SIEMENS

Ingenuity for life

Notes for Secure PLC Communication with TLS Protocol on the SIMATIC S7-1200/S7-1500 Channel

WinCC V7.5 SP2 Update 4

https://support.industry.siemens.com/cs/ww/en/view/109798498

Siemens
Industry
Online
Support

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customers are responsible to prevent unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase the customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Contents

1 STEP 7 "Secure Communication"

WinCC supports the secure communication of STEP 7 via TLS protocol, which is available with TIA Portal V17 and higher.

STEP 7 components for which "Secure Communication" is configured use an asymmetric key procedure with a public key and a private key. TLS (Transport Layer Security) is used as the encryption protocol.

For controllers running firmware ≥ V2.9, "Secure Communication" with TLS is always used for communication in TIA Portal projects V17 and higher.

To use the "Secure Communication" of TIA Portal V17 in the WinCC project, you import the data records from a TIA Portal project with the corresponding settings.

1.1 Behavior in Runtime

During operation, even with "Secure Communication" enabled, the following actions are possible:

- Update Certificates
- Switch between the configured connections of the "SIMATIC S7-1200, S7-1500 Channel"

1.2 Further information

- Industry Online Support "WinCC V7 - Secure Communication" (ID 109798498) (https://support.industry.siemens.com/cs/ww/en/view/109798498)
- Industry Online Support Download "SIMATIC SCADA Export for TIA Portal" (ID 109748955) (https://support.industry.siemens.com/cs/ww/en/view/109748955)
- Industry Online Support Documentation "SIMATIC SCADA Export" (ID 101908495) (https://support.industry.siemens.com/cs/ww/en/view/101908495)
- Industry Online Support Documentation on STEP 7 (TIA Portal V17) (https://support.industry.siemens.com/cs/products?search=%22secure%20communication%22&dtp=Manual&mfn=ps&pnid=24471&lc=de-DE)
- Industry Online Support Questions and answers about the new safety functions in TIA Portal V17 (https://support.industry.siemens.com/cs/ww/en/view/109799540)
- TIA Portal Information System (V17):
  "Edit Devices and Networks > Configure Devices and Networks > Configure Networks > Secure Communication"

1.3 Requirements

- You are using an S7-1500 controller with firmware ≥ V2.9 configured with TIA Portal V17 or higher.
- The AS has been compiled in TIA Portal.

2 Procedure with WinCC Projects

2.1 Configure a New WinCC Project

1. Export the AS data from the TIA Portal project with the tool "SIEMENS SIMATIC SCADA Export":
   In the TIA Portal project, select the "Export to SIMATIC SCADA" item in the pop-up menu of the PLC.
2. If necessary, create the desired connection in the communication channel "SIMATIC S7-1200, S7-1500 Channel".
   Alternatively, select the connection that has already been created.
3. To import the exported AS data in the WinCC Tag Management, select the item "AS Symbol > Load from file" in the pop-up menu of the connection.
4. Select the desired data records to load.
   The available controller data is loaded.
   The necessary certificates are also transferred in the process.
5. Confirm the corresponding prompt with "Yes" to import the required certificates.
6. If the WinCC project was newly created, then configure the imported data in the WinCC project:
   - Tag Management
     Further information: "How to download AS symbols offline" (https://support.industry.siemens.com/cs/ww/en/view/109792611/114063933451)
   - Alarm Logging
     Further information: "Working with WinCC > Setting up a Message System > Working with AS Messages" (https://support.industry.siemens.com/cs/ww/en/view/109792641/138170927627)

2.2 Configure an Existing WinCC Project

1. Export the AS data from the TIA Portal project with the tool "SIEMENS SIMATIC SCADA Export":
   In the TIA Portal project, select the "Export to SIMATIC SCADA" item in the pop-up menu of the PLC.
2. Select the desired connection in the "SIMATIC S7-1200, S7-1500 Channel" communication channel.
3. To import the exported AS data in the WinCC Tag Management, select the item "AS Symbol > Load from file" in the pop-up menu of the connection.
4. Select the desired data records to load.
   The available controller data is loaded.
   The necessary certificates are also transferred in the process.
5. Confirm the corresponding prompt with "Yes" to import the required certificates.

3 Update Certificates

3.1 Certificate Expiration Date

If the certificates used have expired, the secure connection will continue.

The new certificates are used as soon as the connection is terminated and re-established.

However, to increase the security of your plant, you should update certificates as soon as the expiration date is reached.

3.2 Update Certificates in Runtime

You can manage the certificates without exiting Runtime. This allows you to renew or change the certificates on the controllers while the plant continues to run.

To do this, import the current certificates from the TIA Portal project using the "SIEMENS SIMATIC SCADA Export" tool.

The imported certificates are applied the next time you start the Runtime.

Note

Secure Communication and Runtime

A connection established via "Secure Communication" remains established until you terminate WinCC Runtime or disconnect the connection from the controller.

Even in the "CPU Stop" state, the secure connection remains active until the connection is re-established.

This allows you to update certificates independently in the WinCC project and on the controller. Updating the controller and terminating and restarting WinCC Runtime do not have to happen at the same time.

4 Change Connection

Even when using "Secure Communication", you can switch between the connections of the communication channel in WinCC Runtime.

You need a connection change, for example, when you exchange hardware or install hardware updates.

4.1 System Tags for Connection Change

For switching between connections, you create the required system tags in the Tag Management.

For each communication connection, you create system tags that contain the corresponding connection name:

- @<Connection name>@<System tag for connection change>

Table 4-1

Variable	Use	Value	Explanation
@<...>@ForceConnectionState	Establish / terminate connection in the communication channel	1 / 0	Behavior when activating Runtime: • Start value = 1: The connection is established. • Start value = 0: The connection remains disconnected. Data type: Unsigned 32-bit value Access: read / write
@<...>@AlternativeAddress	Alternative CPU connection	String	Properties of the alternative connection The tag must have a start value, for example: • AccessPoint=abc; IPAddress=111.111.111.111; The value can be changed subsequently. Data type: Text tag 8-bit font, length = 255 Access: read / write
@<...>@UseAlternativeAddress	Use alternative connection	1 / 0	Determines the connection currently in use: • 1: Alternative connection • 0: Connection to the original connection Data type: Unsigned 32-bit value Access: read / write

4.2 Example Scenario

Initial situation

- The WinCC project is in Runtime.
- The connection to the CPU "PLC1" is active.
- The system tag "@<PLC1>@AlternativeAddress" includes the valid address of the second CPU "PLC2".

Change connection

- The connection is deactivated:
  @<PLC1>@ForceConnectionState = 0
- The connection parameters are changed:
  @<PLC1>@UseAlternativeAddress = 1

The connection parameters from "@<PLC1>@AlternativeAddress" are applied.

- The connection is reactivated:
  @<PLC1>@ForceConnectionState = 1

WinCC establishes the alternative connection to the CPU "PLC2".

4.3 Requirements for Connection Change

A connection change depends on the installed firmware.

- CPUs with firmware lower than V2.9:
  Switching between two CPUs is possible if a firmware lower than V2.9 is used on both CPUs.
  The connection is always established without "Secure Communication".
- CPUs with firmware V2.9 and higher:
  Both CPUs must run firmware V2.9 or higher.

The possible combinations of the CPUs depend on the type of certificates installed on the CPUs:

Table 4-2

Original CPU	CPU after connection change *	Comments
"Self-Signed End Entity" certificate	Unknown "Self-Signed End Entity" certificate	Manual confirmation required ("Manual Trust")
	Unknown root certificate (CA) "End Entity" certificate	Import of the certificate data from the TIA Portal required
	Known root certificate (CA) "End Entity" certificate	Combination occurs for example if the root certificate has already been imported into WinCC.
Root certificate (CA) and "End Entity" certificate	Unknown "Self-Signed End Entity" certificate	Manual confirmation required ("Manual Trust")
	Unknown root certificate (CA) "End Entity" certificate	Import of the certificate data from the TIA Portal required
	Known root certificate (CA) "End Entity" certificate	Combination occurs for example if the root certificate has already been imported into WinCC.

*) You can also switch to a CPU that is configured with the same connection parameters as the original CPU.

5 Certificate Management: "Manual Trust" and Certificate Revocation List (CRL)

To manage the certificates, you use the Device Certificate Store folder in the following path:

- <Installation path>\Siemens\Automation\device-certificate-store
  Example: "C:\ProgramData\Siemens\Automation\device-certificate-store"

In the "Device Certificate Store" you can store certificate revocation lists and manually confirm or revoke certificates as trustworthy ("Manual Trust").

If the target CPU uses unknown certificates after a connection change, these certificates are stored in the "untrusted" folder.

- To confirm a certificate as trusted, move the corresponding "*.DER" file to the "trusted" folder.
- You can also subsequently move certificates that you want to revoke to the "untrusted" folder.

A certificate revocation list contains certificates that have been revoked. The ".DER" certificate revocation lists are located in the following folder:

- <Installation path>\Siemens\Automation\device-certificate-store\trusted\crl
  Example: "C:\ProgramData\Siemens\Automation\device-certificate-store\trusted\crl"

Note

Root certificate management

To use an "End Entity" certificate combined with a root certificate, you import the root certificate into WinCC. This makes the root certificate known and confirms it as trustworthy.
You cannot manage root certificates with the "Device Certificate Store".

- Further information about root certificates:

Industry Online Support STEP 7 (TIA Portal) - Documentation: Signatures and Certificates (https://support.industry.siemens.com/cs/ww/en/view/109798671/143786688779)