Oracle Utilities Live Energy Connect

Certificate Deployment Procedure for Using Secure ICCP with RTI Server

Release 6.3.4.0.2

November 2020

(Revised April 2021)

ORACLE

Oracle Utilities Live Energy Connect Certificate Deployment Procedure for Using Secure ICCP with RTI Server, Release 6.3.4.0.2

Contents

Introduction

This document provides instructions on how to deploy the certificates required for using Secure ICCP with RTI Server.

Note: Oracle Utilities acquired the LiveData Utilities RTI Platform in April 2020. The Oracle Utilities Live Energy Connect product was formerly called the LiveData Utilities RTI Server Platform.

Important! For more information on configuring RTI Server for Secure ICCP, refer to **Appendix A: Configuring RTI Server for Secure ICCP** in the *Oracle Utilities Live Energy Connect RTI Platform Installation Guide*.

To perform this procedure, you need to have:

- Access to an RTI Server installation from the Oracle Utilities Live Energy Connect 6.3.4.0.2 release.
- The X.509 certificates required for using Secure ICCP or a set of example X.509 certificates provided for testing.

Prerequisites

Make sure that RTI Server is installed. Refer to the *Oracle Utilities Live Energy Connect RTI Platform Installation Guide* for instructions on downloading and installing the software.

Note: When installing releases older than 6.3.4.0.1, make sure the **Secure ICCP** feature is selected in the installer. This will install Stunnel.

Required Certificates

For a given RTI Server configuration that uses Secure ICCP, the following certificates are required:

SSL/TLS Certificates

- For each local VCC configured to use Secure ICCP, a private SSL/TLS X.509 certificate is required.
- For each remote Secure ICCP peer, a public SSL/TSL X.509 certificate and a copy of the CA certificate or chain that was used to sign this public certificate is required.

ACSE Certificates

- For each local VCC configured to use Secure ICCP, a private and public ACSE X.509 certificate is required.
- For each remote Secure ICCP peer VCC, a public ACSE X.509 certificate and a copy of the CA certificate or chain used to sign this public certificate is required.

Note: You can generate your own self-signed X.509 certificates for testing purposes using various tools like openSSL.

Deploying Certificates Used for Secure ICCP

The sections below outline the step-by-step procedure to deploy the certificates required to use Secure ICCP with RTI Server. Make sure to follow the order of the steps.

Deploy the Local RTI Server's SSL/TSL Certificates

1. Obtain a private certificate for the local RTI server in PEM format. The certificate must be a *private* certificate with the RSA key embedded and *the RSA password removed.*
2. Copy this certificate to the *"\Private\"* folder of the Stunnel installation location and save it as *"Private.pem".* Typically, the full file path for this directory is:
3. *"C:\Program Files (x86)\stunnel\config\Private\".*
   The first time you use deploy certificates for Secure ICCP you need to create the *"\Private\"* subdirectory.

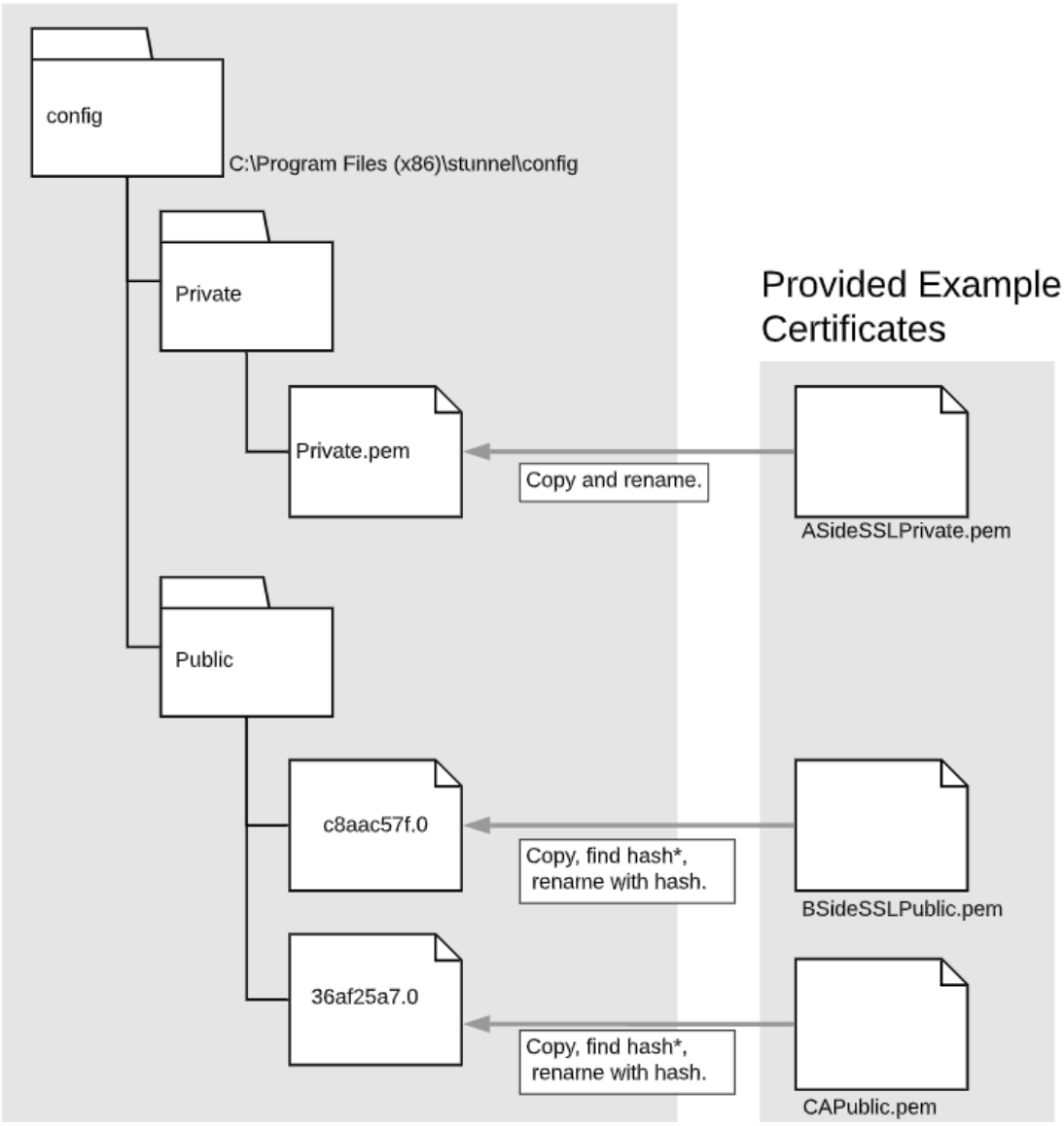
Deploy the Remote ICCP Peers' Public SSL/TLS Certificate(s) and Associated CA Certificates

1. Obtain a copy (or copies) of the public certificate(s) for the remote ICCP peer or peers in PEM format.
2. Use *OpenSSL* or a similar tool to get the secure hash for each remote server's public certificate. For example, if the remote server's public certificate was called *"BSideSSLPublic.pem",* use the command:

   ```
   openssl x509 -inform PEM -in BSideSSLPublic.pem -noout -hash
   ```

3. Using the generated hash value as part of the destination file name, copy each ICCP peer certificate to the *"\Public\"* folder of the Stunnel installation location.
   Save the certificate in this directory as "<the returned hash value>.0".
   For example, if the returned hash value from the command above was "36af25a7", save the copy of the remote server's public certificate as
4. "C:\Program Files (x86)\stunnel\config\Public\36af25a7.0".
5. Repeat steps 1-3 for the public CA certificate used to sign each remote SSL certificate. If the same CA is used to sign multiple SSL certificates, then you only need to do this once for that CA certificate.

The diagram below summarizes the SSL/TLS certificate deployment procedures outlined in detail on the previous page:



Deploy the Local VCC(s) ACSE Certificates

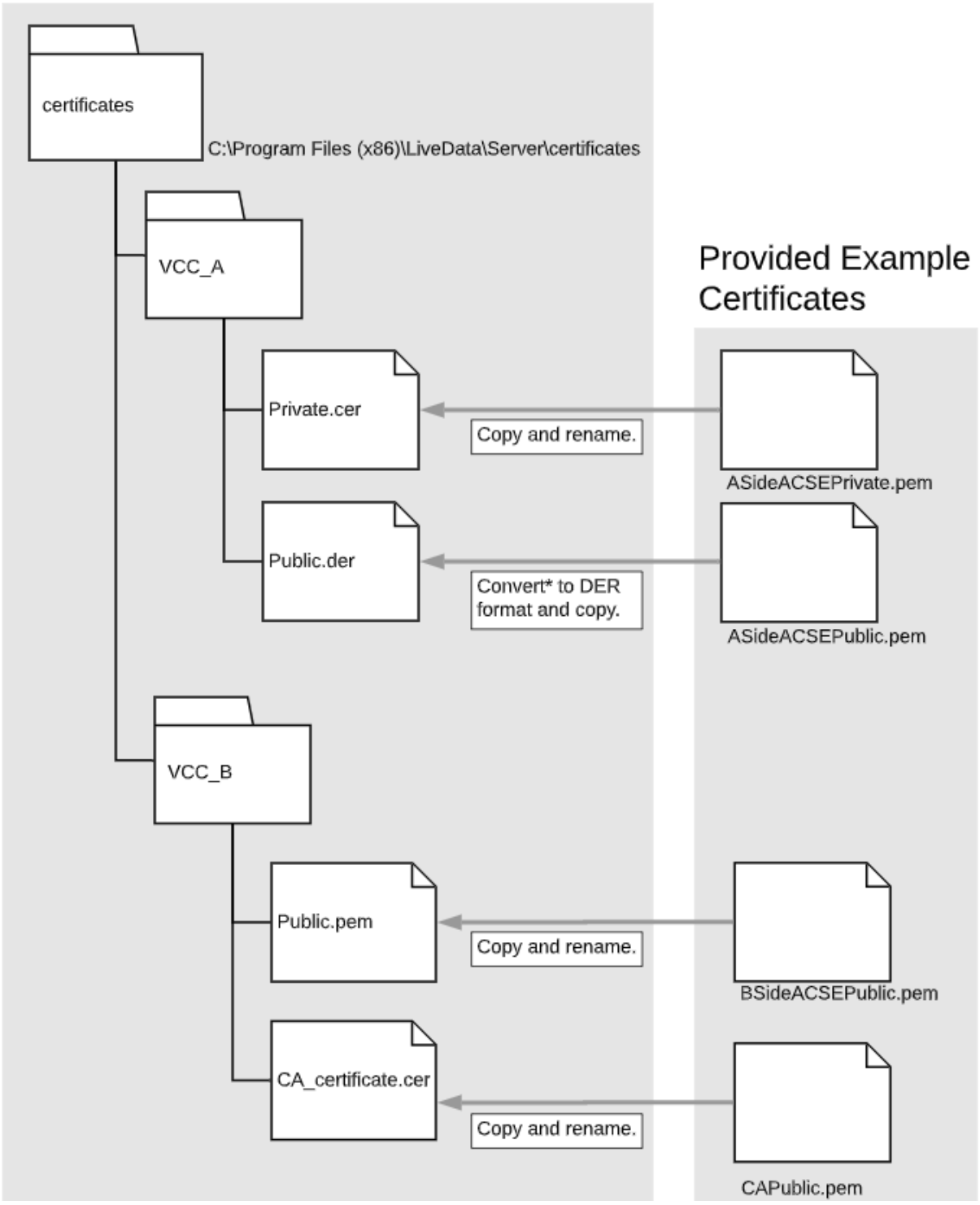
1. Obtain the private ACSE certificate for the local VCC(s) in PEM format. The certificate must be a "private" certificate with the RSA key embedded, and with *RSA password removed*.
2. In the installation directory, under the "Server" directory, create a directory named "certificates". Typically, this folder's path will be "C:\Program Files (x86)\LiveData\Server\certificates".
3. For each local VCC, create a folder under the above directory named for the local VCC. The name of this folder must match the name of the local VCC exactly.
   For example, if your local VCC was named "VCC_A", then this folder's path would be: "C:\Program Files (x86)\LiveData\Server\certificates\VCC_A".
4. Copy the ACSE certificate to the above folder as *"Private.cer"*.
5. Use *OpenSSL* or similar procedure to create a public copy of the ACSE certificate in DER format, and copy to above folder as *"Public.der."*

```
openssl x509 -outform der -in ASideACSEPublic.pem -out Public.der
```

Deploy the Remote VCC(s) Public ACSE Certificate(s) and Associated CA Certificate(s)

1. Obtain a copy of the public ACSE certificate(s) for each remote peer VCC, and a copy of the CA certificate(s) used to sign them in PEM format.
2. For each remote VCC, create a folder under "C:\Program Files (x86)\LiveData\Server\certificates" directory named for that remote VCC. The name of this folder must match the name of the remote VCC exactly.
   For example, if the remote VCC was named "VCC_B" in the Server, the folder's path would be: "C:\Program Files (x86)\LiveData\Server\certificates VCC_B".
3. Copy the public ACSE certificates for that remote VCC to the above folder.
   Here, file name is not important, but the file must have a *".pem"* or *".cer"* file extension.
4. Copy the CA certificate used to sign the remotes VCC's public certificate to the above folder as "*CA_certificate.cer*".

The diagram below summarizes the ACSE certificate deployment procedures outlined in detail on the previous page.



At this point, the certificates required for using Secure ICCP with RTI Server have been deployed. Refer to **Appendix A: Configuring RTI Server for Secure ICCP** in the *Oracle Utilities Live Energy Connect RTI*

Platform Installation Guide for more information about using configuring and running an RTI Server configuration that uses Secure ICCP.

Note: If you have any trouble with the procedures outlined above, contact My Oracle Support (MOS).