OPC UA Security with OPC Data Client 5.3

A Guide for Managing UA Certificates

Software Toolbox
International Corporate
Headquarters, USA

148A East Charles Street
Matthews, NC 28105 USA
www.softwaretoolbox.com

TOLL FREE: 888-665-3678
GLOBAL: 704-849-2773
FAX: 704-849-6388



Table of Contents

Introduction

Purpose

The purpose of this document is to provide a guideline for users of the OPC Data Client library to manage the OPC UA security certificate exchange with their OPC server. The OPC UA standard offers users the ability to encrypt client-server connections using SSL certificates. Successful use of this feature of OPC UA requires certain steps to performed on the OPC UA client and server.

Intended Audience

This document is intended for current users of the UA component of Software Toolbox's OPC Data Client family of development products. The OPC Data Client is a client development toolkit for creating custom OPC UA clients to access information from an OPC UA server. The document assumes some familiarity with the OPC Data Client and its documentation including but not limited to the Concepts Document.

Introduction to OPC UA

The OPC Unified Architecture, also known as OPC-UA, is the latest open-standard architecture developed by the OPC Foundation to improve and expand interoperability standards in the Industrial Automation industry.

Why do we need a new architecture to begin with? OPC-UA was the result of several advancements and changes in the way data was commonly being accessed and exchanged. Some changes that lead to the need for a new architecture include:

- Microsoft's COM and DCOM (the basis for previous standards) were deprecated and are now considered legacy technologies
- Web services gained importance in data exchange between machines and for communications to factory floor devices
- Earlier specifications were decoupled and did not integrate well, e.g. items in a Data Access server could not communicate directly with items in an Alarms and Events server.

OPC-UA is designed for exchanging information in an object-oriented manner, rather than as isolated data points. This increases the accessibility of your plant floor data by letting you re-use information stored in a common object. OPC-UA also incorporates a service-oriented model, which increases interoperability with other platforms and improves security.

OPC-UA is not a replacement for existing OPC-DA standards. Because of the layered design of this architecture, it includes all the functionality of existing OPC-DA servers, but expands upon their functionality with a common interoperability layer. This interoperability layer unifies information exchange and provides a common interface for controlling processes.

What are the benefits of the new architecture? OPC-UA provides a way to connect clients and servers in a secure manner, without relying on Microsoft DCOM. This is a big advantage because it means that you are no longer saddled with the headaches associated with having to configure DCOM. This is because DCOM plays no role in data transport. OPC-UA can also allow users to make secure connections through firewalls and over VPN connections because it uses a single TCP/IP port number that is typically user configurable. In addition, it expands the ability to provide factory floor information to other business systems, as a result of the object-oriented model described above.

Introduction to OPC UA Security

OPC UA uses SSL certificates to ensure secure connections between client and server applications.

The first time you try to connect an OPC UA client, such as one written using the OPC Data Client library, to an OPC UA server, a certificate exchange must take place in order for the two applications to be able to connect and share data. The OPC UA server must have the OPC UA client's certificate, and the UA client must possess and validate the UA server's certificate. The exact behavior of the certificate exchange will vary between OPC UA servers, so you will need to also consult your OPC UA Server documentation unless you are using Software Toolbox's TOP Server which is used in this example. The OPC server will either:

- proceed with the certificate exchange and add it to its trusted store
- proceed with the certificate exchange, but not trust the certificate and place it in its accepted store
- ignore the attempt to connect, until you manually exchange the certificates and add them to the respective trusted stores

Note: This certificate exchange process is only necessary the **first** time that a client and server attempt to communicate with each other. Once this process has been done on the initial connection, subsequent attempts will work without needing further user interaction.

Security Verification Process with OPC Data Client

This section will provide general information on the process that the OPC Data Client library uses to verify security permissions with an OPC UA connection.

1. When a session to the OPC UA server is being established, the OPC Data Client will call the OPC UA SDK method for verifying the server's certificate. The SDK will use the certificate store location defined by the OPC Data Client toolkit, which is set with the **EasyUAClient.SharedParameters.Engine.TrustedPeersCertificateStore** setting.

2. If the verification in step one fails, the library will check to see if the **EasyUAClient.IsolatedParameters.Session.CertificateAcceptancePolicy.AcceptAnyCertificate** property is true. If so, then the certificate is accepted.

3. Else, if the server's URL has been added to the **EasyUAClient.IsolatedParameters.Session.CertificateAcceptancePolicy.TrustedEndpointUrlStrings** definition, then the certificate would also be accepted.

4. If the above statements are not set, the certificate will be rejected by the client.

If a connection to the OPC Server fails because of an authentication issue, the error will be returned in the **UAStatusCode** class. There are a variety of fields that can be returned related to a bad certificate, or certificate authentication failure. For a full list of members, please refer to the OPC Data Client Reference file that installs with the software. It is highly recommended that your application takes into consideration the possibility that the authentication fails and prompts the user to perform the certificate exchange in such a case, and provides friendly error messages and guidance to the user on how to resolve the issue in the context of your specific application and how to contact your firm's help desk for support.

Software Toolbox support cannot directly support users of your custom application written with the OPC Data Client library if they were to contact us regarding certificate exchange issues. Provided you are on a support agreement, we will support you as the developer of the application. When there are support needs, the more accurate information you can provide, the better of a customer experience we can help you provide for your users.

Creating New OPC Data Client Certificates

Windows Applications

The first time you build a Windows application (such as a WinForms app, Windows Service, Windows Console app, etc…), written with the OPC Data Client, the library will automatically create a new UA Client Certificate that will expire 49 years after creation. The default location for this certificate is "%CommonApplicationData%\OPC Foundation\CertificateStores\UA Applications". This path is stored in the **EasyUAClient.SharedParameters.Engine.ApplicationCertificateStore** property by default and can be changed to point to a different certificate store if desired.

The certificate should show up in the folder with the name of the Visual Studio Project followed by a GUID. For example, if application is named WindowsApplication1 the certificate will be name WindowsApplication1[GUID number].der.

The prior fact means that you may have a management step to handle if you were to later make changes to some parts of your application:

The OPC Data Client library uses the application's Assembly Title (accessible from "Project Properties" in Visual Studio) to actually associate the certificate with the application. What this means is that changing just the name of your project or some files in it will not affect the certificate at all, and no new certificate will need to be generated after making such a change.

However, changing the Assembly Title itself will mean that a new certificate is generated, and would subsequently mean that you would have to go through the certificate exchange process again with the newly generated certificate.

Our recommended approach is to use a friendly name for the Assembly Title from the start of development and this will ensure that the certificate is named appropriately and there will be no future management problems.

Note: %CommonApplicationData% is used as a placeholder because the actual folder name changes depending on which operating system is installed. For example, on Windows 7, the %CommonApplicationData% folder would be "C:\ProgramData", so the entire path of the certificate store would be "C:\ProgramData\OPC Foundation\CertificateStores\UA Applications".

On other operating systems, this folder name may change. Using the %CommonApplicationData% token in the **EasyUAClient.SharedParameters.Engine.ApplicationCertificateStore** property helps your application adapt to different operating systems.

Web Applications

When dealing with applications in hosted environments, such as IIS, certificate generation can become a little trickier. This is because of two reasons:

1. It is difficult for the OPC Data Client to automatically determine reasonable and unique parameters for the certificate, because the hosting process is the IIS service, not "your" own application EXE.
2. The page processing code in IIS typically runs with low privileges that do not allow it to call the necessary CertificateGenerator utility that is used to generate the certificate, and even less to save the new certificate to the store.

If you run into a problem when using OPC Data Client in such an environment, please contact us and we will be glad to assist.

Custom Configuration of a Client Certificate

The OPC Data Client library also provides the user with more control over the certificate generation by allowing the user to create a custom app.config file that contains all the necessary parameters for creating the certificate. This would allow you to change the name of the certificate, the type and location of certificate store, and more. In the majority of cases, this level of control is not necessary for the typical developer using the OPC Data Client, but we do make this available. If you have a situation in which you would like to do this, please contact us and we will assist you.

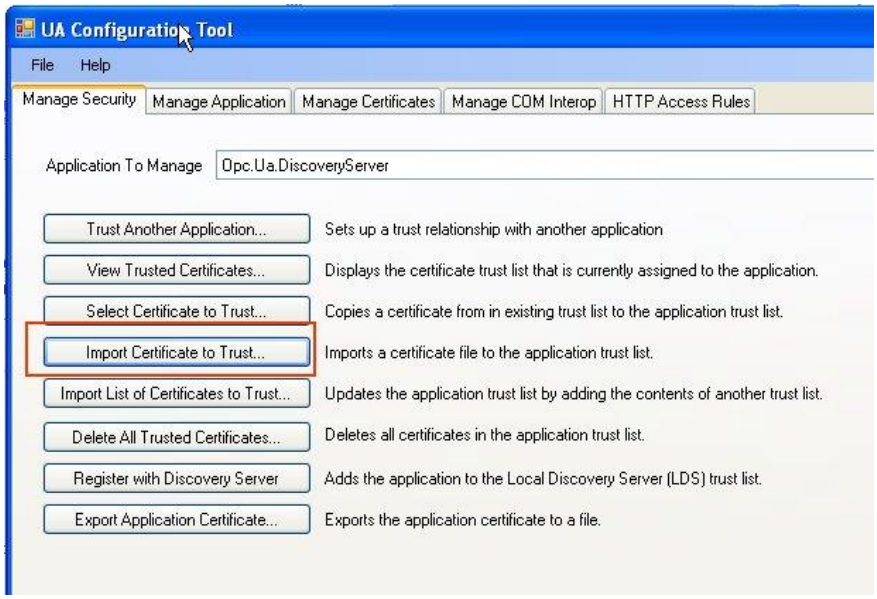
Managing OPC UA Certificates

UA Configuration Tool

OPC Data Client requires the user to manually handle the certificate exchange process between OPC UA servers and the OPC Data Client application the first time that the client and server wish to communicate. This process will only need to be done once, before the initial connection. Once this is done, subsequent connections will work automatically.

To make this process easier on the user, the software installs with a UA Configuration Tool that can be accessed by going to Start | All Programs | OPC Foundation | UA SDK 1.01 | UA Configuration Tool.

On the Manage Security tab you can click the Import Certificate to Trust button, as shown below.



Browse to the location where you have stored your OPC Server's certificate and import the .der file. The server should now be trusted by your OPC Data Client application.

Note: You will need to refer to your OPC server vendor's documentation for information regarding adding the OPC Data Client client's certificate to the OPC server's trusted store.

Manual Certificate Exchange

The default location that the OPC Data Client component checks for trusted servers is "%CommonApplicationData%\OPC Foundation\CertificateStores\UA Applications". You can change this default location by setting the **EasyUAClient.SharedParameters.Engine.TrustedPeersCertificateStore** property of the **EasyUAClient** object.

You can manually add a UA server's certificate to this store by opening the folder in Windows Explorer and then copying the UA server's .der file to the folder.

Example Exchange Process with TOP Server

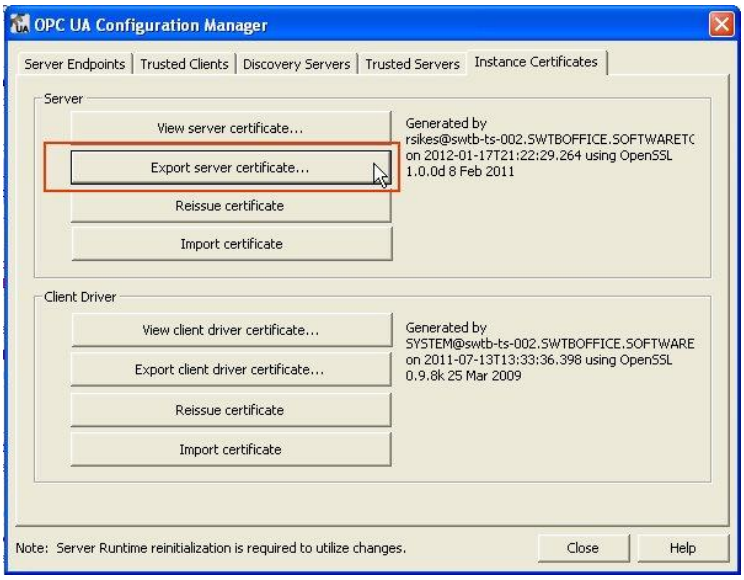
This section will walk you through the process of performing the full client and server certificate exchange using Software Toolbox's TOP Server as the OPC UA server. For more information on UA support with the TOP Server, including how to enable OPC UA on the TOP Server, please read this Application Note.

Again, this is something that is only required to be done **one time** before establishing the initial connection and does not have to be done each time you want to connect your client to the server.

Exporting the TOP Server's Certificate

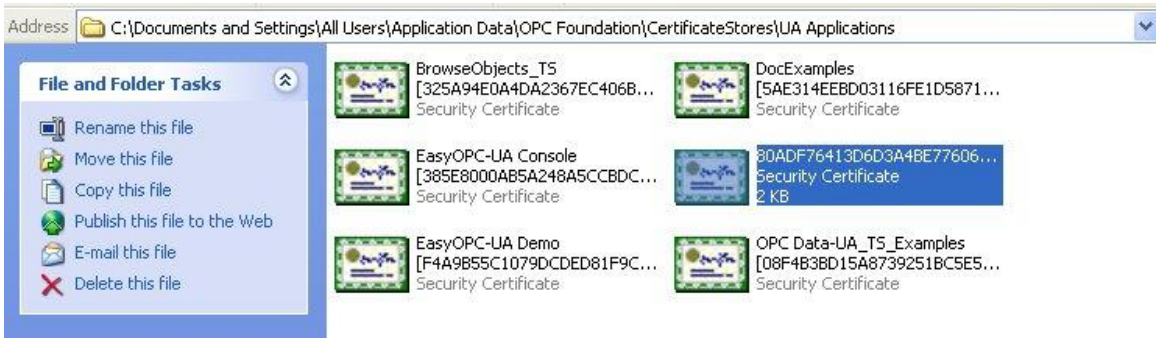
Open the TOP Server UA Configuration by right clicking on the TOP Server Administration icon in the system tray, as shown below.

When the OPC UA Configuration Manager opens, go to the Instance Certificates tab. Click on the Export server certificate button and choose a location where you would like to save the certificate.



Adding the TOP Server's Certificate

To manually add the TOP Server's certificate to the OPC Data Client's trusted list, open the "%CommonApplicationData%\OPC Foundation\certificateStores\UA Applications" folder and place the .der file you saved above into the folder.

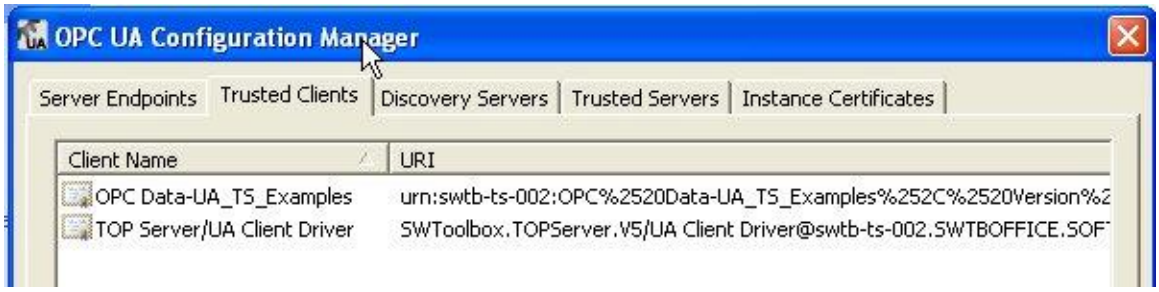


Importing OPC Data Client's Certificate

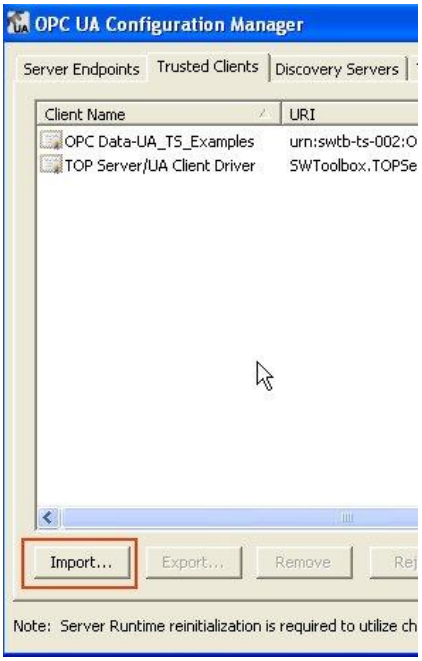
The next step is to make sure that the OPC server recognizes the OPC Data Client's instance certificate as a trusted OPC UA client. The exact instructions for performing this exchange will vary depending on the UA server.

For the TOP Server, the first time a client attempts to connect the TOP Server will automatically attempt to exchange the certificates between itself and the client. If the client's instance certificate

shows up in the Trusted Clients tab of the OPC UA Configuration Manager, as shown below, no further action is required.



If your client's certificate is not in this list, you can manually import the certificate by opening the UA Configuration Manager, clicking on the Import button at the bottom of the Trusted Clients tab, and browsing to the instance certificate in the location of the OPC Data Client certificate ("%CommonApplicationData%\OPC Foundation\CertificateStores\UA Applications" by default) to complete the import.



Now, the TOP Server and your OPC Data Client application should trust each other and be able to communicate securely.

Contact Us

If you have any questions or are seeking further assistance, please contact us at:

Online Support: http://support.softwaretoolbox.com

Email Support: support@softwaretoolbox.com

Phone Support: +1 (704) 849-2773

Fax: +1 (704) 849- 6388

Mailing Address: Software Toolbox, Inc. 148A East Charles Street, Matthews, NC 28105, USA