This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Interaction Recording Solution Guide

Sample Certificate and Key File Generation

12/15/2025

Sample Certificate and Key File Generation

Before generating the key file, create a Root Certificate Authority (CA). For more information about creating a CA using openSSL or Windows Certificate Services, see the Genesys Security Deployment Guide at Certificate Generation and Installation.

The certificates generated using the procedures in the Genesys Security Deployment Guide can be used for recording encryption only if the certificate fields are set appropriately for the "HOST" certificate.

You can choose to generate to CA files themselves using non-Genesys procedures—for example, if you have a system with OpenSSL installed in your environment, a more general certificate can be created directly using openSSL. The following commands use an openSSL Root CA, and must be executed from the Root CA directory:

```
openssl req -nodes -newkey rsa:2048 -keyout cert.key -out cert.req
openssl ca -out cert.pem -infiles cert.req
```

For the steps required to encrypt voice and screen recordings, see Encrypting and Provisioning Certificates.