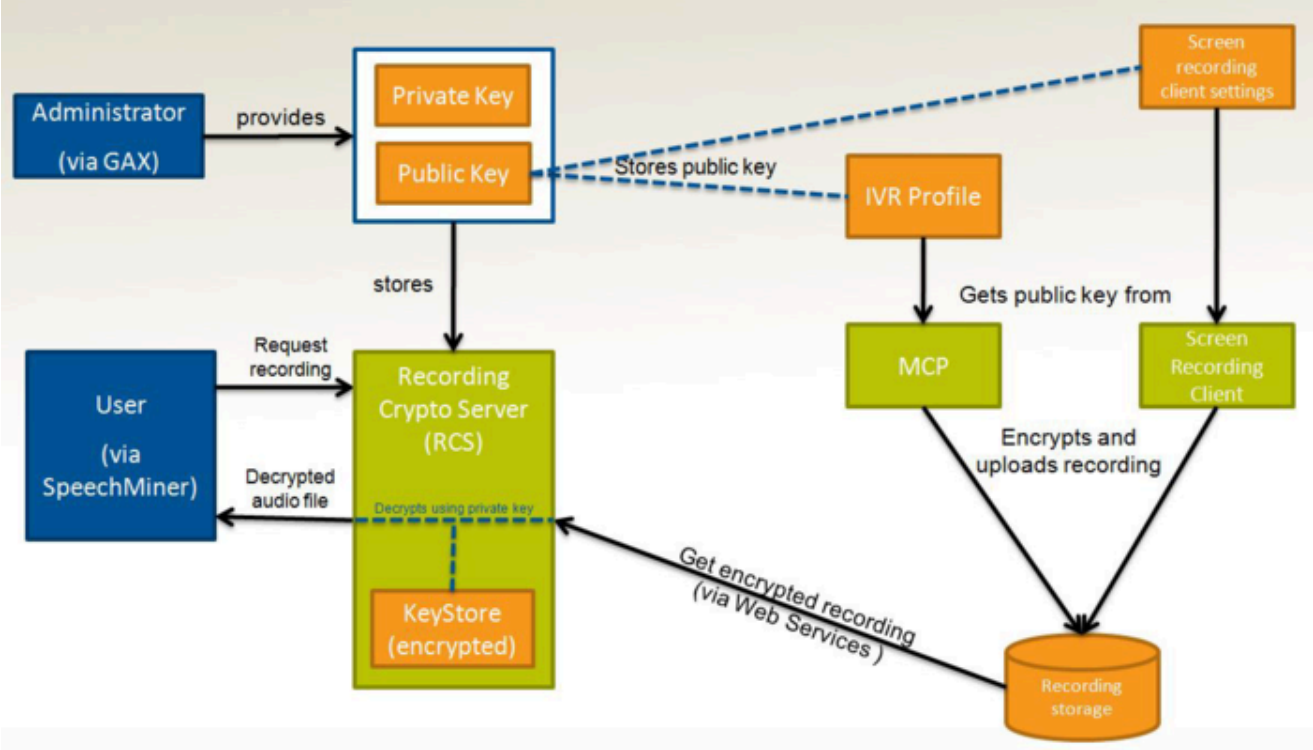
12/12/2025

Security and Encryption

Contents

A key management system allows users to decrypt call and screen recordings for playback purposes.

The following diagram provides a quick overview on how the encryption keys are managed:



Security Keys and Storage

The administrator for the customer tenant provides two keys:

1. Private key—For decrypting audio files.
2. Public key—For encrypting audio files.

Private Key Storage

The Recording Crypto Server (RCS) uses Java Cryptography Architecture (JCA) to store and access private keys in the Java KeyStore.

Key Size Limit

In older versions of Java 8, the default installation limits key sizes to 128 bits. Larger key sizes can be enabled by installing Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. For information about installing JCE, see Deploying Recording Crypto Server. Java 8u161 and later versions support the unlimited policy by default.

Public Key Storage

Public keys for voice recordings are stored in the IVR profile for the tenant. The Media Control Platform (MCP) reads the certificate from this IVR Profile. A customer may include multiple private/public keys for a tenant;however, private keys per user are not necessary.

Since MCP is shared across multiple tenants, there must be a single place to store all certificates that are accessible. Configuration Server stores all certificates (text format) as parameters in the IVR Profile for call recording. MCP loads all call recording IVR Profiles and receive updates for the IVR Profiles. When Resource Manager forwards a recording request to MCP, it inserts the IVR Profile DBID so MCP can look up the list of certificates to perform encryption.

The certificates are stored in the IVR Profile Annex tab in the `recording-certificates` section. For information about configuring encryption, see Encryption

Public keys for screen recordings are stored in the screen-recording-encryption settings of Interaction Recording Web Services (or Web Services if you're using version 8.5.210.02 or earlier). For more information about storing these keys, see Deploying Interaction Recording Web Services or Deploying Workspace Web Edition and Web Services for GIR.

Encrypting Recordings

MCP encrypts call recordings in two parts:

1. The audio file itself is encrypted with a session key using AES encryption.
2. MCP posts the encrypted audio data to WebDAV storage and sends metadata to the Recording Processor. The session key is encrypted (using the GIR public key) and stored in a PKCS7 envelope. This envelope is included in the media file's call recording metadata.

> ### Important
>
> It is your responsibility to store your private keys and certificates, including the expired ones.
>
> You should also backup your keystore, keystore password, certificates and private keys in a secure location offsite to protect against site level disasters. When Genesys Interaction Recording encryption is enabled, loss of the keystore and private key would result in loss of recording files.

For more information, see Encrypting and Provisioning Certificates.

File Format

The Genesys Interaction Recording solution supports RSA certificates and keys for the recording encryption. Certificates and keys are uploaded from files in PEM format. Certificates files must be X.509 PEM format. This is the default format generated by OpenSSL.

The following formats are supported for private key files:

- OpenSSL RSA private key format. The PEM file must start with `-----BEGIN RSA PRIVATE KEY-----`.
- PKCS#8 private key format. The PEM must start with `-----BEGIN PRIVATE KEY-----`.
- PKCS#8 encrypted private key format. The PEM file must start with `-----BEGIN ENCRYPTED PRIVATE KEY-----`.

For an example of encryption using OpenSSL, see Sample Encryption Using OpenSSL.

Certificate Validation

Certificate validation is performed when certificates are uploaded to the system and upon each use of a certificate to encrypt a recording. The validation consists of checking the certificate signatures from the recording certificate up to the root CA certificate, and checking that the certificate "not valid before" date has passed and "current" date is within the "not valid before" and "not valid after" dates.

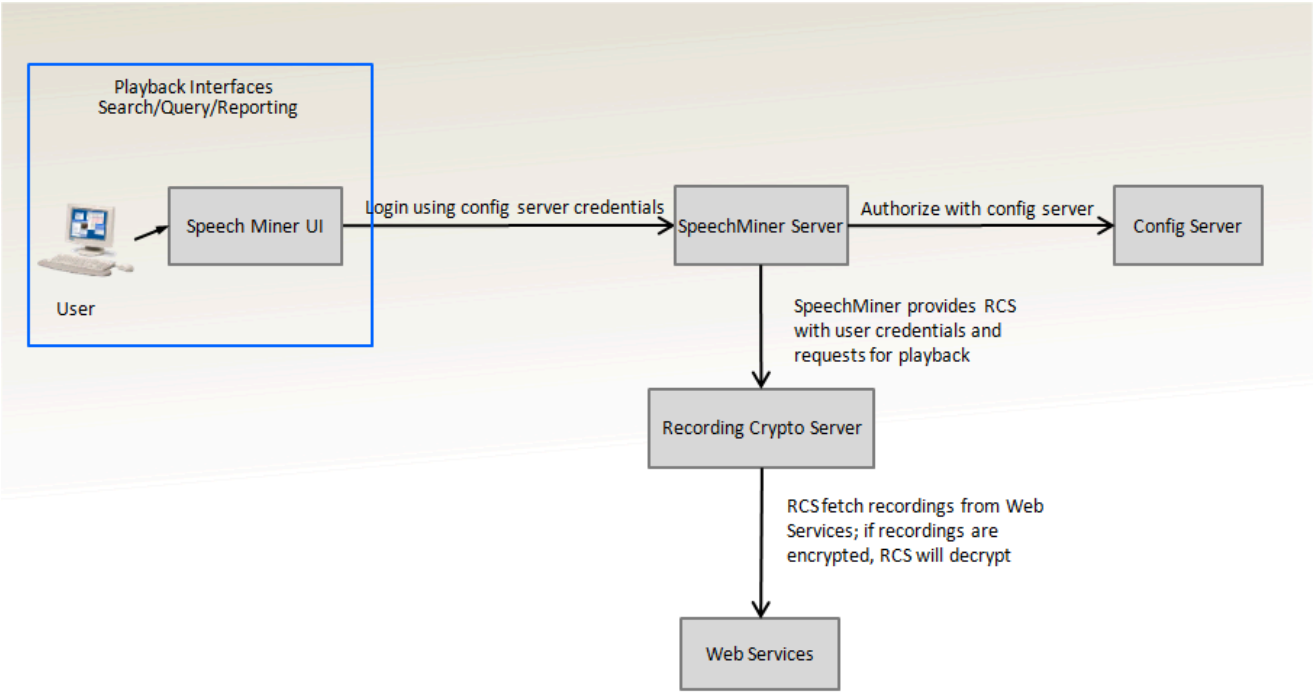
A certificate that is not yet valid can be imported, but an error will occur if it used for a recording.

For configuration of the Root CA for certificate upload, see the The certificates are stored in the IVR Profile Annex tab in the `recording-certificates` section. For information about configuring encryption, see Encryption.

For configuration of the Root CA for the certificates used for each recording, see Configuring GVP.

Decrypting Recordings

If the user wants to play back a specific recorded call, the SpeechMiner Server checks for the user's permission and makes a request to the Recording Crypto Server to fetch and decrypt the recording. The Recording Crypto Server retrieves the call metadata and fetches the recording from Interaction Recording Web Services (Web Services). The recording files are decrypted using the private key, and the audio is sent back to the SpeechMinder Server to be played in a browser.



Playback of Archived Files

The archiving function provides a zip file containing multiple encrypted recording files. Each encrypted file is in the PKCS#7 format.

Each encrypted file can be played back with the following OpenSSL command:

```
openssl smime -decrypt –inform DER -in <encrypted_file>.bin -inkey <private_key_file>
-out <output_file>
```

where:
<encrypted_file> is the file to be decrypted
<private_key_file> is the private key that you used to initially configure file encryption
<output_file> is the file to be written after decryption has taken place