Oracle Utilities Live Energy Connect

Certificate Deployment Procedure for Using Secure ICCP with RTI Server

Release 6.3.4.0.1

September 2020

ORACLE

Oracle Utilities Live Energy Connect Certificate Deployment Procedure for Using Secure ICCP with RTI Server, Release 6.3.4.0.1

Exxxxx-01

LiveData UTILITIES

Contents

LiveData UTILITIES

Revision History

Author	Date	Description	Version
Chris DiTrani	03/14/2019	Unofficial email sent to ABB describing the process.	0.0
Daniel Lynch	01/13/2020	Formatted, annotated process, added figures.	1.0
Daniel Lynch	04/25/2020	Fixed Typos	1.1

Introduction

This document provides users with instructions on how to deploy the certificates required for using Secure ICCP with LiveData Utilities' RTI Server. The procedure outlined in this document does not require the use of LiveData Utilities' Certificate Manager and therefore can be more easily implemented as an automated process.

Other information regarding the operation of the LiveData Utilities' RTI Platfrom products can be found in the *LiveData Utilities RTI Platform Installation Guide* and **the** *RTI Configuration Manager User's Guide.*

This document assumes the reader has:

- Access to a recent release of the LiveData Utilities RTI and RCM products (6.02.001 or later)
- The X.509 certificates required for using Secure ICCP (see the next section for more information) or a set of example X.509 certificates provided by LiveData Utilities for testing

After deploying these required certificates, refer to **"Appendix A: Enabling Secure ICCP on New RTI Configurations"** if you need to use Secure ICCP on a new RTI Server configuration or on an RTI Server configuration that was not originally using Secure ICCP.

Procedure for Deploying Certificates for Secure ICCP on RTI Servers

The following is a step-by-step procedure for deploying the certificates required to use Secure ICCP with an RTI server. If desired, the reader can follow along using a set of example certificates, which are available upon request from the LiveData Utilities Professional Services Team (support@livedatautilities.com).

Prerequisites:

Install the Latest Release of RCM and RTI:

If you have not already, install RTI Server and RCM using the LiveData Utilities RTI Platform Installer. You can follow the *LiveData Utilities: RTI Platform Installation Guide* to install and license your RTI product.

Note: During installation of the RTI Server Platform, be sure to select the "Secure ICCP" feature in the installer. This will install all of the required components for using Secure ICCP with RTI Server.

Required Materials

For a given RTI Server configuration, you will need the following certificates:

SSL/TLS Certificates:

- For each local VCC in your RTI server configuration you will need a private SSL/TLS X.509 certificate.
- For each remote ICCP peer, you will need a public SSL/TSL X.509 certificate and a copy of the CA certificate or chain that was used to sign it.

ACSE Certificates:

- For each local VCC on your local RTI server you will need a private and public ACSE X.509 certificate.
- For each remote VCC in your setup you will need a public ACSE X.509 certificate and a copy of the CA certificate or chain used to sign it.

Commented [d1]: Right?

Deploy the Local RTI Server's SSL/TSL Certificate

1. Obtain the private certificate for the local RTI server in PEM format. The certificate must be a ***private*** certificate with the RSA key embedded and with the RSA password removed.
2. Copy this certificate to the *"\Private\"* folder of the Stunnel installation location and save it as *"Private.pem"*.
   Typically, this folder is located at *"C:\Program Files (x86)\stunnel\config\Private\",* but you may need to create the *"\Private\"* subdirectory depending on your stunnel installation.

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

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"* you could 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.
   Typically, this folder is located at *"C:\Program Files (x86)\stunnel\config\Public"* and the file would be named *"<the returned hash value>.0"*
   For example, if the returned hash value from the command above was "36af25a7", then you would save the copy of the remote server's public certificate as *"C:\Program Files (x86)\stunnel\Public\36af25a7.0"*.
4. Repeat steps 1-3 above for the public CA certificate used to sign each remote SSL certificate. If the same CA is used to sign multiple SSL certificates, you only need to do this once that that CA certificate

Commented [d2]: I put them in this directory and had to create it. Once I ran RTI, stunnel moved them to "C:\Program Files (x86)\stunnel\config\Public". Maybe you're supposed to put them there in the first place.

Commented [d3]: These just go in public with their hash as filename, right?

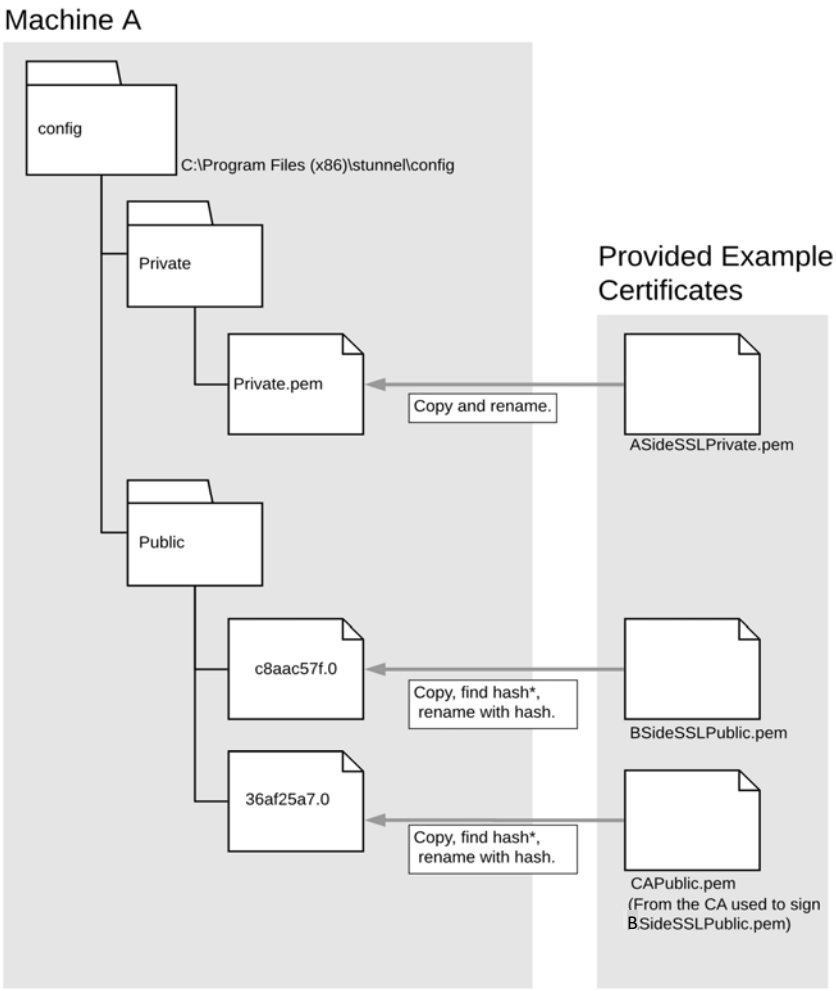

Fig. 1 – The LiveData Utilities Professional Services Team can provide you with a set of example certificates that to use to validate setting up Secure ICCP on a machine running RTI server. The diagram above outlines how to deploy the SSL/TLS X.509 certificates from this provided example set. *Note: To find the hash of the "BSideSSLPulblic.pem" you can use the command in Step 2 of the previous section. The actions in this diagram (i.e. the arrows and their text boxes) correspond to the steps outlined in the previous two sections.

Deploy the Local VCC ACSE Certificate(s)

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 RTI installation directory, under the "Server" directory, create a directory named "certificates".
   Typically, this folder's path would 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" in RTI server, 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 the above directory named for that remote VCC.
   The name of this folder must match the name of the remote VCC exactly.
   For example, if your remote VCC was named "VCC_B" in RTI server, then 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.
   The 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*".

Commented [d4]: Which certificate?

Commented [d5]: This seemed a little weird. You definitely change it from (for example) from 'ASideACSEPrivate.pem' to 'Private.cer'

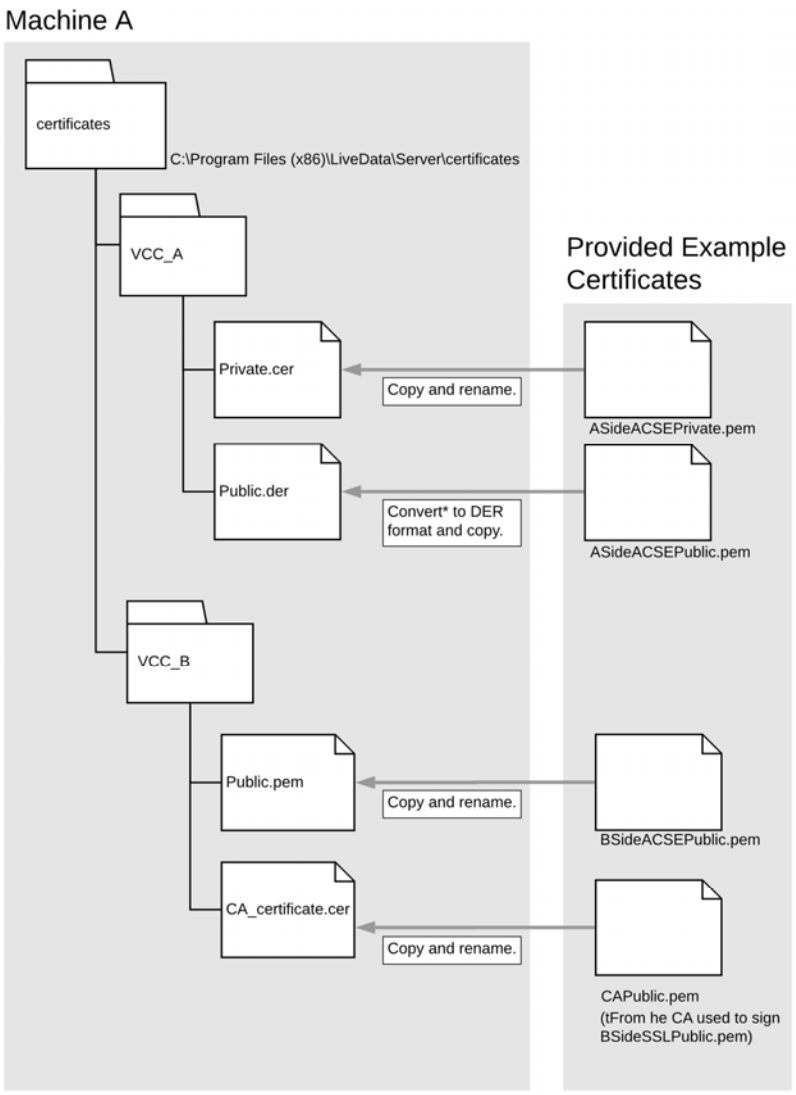

Fig. 2 – The diagram above outlines how to deploy the X.509 certificates for ACSE -level security using certificates from an example set of certificates available from LiveData Utilities Professional Service Team. *Note: To convert "ASideACSEPulblic.pem" to DER format you can use the command in Step 2 of the previous section. The actions in this diagram (i.e. the arrows and their text boxes) correspond to the steps outlined in the previous two sections.

Appendices

Appendix A: Enabling Secure ICCP on New RTI Configurations

If you are creating an RTI Server configuration from scratch or based on an existing configuration that was not previously using Secure ICCP, then you will need to change some configuration parameters on your RTI server.

To tell RTI server to use Secure ICCP, the you will need to:

1. Change the “Global flags” setting to “3” (See Fig. 3)
2. Enable the “SECURITY_FLAG” on each VCC that will be using Secure ICCP (See Fig. 4)
3. Enable the “Secure ICCP” setting in the “LDIB Editor” for each VCC that will be using Secure ICCP (See Fig. 5).

Server Global Macros

In the “Server” tab of the RTI Configuration Manager, change the “Global flags” field from “1” to “3”.

Fig. 3 – This is a screenshot of the “Server Properties” window in RTI Configuration Manager. In order to use Secure ICCP the “Global flags” field must be set at ‘3’. To set this flag, change the “Global flags” text input to ‘3’ and then select “Apply”.

VCC Configuration

For each VCC that will be using Secure ICCP, make sure to enable the “SECURITY_FLAG” in the “Flags” field of the VCC’s “VMD Properties” window.

Note: If a VCC’s flags are generated by a setup batch file you will need to specify this flag in the setup batch file instead.

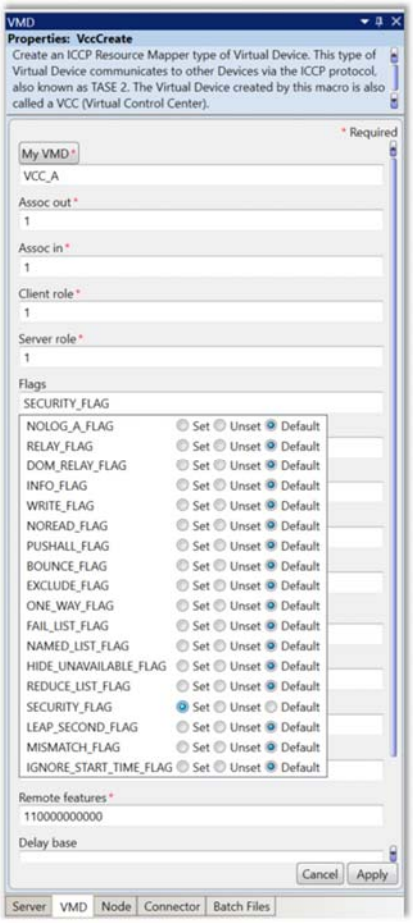

Fig. 4 – This is a screenshot of an example VCC VMD properties window in RTI Configuration Manager. In order to use Secure ICCP with a particular VCC, that VCC’s “SECURITY_FLAG” must be set. To set this flag, select the “Flags” field input box, click the radio button for “SECURITY_FLAG” from the drop-down, and then hit the “Apply” button.

LDIB Editor:

For each local and remote VCC that will be using Secure ICCP, enable this feature in the "LDIB Editor" pane in RCM.

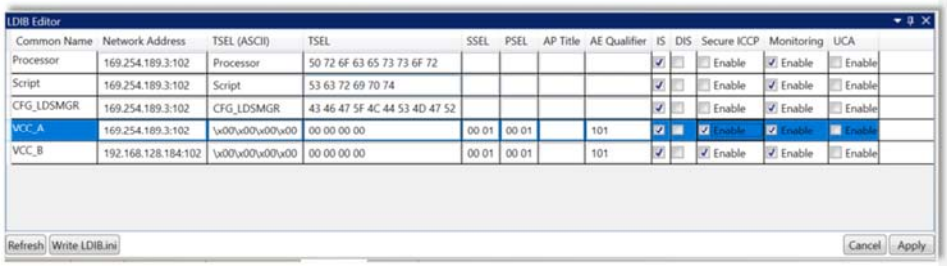

Fig. 5 – This is a screenshot of "LDIB Editor" properties window in RTI Configuration Manager. In order to use Secure ICCP with a particular VCC, that VCC's row must have the "Secure ICCP" field set. To do this, click the radio button and hit the "Apply" button.