Hinweise zur sicheren PLC-Kommunikation mit TLS-Protokoll auf dem SIMATIC S7-1200/S7-1500 Kanal

WinCC V7.5 SP2 Update 4

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

Siemens Industry Online Support

Dieser Beitrag stammt aus dem Siemens Industry Online Support. Es gelten die dort genannten Nutzungsbedingungen (www.siemens.com/nutzungsbedingungen).

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter http://www.siemens.com/industrialsecurity.

Inhaltsverzeichnis

1 STEP 7 "Secure Communication"

WinCC unterstützt die sichere Kommunikation von STEP 7 über TLS-Protokoll, die mit TIA Portal ab V17 verfügbar ist.

STEP 7-Komponenten, für die "Secure Communication" projektiert ist, verwenden ein asymmetrisches Schlüsselverfahren mit öffentlichem Schlüssel (Public Key) und privatem Schlüssel (Private Key). Als Verschlüsselungsprotokoll wird TLS (Transport Layer Security) eingesetzt.

Bei Steuerungen, auf denen Firmware ≥ V2.9 läuft, wird grundsätzlich "Secure Communication" mit TLS für die Kommunikation in TIA Portal-Projekten ab V17 eingesetzt.

Um die "Secure Communication" von TIA Portal V17 im WinCC-Projekt einzusetzen, importieren Sie die Datensätze aus einem TIA Portal-Projekt mit den entsprechenden Einstellungen.

1.1 Verhalten in Runtime

Im laufenden Betrieb sind auch mit aktivierter "Secure Communication" die folgenden Aktionen möglich:

- Zertifikate aktualisieren
- Zwischen den projektierten Verbindungen des Kanals "SIMATIC S7-1200, S7-1500 Channel" wechseln

1.2 Weiterführende Informationen

- Industry Online Support: "WinCC V7 - Secure Communication" (ID 109798498) (https://support.industry.siemens.com/cs/ww/de/view/109798498)
- Industry Online Support: Download "SIMATIC SCADA Export für TIA Portal" (ID 109748955) (https://support.industry.siemens.com/cs/ww/de/view/109748955)
- Industry Online Support: Dokumentation "SIMATIC SCADA Export" (ID 101908495) (https://support.industry.siemens.com/cs/ww/de/view/101908495)
- Industry Online Support: Dokumentation zu 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: Fragen und Antworten zu den neuen Sicherheitsfunktionen in TIA Portal V17 (https://support.industry.siemens.com/cs/ww/de/view/109799540)
- TIA Portal Informationssystem (V17): "Geräte und Netze bearbeiten > Geräte und Netze konfigurieren > Netze konfigurieren > Secure Communication"

1.3 Voraussetzungen

- Sie verwenden eine Steuerung "S7-1500" mit Firmware ≥ V2.9, die mit TIA Portal ab V17 konfiguriert ist.
- Die AS wurde inTIA Portal übersetzt.

2 Vorgehen mit WinCC Projekten

2.1 Neues WinCC-Projekt konfigurieren

1. Exportieren Sie die AS-Daten aus dem TIA Portal-Projekt mit dem Tool "SIEMENS SIMATIC SCADA Export":
   Wählen Sie im TIA Portal-Projekt im Kontextmenü der SPS den Eintrag "Export nach SIMATIC SCADA".
2. Legen Sie gegebenenfalls im Kommunikationskanal "SIMATIC S7-1200, S7-1500 Channel" die gewünschte Verbindung an.
   Alternativ wählen Sie die bereits angelegte Verbindung.
3. Um die exportierten AS-Daten im WinCC Variablenhaushalt zu importieren, wählen Sie im Kontextmenü der Verbindung den Eintrag "AS Symbol > Laden aus Datei".
4. Wählen Sie die gewünschten Datensätze zum Laden.
   Die verfügbaren Daten der Steuerung werden geladen.
   Dabei werden auch die nötigen Zertifikate übertragen.
5. Um die benötigten Zertifikate zu importieren, bestätigen Sie die entsprechende Rückfrage mit "Ja".
6. Wenn das WinCC-Projekt neu angelegt wurde, dann konfigurieren Sie im WinCC-Projekt die importierten Daten:
   - Variablenhaushalt
     Weitere Informationen: "So laden Sie AS Symbole offline"
     (https://support.industry.siemens.com/cs/ww/de/view/109792611/114063933451)
   - Alarm Logging
     Weitere Informationen: "Arbeiten mit WinCC > Aufbau eines Meldesystems > Arbeiten mit AS Meldungen"
     (https://support.industry.siemens.com/cs/ww/de/view/109792641/138170927627)

2.2 Bestehendes WinCC-Projekt konfigurieren

1. Exportieren Sie die AS-Daten aus dem TIA Portal-Projekt mit dem Tool "SIEMENS SIMATIC SCADA Export":
   Wählen Sie im TIA Portal-Projekt im Kontextmenü der SPS den Eintrag "Export nach SIMATIC SCADA".
2. Wählen Sie im Kommunikationskanal "SIMATIC S7-1200, S7-1500 Channel" die gewünschte Verbindung.
3. Um die exportierten AS-Daten im WinCC Variablenhaushalt zu importieren, wählen Sie im Kontextmenü der Verbindung den Eintrag "AS Symbol > Laden aus Datei".
4. Wählen Sie die gewünschten Datensätze zum Laden.
   Die verfügbaren Daten der Steuerung werden geladen.
   Dabei werden auch die nötigen Zertifikate übertragen.
5. Um die benötigten Zertifikate zu importieren, bestätigen Sie die entsprechende Rückfrage mit "Ja".

3 Zertifikate aktualisieren

3.1 Ablaufdatum von Zertifikaten

Wenn die verwendeten Zertifikate abgelaufen sind, bleibt die sichere Verbindung weiterhin bestehen.

Die neuen Zertifikate werden verwendet, sobald die Verbindung beendet und neu aufgebaut wird.

Um die Sicherheit Ihrer Anlage zu erhöhen, aktualisieren Sie Zertifikate jedoch, sobald das Ablaufdatum erreicht ist.

3.2 Zertifikat in Runtime aktualisieren

Sie können die Zertifikate verwalten, ohne Runtime zu beenden. Damit können Sie die Zertifikate auf den Steuerungen erneuern oder ändern, während die Anlage weiter läuft.

Dafür importieren Sie die aktuellen Zertifikate aus dem TIA Portal-Projekt mit dem Tool "SIEMENS SIMATIC SCADA Export".

Beim nächsten Runtime-Start werden die importierten Zertifikate übernommen.

Hinweis **Secure Communication und Runtime**

Eine über "Secure Communication" aufgebaute Verbindung bleibt bestehen, bis Sie WinCC Runtime beenden oder die Verbindung von der Steuerung aus trennen.

Auch im Zustand "CPU Stop" bleibt die sichere Verbindung aktiv, bis die Verbindung neu aufgebaut wird.

Dadurch können Sie Zertifikate unabhängig voneinander im WinCC-Projekt und auf der Steuerung aktualisieren. Die Aktualisierung der Steuerung und das Beenden und Neustart von WinCC Runtime müssen nicht zeitgleich geschehen.

4 Verbindung wechseln ("Change Connection")

Auch beim Einsatz der "Secure Communication" können Sie in WinCC Runtime zwischen den Verbindungen des Kommunikationskanals wechseln.

Einen Verbindungswechsel benötigen Sie z. B., wenn Sie Hardware tauschen oder Hardware-Updates installieren.

4.1 Systemvariablen für Verbindungswechsel

Für das Wechseln zwischen Verbindungen legen Sie die benötigten Systemvariablen im Variablenhaushalt an.

Für jede Kommunikationsverbindung legen Sie jeweils Systemvariablen an, die den entsprechenden Verbindungsnamen enthalten:

- @<Verbindungsname>@<Systemvariable für Verbindungswechsel>

Tabelle 4-1

Variable	Verwendung	Wert	Erklärung
@<...>@ForceConnectionState	Verbindung im Kommunikations-kanal aufbauen / abbauen	1 / 0	Verhalten beim Aktivieren von Runtime: • Startwert = 1: Die Verbindung wird aufgebaut. • Startwert = 0: Die Verbindung bleibt deaktiviert. Datentyp: Vorzeichenloser 32-Bit Wert Zugriff: lesend / schreibend
@<...>@AlternativeAddress	Alternative CPU-Verbindung	String	Eigenschaften der alternativen Verbindung Die Variable muss einen Startwert haben, z. B.: • AccessPoint=abc; IPAddress=111.111.111.111; Der Wert kann nachträglich geändert werden. Datentyp: Textvariable 8-Bit Zeichensatz, Länge = 255 Zugriff: lesend / schreibend
@<...>@UseAlternativeAddress	Alternative Verbindung verwenden	1 / 0	Bestimmt die aktuell verwendete Verbindung: • 1: Alternative Verbindung • 0: Verbindung zur ursprünglichen Verbindung Datentyp: Vorzeichenloser 32-Bit Wert Zugriff: lesend / schreibend

4.2 Beispiel-Szenario

Ausgangssituation

- Das WinCC-Projekt ist in Runtime.
- Die Verbindung zur CPU "PLC1" ist aktiv.
- Die Systemvariable "@<PLC1>@AlternativeAddress" enthält die gültige Adresse der zweiten CPU "PLC2".

Verbindung wechseln

- Die Verbindung wird deaktiviert:
  @<PLC1>@ForceConnectionState = 0
- Die Verbindungsparameter werden geändert:
  @<PLC1>@UseAlternativeAddress = 1

Die Verbindungsparameter aus "@<PLC1>@AlternativeAddress" werden übernommen.

- Die Verbindung wird wieder aktiviert:
  @<PLC1>@ForceConnectionState = 1

WinCC baut die alternative Verbindung zur CPU "PLC2" auf.

4.3 Voraussetzungen für Verbindungswechsel

Ein Verbindungswechsel ist abhängig von der installierten Firmware.

- CPUs Firmware vor V2.9:
  Wechsel zwischen zwei CPUs ist möglich, wenn auf beiden CPUs eine Firmware kleiner V2.9 eingesetzt wird.
  Die Verbindung wird immer ohne "Secure Communication" aufgebaut.
- CPUs mit Firmware ab V2.9:
  Auf beiden CPUs muss eine Firmware größer oder gleich V2.9 laufen.

Die Kombinationsmöglichkeiten der CPUs sind abhängig von der Art der installierten Zertifikate auf den CPUs:

Tabelle 4-2

Ausgangs-CPU	CPU nach Verbindungswechsel *	Bemerkungen
"Self-Signed End-Entity"-Zertifikat	Unbekanntes "Self-Signed End-Entity"-Zertifikat	Manuelle Bestätigung nötig ("Manual Trust")
	Unbekanntes Root-Zertifikat (CA) "End-Entity"-Zertifikat	Import der Zertifikat-Daten aus dem TIA Portal nötig
	Bekanntes Root-Zertifikat (CA) "End-Entity"-Zertifikat	Kombination tritt z. B. auf, wenn das Root-Zertifikat bereits in WinCC importiert wurde.
Root-Zertifikat (CA) und "End-Entity"-Zertifikat	Unbekanntes "Self-Signed End-Entity"-Zertifikat	Manuelle Bestätigung nötig ("Manual Trust")
	Unbekanntes Root-Zertifikat (CA) "End-Entity"-Zertifikat	Import der Zertifikat-Daten aus dem TIA Portal nötig
	Bekanntes Root-Zertifikat (CA) "End-Entity"-Zertifikat	Kombination tritt z. B. auf, wenn das Root-Zertifikat bereits in WinCC importiert wurde.

*) Sie können auch auf eine CPU wechseln, die mit denselben Verbindungsparametern wie die Ausgangs-CPU konfiguriert ist.

5 Zertifikats-Management: "Manual Trust" und Zertifikatssperrlisten (CRL)

Zur Verwaltung der Zertifikate verwenden Sie den Ordner "Device Certificate Store" im folgenden Pfad:

- <Installationspfad>\Siemens\Automation\device-certificate-store
  Beispiel: "C:\ProgramData\Siemens\Automation\device-certificate-store"

Im "Device Certificate Store" können Sie Zertifikatssperrlisten hinterlegen, sowie Zertifikate manuell als vertrauenswürdig bestätigen oder ablehnen ("Manual Trust").

Wenn die Ziel-CPU nach einem Verbindungswechsel unbekannte Zertifikate verwendet, werden diese Zertifikate im Ordner "untrusted" abgelegt.

- Um ein Zertifikat als vertrauenswürdig zu bestätigen, verschieben Sie die entsprechende Datei "*.DER" in den Ordner "trusted".
- Zertifikate, die Sie ablehnen wollen, können Sie auch nachträglich in den Ordner "untrusted" verschieben.

Eine Zertifikatssperrliste enthält Zertifikate, die zurückgezogen wurden. Die Zertifikatssperrlisten "*.DER" liegen im folgenden Ordner:

- <Installationspfad>\Siemens\Automation\device-certificate-store\trusted\crl
  Beispiel: "C:\ProgramData\Siemens\Automation\device-certificate-store\trusted\crl"

Hinweis

Root-Zertifikate verwalten

Um ein "End-Entity"-Zertifikat mit einem Root-Zertifikat kombiniert zu verwenden, importieren Sie das Root-Zertifikat in WinCC. Damit ist das Root-Zertifikat bekannt und als vertrauenswürdig bestätigt.

Root-Zertifikate können Sie nicht mit dem "Device Certificate Store" verwalten.

- Weitere Informationen zu Root-Zertifikaten:

Industry Online Support: STEP 7 (TIA Portal) - Dokumentation: Signaturen und Zertifikate (https://support.industry.siemens.com/cs/ww/de/view/109798671/143786688779)