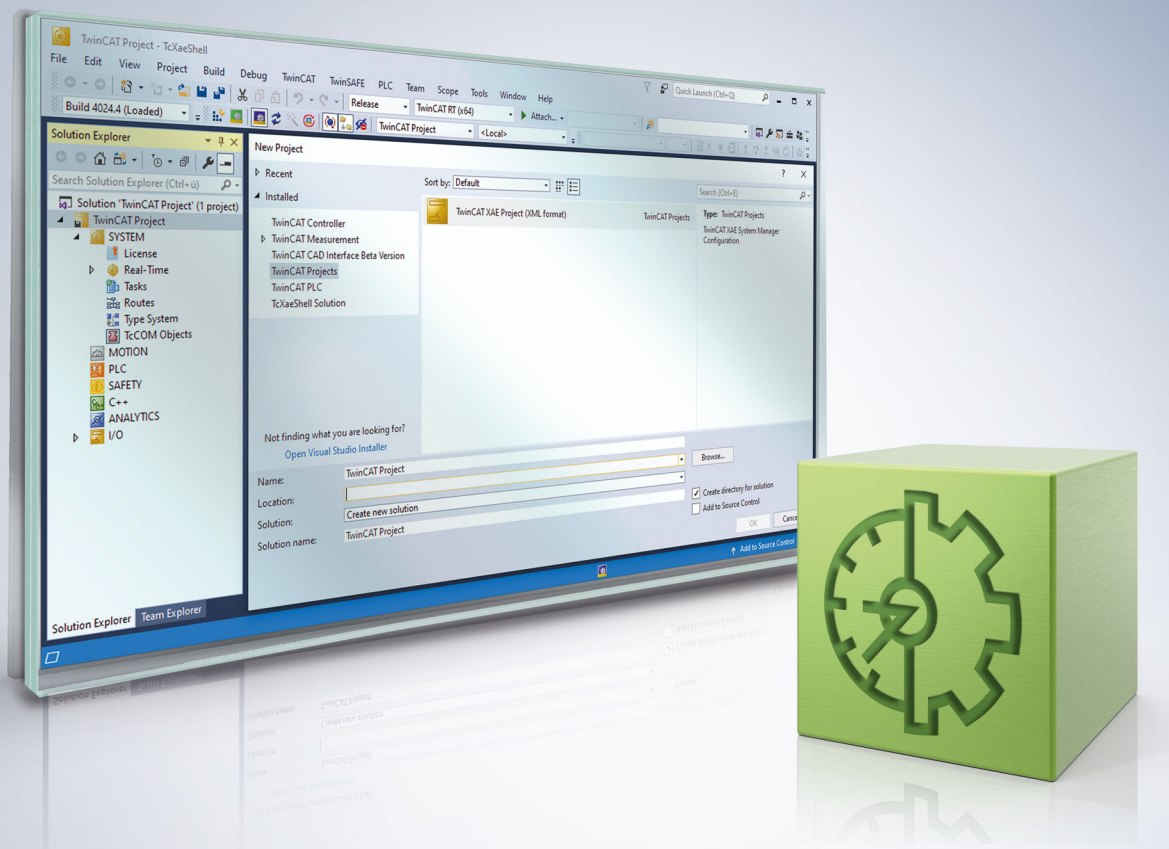
BECKHOFF New Automation Technology

Handbuch | DE

TE1000

TwinCAT 3 | Software Protection



16.05.2025 | Version: 1.17.7

Inhaltsverzeichnis

1 Vorwort 5
1.1 Hinweise zur Dokumentation 5
1.2 Zu Ihrer Sicherheit 6
1.3 Hinweise zur Informationssicherheit 7

2 Einführung 8
2.1 Allgemeine Systemvoraussetzungen 8
2.2 Die drei Säulen des Softwarezugriffschutzes 9
2.3 Benutzerdatenbank als zentrale Schaltstelle 9
2.4 Software-Protection-Konfigurator 11

3 Schnelleinstieg 13
3.1 Regelung des Zugriffs auf den PLC-Quellcode 13
3.2 OEM-Lizenzen: Schutz gegen unberechtigte Benutzung von Software-Funktionen 14

4 TwinCAT-OEM-Zertifikate 19
4.1 Erstellung des "OEM Certificate Request Files" 22
4.2 File Fingerprint der OEM-Zertifikatsdatei ermitteln 27
4.3 OEM-Zertifikat beantragen 28
4.4 OEM-Zertifikat installieren 30
4.5 OEM-Zertifikat verlängern 31
4.6 Update eines bestehenden OEM-Zertifikats? 31

5 Benutzerdatenbanken (User DBs) 33
5.1 Benutzerdatenbank anlegen 33
5.2 Standardeinstellungen für die Benutzerdatenbank in Visual Studio festlegen 38
5.3 Aktuelle Benutzerdatenbank in Visual Studio auswählen 39
5.4 Standard-Benutzer in der Benutzerdatenbank 41
5.5 Extensions für Benutzerdatenbanken 41
5.5.1 Zugehörige Elemente in der Konfigurationskonsole der Software Protection 43
5.5.2 Anlegen von Extensions und Benutzern im TwinCAT 3 Engineering 45
5.6 Benutzerdatenbank erweitern 50
5.6.1 Hinzufügen/Ändern von Datenbank-Administratoren 50
5.6.2 Trennung der Funktionen Datenbank-Administrator und Entwickler 54
5.6.3 Hinzufügen von Benutzern zu einer Gruppe 55
5.6.4 Eigene Gruppenzugriffsberechtigungen definieren 57
5.7 Benutzerdatenbank mit Projekt verbinden 70
5.8 Benutzerzugriffsberechtigungen im Projekt zuweisen 71
5.9 Distribution / Austausch von Benutzerdatenbanken 73

6 Einloggen / Auswahl eines Benutzerkontos 74
6.1 Build 4022 74

7 Grundschutz der PLC-Anwendungssoftware einrichten 76
7.1 Verschlüsselung 76
7.1.1 PLC-Quellcode verschlüsseln 77
7.1.2 Projektdatei verschlüsseln 77
7.1.3 Boot-Projekt verschlüsseln 78
7.1.4 Anzeige des Objektschutzstatus 79

7.1.5 Anzeige der aktuellen Verschlüsselungsversion ... 80
7.2 Dateien signieren (Schutz gegen unautorisierte Änderungen) ... 81
7.3 Übersicht der Softwareschutz-Einstellungen des PLC-Projektes anzeigen ... 82
8 Eigene OEM-Lizenzen ausstellen und nutzen ... 84
8.1 OEM-Applikationslizenzen erstellen ... 85
8.1.1 Vorbereitung des TwinCAT 3 Engineering ... 86
8.1.2 Lizenzbeschreibungsdatei für eine OEM-Applikationslizenz erstellen ... 86
8.1.3 License Request Files für eine OEM-Applikationslizenz erstellen ... 89
8.1.4 License Response Files für eine OEM-Applikationslizenz erstellen ... 90
8.1.5 License Response Files für eine OEM-Applikationslizenz importieren ... 92
8.2 OEM-Applikationslizenzen auf einem Dongle ablegen ... 92
8.3 OEM-Applikationslizenz in einer SPS-Applikation abfragen ... 93
8.4 OEM SPS-Libraries mit einem Lizenzschutz versehen ... 97
9 Anwendung gegen Klonen schützen ... 98
10 Support und Service ... 99

1 Vorwort

1.1 Hinweise zur Dokumentation

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist.
Zur Installation und Inbetriebnahme der Komponenten ist die Beachtung der Dokumentation und der nachfolgenden Hinweise und Erklärungen unbedingt notwendig.
Das Fachpersonal ist verpflichtet, stets die aktuell gültige Dokumentation zu verwenden.

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbaren Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

Disclaimer

Diese Dokumentation wurde sorgfältig erstellt. Die beschriebenen Produkte werden jedoch ständig weiterentwickelt.
Wir behalten uns das Recht vor, die Dokumentation jederzeit und ohne Ankündigung zu überarbeiten und zu ändern.
Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte geltend gemacht werden.

Marken

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® und XTS® sind eingetragene und lizenzierte Marken der Beckhoff Automation GmbH.
Die Verwendung anderer in dieser Dokumentation enthaltenen Marken oder Kennzeichen durch Dritte kann zu einer Verletzung von Rechten der Inhaber der entsprechenden Kennzeichnungen führen.

EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.

Copyright

Fremdmarken

In dieser Dokumentation können Marken Dritter verwendet werden. Die zugehörigen Markenvermerke finden Sie unter: https://www.beckhoff.com/trademarks.

1.2 Zu Ihrer Sicherheit

Sicherheitsbestimmungen

Lesen Sie die folgenden Erklärungen zu Ihrer Sicherheit.
Beachten und befolgen Sie stets produktspezifische Sicherheitshinweise, die Sie gegebenenfalls an den entsprechenden Stellen in diesem Dokument vorfinden.

Haftungsausschluss

Die gesamten Komponenten werden je nach Anwendungsbestimmungen in bestimmten Hard- und Software-Konfigurationen ausgeliefert. Änderungen der Hard- oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen, sind unzulässig und bewirken den Haftungsausschluss der Beckhoff Automation GmbH & Co. KG.

Qualifikation des Personals

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs-, Automatisierungs- und Antriebstechnik, das mit den geltenden Normen vertraut ist.

Signalwörter

Im Folgenden werden die Signalwörter eingeordnet, die in der Dokumentation verwendet werden. Um Personen- und Sachschäden zu vermeiden, lesen und befolgen Sie die Sicherheits- und Warnhinweise.

Warnungen vor Personenschäden

⚠ GEFAHR

Es besteht eine Gefährdung mit hohem Risikograd, die den Tod oder eine schwere Verletzung zur Folge hat.

⚠ WARNUNG

Es besteht eine Gefährdung mit mittlerem Risikograd, die den Tod oder eine schwere Verletzung zur Folge haben kann.

⚠ VORSICHT

Es besteht eine Gefährdung mit geringem Risikograd, die eine mittelschwere oder leichte Verletzung zur Folge haben kann.

Warnung vor Umwelt- oder Sachschäden

HINWEIS

Es besteht eine mögliche Schädigung für Umwelt, Geräte oder Daten.

Information zum Umgang mit dem Produkt

Diese Information beinhaltet z. B.:
Handlungsempfehlungen, Hilfestellungen oder weiterführende Informationen zum Produkt.

1.3 Hinweise zur Informationssicherheit

Die Produkte der Beckhoff Automation GmbH & Co. KG (Beckhoff) sind, sofern sie online zu erreichen sind, mit Security-Funktionen ausgestattet, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Trotz der Security-Funktionen sind die Erstellung, Implementierung und ständige Aktualisierung eines ganzheitlichen Security-Konzepts für den Betrieb notwendig, um die jeweilige Anlage, das System, die Maschine und die Netzwerke gegen Cyber-Bedrohungen zu schützen. Die von Beckhoff verkauften Produkte bilden dabei nur einen Teil des gesamtheitlichen Security-Konzepts. Der Kunde ist dafür verantwortlich, dass unbefugte Zugriffe durch Dritte auf seine Anlagen, Systeme, Maschinen und Netzwerke verhindert werden. Letztere sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn entsprechende Schutzmaßnahmen eingerichtet wurden.

Zusätzlich sollten die Empfehlungen von Beckhoff zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Informationssicherheit und Industrial Security finden Sie in unserem https://www.beckhoff.de/secguide.

Die Produkte und Lösungen von Beckhoff werden ständig weiterentwickelt. Dies betrifft auch die Security-Funktionen. Aufgrund der stetigen Weiterentwicklung empfiehlt Beckhoff ausdrücklich, die Produkte ständig auf dem aktuellen Stand zu halten und nach Bereitstellung von Updates diese auf die Produkte aufzuspielen. Die Verwendung veralteter oder nicht mehr unterstützter Produktversionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Hinweise zur Informationssicherheit zu Produkten von Beckhoff informiert zu sein, abonnieren Sie den RSS Feed unter https://www.beckhoff.de/secinfo.

2 Einführung

Das TwinCAT 3 Engineering ist mit verschiedenen Funktionen zum Schutz der PLC-Anwendungssoftware ausgestattet:

- Konfigurierbare Zugangsbeschränkungen zum PLC-Quellcode durch die Definition von Benutzergruppen und die Zuweisung von Zugriffsleveln („Object Protection Level“)
- Know-How-Schutz durch Verschlüsselung von PLC-Quellcode und Boot-Datei
- Klonschutz durch den Einsatz der TwinCAT-3-Lizenztechnologie für die OEM-Anwendungssoftware (erfordert einen Beckhoff IPC/EPC oder TwinCAT-3-Dongle)

Durch die Nutzung der TwinCAT-3-Lizenztechnologie kann der OEM zudem selbst Lizenzen für Funktionserweiterungen seiner Anwendungssoftware generieren und diese vermarkten (erfordert einen Beckhoff IPC/EPC oder TwinCAT-3-Dongle).

Diese Funktionen stehen aktuell nur für den PLC-Bereich von TwinCAT 3 zur Verfügung.

Um die Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist ein von Beckhoff signiertes OEM-Zertifikat erforderlich. Details dazu finden Sie im Kapitel TwinCAT-OEM-Zertifikate [▶ 19].

Zentrale Schaltstelle des Zugriffschutzes bildet eine Benutzerdatenbank.

Inhalte

Einführung [▶ 8]	In diesem Abschnitt werden allgemeine Informationen zu den Systemvoraussetzungen, dem Softwarezugriffschutz, der Benutzerdatenbank und dem Software-Protection-Konfigurator gegeben.
Schnelleinstieg [▶ 13]	Dieser Abschnitt ermöglicht Ihnen einen Schnelleinstieg in die beiden wichtigsten Themen: - Regelung des Zugriffs auf den Quellcode - Schutz gegen unberechtigte Nutzung von Software-Funktionen mit eigenen Lizenzen
TwinCAT-OEM-Zertifikate [▶ 19]	In diesem Abschnitt wird beschrieben, wie Sie das zum Schutz von Anwendungssoftware notwendige OEM-Zertifikat beantragen, installieren und verlängern.
Benutzerdatenbanken (User DBs) [▶ 33]	In diesem Abschnitt wird beschrieben, wie Sie Benutzerdatenbanken anlegen und mit dem Projekt verbinden.
Grundschutz der PLC-Anwendungssoftware einrichten [▶ 76]	In diesem Abschnitt wird beschrieben, wie Sie die OEM-Anwendungssoftware schützen. Insbesondere werden die Themen Benutzerzugriffsberechtigungen, Verschlüsselung, Signierung, OEM-Applikationslizenzen detailliert erläutert.

2.1 Allgemeine Systemvoraussetzungen

Betriebssystem:

- Um alle Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist mindestens Windows 10 erforderlich.
- Anmerkung: Windows CE (Windows Embedded Compact) unterstützt weder die Verschlüsselung der Boot-Datei noch OEM-Lizenzen.

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

2.2 Die drei Säulen des Softwarezugriffschutzes

Die drei Säulen des Softwarezugriffschutzes sind:

- Verschlüsselung *(= nicht mehr lesbar*)
- Signierung *(= nicht mehr austauschbar)*
- Zuweisung von Zugriffsrechten (-> „Object Protection Level [▶ 71]“)

Der Schutz eines Projekts vor unbefugtem Zugriff umfasst daher folgende Maßnahmen:

- Verschlüsselung und Signierung der Projektkomponenten
- Festlegen der Zugriffsrechte auf die Projektkomponenten
- **Wichtig: Verschlüsselung und Signierung der zugehörigen Projektdatei**

Die Verschlüsselung ohne Einstellung des korrekten Zugriffslevels schützt zwar die entsprechende Datei auf Betriebssystemebene, würde aber weiterhin einen Zugriff über das TwinCAT 3 Engineering zulassen.

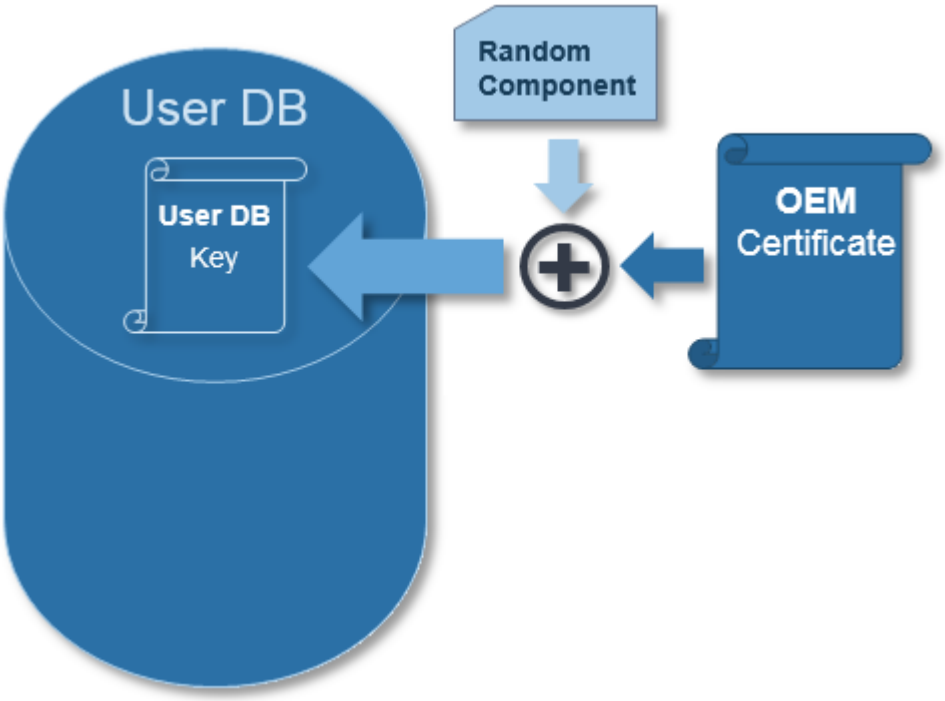
Umgekehrt würde die Einstellung eines korrekten Zugriffslevels zwar den Zugriff innerhalb des TwinCAT 3 Engineerings festlegen, aber ein Zugriff auf den Quellcode über die Betriebssystemebene wäre weiterhin möglich.

Ohne Signatur könnte eine Projektdatei oder eine Projektkomponente gegen eine andere Datei mit gleichem Namen ausgetauscht werden.

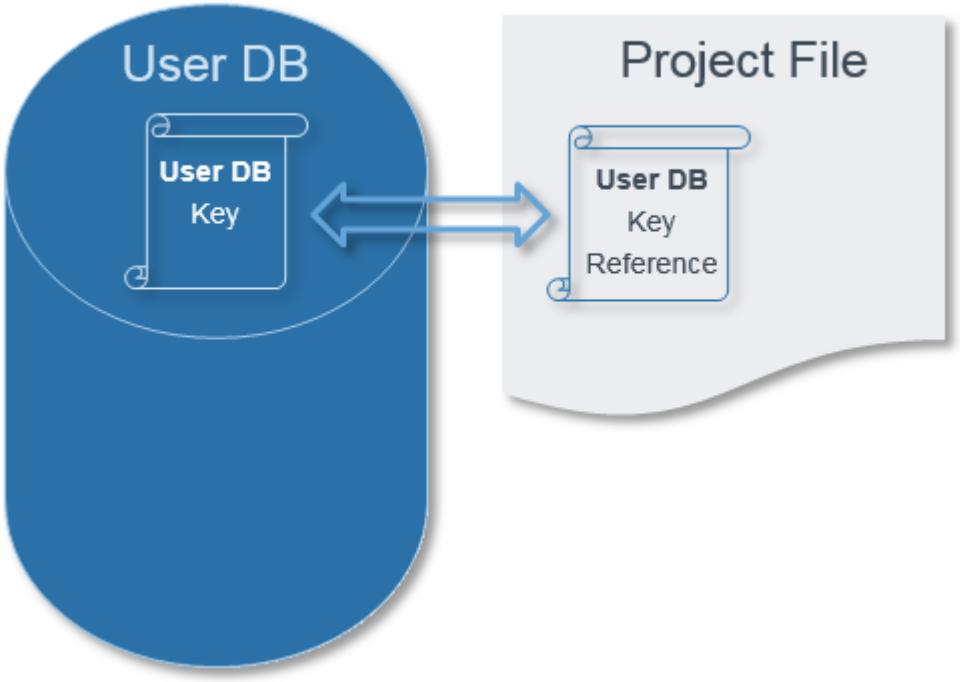
2.3 Benutzerdatenbank als zentrale Schaltstelle

Der Zugriff auf die PLC-Projektkomponenten wird über eine Benutzerdatenbank (User DB) [▶ 33] geregelt.

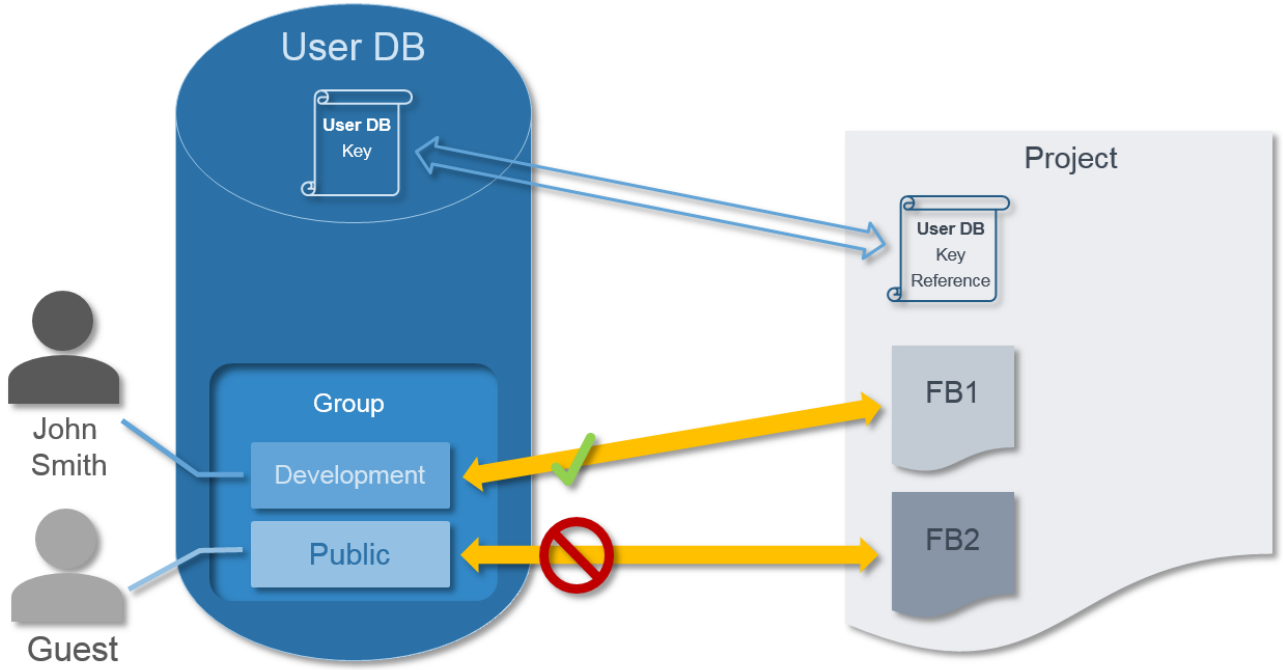
Der Inhalt der Datenbank wird über eine Signierung durch den Administrator gegen unautorisierte Änderungen geschützt. Zur eindeutigen Identifizierung der Datenbank enthält diese einen sogenannten „User DB Key“, eine eindeutige Kennung, die sich aus Komponenten des OEM-Zertifikates und einer Zufallskomponente zusammensetzt. Über die Zufallskomponente wird sichergestellt, dass jede erzeugte User DB einen eineindeutigen User DB Key erhält.



Wenn ein Projekt von einem autorisierten Anwender mit einer spezifischen User DB verknüpft wird, wird in dem Projekt deren User DB Key hinterlegt. Dieses Projekt kann danach nur noch in Verbindung mit dieser User DB geöffnet werden.



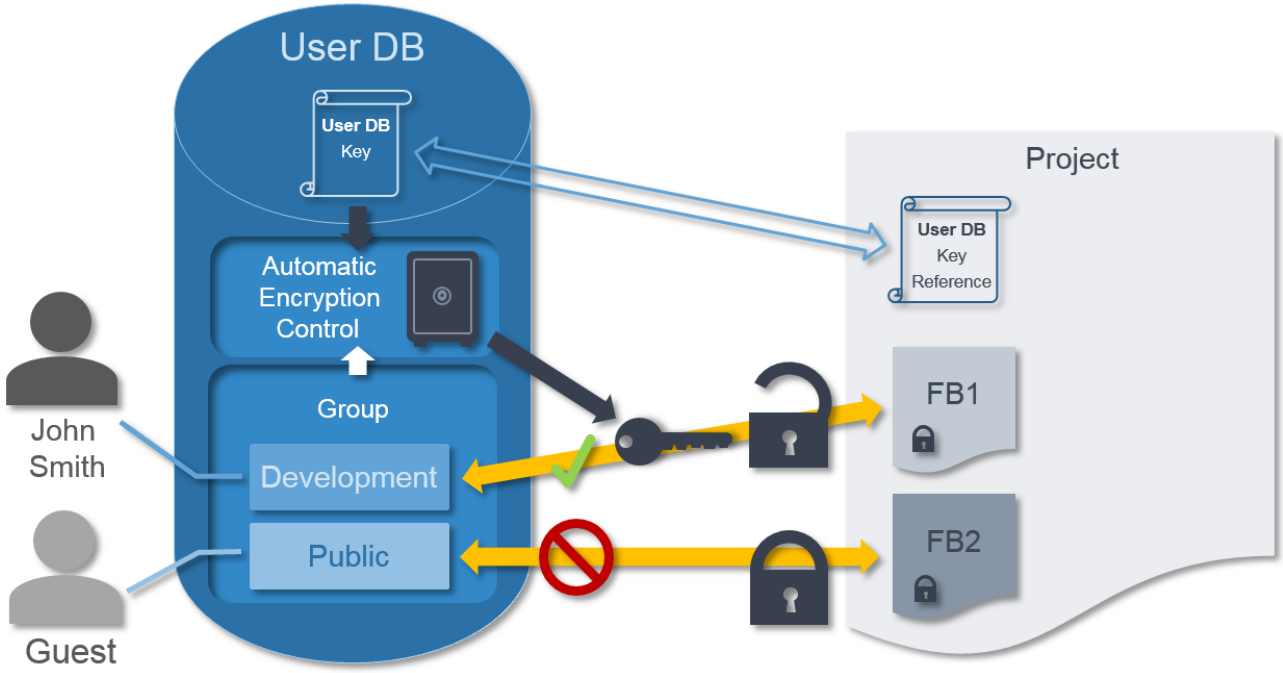
Die Einführung [▶ 57] eines Benutzers werden innerhalb der User DB über Gruppen geregelt.



Damit sind zunächst die Zugriffsrechte innerhalb des TwinCAT 3 Engineering festgelegt. Über die Betriebssystemebene wäre aber weiterhin ein Zugriff auf den PLC-Quellcode oder ein Austausch von Projektdateien möglich. Daher gibt es neben der Regelung der Zugriffsrechte zwei weitere Schutzmaßnahmen im TwinCAT 3 Engineering: die Signierung und Verschlüsselung der Projektdatei.

Mit der Signierung der Projektdatei wird sichergestellt, dass die Projektdatei nicht gegen eine andere Datei gleichen Namens auf Betriebssystemebene ausgetauscht werden kann. Die Signaturdaten der Datei werden im überlagerten Projektknoten gespeichert. Das Projekt muss mit der Benutzerdatenbank verbunden sein.

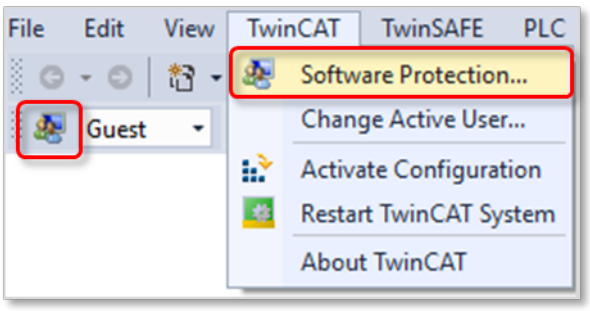
Der für die Verschlüsselung der Projektdatei verwendete Schlüssel ist in der Benutzerdatenbank gesichert. Die zugehörige Benutzerdatenbank muss daher immer auf dem **Engineering-Rechner** vorhanden sein (Verzeichnis: *c:\Twincat\3.1\CustomConfig\userDBs*).



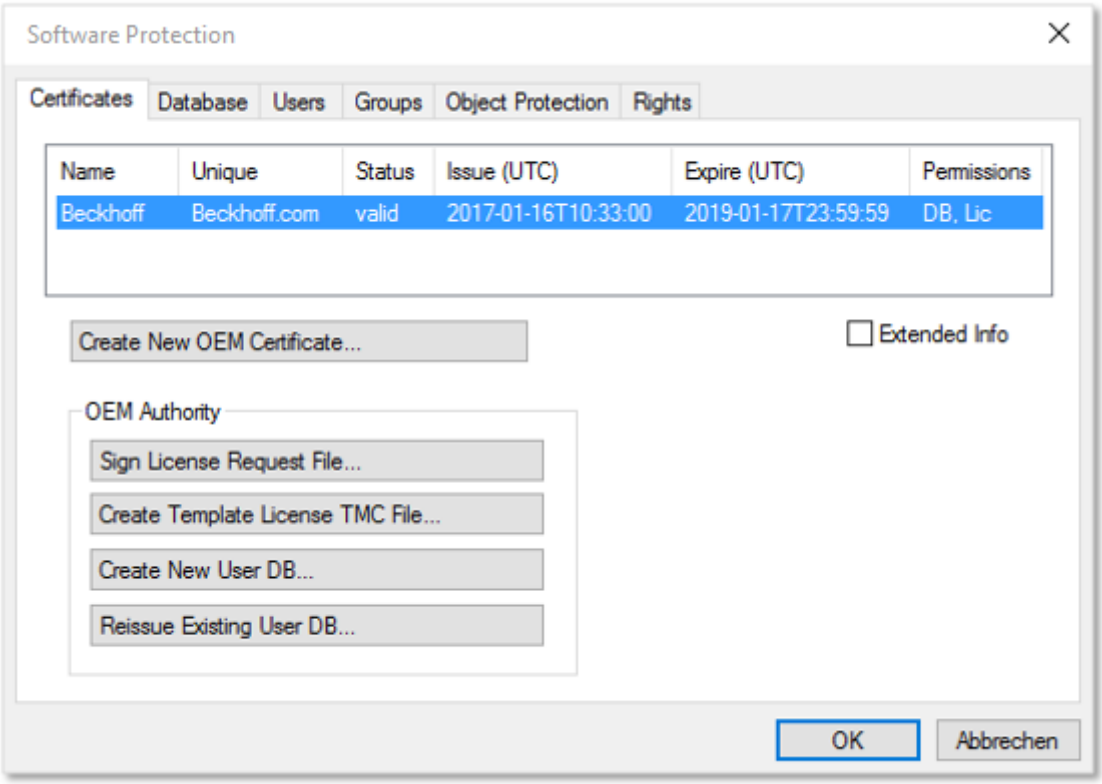
2.4 Software-Protection-Konfigurator

Zur Konfiguration der generellen Software-Protection-Funktionen steht Ihnen ein zentraler Konfigurator zur Verfügung.

Um den Konfigurator **Software Protection** aufzurufen, wählen Sie im Menü **TwinCAT** den Befehl **Software Protection** oder klicken Sie in der Symbolleiste **TwinCAT XAE Software Protection** auf die zugehörige Schaltfläche. Um die Symbolleiste der Benutzeroberfläche hinzuzufügen, aktivieren Sie diese im Menü **Ansicht > Toolbars**.



In dem sich öffnenden Konfigurator können Sie den Schutz der Anwendungssoftware konfigurieren.



Hinweise zur Konfiguration finden Sie in den folgenden Abschnitten:

- TwinCAT-OEM-Zertifikate [▶ 19]
- Benutzerdatenbanken (User DBs) [▶ 33]
- Grundschutz der PLC-Anwendungssoftware einrichten [▶ 76]

3 Schnelleinstieg

3.1 Regelung des Zugriffs auf den PLC-Quellcode

TwinCAT 3 bietet ab der Version Build 4024 die Möglichkeit, PLC-Quellcode zu verschlüsseln und den Zugriff auf den PLC-Quellcode über ein Rechte-Management zu regeln. Zentrales Element ist eine Benutzerdatenbank (User DB), die unter Einbezug des OEM-Zertifikats (als Verifizierungsbasis) erstellt wird.

Anmerkung: Das OEM-Zertifikat ist nur für die Erstellung der Benutzerdatenbank erforderlich, nicht für deren Nutzung oder Modifikation.

Voraussetzung für die Nutzung dieser Funktion: Ausstellung eines TwinCAT OEM Zertifikates [▶ 19]

Systemvoraussetzungen

- TwinCAT 3 OEM-Zertifikat TC0007 (Crypto-Version 1 oder 2)
- Betriebssystem: mind. Windows 10
- TwinCAT-Version: mind. TwinCAT 3.1 Build 4024

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

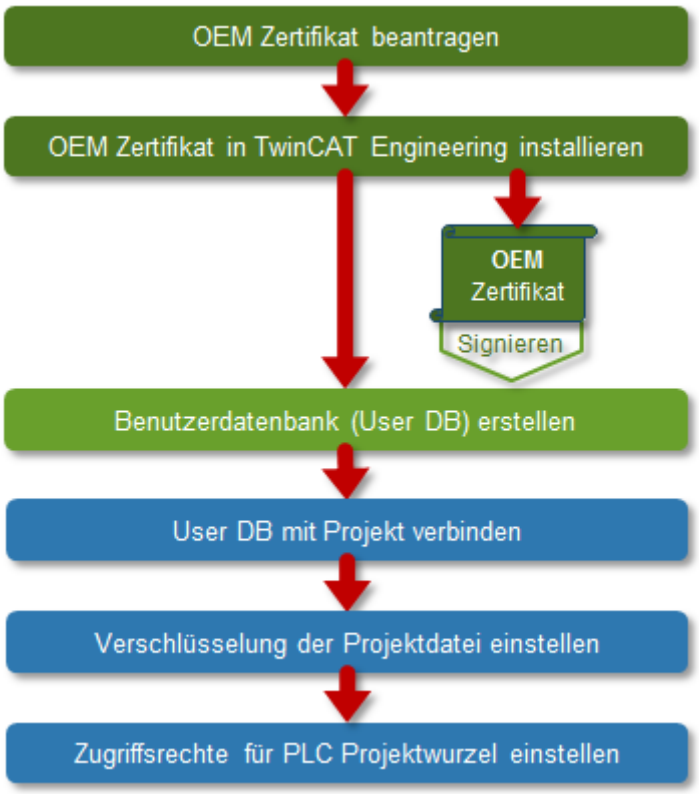
Allgemeine Hinweise

- Beachten Sie die generellen Informationen zu OEM-Zertifikaten.
- Das OEM-Zertifikat wird nur einmalig zum Erstellen der User DB benötigt.
- Änderungen der User DB müssen danach lediglich vom Admin der User DB signiert werden (ohne Einsatz des OEM-Zertifikats).
- Der Administrator der User DB muss unbedingt ein starkes Passwort haben. Ansonsten ist die User DB leicht angreifbar.
- Die Gültigkeit der User DB ist unabhängig von der Gültigkeitsdauer des OEM-Zertifikates. Die User DB bleibt also auch nach Ablauf der Gültigkeitsdauer des OEM-Zertifikats gültig und kann auch danach noch modifiziert werden.
- Anmerkungen zur späteren Verlängerung des Zertifikats (nach 2 Jahren) finden Sie hier OEM-Zertifikat verlängern [▶ 31].
- **Wichtig:** Hinterlegen Sie das Passwort des OEM-Zertifikats und des Administrators der User DB an einer sicheren Stelle. Beckhoff kann die Passwörter bei Verlust nicht wiederherstellen!
- Das OEM-Zertifikat ist nicht auf den Zielsystemen erforderlich und sollte dort aus Sicherheitsgründen nicht gespeichert werden!

Vorgehensweise

Der folgende Ablauf beschreibt den einfachsten Fall:

- Es gibt einen Benutzer („Admin“), der vollen Zugriff auf das Projekt hat
- Alle anderen („Guest“) dürfen das Projekt weder ansehen noch verändern.
- Der Admin authentifiziert sich über ein (sicheres!) Passwort



Links zur Dokumentation

1. OEM-Zertifikat beantragen [▶ 28] (bestellen)
2. OEM-Zertifikat installieren [▶ 30]
3. Benutzerdatenbank erstellen [▶ 33]
   Für den einfachsten Standardfall müssen sie lediglich den Namen des Administrators und sein Passwort definieren und keine weiteren Einstellungen (z. B. kein Anlegen weiterer Benutzer) in der User DB vornehmen.
4. Benutzerdatenbank mit Projekt verbinden [▶ 70]
5. Verschlüsselung der Projektdatei einstellen [▶ 77]
6. Zugriffsrechte für PLC Projektwurzel einstellen [▶ 71]

3.2 OEM-Lizenzen: Schutz gegen unberechtigte Benutzung von Software-Funktionen

Mit Hilfe der TwinCAT 3 Lizenztechnologie kann eine SPS-Anwendung durch Bindung an eine Hardware (Beckhoff IPC oder TwinCAT-Dongle) vor unberechtigter Benutzung/Klonen geschützt werden. Mit der gleichen Lizenztechnik können auch Zusatzfunktionalitäten der SPS-Anwendung für Endkunden freigeschaltet werden.

Voraussetzung für die Nutzung dieser Funktion: Ausstellung eines TwinCAT OEM Zertifikates [▶ 19]

Systemvoraussetzungen

- TwinCAT 3-OEM-Zertifikat
  (nur für das **Erstellen** eines Lizenztyps und der **Signierung** von Lizenzdateien, nicht für die **Nutzung** einer OEM-Lizenz)
- Betriebssystem: mind. Windows 10
  (Windows CE / Windows Embedded Compact wird nicht unterstützt!)
- Beckhoff IPC oder TwinCAT 3 Lizenzdongle
- TwinCAT-Version: Mind. TwinCAT 3.1 Build 4024

- TC3 PLC Lib Tc2_Utilities v3.3.24 (oder höher)

Hinweis: Eine User DB ist für die Nutzung von OEM-Lizenzen nicht erforderlich.

Sicherer Schutz nur bei Verwendung von Beckhoff IPC oder TwinCAT Lizenzdongle

Verwenden Sie für einen sicheren Schutz unbedingt einen Beckhoff IPC oder einen TwinCAT 3 Lizenzdongle. Der Einsatz von OEM-Lizenzen auf Nicht-Beckhoff-Rechnern ohne TwinCAT 3 Lizenzdongle wird nicht unterstützt und ist unsicher!

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

Allgemeine Hinweise

Nutzung von OEM-Lizenzen = Bootprojekt verschlüsseln!

Denken Sie daran, dass die per FB_CheckLicense [▶ 93] abgefragte License-ID [▶ 86] im Binärcode mit einem Hex-Editor leicht gefunden und (mit einem gewissen Aufwand) manipuliert werden kann. Arbeiten Sie daher unbedingt mit einer Verschlüsselung des Bootprojektes [▶ 78] (am sichersten), oder verschleiern Sie zumindest die abgefragte License-ID im Quellcode bestmöglich.

- Für die Anwendungslizenzierung ist keine Benutzerdatenbank erforderlich.
- Die Lizenzvalidierung erfolgt durch die TwinCAT-3-Runtime (XAR). Die TwinCAT-3-Runtime muss also auf dem IPC installiert sein.
- Die Gültigkeit der Anwendungslizenz ist unabhängig von der Gültigkeitsdauer des OEM-Zertifikates. Die Anwendungslizenz bleibt also auch nach Ablauf der Gültigkeitsdauer des OEM-Zertifikates gültig.
- Die Nutzung von OEM-Applikationslizenzen erfordert immer einen TwinCAT-3-Dongle oder einen Beckhoff IPC.
- Bei IPCs mit einem Plattform-Level >= 90 (Nicht-Beckhoff-IPCs) muss aus Sicherheitsgründen immer ein TwinCAT-3-Dongle als „License Device“ verwendet werden!

Typische Anwendungsfälle

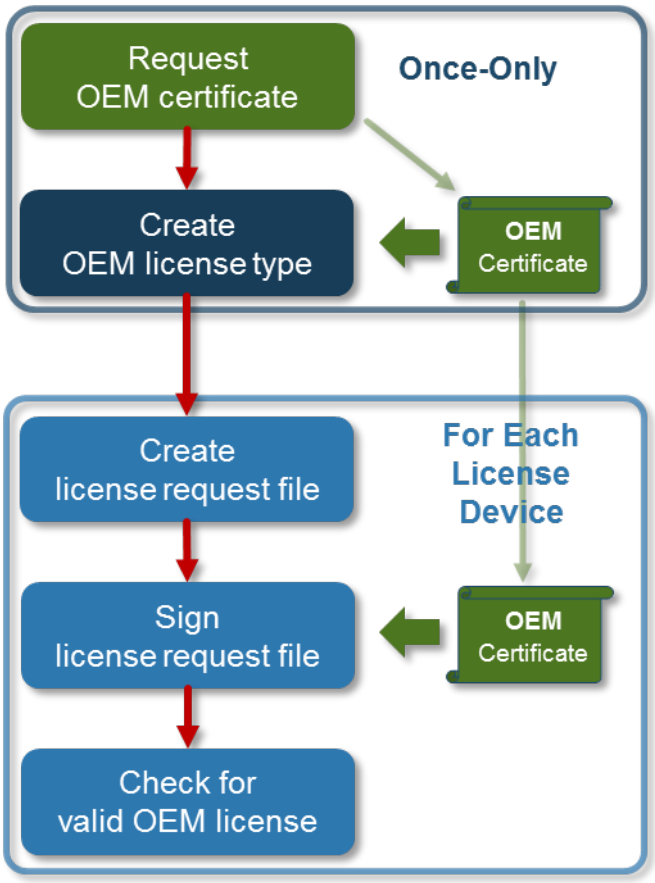
- Die Anwendung soll durch Binden an eine Hardware (TwinCAT-3-Dongle oder Beckhoff IPC) gegen Klonen geschützt werden.
- In der Anwendung sollen bestimmte Zusatzfunktionen durch eine zugehörige Lizenz freigeschaltet werden.

Ablauf

Zunächst muss das TwinCAT 3 Engineering für die Erzeugung von Anwendungslizenzen konfiguriert werden. Sie benötigen dazu u. a. ein kleines Tool, das nicht Bestandteil des serienmäßigen Auslieferungsumfangs des TwinCAT 3 Engineerings ist.

Wie Sie das TwinCAT 3 Engineering für Anwendungslizenzen vorbereiten, wird im Abschnitt Vorbereitung des TwinCAT 3 Engineering [▶ 86] beschrieben.

In der folgenden Grafik ist der prinzipielle Ablauf der Lizenzierung dargestellt:



Request OEM certificate

Basis für die Lizenzierung ist ein von Beckhoff signiertes OEM-Zertifikat, mit dem das Ausstellen der Lizenzen erfolgt (durch Signierung des License Request Files).

Wie Sie dieses Zertifikat beantragen und installieren, wird im Abschnitt Erstellung des "OEM Certificate Request Files" [▶ 22] beschrieben.

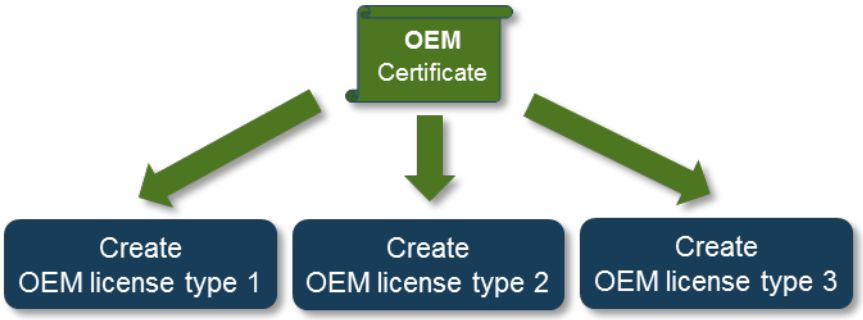
Verwenden Sie unbedingt ein starkes Passwort für Ihr OEM-Zertifikat!

Create OEM license type

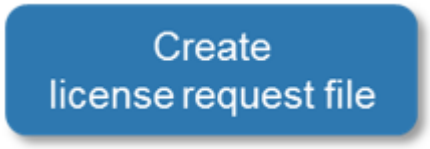
Mithilfe von Daten (OEM GUID) aus dem OEM-Zertifikat wird eine Beschreibungsdatei für einen Lizenztyp erzeugt. Diese Lizenzbeschreibungsdatei ist die Basis für die Erstellung eines „License Request Files“ (siehe nachfolgender Schritt).

Wie Sie die Lizenzbeschreibungsdatei erzeugen, wird im Abschnitt Lizenzbeschreibungsdatei für eine OEM-Applikationslizenz erstellen [▶ 86] beschrieben.

Mit einem OEM-Zertifikat kann eine beliebige Anzahl an Lizenzbeschreibungsdateien erzeugt werden:



Create license request file



Nun können Sie für ein spezifisches „License Device“ (TwinCAT-3-Dongle oder Beckhoff IPC) eine „License Request File“ erzeugen.

Wie Sie die Datei erzeugen, wird im Abschnitt License Request Files für eine OEM-Applikationslizenz erstellen [▶ 89] beschrieben.

Anwendungslizenzen für einen Nicht-Beckhoff-IPC (Plattform-Level 90 oder größer) erfordern aus Sicherheitsgründen immer einen TwinCAT-3-Dongle!

Sign license request file

Das erzeugte „License Request File“ muss mit dem OEM-Zertifikat signiert werden und wird dadurch zum „License Response File“. Dieses ist die eigentliche Lizenzdatei, die an das spezifische Gerät gebunden ist, das beim Erstellen das „License Request File“ angegeben wurde.

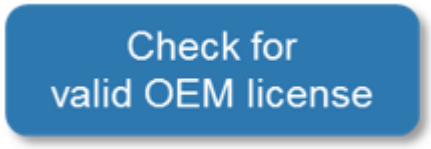
Wie Sie das „License Request File“ mit dem OEM-Zertifikat signieren, wird im Abschnitt Manuelle Erstellung über das TwinCAT Engineering [▶ 90] beschrieben.

Anschließend muss die erzeugte Lizenzdatei auf dem „License Device“ (TwinCAT-3-Dongle oder Beckhoff IPC) zur Verfügung gestellt werden (siehe License Response Files für eine OEM-Applikationslizenz importieren [▶ 92]).

Ab TwinCAT 3 Build 4022.16 steht die TwinCAT 3 PLC-Bibliothek Tc2_Utilities in der Version 3.3.24 zur Verfügung, die verschiedene Funktionsbausteine zum Lizenzhandling bietet. Sie umfasst unter anderem Funktionsbausteine, mit deren Hilfe Lizenzdateien direkt in einer SPS-Anwendung auf einem TwinCAT-3-Dongle abgelegt oder von diesem heruntergeladen werden können. (Siehe Dokumentation TwinCAT 3 PLC-Bibliothek Tc2 Utilities)

Die erforderliche TwinCAT 3 PLC-Bibliothek Tc2_Utilities können Sie herunterladen: https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/5299845387.zip

Check for valid OEM license



Die TwinCAT-3-Runtime überprüft beim Start (und während der Laufzeit), ob die Anwendungslizenz gültig ist. Das Ergebnis dieser Überprüfung können Sie mit dem SPS-Funktionsbaustein FB_CheckLicense abfragen (siehe OEM-Applikationslizenz in einer SPS-Applikation abfragen [▶ 93]).

In Ihrer SPS-Anwendung können Sie dann wie erforderlich auf das Ergebnis der Lizenz-Validitätsprüfung reagieren und haben somit unter Kontrolle, wie auf das Vorhandensein oder Fehlen Ihrer Anwendungslizenz reagiert werden soll.

4 TwinCAT-OEM-Zertifikate

Um die Funktionen zum Schutz von Anwendungssoftware nutzen zu können, ist ein von Beckhoff signiertes TwinCAT-OEM-Zertifikat erforderlich.

Das TwinCAT-OEM-Zertifikat ist ausschließlich für die Nutzung zusammen mit TwinCAT vorgesehen.

Mit TwinCAT Build 4024 können mit der TwinCAT OEM-Zertifikatsversion TC0008 zusätzlich mit TwinCAT 3 in C++ erstellte TwinCAT *.tmx-Dateien signiert werden.

Mit dem Launch von TwinCAT 3.1 Build 4024 ergeben sich bei TwinCAT-OEM-Zertifikaten einige Neuerungen gegenüber Build 4022:

- Update auf eine neuere Verschlüsselungsversion für die internen Zertifikatsdaten
- Einführung einer erweiterten Zertifikatsversion TC0008, mit der auch in TwinCAT 3 erstellte C++ TwinCAT-Treiber-Software signiert werden kann
- Diese Zertifikatsversion erfordert durch die Nutzung im Windows-Umfeld eine sichere Validierung der Antragstellerdaten.
- Dafür wurde der Prozess zur Beantragung eines TwinCAT-OEM-Zertifikats angepasst. **Alle OEM-Zertifikate müssen** zur Validierung der Adress- und Kontaktdaten offiziell **bestellt werden**. (Die Ausstellung eines TwinCAT-OEM-Zertifikats ist kostenlos.)
- TwinCAT-OEM-Zertifikate Extended Validation (TC0008) werden nur an Beckhoff Bestandskunden vergeben.

Bestellnummern TwinCAT-OEM-Zertifikate

TC0007: TwinCAT OEM Certificate Standard (TwinCAT Software Protection)

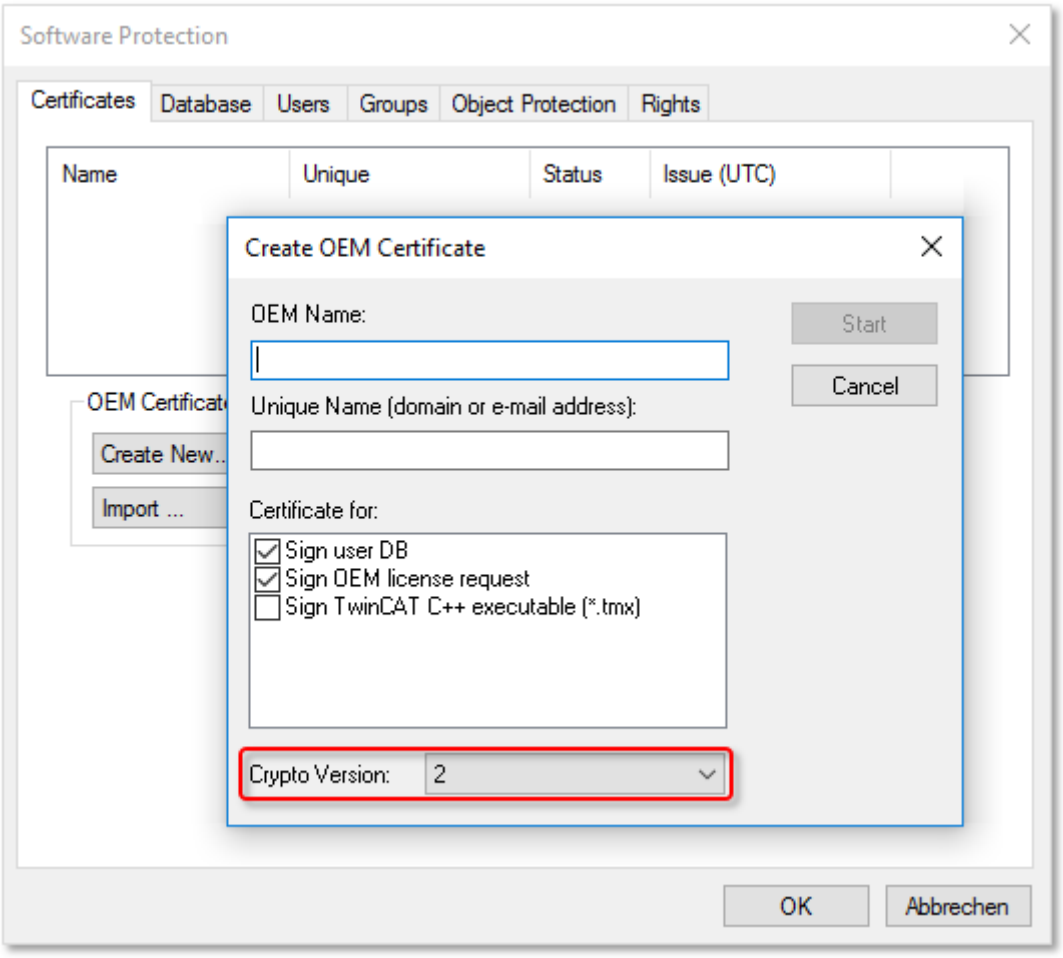
TC0008: TwinCAT OEM Certificate Extended Validation (wie TC0007, zusätzlich Signierung von mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software)

Gilt nur für TwinCAT 3.1 Build 4024.0: Erstellung einer User DB erfordert Crypto Version 1

Die Erstellung einer Benutzerdatenbank [▶ 33] für die TwinCAT Software Protection darf in der TwinCAT-Version Build **4024.0** nur mit einem OEM-Zertifikat mit der Crypto Version 1 erfolgen!

Bitte beachten:

- **TC0008** beinhaltet auch alle Funktionalitäten von TC0007
- Die Standard-Zertifikatsversion **TC0007** kann wahlweise mit der Verschlüsselungsversion von TwinCAT 3.1 Build 4022 oder 4024 ausgestellt werden.
- Die Zertifikatsversion **TC0008** mit erweiterter Validierung kann nur mit der neueren Verschlüsselungsversion von TwinCAT 3.1 Build **4024** ausgestellt werden.
- Die Verschlüsselungsversion des Zertifikats wird beim Erstellen des „OEM Certificate Request Files“ [▶ 22] durch den Anwender festgelegt (nicht bei der Bestellung!):



Kompatibilität von OEM-Zertifikaten: Build 4022 <-> Build 4024:

- Die Verschlüsselungsversion (=1) von Build 4022 (= z. B. ein mit Build 4022 erstelltes, bestehendes OEM-Zertifikat bzw. damit erzeugte UserDBs oder OEM Applikationslizenzen) können auch bei Build 4024 eingesetzt werden (umgekehrt funktioniert es nur bei Verwendung der Verschlüsselungsversion 1!)
- Ein TwinCAT OEM-Zertifikat (nur Standard) mit der Verschlüsselungsversion **1** von Build **4024** (bzw. damit erzeugte UserDBs oder OEM Applikationslizenzen) können mit TwinCAT 3.1 Build **4022** verwendet werden. (-> Build 4022 kann die Zertifikatsdaten der Verschlüsselungsversion 1 entschlüsseln)
- Ein TwinCAT OEM-Zertifikat mit der Verschlüsselungsversion **2** von Build **4024** (bzw. damit erzeugte UserDBs oder OEM-Applikationslizenzen) können **nicht** mit TwinCAT 3.1 Build **4022** verwendet werden! (-> Build 4022 kann die Zertifikatsdaten der Verschlüsselungsversion 2 nicht entschlüsseln!)
- TwinCAT OEM-Zertifikate mit unterschiedlichen Verschlüsselungsversionen können in TwinCAT 3.1 Build **4024** parallel verwendet werden: Ein OEM-Zertifikat mit der Verschlüsselungsversion von TwinCAT 3.1 Build 4022 für den Schutz der Anwendersoftware, und ein zweites OEM-Zertifikat mit der Verschlüsselungsversion von TwinCAT 3.1 Build 4024 für die Signierung von TwinCAT-Treiber-Software.

Speicherhinweise für den Anwendungsbereich: Schutz der OEM-Anwendungssoftware

Mit dem in allen Zertifikatsversionen enthaltenen OEM Key können die Funktionen zum Schutz der TwinCAT 3 Anwendungssoftware genutzt werden:

- Erstellen einer Benutzerdatenbank (User DB) zur Benutzerzugriffssteuerung
- Erstellen von OEM-Applikationslizenzbeschreibungsdateien
  (Basis für das Ausstellen von OEM-Applikationslizenzen)
- Ausstellen (Signieren) von OEM-Applikationslizenzen

Das OEM-Zertifikat Standard (TC0007) wird ausschließlich für diese drei Tätigkeiten benötigt.

Auf welchem Rechner muss das OEM-Zertifikat TC0007 gespeichert werden?

Das OEM-Zertifikat sollte sich ausschließlich auf dem Rechner befinden, auf dem die drei oben aufgeführten Tätigkeiten ausgeführt werden.

Das OEM-Zertifikat TC0007 ist nicht erforderlich:

- Zur Nutzung einer User DB
- Zum Programmablauf
- Zur Nutzung von OEM-Applikationslizenzen

Das Zertifikat sollte aus Sicherheitsgründen auf keinen Fall auf Steuerungsrechnern ausgeliefert werden oder auf allen möglichen Rechnern mit dem TwinCAT Engineering aufgespielt werden.

Beim Einsatz von OEM-Lizenzen wird das OEM-Zertifikat ausschließlich einmalig zum **Ausstellen** der Lizenz benötigt (da das Lizenzfile hiermit signiert wird).

Speicherhinweise für den Anwendungsbereich: Signierung von TwinCAT-Treiber-Software

Mit dem in der Zertifikatsversion TC0008 (TwinCAT OEM Certificate Extended Validation) enthaltenen OEM Key kann zusätzlich mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software signiert werden.

Sofern Sie TC0008 nur für diesen Einsatzzweck nutzen, gilt:

Auf welchem Rechner muss das OEM-Zertifikat TC0008 gespeichert werden?

Das OEM-Zertifikat sollte sich ausschließlich auf dem Rechner befinden, auf dem mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software signiert wird.

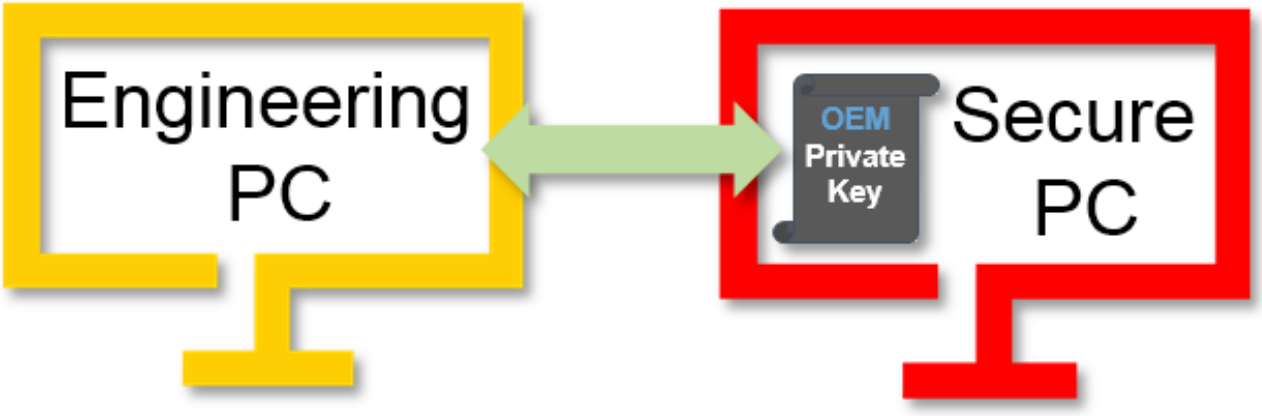
Falls Sie TC0008 ebenfalls für die TwinCAT Software Protection nutzen, gelten auch die diesbezüglichen Hinweise für die Rechner, auf denen das Zertifikat gespeichert sein darf/sollte.

Das OEM-Zertifikat TC0008 ist nicht zum Ablauf der damit signierten TwinCAT-Treiber-Software erforderlich.

Das Zertifikat soll auf keinen Fall auf Steuerungsrechnern ausgeliefert werden oder auf allen möglichen Rechnern mit TwinCAT Engineering aufgespielt werden.

Verwendung eines sicheren PCs

Verwenden Sie für Tätigkeiten, die den Umgang mit dem Passwort des Private Keys des OEM-Zertifikats erfordern, einen sicheren PC, um ein Ausspähen des Passwortes vorzubeugen.



Gültigkeit des TwinCAT OEM-Zertifikats

Die Gültigkeit des OEM-Zertifikats ist aus Sicherheitsgründen auf zwei Jahre begrenzt.

Der OEM kann vor Ablauf der zwei Jahre (und auch noch danach) eine Verlängerung seines Zertifikats beantragen, um ohne Unterbrechung weiterarbeiten zu können. (Siehe OEM-Zertifikat verlängern [▶ 31])

Was passiert, wenn die Gültigkeit des Zertifikats abgelaufen ist?

Diese Funktionen sind mit einem ungültigen (abgelaufenen) OEM-Zertifikat **nicht** mehr möglich:

- Erstellen einer Benutzerdatenbank
- Erstellen von OEM-Applikationslizenzbeschreibungsdateien
- Ausstellen (Signieren) von OEM-Applikationslizenzen
- Signieren von C++ Executables (Build 4024) mit dem OEM-Zertifikat

Alles andere funktioniert weiterhin:

- Die Programmausführung ist weiterhin möglich.
- Ausgestellte OEM-Lizenzen behalten weiterhin ihre Gültigkeit.
- Mit TC0008 signierte C++ Executables laufen weiterhin (Build 4024).
- Die Benutzerdatenbank behält weiterhin ihre Gültigkeit und der Administrator kann auch weiterhin Änderungen/Anpassungen in der Datenbank machen. (Eine neue Benutzerdatenbank kann jedoch nicht mehr erstellt werden.)

4.1 Erstellung des "OEM Certificate Request Files"

TwinCAT OEM-Zertifikate werden nur für Beckhoff-Bestandskunden ausgestellt.

Bei Fragen wenden Sie sich bitte an Ihren Beckhoff Vertriebskontakt.

Systemvoraussetzungen

- Min. TwinCAT 3.1 Build 4024
- Min. Windows 10 oder TwinCAT/BSD (auf dem Zielsystem)

Für Firmenname und Passwort keine Sonderzeichen (ä, é, ...) verwenden!

Der Algorithmus zur Verarbeitung des OEM-Zertifikats in TwinCAT kann keine Sonderzeichen verarbeiten.

Bestellnummern TwinCAT-OEM-Zertifikate

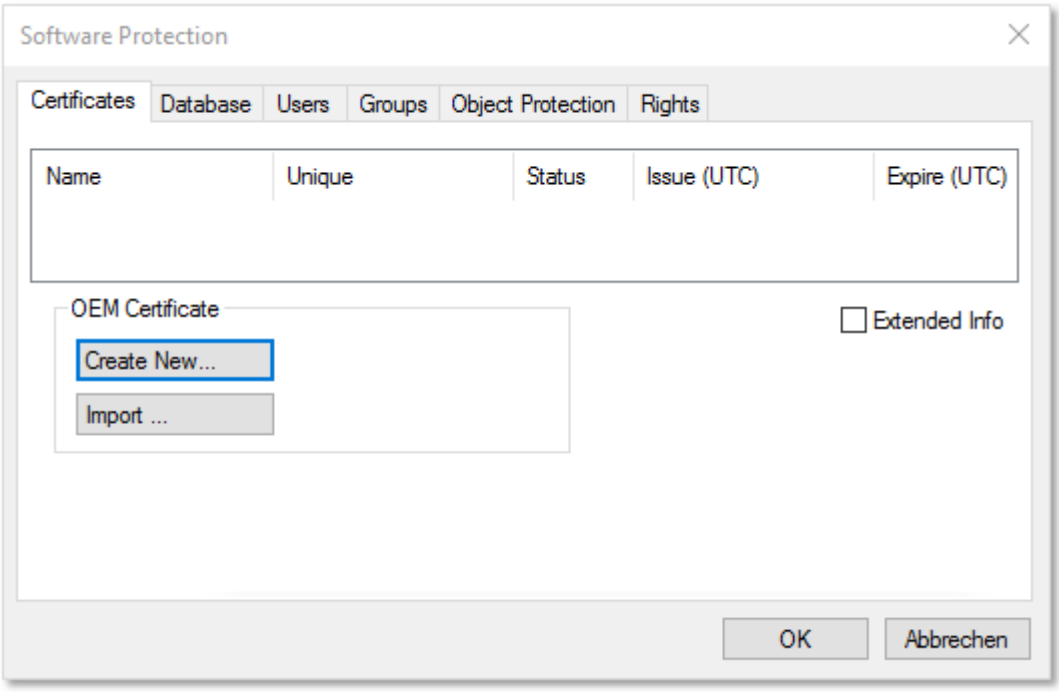
TC0007: TwinCAT OEM Certificate Standard (TwinCAT Software Protection)

TC0008: TwinCAT OEM Certificate Extended Validation (wie TC0007, zusätzlich Signierung von mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software)

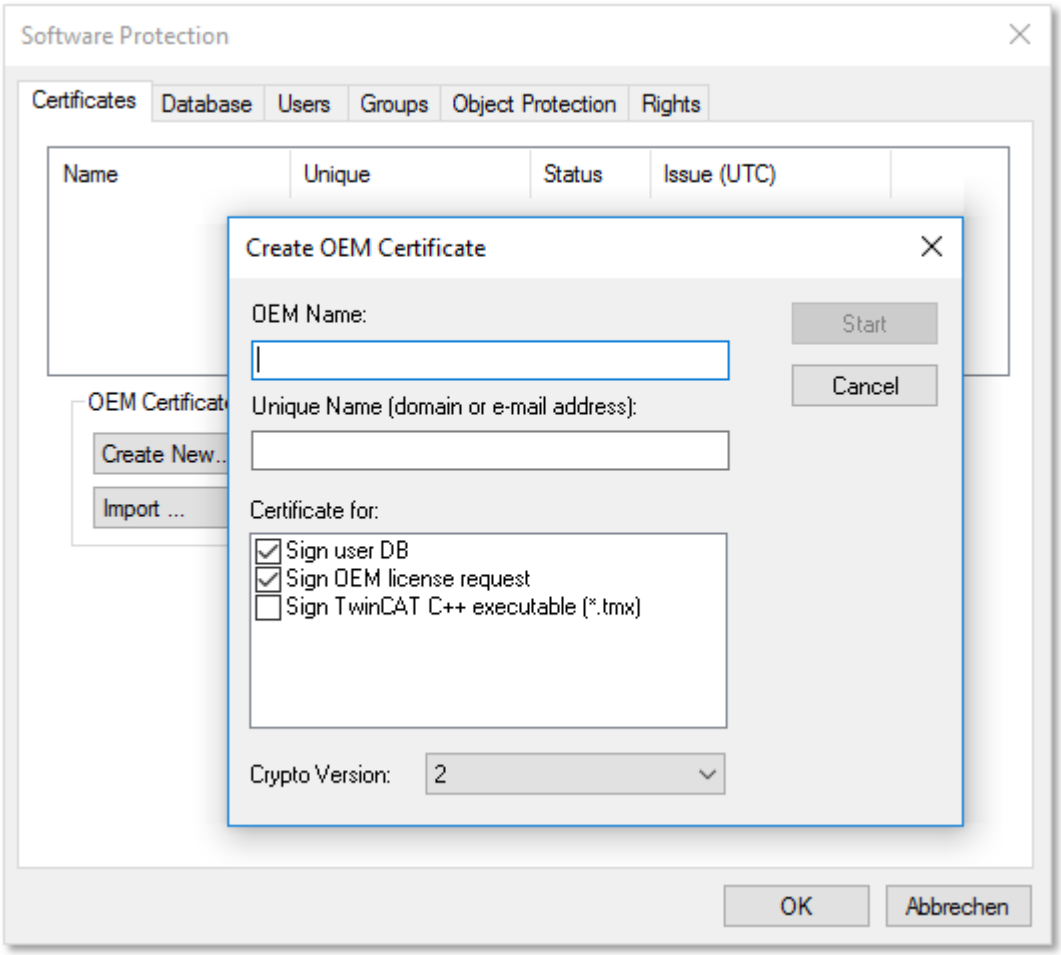
✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

1. Wählen Sie die Registerkarte **Certificates** aus.

2. Klicken Sie auf **Create New…**.



⇨ Das Eingabefenster **Create OEM Certificate** öffnet sich.

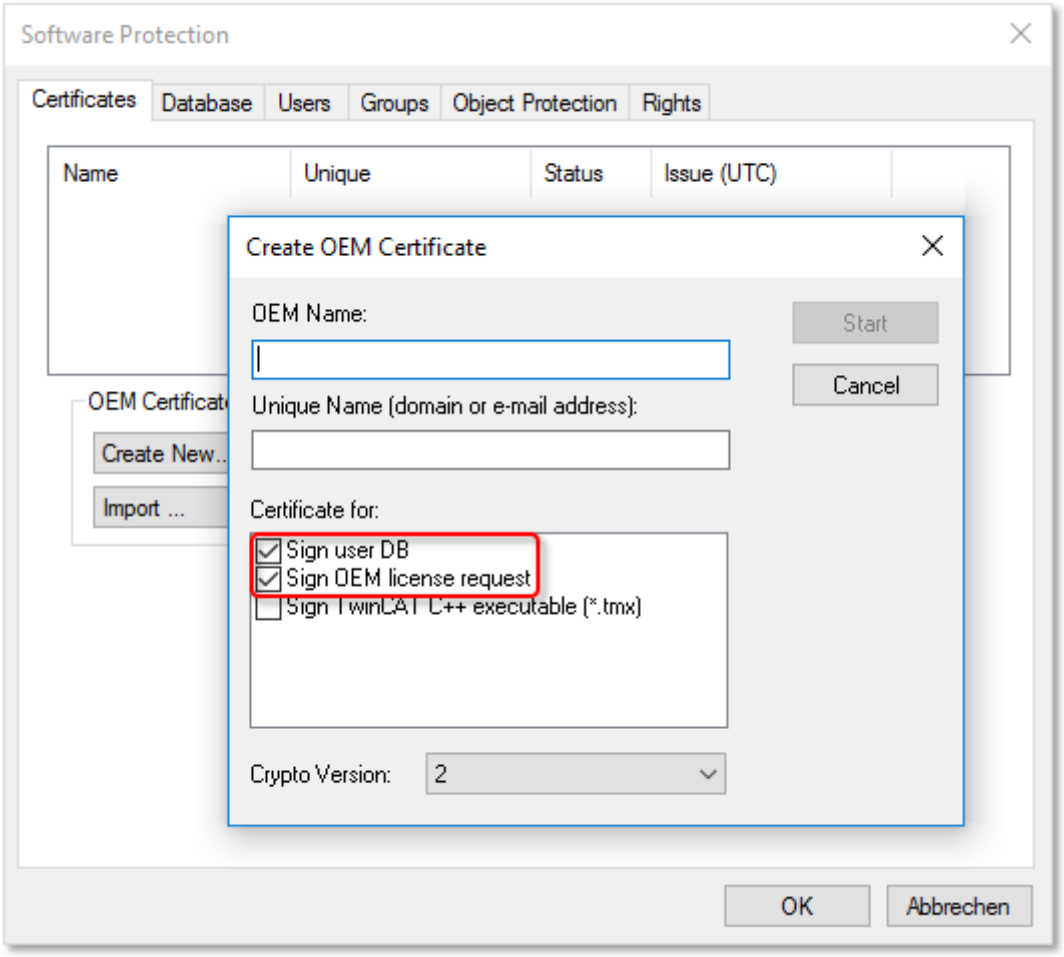


3. Geben Sie die erforderlichen Daten für ein „OEM Certificate Request File“ ein:
   - Geben Sie im Textfeld **OEM Name** Ihren Firmennamen ein. Der Name muss einen klaren Bezug zu Ihrer Firma oder Ihrem Unternehmensteil haben.

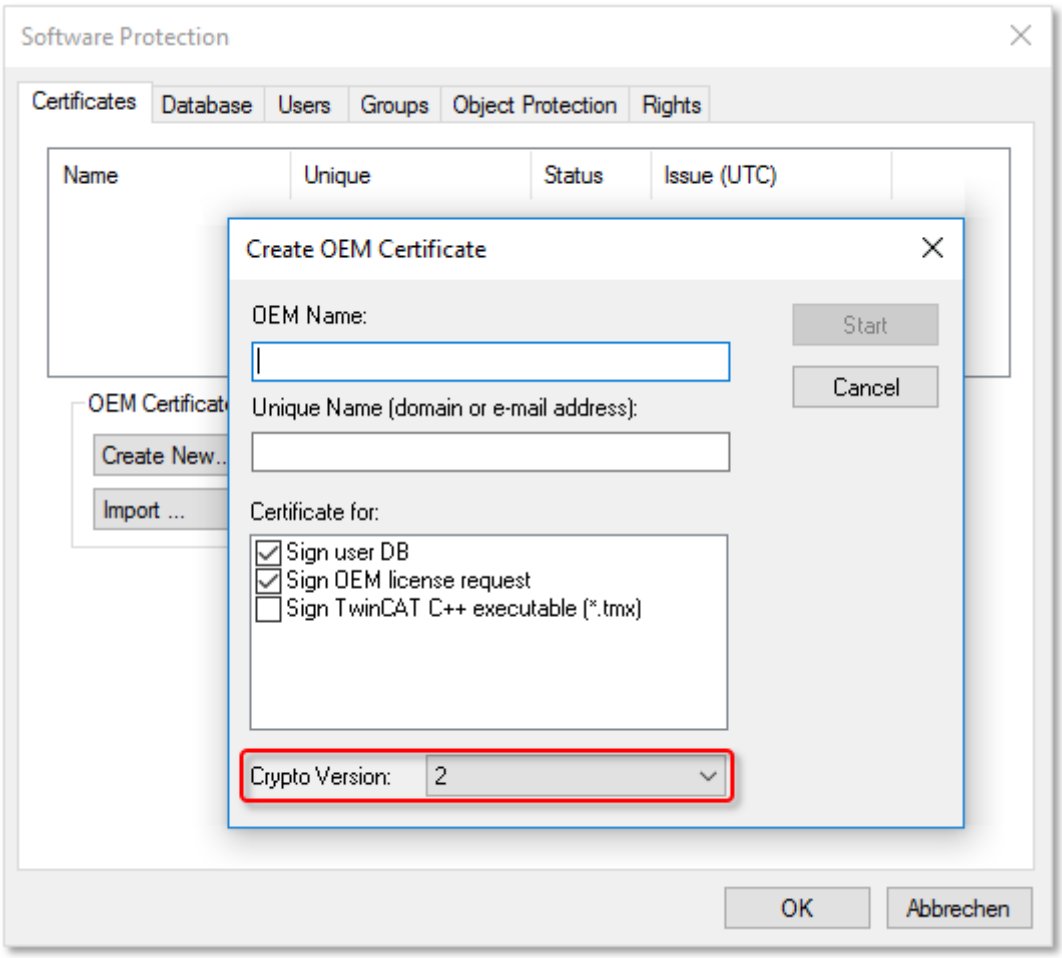
Für Firmenname und Passwort keine Sonderzeichen (ä, é, ...) verwenden!

Der Algorithmus zur Verarbeitung des OEM-Zertifikats in TwinCAT kann keine Sonderzeichen verarbeiten.

- Geben Sie einen **Unique Name** ein. Der „OEM Unique Name“ muss ein einmaliger Name sein, anhand dessen der Eigentümer des Zertifikats weltweit eindeutig identifiziert werden kann, vorzugsweise die URL der Webseite Ihrer Firma oder Ihre E-Mail-Adresse. Die E-Mail-Adresse muss eine Firmen-E-Mail-Adresse sein, also eindeutig einer Firma zugeordnet werden können.
- Achten Sie darauf, dass für ein **Standard-Zertifikat** (TC0007) maximal diese beiden Checkboxen für den Einsatzbereich des Zertifikats markiert sind:



- Die aktuelle Crypto-Version (für den verschlüsselten Inhalt des Zertifikatsinhaltes) ist „2“. Die ältere Crypto-Version „1“ sollten Sie nur wählen, wenn Sie dieses Zertifikat auch mit TwinCAT 3.1 Build 4022.x verwenden wollen.
  Information: Die Crypto-Version „1“ kann nur für ein Standard-Zertifikat (TC0007) ausgewählt werden.

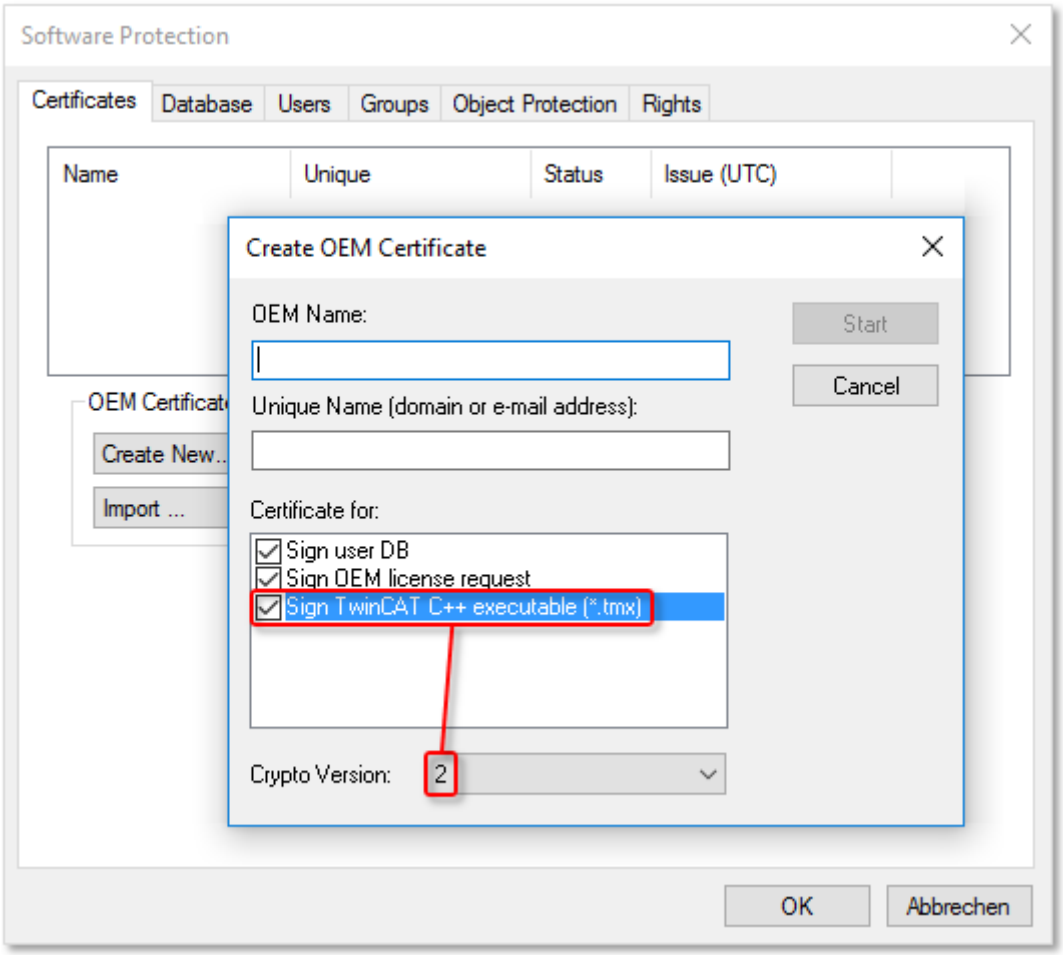


Gilt nur für TwinCAT 3.1 Build 4024.0: Erstellung einer User DB erfordert Crypto Version 1

Die Erstellung einer Benutzerdatenbank [▶ 33] für die TwinCAT Software Protection darf in der TwinCAT-Version Build **4024.0** nur mit einem OEM-Zertifikat mit der Crypto Version 1 erfolgen!

- Für den Einsatzzweck des Zertifikats darf die Auswahl der Checkbox „**Sign TwinCAT C++ executables** (*.tmx)“ nur erfolgen, wenn Sie ein Zertifikat mit „**Extended Validation**“ (TC0008) beantragen wollen, das für die Signierung von mit TwinCAT 3 erzeugtem C++ Executables (inkl. Matlab/Simulink) genutzt werden kann. Diese Zertifikatsversion erfordert im Bestellprozess des

Zertifikats ein **deutlich aufwändigeres Validierungsverfahren** Ihrer Kontaktdaten (und damit auch mehr Zeit) und sollte daher nur gewählt werden, wenn Sie diese Option wirklich benötigen:



- Ein Zertifikat mit „Extended Validation“ (TC0008) erfordert immer die Crypto-Version „2“. (Bitte beachten: Diese Zertifikatsversion kann nicht mit TwinCAT 3 Build 4022.x genutzt werden!)

1. Wenn Sie die Daten eingegeben haben, klicken Sie auf **Start** und Sie können ein Verzeichnis auswählen, um die Datei zu speichern.
   Information: Übernehmen Sie das jeweils vorgeschlagene Verzeichnis:
   >=TC3.1.4026.0: *c:\twincat\3.1\customconfig\certificates*
   >=TC3.1.4026.0: *c:\ProgramData\Beckhoff\TwinCAT\3.1\customconfig\certificates*
   Sie benötigen die neu erzeugte Datei in diesem Verzeichnis, um in einem späteren Schritt den „File Fingerprint“ für diese Datei auslesen zu können.
   ⇨ Ein Dialog zur Auswahl eines Passworts für den OEM Private Key öffnet sich.
2. Vergeben Sie ein Passwort für den OEM Private Key.

Für Firmenname und Passwort keine Sonderzeichen (ä, é, ...) verwenden!

Der Algorithmus zur Verarbeitung des OEM-Zertifikats in TwinCAT kann keine Sonderzeichen verarbeiten.

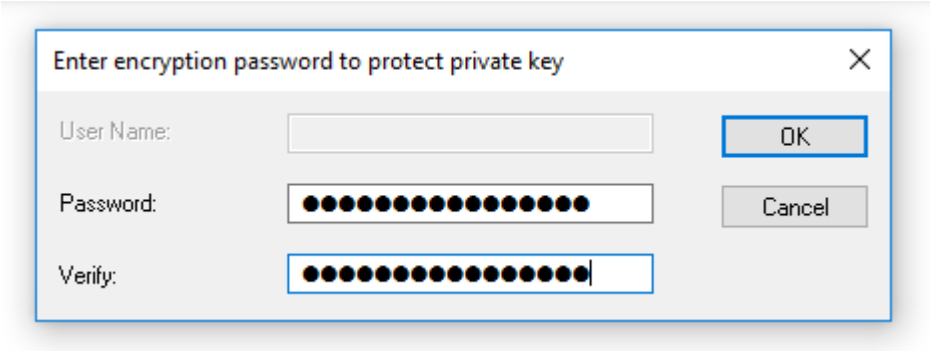
Passwortsicherheit!

- Verwenden Sie ein starkes Passwort für Ihr OEM-Zertifikat!
- Schützen Sie Ihr Passwort durch geeignete Maßnahmen, damit es nicht in fremde Hände fallen kann!

Passwort bei Verlust nicht wiederherstellbar

Beckhoff kann Ihr Passwort nicht wiederherstellen oder zurücksetzen. Wenn Sie das Passwort für Ihr OEM-Zertifikat vergessen oder verlieren, können Sie das Zertifikat nicht mehr verwenden und müssen ein neues OEM-Zertifikat ausstellen lassen.

1. Bestätigen Sie das Passwort durch eine wiederholte Eingabe und schließen Sie den Dialog mit **OK**.



⇨ Die Datei wird gespeichert.

Die so erzeugte „OEM Certificate Request Datei“ muss nun noch von der Beckhoff Zertifikatsstelle signiert werden, um gültig zu sein. Das Verfahren dazu wird im Kapitel „OEM-Zertifikat beantragen [▶ 28]“ beschrieben.

4.2 File Fingerprint der OEM-Zertifikatsdatei ermitteln

Diese Funktionalität benötigen Sie für die Beantragung eines **TwinCAT OEM Certificate Extended Validation** (TC0008).

Systemvoraussetzung

Diese Funktionalität erfordert mindestens die Version TwinCAT 3.1 Build 4024.

Die OEM Certificate Request Datei wird durch die Signierung von Beckhoff zum TwinCAT OEM-Zertifikat. Bis auf diese Signatur unterscheiden sich die Dateien nicht. Daher wird im Folgenden für beide Dateiversionen der Begriff „TwinCAT OEM-Zertifikatsdatei“ verwendet.

Den „File Fingerprint“ einer OEM-Zertifikatsdatei über das TwinCAT 3 Engineering auslesen

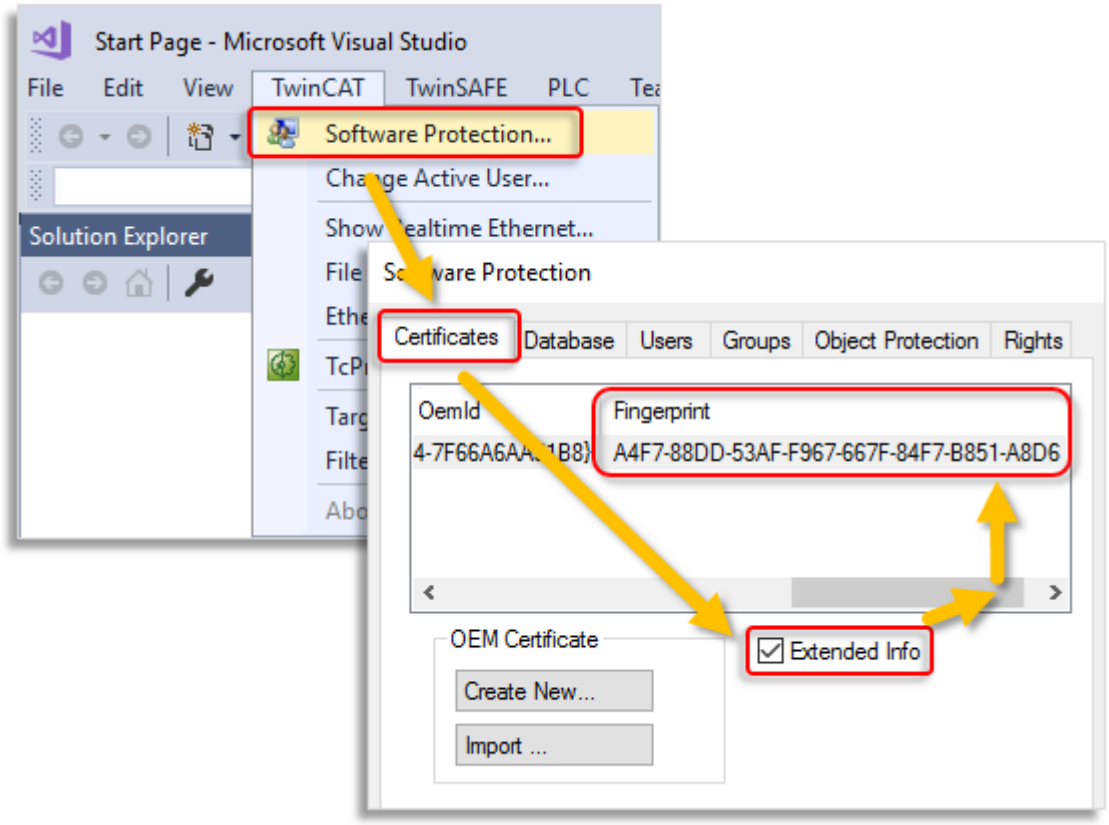
Für diese Funktion ist es erforderlich, dass die OEM-Zertifikatsdatei in diesem Verzeichnis liegt: „c:\twincat\3.1\customconfig\certificates“.

In diesem Verzeichnis liegt ihr OEM-Zertifikat, sofern Sie bereits eines haben und dieses verlängern wollen.

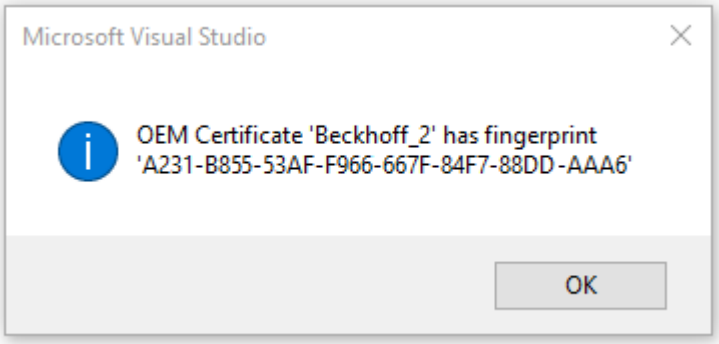
Sofern Sie beim Erstellen der „OEM Certificate Request Datei“ das vorgeschlagene Verzeichnis nicht geändert haben, liegt die Datei bereits in diesem Verzeichnis.

Vorgehensweise:

1. Rufen Sie den TwinCAT 3 Software Protection Konfigurator auf.



2. Wählen Sie den Tab **Certificates** aus.
3. Markieren Sie die Checkbox **Extended Info.**
4. Scrollen Sie im Fenster so weit nach rechts, bis Sie die Spalte **Fingerprint** sehen. (Alternativ können Sie auch einfach einen Doppelklick auf die Zertifikatszeile machen. In einem Popup-Fenster wird dann der File Fingerprint angezeigt):



Mit [Ctrl] + [C] können Sie die Fingerprint-Daten aus dem Meldungsfenster ins Windows Clipboard kopieren.

4.3 OEM-Zertifikat beantragen

Bitte beachten Sie die Information aus den vorhergehenden Kapiteln und gegebenenfalls zum Verlängern eines OEM-Zertifikats:

TwinCAT OEM-Zertifikate [▶ 19]

Erstellung des "OEM Certificate Request Files" [▶ 22]

OEM-Zertifikat verlängern [▶ 31]

Bestellprozess TwinCAT OEM-Zertifikate

Die Beantragung eines TwinCAT OEM-Zertifikats erfolgt über eine offizielle Bestellung. Kontaktieren Sie dazu bitte Ihren Beckhoff Vertriebskontakt.

Hinweise:

- Die Ausstellung und Verlängerung eines TwinCAT OEM-Zertifikats ist kostenlos.
- Die Ausstellung eines TwinCAT OEM-Zertifikats erfolgt nur für Beckhoff Bestandskunden.
- Bei einem neuen OEM-Zertifikat erstellen Sie im TwinCAT Engineering die „OEM Certificate Request Datei“ [▶ 22].
- Bei einer Verlängerung des Zertifikats wird die bestehende OEM-Zertifikatsdatei lediglich neu signiert und ist damit weitere 2 Jahre gültig. (In diesem Fall erstellen Sie also keine „OEM Certificate Request Datei“.)
- Die „OEM Certificate Request Datei“ wird durch die Signierung von Beckhoff zum TwinCAT OEM-Zertifikat. Bis auf diese Signatur unterscheiden sich die Dateien nicht.
- Im folgenden Text wird der Einfachheit halber für beide Varianten die Bezeichnung „OEM-Zertifikatsdatei“ verwendet.
- Da es sich bei einem TwinCAT OEM-Zertifikat um einen digitalen Ausweis handelt, ist eine Verifizierung der Kontaktdaten des Anfragers erforderlich.
- Die beiden OEM-Zertifikatsversionen repräsentieren unterschiedliche Sicherheitslevel, daher unterscheiden sich die Verifizierungsprozesse etwas.
- TC0008 (TwinCAT OEM Certificate Extended Validation) sollten Sie nur bestellen, wenn Sie es wirklich benötigen (Signierung von TwinCAT 3 C++ Executables).

Bestellnummern TwinCAT-OEM-Zertifikate

TC0007: TwinCAT OEM Certificate Standard (TwinCAT Software Protection)

TC0008: TwinCAT OEM Certificate Extended Validation (wie TC0007, zusätzlich Signierung von mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software)

Übersicht über den Bestell- und Validierungsprozess

Ihre Email-Adresse muss ein Firmen-Email-Account sein (Freemailer wie GMail oder Ähnliches sind nicht zulässig) und mit dem Firmennamen des Bestellers korrespondieren.

1. Kontaktieren Sie Ihren Beckhoff Vertriebskontakt und kündigen Sie die Beantragung eines TwinCAT 3 OEM-Zertifikats an. Bestellen Sie “TC0007” oder “TC0008”.
2. Wichtig: Geben Sie, als Anfrager, Ihre Kontaktdaten als Lieferadresse (= Kontaktname und Email-Adresse) und den Einsatzbereich des Zertifikats an (Firmenname, Adresse).
3. Die im Auftrag angegebenen Kontaktdaten werden verifiziert und Sie (der in der Lieferadresse genannte Anfrager) werden vom Beckhoff Vertrieb kontaktiert.
4. Bei der Beantragung eines neuen OEM-Zertifikats erstellen Sie im TwinCAT 3 Engineering eine „OEM Certificate Request Datei“ [▶ 22].
5. Nur TC0008: Ermitteln Sie mit Hilfe des TwinCAT Engineerings den „File Fingerprint“ der OEM-Zertifikatsdatei (siehe File Fingerprint der OEM-Zertifikatsdatei ermitteln [▶ 27]). Teilen Sie diesen File Fingerprint im Rahmen Ihrer Kontaktdatenverifizierung dem Beckhoff Vertriebskontakt mit. Die Übermittlung des File Fingerprints muss auf einem anderen Kommunikationsweg erfolgen als für die Zusendung der OEM-Zertifikatsanfragedatei.
6. Schicken Sie die „OEM-Zertifikatsdatei“ nun an den Beckhoff Vertriebskontakt.
7. Nach der Signierung der Zertifikatsdatei in der Beckhoff Zentrale erhalten Sie diese über Ihren Ansprechpartner per Email zugesandt.

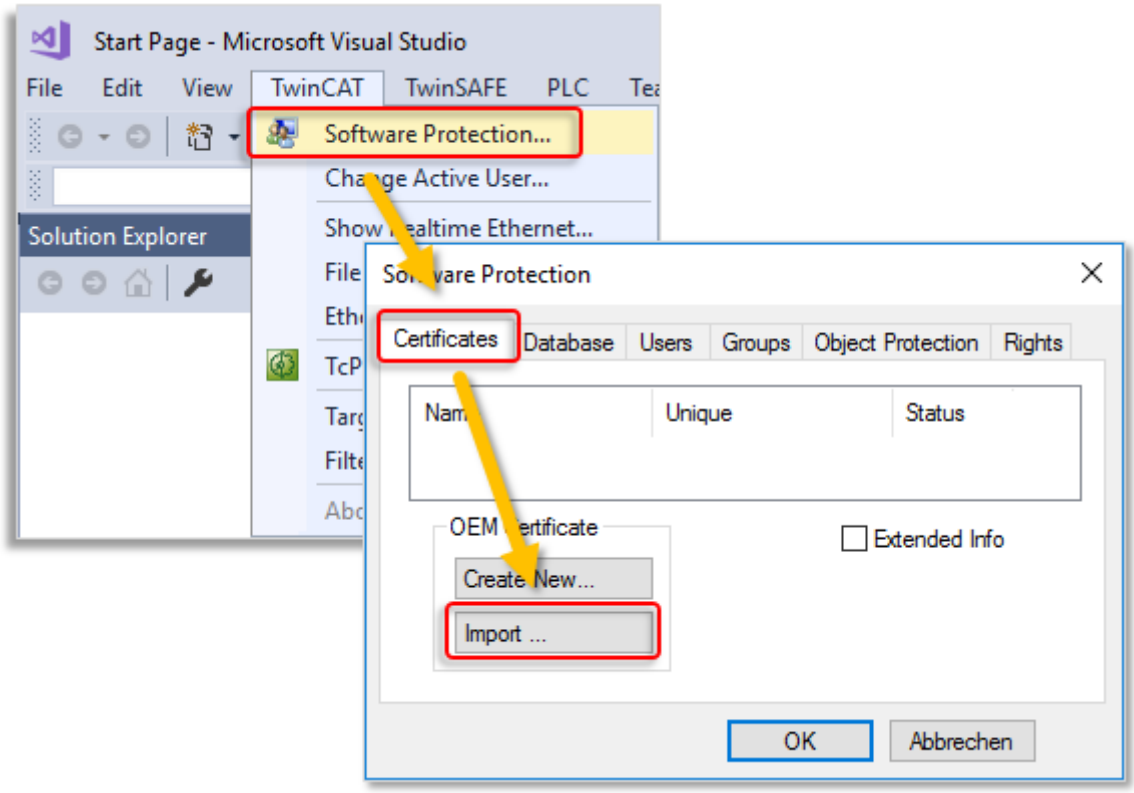
Beachten Sie, dass die Validierung der Kontaktdaten und die Ausstellung des Zertifikats einige Tage Zeit in Anspruch nehmen können.

4.4 OEM-Zertifikat installieren

TwinCAT Root-Verzeichnis <TwinCAT_ROOT>

Bis einschließlich TwinCAT 3.1.4024: **C:\TwinCAT**
Ab TwinCAT 3.1.4026: **C:\ProgramData\Beckhoff\TwinCAT**

Wenn Sie das Zertifikat signiert zurückerhalten haben, importieren Sie dieses über das Software Protection Control Center:



Anmerkung: Diese Importfunktion steht erst ab TwinCAT 3.1. Build 4024 zur Verfügung.

Alternativ können Sie die Datei auch manuell auf Ihrem Engineering-System speichern, und zwar im Verzeichnis *<TwinCAT_ROOT>\3.1\customconfig\certificates*.

Nach dem Neustart des TwinCAT Engineering wird das Zertifikat in dem Software-Protection-Konfigurator in der Registerkarte **Certificates** aufgeführt.

Kontrollieren Sie, ob das Zertifikat dort auch als „valid“ (gültig) angezeigt wird.

Speicherhinweise für den Anwendungsbereich: Schutz der OEM-Anwendungssoftware

Mit dem in allen Zertifikatsversionen enthaltenen OEM Key können die Funktionen zum Schutz der TwinCAT 3 Anwendungssoftware genutzt werden:

- Erstellen einer Benutzerdatenbank (User DB) zur Benutzerzugriffssteuerung
- Erstellen von OEM-Applikationslizenzbeschreibungsdateien
  (Basis für das Ausstellen von OEM-Applikationslizenzen)
- Ausstellen (Signieren) von OEM-Applikationslizenzen

Das OEM-Zertifikat Standard (TC0007) wird ausschließlich für diese drei Tätigkeiten benötigt.

Auf welchem Rechner muss das OEM-Zertifikat TC0007 gespeichert werden?

Das OEM-Zertifikat sollte sich ausschließlich auf dem Rechner befinden, auf dem die drei oben aufgeführten Tätigkeiten ausgeführt werden.

Das OEM-Zertifikat TC0007 ist nicht erforderlich:

- Zur Nutzung einer User DB
- Zum Programmablauf
- Zur Nutzung von OEM-Applikationslizenzen

Das Zertifikat sollte aus Sicherheitsgründen auf keinen Fall auf Steuerungsrechnern ausgeliefert werden oder auf allen möglichen Rechnern mit dem TwinCAT Engineering aufgespielt werden.

Beim Einsatz von OEM-Lizenzen wird das OEM-Zertifikat ausschließlich einmalig zum **Ausstellen** der Lizenz benötigt (da das Lizenzfile hiermit signiert wird).

Speicherhinweise für den Anwendungsbereich: Signierung von TwinCAT-Treiber-Software

Mit dem in der Zertifikatsversion TC0008 (TwinCAT OEM Certificate Extended Validation) enthaltenen OEM Key kann zusätzlich mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software signiert werden.

Sofern Sie TC0008 nur für diesen Einsatzzweck nutzen, gilt:

Auf welchem Rechner muss das OEM-Zertifikat TC0008 gespeichert werden?

Das OEM-Zertifikat sollte sich ausschließlich auf dem Rechner befinden, auf dem mit TwinCAT 3 in C++ erstellte TwinCAT-Treiber-Software signiert wird.

Falls Sie TC0008 ebenfalls für die TwinCAT Software Protection nutzen, gelten auch die diesbezüglichen Hinweise für die Rechner, auf denen das Zertifikat gespeichert sein darf/sollte.

Das OEM-Zertifikat TC0008 ist nicht zum Ablauf der damit signierten TwinCAT-Treiber-Software erforderlich.

Das Zertifikat soll auf keinen Fall auf Steuerungsrechnern ausgeliefert werden oder auf allen möglichen Rechnern mit TwinCAT Engineering aufgespielt werden.

4.5 OEM-Zertifikat verlängern

Um ein OEM-Zertifikat zu verlängern, gilt der gleiche Prozess, wie bei der Beantragung eines neuen Zertifikats. Auch in diesem Fall muss das Zertifikat bestellt werden (die Bestellnummern für eine Zertifikatsverlängerung sind dieselben wie zur Zertifikatsneubeantragung).

Sie erzeugen in diesem Fall aber kein neues „OEM Certificate Request File“, sondern schicken Ihr bestehendes Zertifikat zur Verlängerung an die Beckhoff Zertifikatsstelle. Teilen Sie in der E-Mail mit, dass es sich um eine Zertifikatsverlängerung und keine Neuausstellung handelt. Für den restlichen Inhalt der E-Mail gelten ansonsten dieselben Kriterien wie bei der Beantragung eines neuen Zertifikats.

Das bestehende Zertifikat wird dann neu signiert und ist weitere 2 Jahre gültig.

Da das Zertifikat lediglich eine neue Signatur erhält, ist es vollständig kompatibel zur Ursprungsversion.

4.6 Update eines bestehenden OEM-Zertifikats?

Ein bestehendes OEM-Zertifikat kann leider nicht upgedatet werden (neue Crypto-Version oder geänderter Einsatzbereich). In diesem Falle ist immer die Ausstellung eines neuen OEM-Zertifikats erforderlich. Lediglich die Gültigkeitsdauer des OEM-Zertifikats kann durch Neusignierung verlängert werden.

Was für Folgen hat ein neues OEM-Zertifikat für Anwendungen mit bereits vorhandenen oder neu zu erstellenden TwinCAT UserDBs [▶ 33], OEM Lizenzbeschreibungsdateien [▶ 86] und OEM-Applikationslizenzen [▶ 90]?

TwinCAT User DB

- Anwendungsfall: Eine bestehende User DB soll weiterverwendet und gleichzeitig ein neues OEM-Zertifikat genutzt werden. Kein Problem: Die vorhandenen User DBs können weiterhin genutzt und verändert werden, da ein OEM-Zertifikat für beide Fälle gar nicht erforderlich ist. Dies gilt auch für den Umstieg von Build 4022 auf Build 4024 (und der Mitnahme der User DB von Build 4022).
- Anwendungsfall: Eine bestehende User DB (erstellt mit altem OEM-Zertifikat 1) soll durch eine neue User DB (erstellt mit neuem OEM-Zertifikat 2) ersetzt werden. Sofern die Anforderung des nachfolgenden Punktes zur Crypto-Version beachtet wird, kein Problem. Das Projekt muss aber einmalig mit der neuen User DB verknüpft werden [▶ 70]. Ein einfacher Austausch auf Dateiebene ist nicht möglich, es muss immer eine Neuzuweisung der ausgetauschten User DB zum Projekt erfolgen, da die neue User DB einen anderen User DB Key hat.

  Anmerkung: Alle Sicherheitseinstellungen für das Projekt gehen dabei verloren!
- Eine User DB, die auf Basis eines Zertifikats mit Crypto-Version 2 erstellt wurde, ist unter Build 4022 nicht nutzbar. (Die in der UserDB verschlüsselt enthaltenen Informationen können von Build 4022 nicht entschlüsselt werden.)

TwinCAT OEM-Applikationslizenzen

OEM Lizenzbeschreibungsdateien: Generell gilt, dass eine OEM Lizenzbeschreibungsdatei immer mit demselben Zertifikat erstellt sein muss, mit der die Ausstellung (Signierung) der OEM Applikationslizenz erfolgt. (Sonst stimmt der OEM Key in der Lizenzbeschreibungsdatei nicht mit dem OEM Key in der Applikationslizenz überein.)

Dieses ist unabhängig von der TwinCAT-Version oder der Crypto-Version.

Anmerkungen:

- Mit einem Zertifikat mit der Crypto-Version 2 erstellte OEM Lizenzbeschreibungsdateien und OEM Applikationslizenzen können nicht in Build 4022 verwendet werden.
- Mit einem Zertifikat mit der Crypto-Version 1 erstellte OEM Lizenzbeschreibungsdateien und OEM Applikationslizenzen können aber in Build 4024 verwendet werden.

5 Benutzerdatenbanken (User DBs)

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Änderungen von Einstellungen einer Benutzerdatenbank nicht bei geöffnetem Projekt

Für eine Änderung der Einstellungen einer Benutzerdatenbank darf kein Projekt geöffnet sein.

Wechsel eines Benutzers nicht bei geöffnetem Projekt

Für den Wechsel eines Benutzers darf kein Projekt geöffnet sein.

Neu ab TwinCAT 3 Build 4024.8: Extensions für Benutzerdatenbanken

Eine Benutzerdatenbank kann ab dieser Version um sogenannte „Extensions“ erweitert werden. Details dazu finden Sie im Kapitel Extensions für Benutzerdatenbanken [▶ 41].

5.1 Benutzerdatenbank anlegen

Gilt nur für TwinCAT 3.1 Build 4024.0: Erstellung einer User DB erfordert Crypto Version 1

Die Erstellung einer Benutzerdatenbank [▶ 33] für die TwinCAT Software Protection darf in der TwinCAT-Version Build **4024.0** nur mit einem OEM-Zertifikat mit der Crypto Version 1 erfolgen!

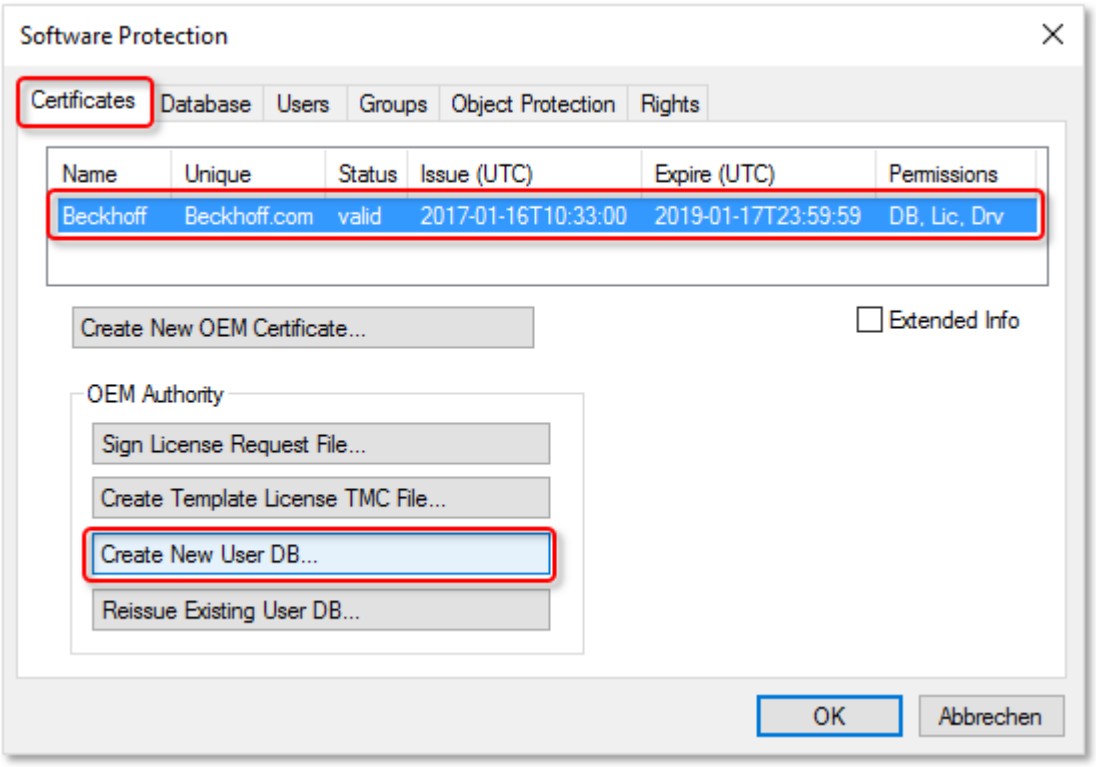
Verzeichnis zum Speichern von Benutzerdatenbanken

Benutzerdatenbanken müssen im folgenden Verzeichnis gespeichert sein, um im TwinCAT Engineering genutzt werden zu können: C:\TwinCAT\3.1\CustomConfig\UserDBs

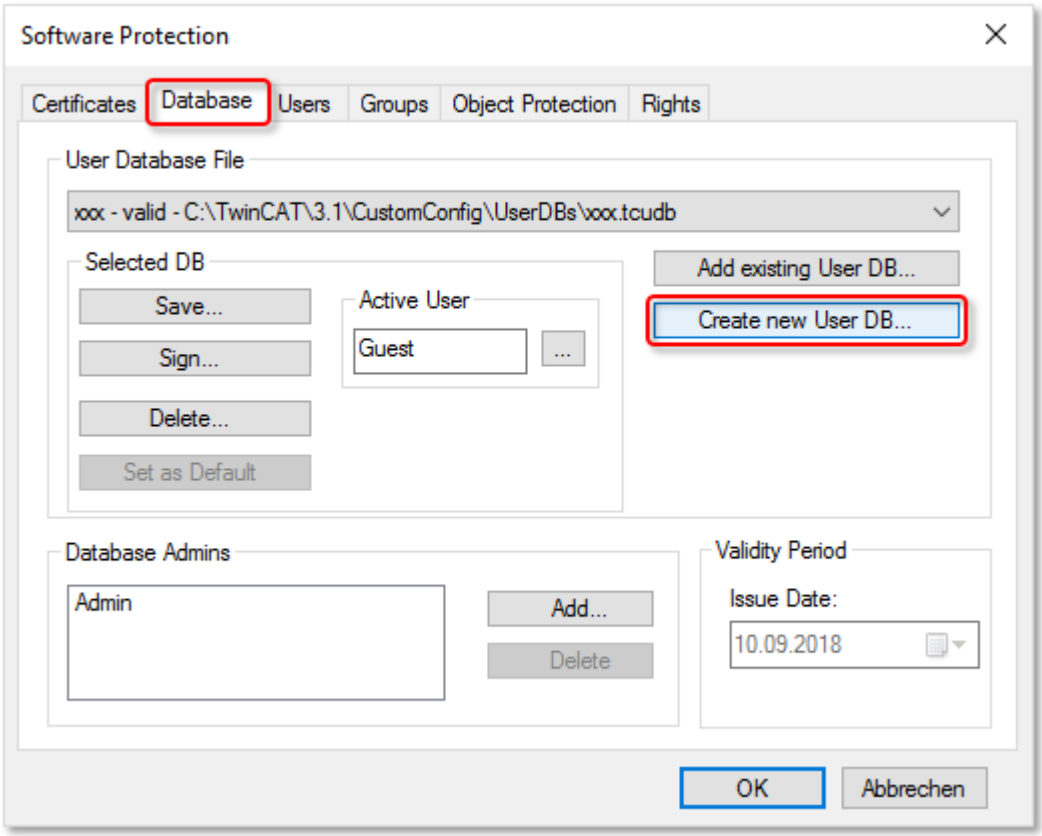
In Abhängigkeit von der TwinCAT-Version stehen Ihnen zwei verschiedene Wege zur Verfügung, das Anlegen einer Benutzerdatenbank zu starten.

- ✓ Benutzerdatenbanken können nur angelegt oder editiert werden, wenn kein Projekt geöffnet ist. Schließen Sie eventuell geöffnete Projekte.
- ✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

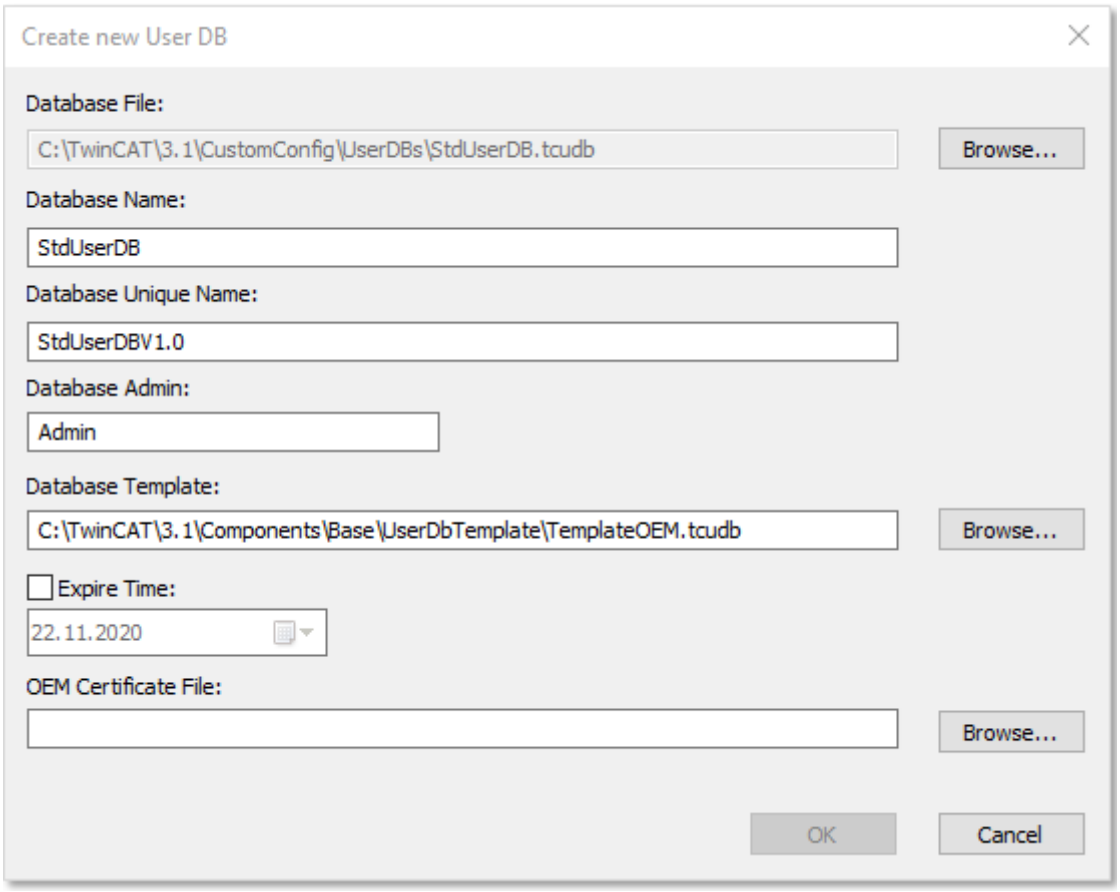
1. Wenn Sie eine TwinCAT-Version <Build 4022.25 verwenden, öffnen Sie die Registerkarte **Certificates**, wählen Sie das OEM-Zertifikat aus und klicken Sie dann auf **Create New User DB...**



2. Wenn Sie eine TwinCAT-Versionen >=Build 4022.25 verwenden, steht Ihnen die Schaltfläche **Create New User DB...** zusätzlich in der Registerkarte **Database** zur Verfügung. Hier wählen Sie das OEM-Zertifikat direkt in der Eingabemaske aus. Klicken Sie auf **Create New User DB...**.



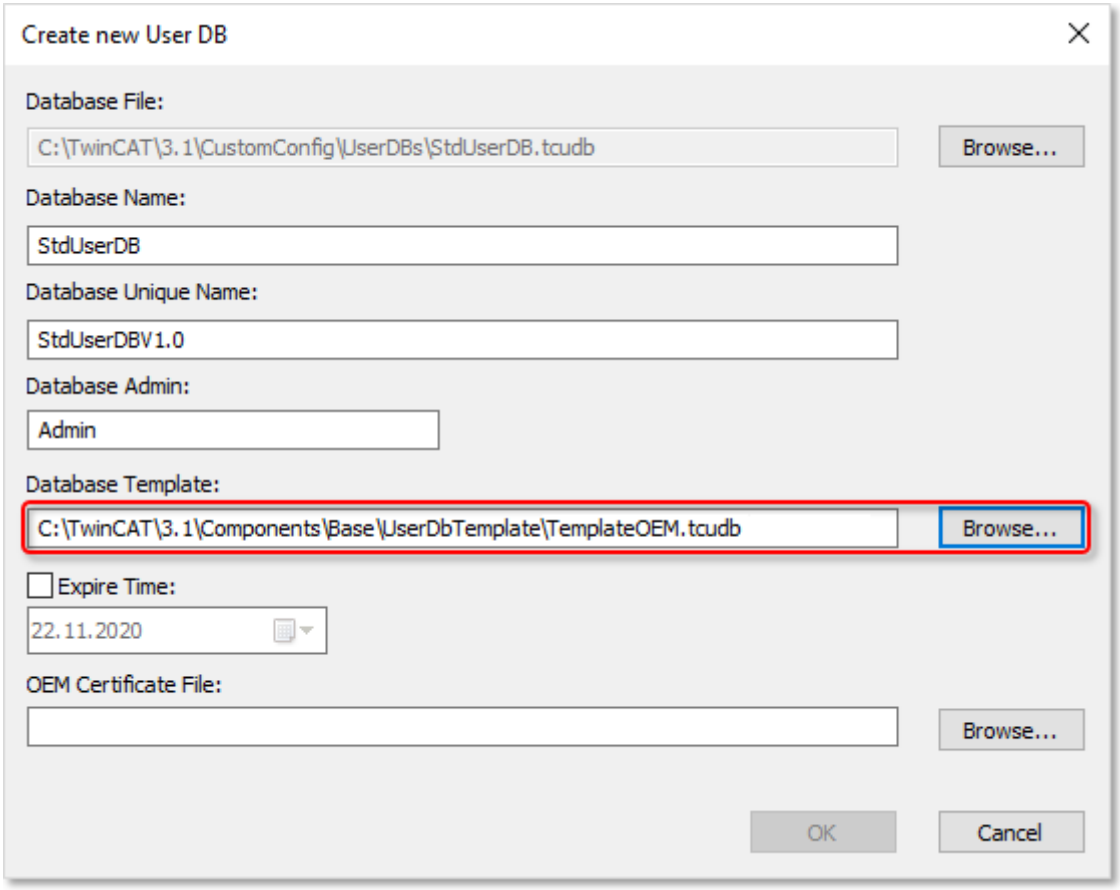
⇨ Der Dialog **Create new User DB** öffnet sich.



3. Geben Sie einen Namen für die Datenbank (**Database Name**) ein. Dieser wird im Programm zur Anzeige der ausgewählten Datenbank benutzt.
4. Geben Sie einen **Database Unique Name** an (z. B. mit einer Versionsnummer), der die eindeutige Identifizierung dieser Datenbank (-version) innerhalb Ihres Unternehmens ermöglicht.
5. Geben Sie einen Namen für den Administrator der Datenbank an. Der hier angelegte **Database Admin** wird ausschließlich zum Signieren der Datenbank verwendet und kann nicht zum Einloggen oder für Änderungen in der Datenbank verwendet werden. Um Änderungen in der Datenbank machen zu können, muss mindestens ein Benutzer der Datenbank der Administratorgruppe angehören.
6. Legen Sie die Vorlage für die neue Datenbank fest.
   Als einfach zu benutzende Basis sollten Sie die Vorlage *TemplateOEM.tcudb* verwenden. Wenn Ihre TwinCAT-Version die Vorlage noch nicht beinhaltet, können Sie sie hier herunterladen: https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/5943612299.zip.

   Zum Auswahl einer anderen Vorlage klicken Sie neben dem Feld **Database Template** auf **Browse…** und wählen Sie die gewünschte Datei über das Explorer-Fenster aus.

⇨ Das Template wird im Feld **Database Template** angezeigt.



Hinweis **Sie können sich auch eigene Vorlagen für eine Datenbank anlegen, z. B. auf Basis einer von Ihnen bereits erstellten Datenbank.**

7. Die erstellte Datenbank muss initial mit einem gültigen OEM-Zertifikat signiert werden. Daten aus dem OEM-Zertifikat werden außerdem für die Generierung des User DB Keys verwendet, das die Datenbank eindeutig individuell identifiziert.

   Sofern im Feld **OEM Certificate File** das gewünschte Zertifikat nicht eingestellt ist, wählen Sie das OEM-Zertifikat über einen Klick auf **Browse…** aus.

   Das Standardverzeichnis für OEM-Zertifikate lautet: *c:\twincat\3.1\customconfig\certificates*.

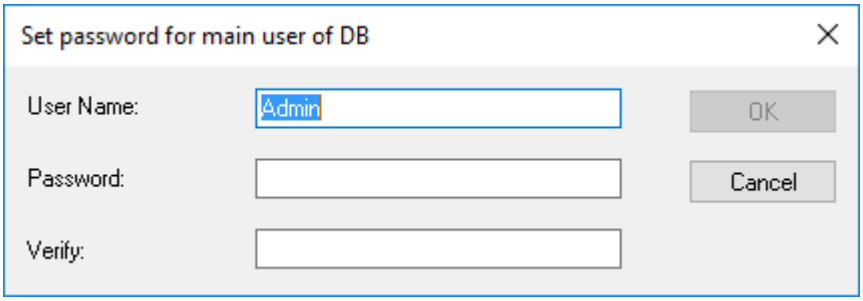
   ⇨ Das Zertifikat wird im Feld **OEM Certificate File** angezeigt.

8. Klicken Sie auf **OK**.

   ⇨ Sie werden nun in einem Dialog dazu aufgefordert, ein Passwort für den (signierenden) Administrator der Datenbank anzugeben.

9. Geben Sie ein Passwort an und bestätigen Sie das Passwort durch eine wiederholte Eingabe. Verwenden Sie unbedingt ein starkes Passwort, da die Datenbank sonst leicht angreifbar wird!
10. Klicken Sie auf **OK**.

11. Nur Build 4024: Nun werden Sie aufgefordert, den zweiten (inhaltverwaltenden) Administrator der Datenbank anzulegen:

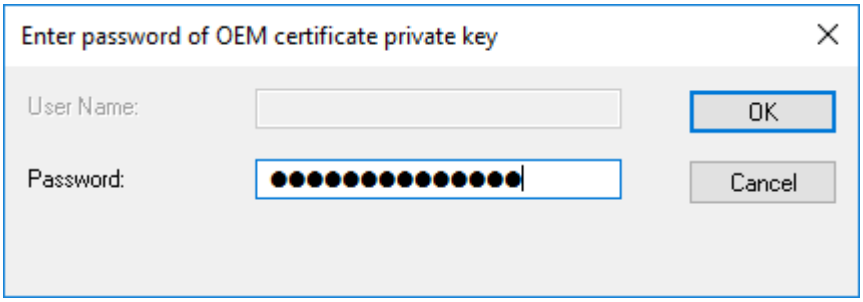


Diesen können Sie mit dem gleichen Benutzernamen und demselben Passwort wie den signierende Administrator ausstatten. Dadurch ist die Verwaltung der Datenbank einfacher. Der Benutzername des vorher angelegten signierenden Administrators wird hier daher als Default-Wert vorgeschlagen.

Sie können aber auch die Funktion Inhaltsverwaltung (= dieser Administrator) und die Funktion Freigabe der Änderungen (= signierender Administrator) trennen, wenn Sie dieses wünschen.

Hinweis **Sie können später, nach Erstellung der Datenbank, noch weitere Administratoren anlegen oder Änderungen vornehmen.**
Hinweis **Sofern Sie nur einen einzigen Benutzer benötigen, der alles machen darf, müssen Sie keine weiteren Benutzer mehr anlegen. Dies ist z. B. der Fall, wenn Sie Ihr Projekt einfach nur verschlüsseln, und keine weitere Unterscheidung bei Zugriffsrechten machen wollen.**

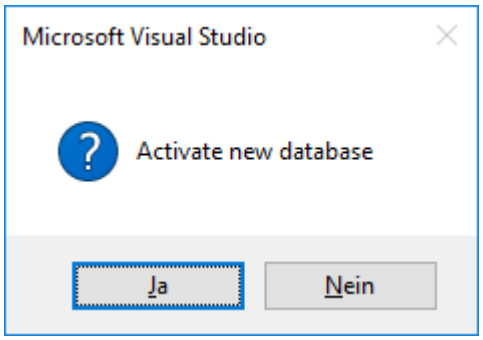
12. Klicken Sie auf **OK**.
    ⇨ Die Datenbank wird gespeichert. Sie werden in einem Dialog dazu aufgefordert, das Passwort des OEM Private Key einzugeben, mit dem die Datenbank signiert werden muss, um verwendet werden zu können.
13. Geben Sie das Passwort des OEM Zertifikates an und bestätigen Sie den Dialog mit **OK**.



Hinweis: Das OEM-Zertifikat benötigen Sie ab nun nicht mehr, wenn Sie mit dieser Datenbank arbeiten (z. B. Änderungen am Inhalt vornehmen).

⇨ Ein weiterer Dialog öffnet sich mit der Nachfrage, ob die Datenbank auch gleich in Visual Studio als aktuelle Datenbank eingestellt („aktiviert“) werden soll.

14. Falls ja, bestätigen Sie den Dialog mit **OK**.



⇨ Die neue Datenbank wird damit als **aktuelle** Datenbank in Visual Studio eingestellt.

Die aktuell eingestellte Datenbank wird jeweils für die (neue) Verbindung eines Projektes zu einer Datenbank genutzt.

Die einem Projekt zugeordnete Datenbank wird im Projekt hinterlegt (Dateiname und User DB Key).

Der Speicherort der Datenbank ist C:\TwinCAT\3.1\CustomConfig\UserDBs.

Wenn Sie diese (oder eine andere) Datenbank als Standarddatenbank festlegen wollen (die standardmäßig beim Start von Visual Studio verwendet werden soll), legen Sie dieses in der Registerkarte **Database** des Konfigurationsfensters fest. Die Vorgehensweise wird im nächsten Kapitel beschrieben.

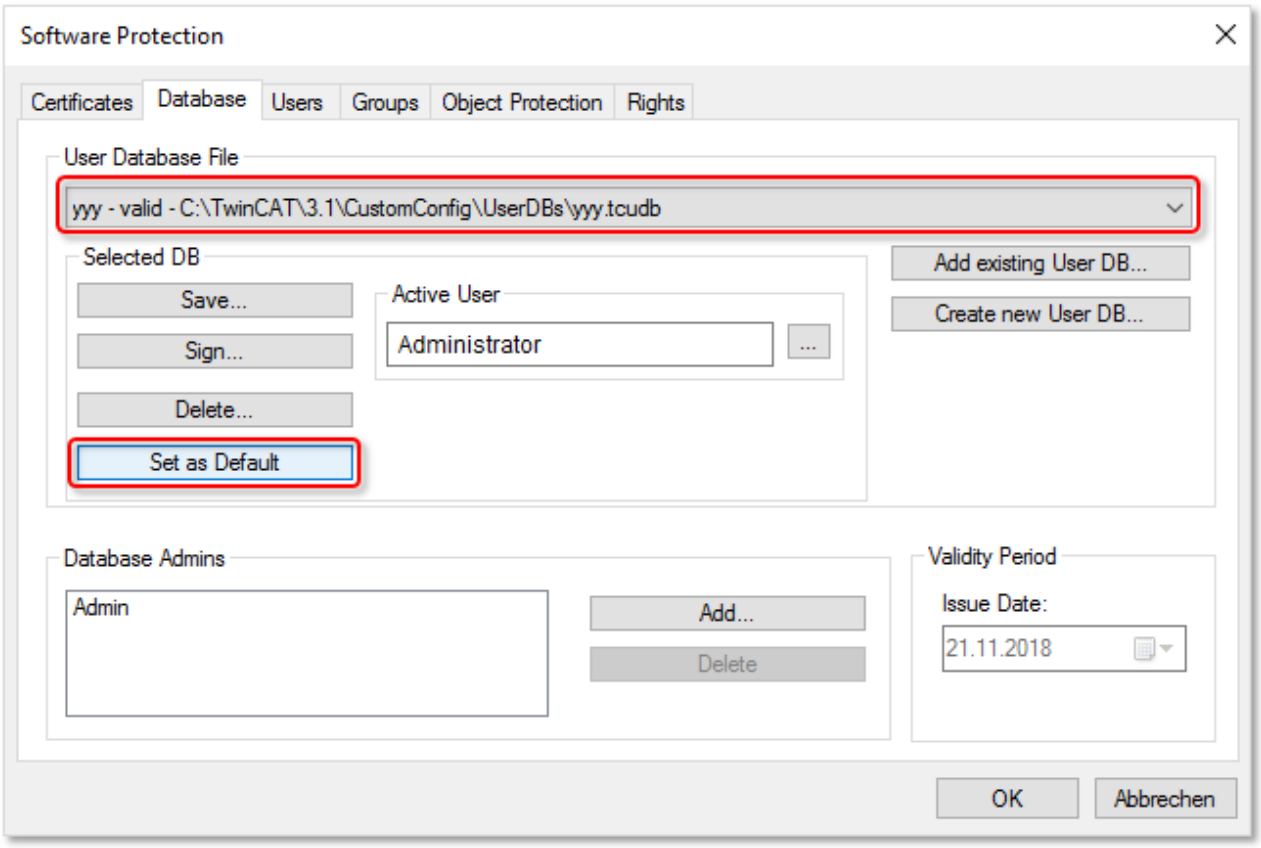
5.2 Standardeinstellungen für die Benutzerdatenbank in Visual Studio festlegen

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Vorgabe der Standardeinstellungen beim Start von Visual Studio

Wenn Sie eine Datenbank als Standarddatenbank festlegen wollen (die standardmäßig beim Start von Visual Studio verwendet werden soll), wählen Sie in der Registerkarte **Database** des Software Protection Konfigurationsfensters die gewünschte Datenbank aus und klicken auf **Set as Default**.

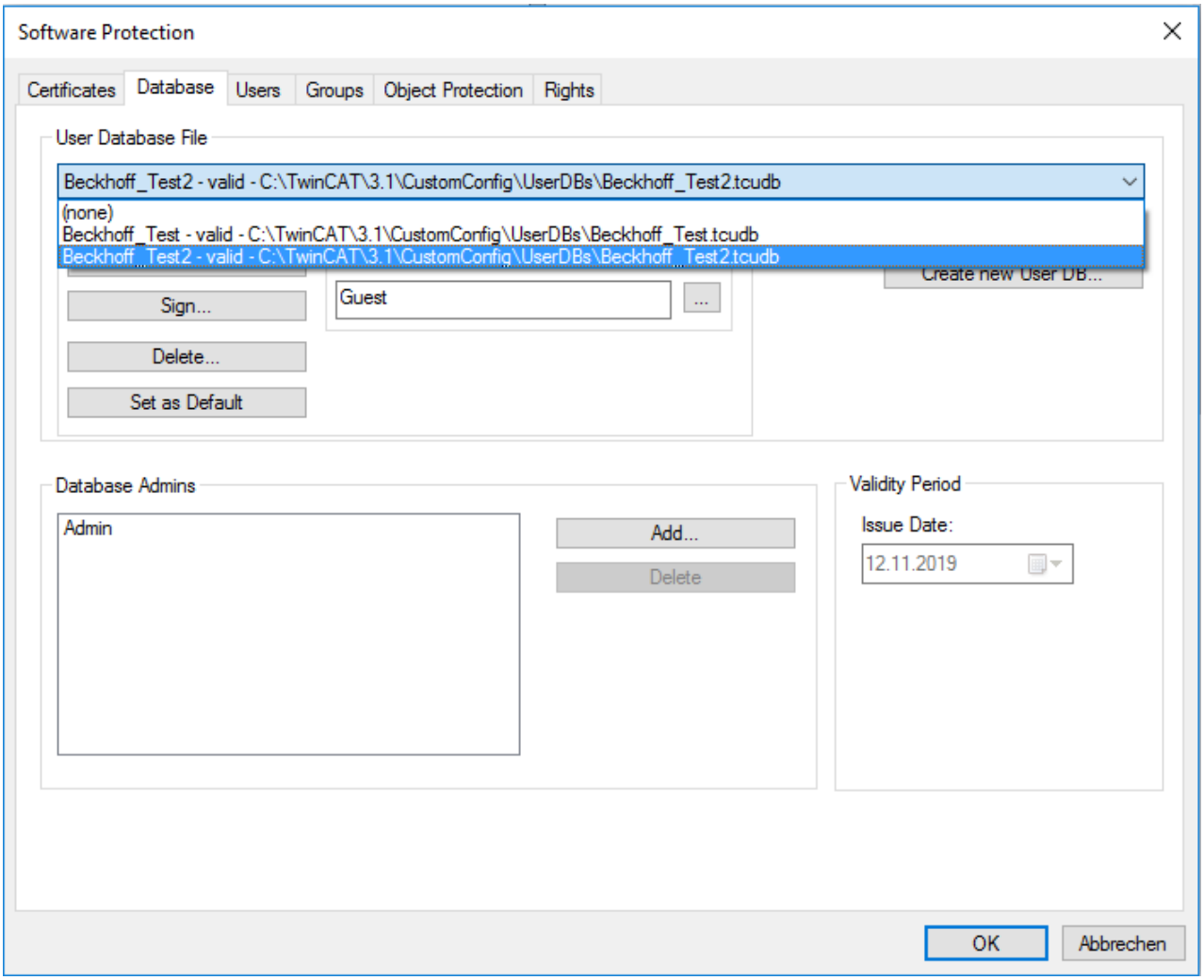


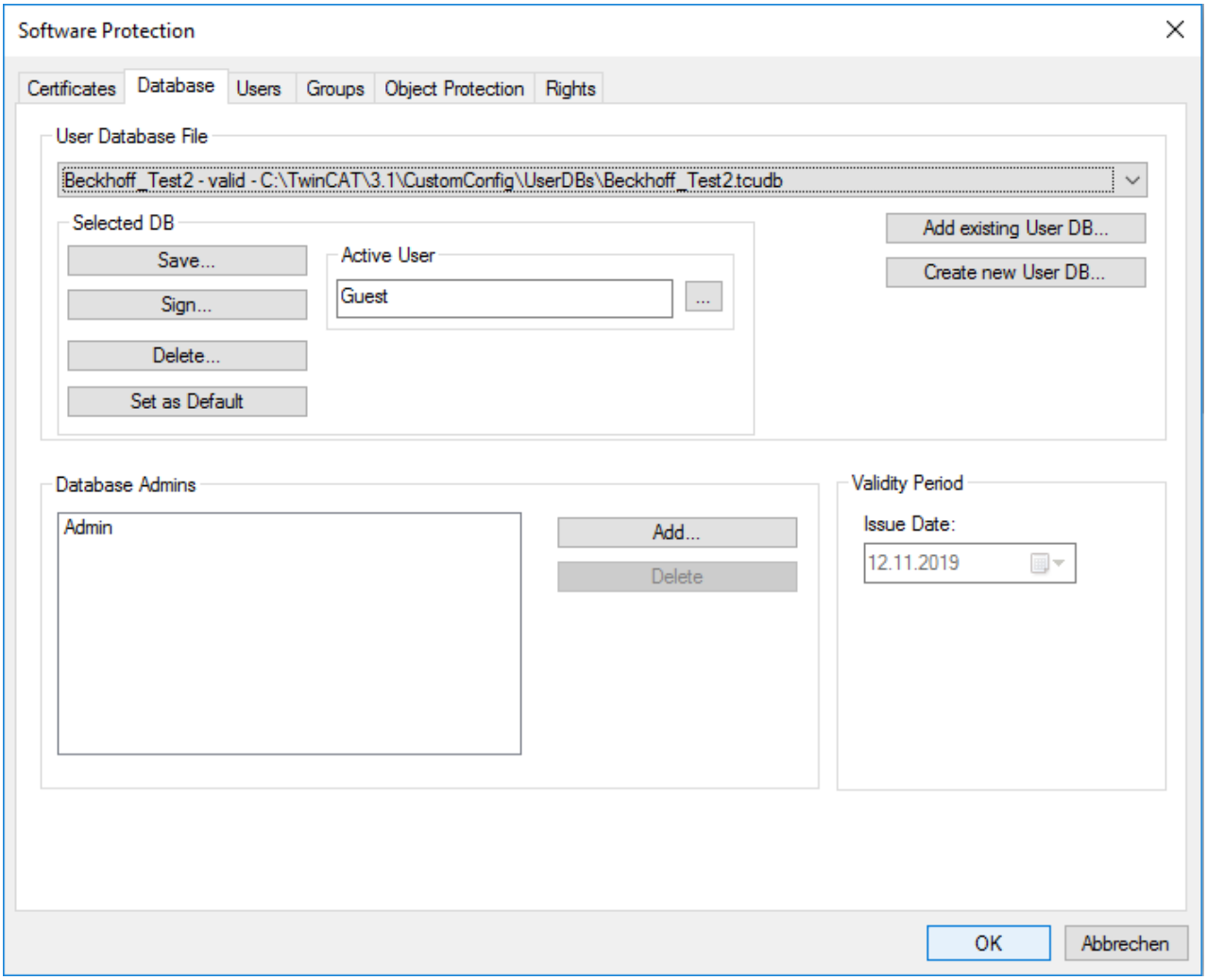
Sie können auch angeben, welcher Benutzer nach dem Start von Visual Studio automatisch aktiv sein soll. Dieses geben Sie im Textfeld **Active User** an.

5.3 Aktuelle Benutzerdatenbank in Visual Studio auswählen

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.


Software Protection
Certificates
Database
Users
Groups
Object Protection
Rights
User Database File
Beckhoff_Test2 - valid - C:\TwinCAT\3.1\CustomConfig\UserDBs\Beckhoff_Test2.tcudb
(none)
Beckhoff_Test - valid - C:\TwinCAT\3.1\CustomConfig\UserDBs\Beckhoff_Test.tcudb
Beckhoff_Test2 - valid - C:\TwinCAT\3.1\CustomConfig\UserDBs\Beckhoff_Test2.tcudb
Create new User DB...
Sign...
Guest
...
Delete...
Set as Default
Database Admins
Admin
Add...
Delete
Validity Period
Issue Date:
12.11.2019
OK
Abbrechen



5.4 Standard-Benutzer in der Benutzerdatenbank

Nach dem Anlegen der Benutzerdatenbank unter Benutzung der Vorlage „TemplateOEM“ beinhaltet diese zwei Standard-Benutzer:

- Guest (darf nichts)
- Administrator* (darf alles)
  * Der Name des Administrators wird beim Anlegen der Benutzerdatenbank [▶ 33] festgelegt.

Sofern es um den einfachsten Anwendungsfall geht – es gibt einen Benutzer, der alles darf (Administrator) und einen Benutzer der nichts darf (Guest), ist es nicht erforderlich, weitere Benutzer anzulegen, und man kann die frisch anlegte Benutzerdatenbank ohne weitere Konfiguration einsetzen. In diesem Fall können Sie gleich hier weitermachen: Benutzerdatenbank mit dem Projekt verbinden [▶ 70]

Falls Sie komplexere Zugriffsszenarien abdecken möchten, können Sie die Benutzerdatenbank nach Bedarf erweitern. Das wird im Kapitel Benutzerdatenbank erweitern [▶ 50] beschrieben.

5.5 Extensions für Benutzerdatenbanken

Voraussetzung: Mindestens TwinCAT 3 Build 4024.8

Die im Folgenden beschriebenen Funktionen erfordern mindestens TwinCAT 3 Build 4024.8.

Verzeichnis zum Speichern von Benutzerdatenbanken

Benutzerdatenbanken müssen im folgenden Verzeichnis gespeichert sein, um im TwinCAT Engineering genutzt werden zu können: C:\TwinCAT\3.1\CustomConfig\UserDBs

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Einführung

Ab Build 4024.8 unterstützt die TwinCAT Software Protection Erweiterungsdateien für die Benutzerdatenbank, sogenannte „User DB Extensions“.

- Eine Benutzerdatenbank kann mit diesen „Extensions“ erweitert werden.
- Eine Extension ist eine zusätzliche XML-Datei, die vom Aufbau her der Haupt-Benutzerdatenbank entspricht, aber nur zusammen mit der Haupt-Benutzerdatenbank verwendet werden kann. Eine Extension ist also allein, ohne Haupt-Benutzerdatenbank, nicht nutzbar.
- Eine Extension kann nur die Definition von Benutzern, aber nicht die Definition von Gruppen oder Object Protection Leveln enthalten.
- Eine Extension hat keinen eigenen Administrator. Der signierende Administrator der Haupt-Benutzerdatenbank ist ebenfalls der signierende Administrator der zugehörigen Extension.
- Eine vorhandene Extension-Datei kann auf Dateiebene hinzugefügt oder entfernt werden. Dafür ist keine Konfiguration in der zugehörigen Haupt-Benutzerdatenbank erforderlich (erfordert also keine Administrator-Rechte).
- Die Extensions werden in einem Unterverzeichnis mit dem Namen der Haupt-Benutzerdatenbank abgelegt (unterhalb des Verzeichnisses, dass die Haupt- Benutzerdatenbank enthält): C:\TwinCAT\3.1\CustomConfig\UserDBs\<Name der UserDB>.
- Eine Extension ist in der Regel zeitlich begrenzt.
- Eine Benutzerdatenbank kann eine beliebige Anzahl Extensions haben.

Hinweis **Eine sichere zeitliche Beschränkung erfordert eine manipulationsgeschützte Zeitreferenz.**

Anwendung:

- In der Haupt-Benutzerdatenbank werden statische Informationen (wie die Definition von Gruppen oder Object Protection Leveln) abgelegt.
- In der Extension werden zeitlich begrenzte Informationen (Benutzer) gespeichert, z. B. für Servicezwecke.

Eine Benutzerdatenbank kann auf Dateiebene ohne Weiteres gegen eine andere Version (mit gleichem Namen und gleichem User DB Key) ausgetauscht werden. Um Änderungen in der Benutzerdatenbank manipulationssicher zu machen (Schutz vor Austausch gegen eine ältere Version ohne die Änderungen), müsste eine komplett neue Benutzerdatenbank (mit einem anderen User DB Key) erzeugt und erneut mit dem Projekt verbunden werden. Das ist aber in der Praxis häufig nicht realisierbar. Das kann einfach und elegant mit Extensions der Benutzerdatenbank gelöst werden.:

- Die Haupt-Benutzerdatenbank (mit den statischen Informationen wie der Definition von Gruppen oder Object Protection Leveln) ist fest mit dem Projekt verbunden.
- Die (zeitlich begrenzte) Extension enthält alle Informationen (Benutzer), die sich über die Zeit ändern können.

Hinweis **In einfachen Szenarien (wenige Benutzer) könnte man das auch mit einer zeitlich beschränkten Benutzerdatenbank (ohne die Nutzung von Extensions) lösen. Bei komplexeren Szenarien, speziell im Service-Bereich, ist das jedoch keine praxisgerechte Lösung.**

Szenarien mit verschiedenen Benutzergruppen / Object Protection Leveln sind mit Extensions einfacher zu realisieren. So können z. B. Inhouse-Entwickler in einer eigenen Extension zusammengefasst werden, die bei der Auslieferung einfach nicht mit auf das Zielsystem kopiert wird. So können Bereiche (oder einzelne Benutzer) nach Bedarf hinzugefügt oder entfernt werden, ohne jeweils die ganze Benutzerdatenbank anpassen zu müssen.

Das ermöglicht auch eine deutliche Vereinfachung bei der Versionsverwaltung einer Benutzerdatenbank.

Beispielanwendung aus dem Service-Bereich

- Die Main User DB enthält nur die notwendigsten Informationen (signierende und ändernde Administratoren, Definition der OPLs und Gruppen).
- Die Extension wird speziell für den Service-Einsatz erzeugt und enthält lediglich die Servicekraft als Benutzer. Die Extension ist für den Zeitraum des Service-Einsatzes zeitbeschränkt.
- Die Servicekraft bringt die Extension auf dem Service-Notebook (oder einem USB Stick) mit.

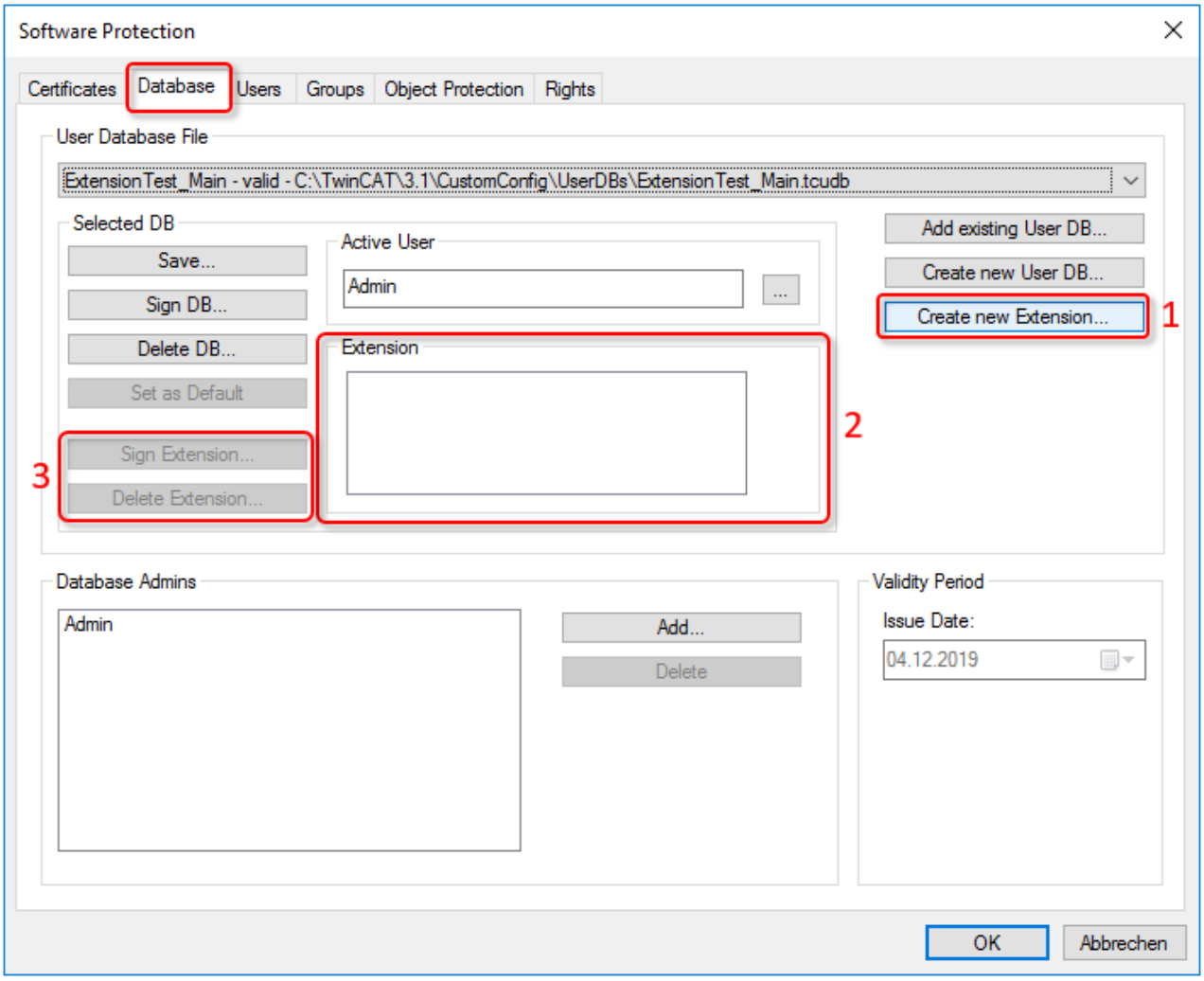
Zeitliche Beschränkung einer Benutzerdatenbank / Extension

Eine manipulationssichere zeitliche Beschränkung erfordert eine manipulationsgeschützte Zeitreferenz!

5.5.1 Zugehörige Elemente in der Konfigurationskonsole der Software Protection

Zum Management von Extensions und der darin definierten Benutzer stehen die im Folgenden beschriebenen Elemente in der Oberfläche der Konfigurationskonsole der Software Protection zur Verfügung.

Tab Database:

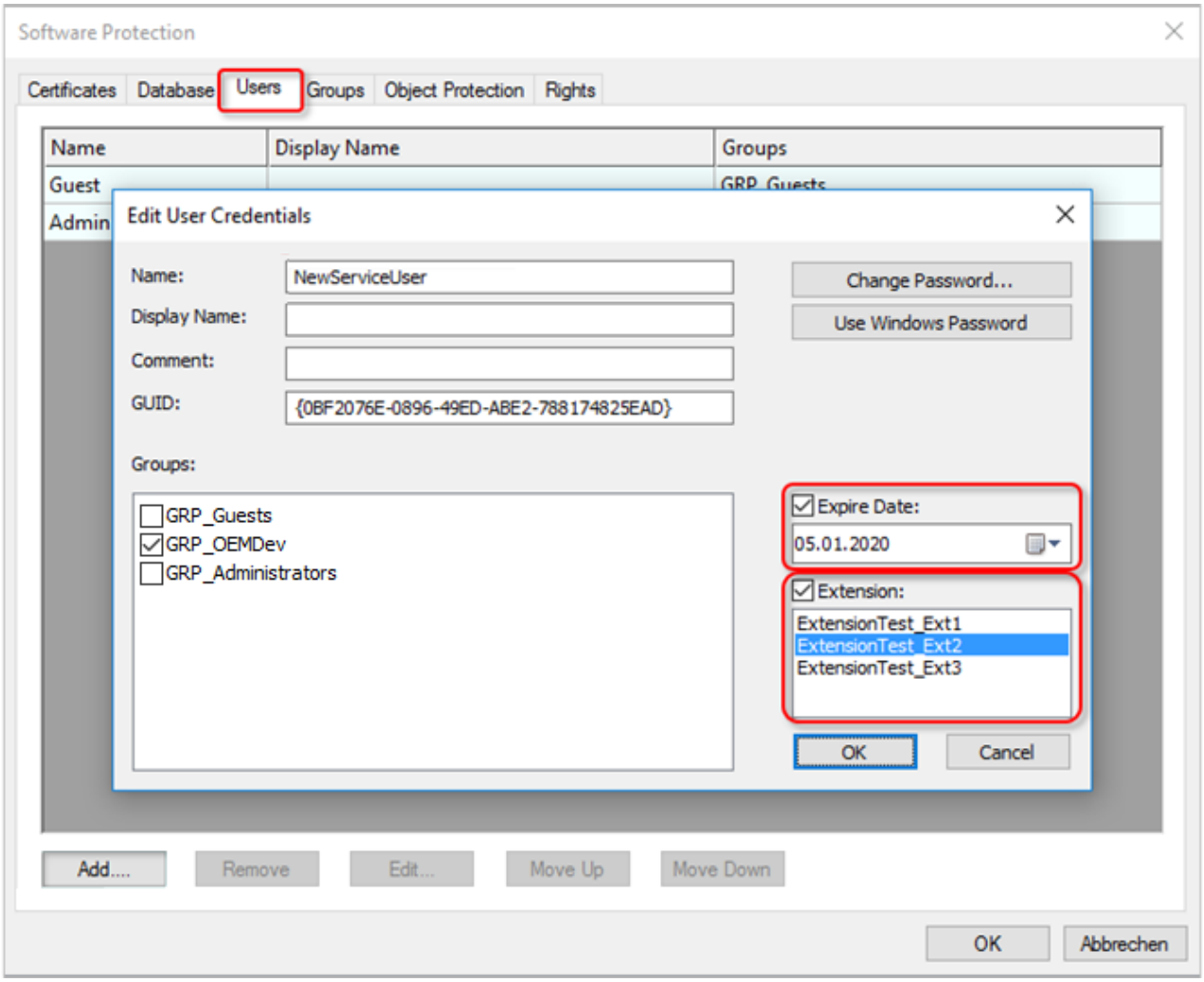


1: Erzeugen einer neuen Extension für die aktuell ausgewählte User DB

2: Liste der vorhandenen Extensions

3: Signieren oder Löschen der in (2) ausgewählten Extension

Tab Users:



Ein Benutzeraccount kann hier einer vorhandenen Extension zugeordnet und ein Ablaufdatum für den Account festgelegt werden.

5.5.2 Anlegen von Extensions und Benutzern im TwinCAT 3 Engineering

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

5.5.2.1 Anlegen von Extensions

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

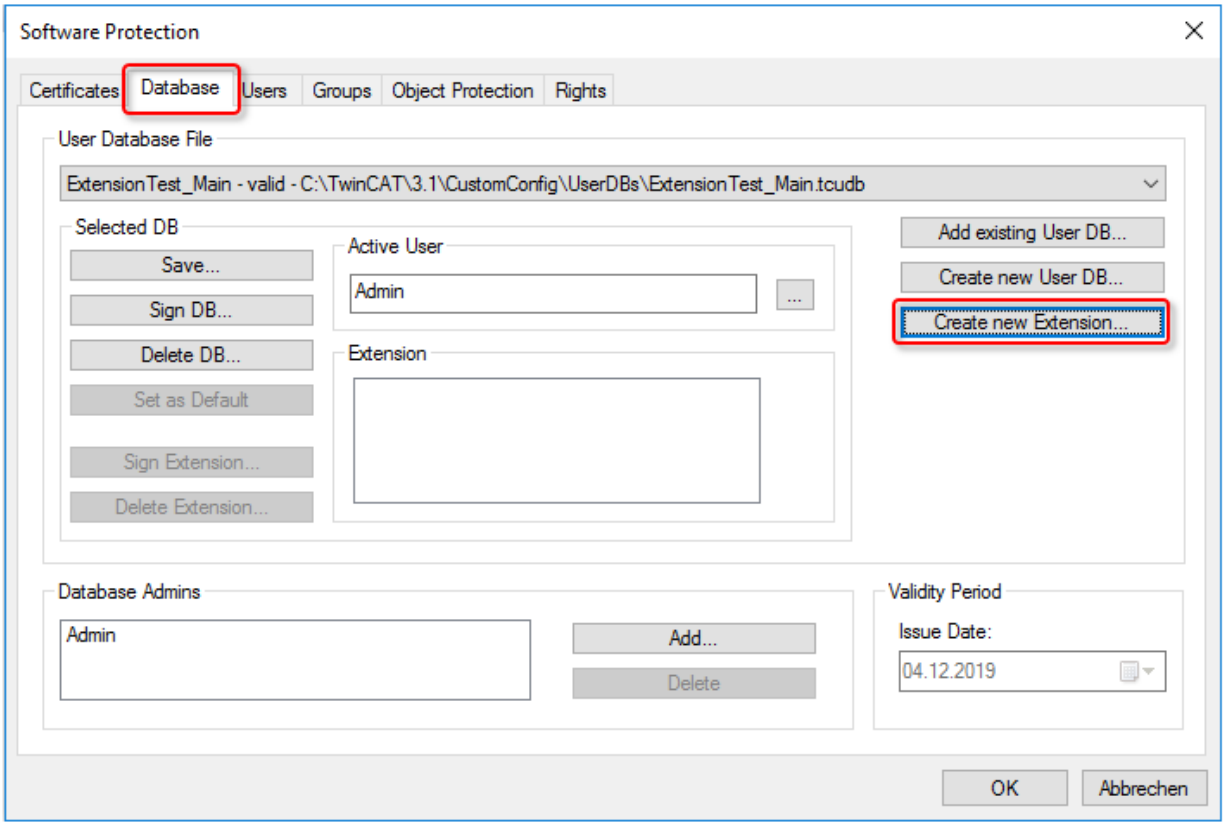
Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Änderungen in einer Extension müssen signiert werden

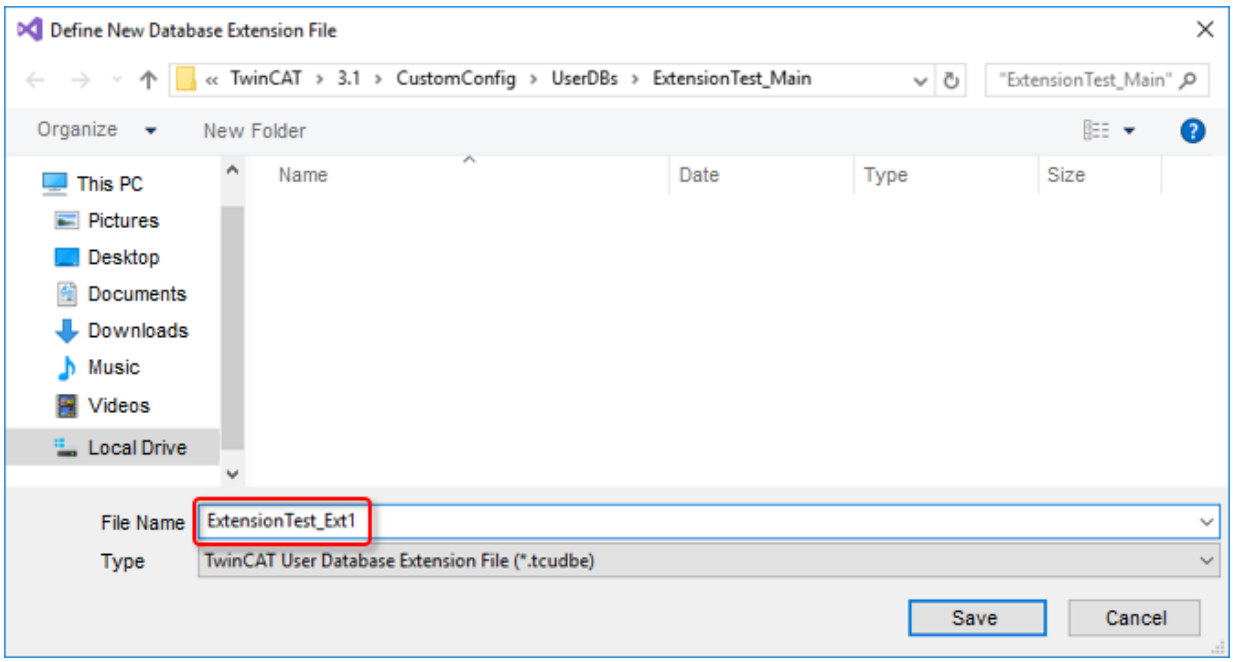
Die Änderungen in einer Extension (dazu gehört auch die initiale Erzeugung der Extension) müssen vom signierenden Administrator signiert werden, sonst ist die Extension ungültig.

Anlegen einer neuen Extension

✓ Der aktuelle Benutzer muss (editierende) Administrator-Rechte haben!

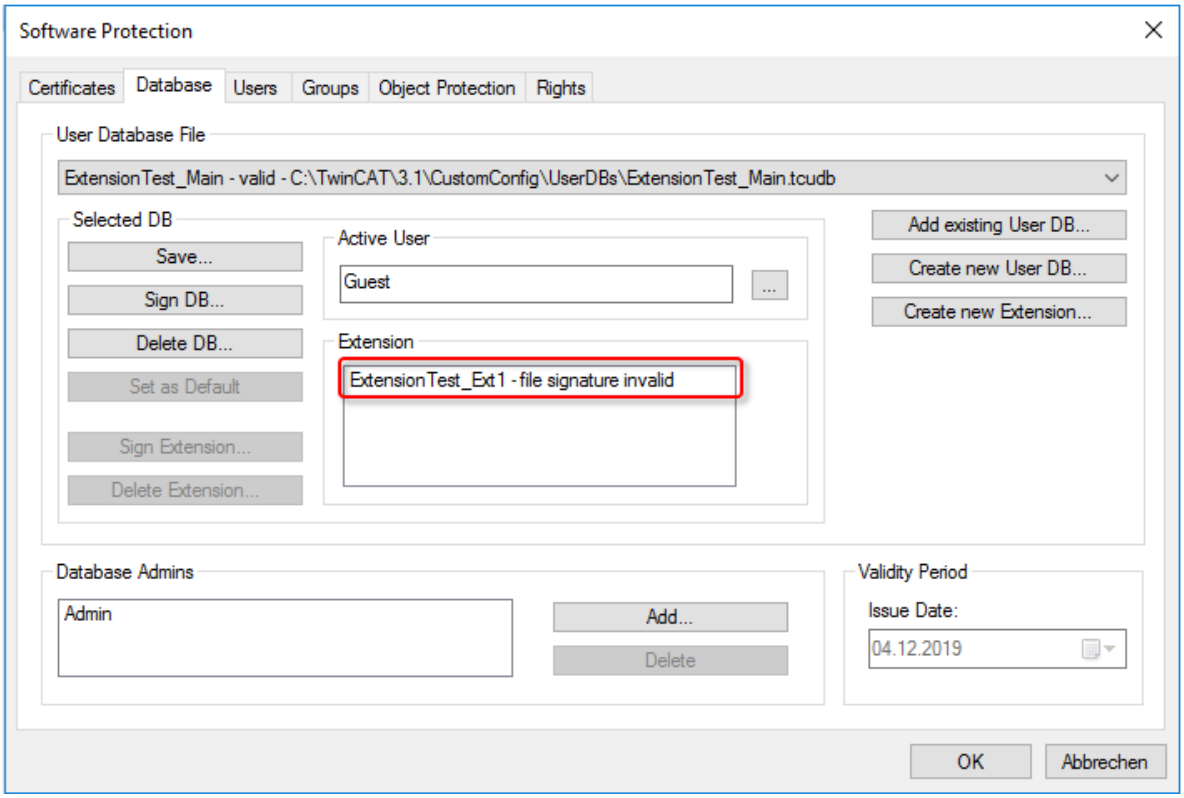


1. Mit einem Klick auf **Create new Extension** öffnet sich ein Dialog zum Anlegen einer neuen Extension:

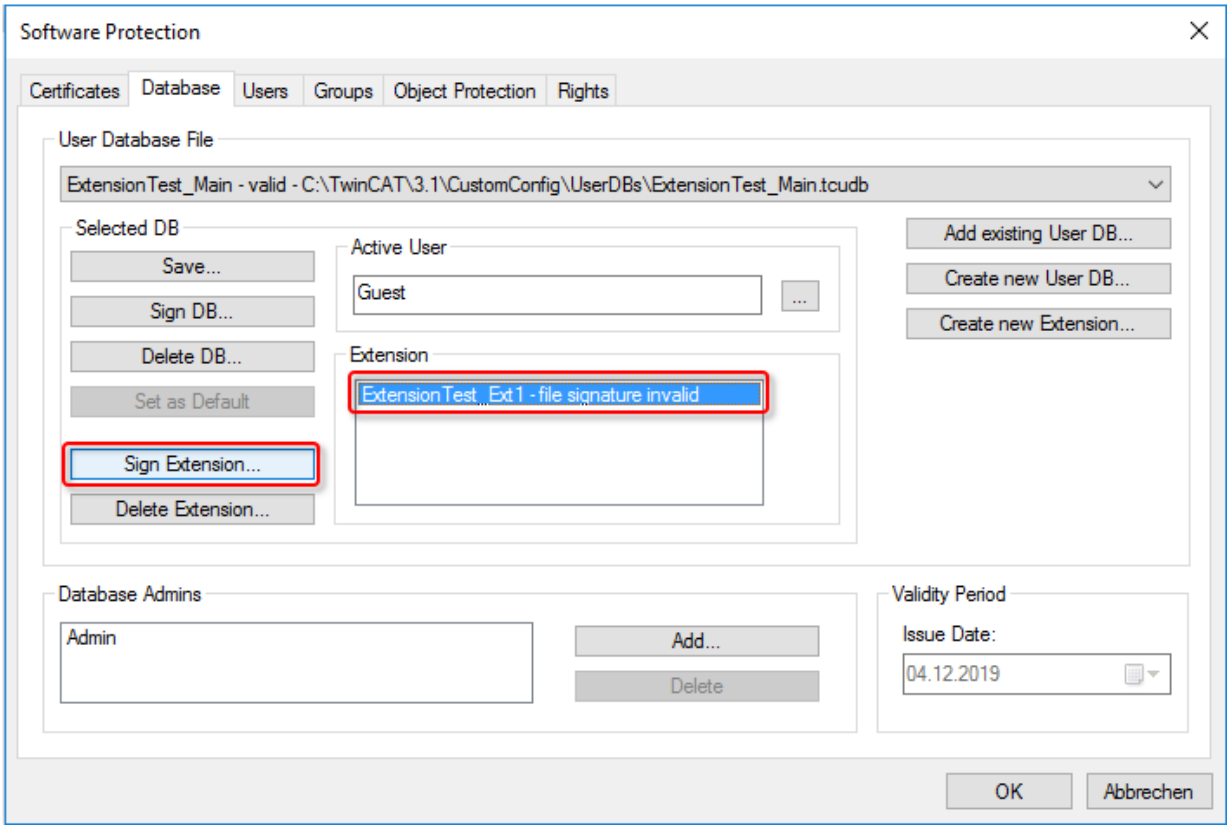


Hinweis **Das vorgegebene Verzeichnis darf nicht verändert werden!**

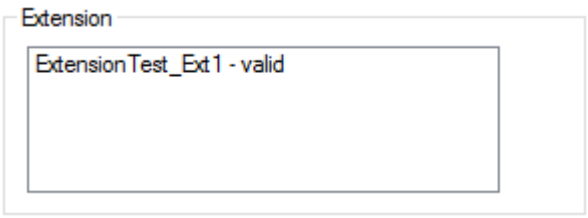
⇨ Die neue Extension ist nun angelegt – allerdings zunächst noch mit dem Status „invalid“, da sie noch nicht signiert wurde:



1. Die Extension wird dazu im Tab **Database** in der Liste der Extensions durch einen Klick angewählt, dann kann sie vom signierenden Administrator (der Main User DB) signiert …



2. … und somit gültig gemacht werden:



Die Extension ist jetzt als leere Hülle angelegt und muss nun noch mit Inhalt (Benutzern) gefüllt werden.

5.5.2.2 Anlegen von Benutzern in Extensions

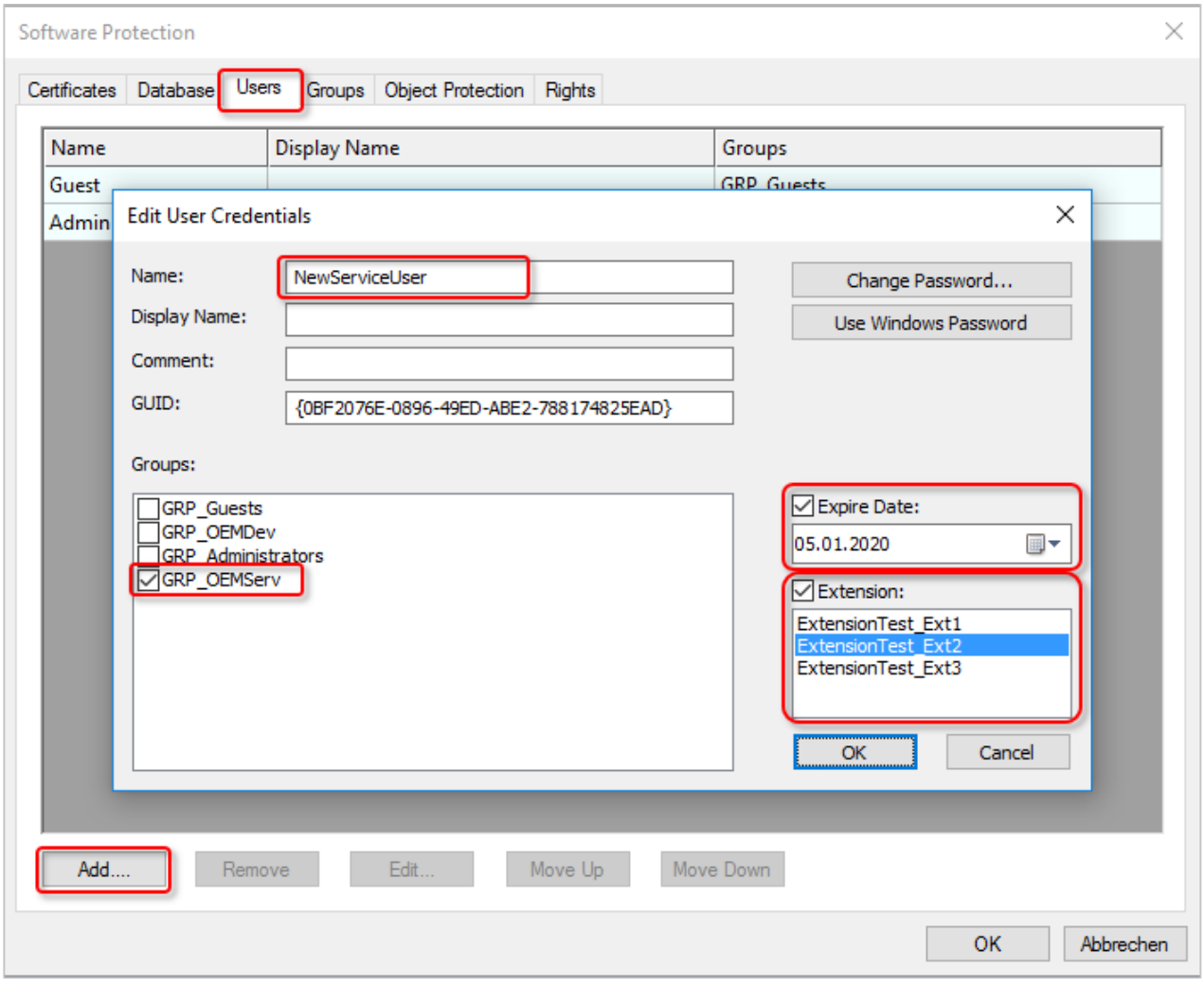
Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Änderungen in einer Extension müssen signiert werden

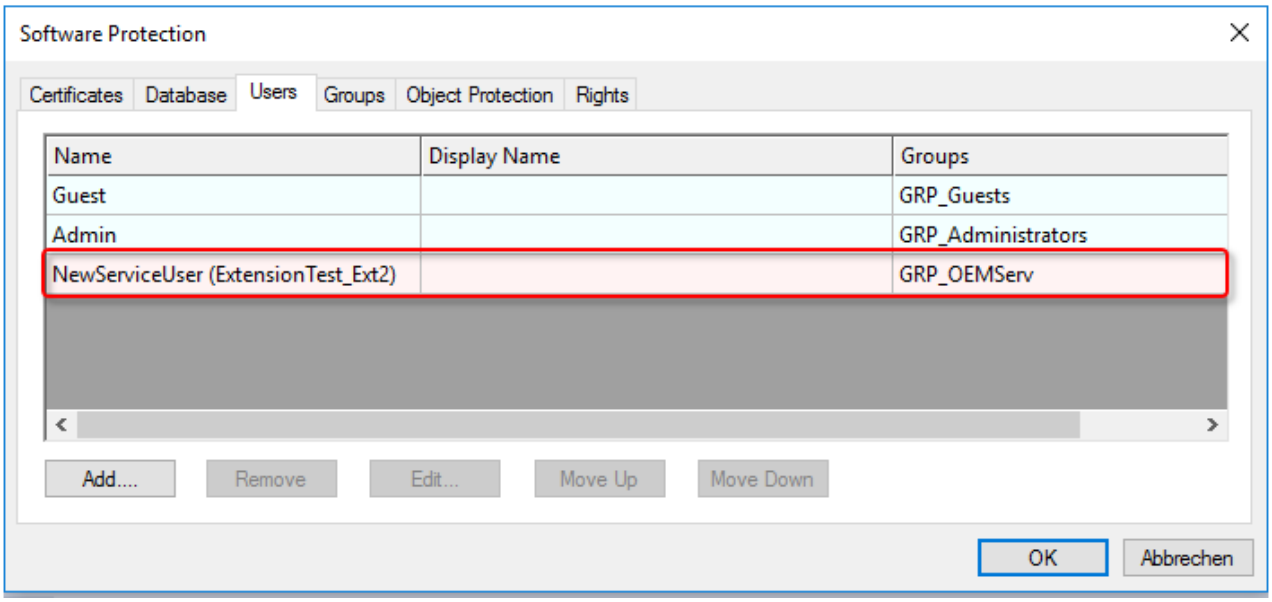
Die Änderungen in einer Extension (dazu gehört auch die initiale Erzeugung der Extension) müssen vom signierenden Administrator signiert werden, sonst ist die Extension ungültig.

Beispiel: Im Reiter **Users** wird ein neuer Benutzer („NewServiceUser“) angelegt, der Gruppe „GRP_OEMServ“ sowie einer Extension zugeordnet, und die gewünschte zeitliche Begrenzung eingestellt:



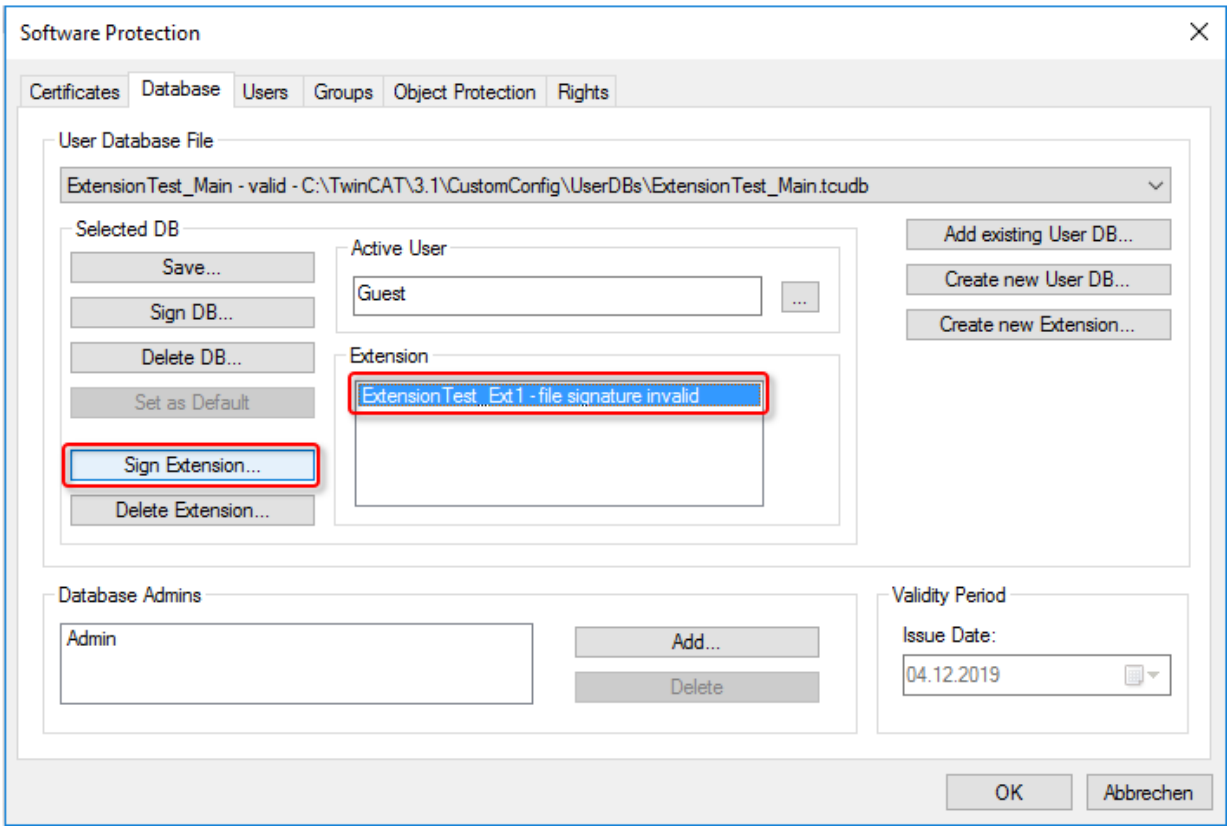
Damit ist der neue Benutzer in der ausgewählten Extension angelegt.

Seine Zugehörigkeit zu einer Extension wird in der Liste der vorhandenen Benutzeraccounts durch eine andere Farbe und die Nennung der Extension in Klammern hinter dem Benutzernamen dargestellt:

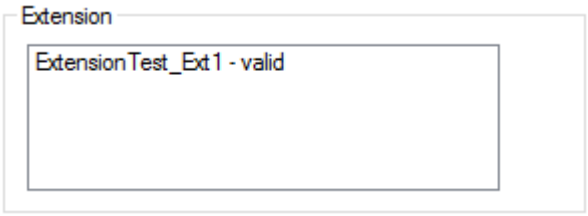


Nun müssen die Änderungen in der Extension noch signiert werden, damit sie gültig sind.

1. Die Extension wird dazu im Tab **Database** in der Liste der Extensions durch einen Klick angewählt, dann kann sie vom signierenden Administrator (der Main User DB) signiert …



2. … und somit gültig gemacht werden:



5.6 Benutzerdatenbank erweitern

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Änderungen in der Datenbank müssen beim Speichern signiert werden

Die Änderungen in der Datenbank müssen vom signierenden Administrator signiert werden, sonst ist die Datenbank ungültig. Das Signieren wird automatisch beim Speicherprozess abgefragt.

Datenbankvorlage „TemplateOEM“

Die Datenbankvorlage „*TemplateOEM*“ ist so ausgelegt, dass die häufigsten (einfachen) Anwendungsfälle abgedeckt werden können, ohne eigene Gruppenberechtigungen definieren zu müssen. Diese sind:

- Zwei Benutzer: Einer darf alles, der andere nichts [▶ 41].
- Hinzufügen/Ändern von Datenbank-Administratoren [▶ 50]
- Trennung der Funktionen Datenbank-Administrator und Entwickler [▶ 54]
- Hinzufügen weiterer Benutzer mit der Gruppenzuordnung „Developer“ [▶ 55]

Für weitere Anwendungsfälle müssen eigene Gruppenberechtigungen [▶ 57] definiert werden.

Download-Link: Planungstabelle für Gruppenrechte und Object Protection Level

Eine Excel-Tabelle zur einfachen Planung von Gruppenrechten und Zugriffsberechtigungsgruppensets (Object Protection Level) können Sie https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip herunterladen.

5.6.1 Hinzufügen/Ändern von Datenbank-Administratoren

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

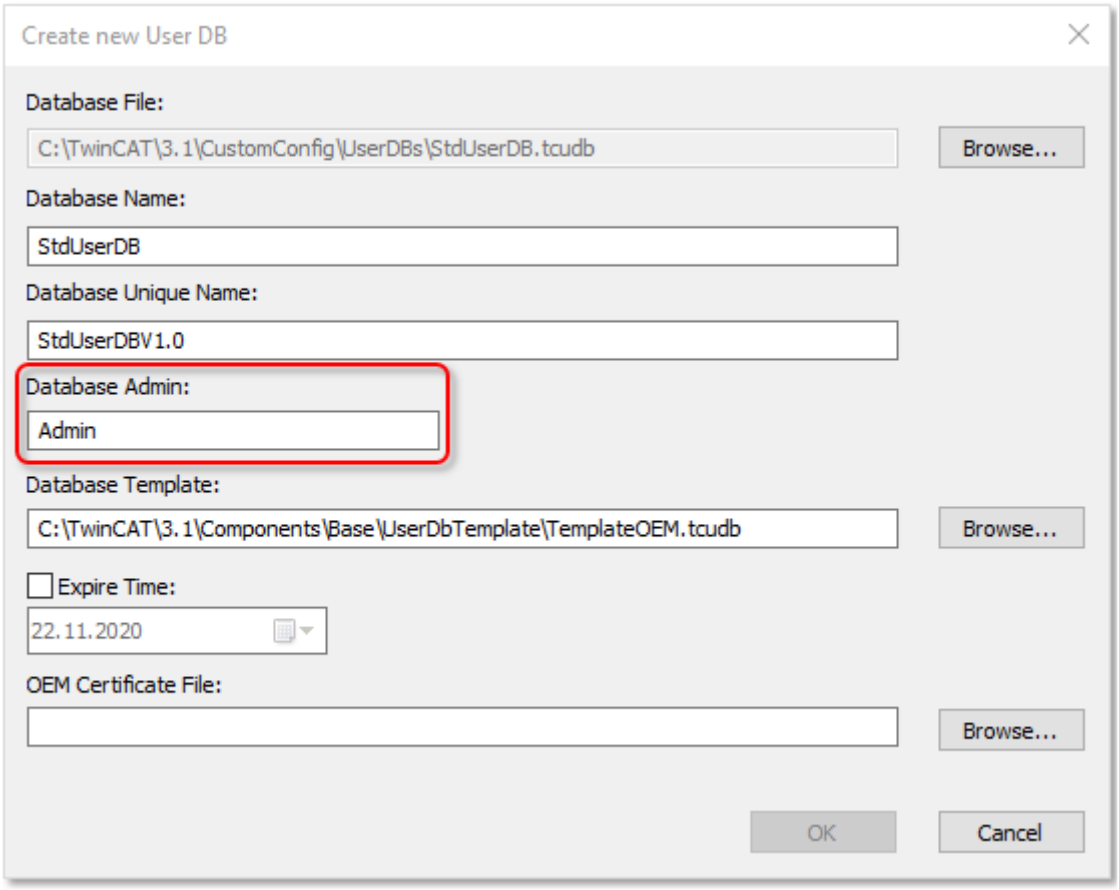
Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Diese Beschreibung ist für **Build 4024** ausgelegt.

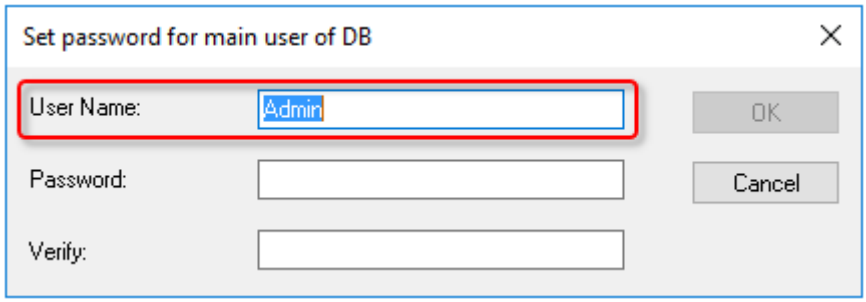
Die Benutzerdatenbank beinhaltet zwei Administratoren mit unterschiedlichen Aufgabenbereichen:

1. Signieren (freigeben) von Änderungen an der Datenbank
2. Inhalt der Datenbank ändern

Der erste (signierende) Administrator wird direkt beim Erstellen der Benutzerdatenbank angelegt:



Nach dem Anlegen des ersten Datenbank-Administrators legt TwinCAT 3 den zweiten (editierenden) Administrator als Benutzer in der Datenbank an („main user“) und schlägt als Benutzernamen den des ersten (= signierenden) Administrators vor. So können bei Bedarf beide Administrator-Funktionen einfach zusammengefasst und mit demselben Benutzernamen und demselben Passwort angelegt und genutzt werden:



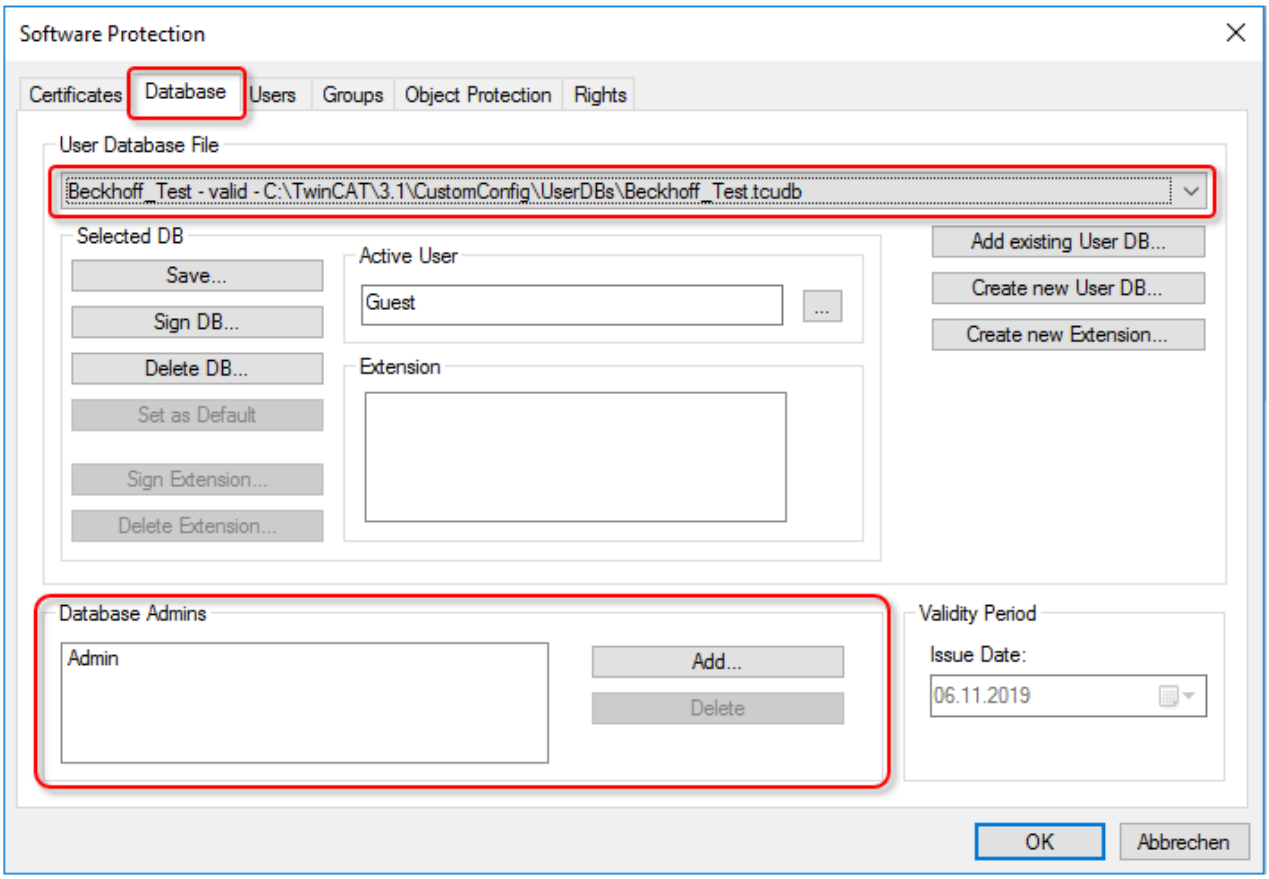
Build 4022:

Dieses Eingabefenster ist dort noch nicht vorhanden. Nach dem Anlegen der Benutzerdatenbank muss der editierende Datenbank-Administrator daher manuell als Benutzer angelegt und der Gruppe „GRP_Administrators“ zugewiesen werden.

Neue signierende Datenbank-Administratoren anlegen

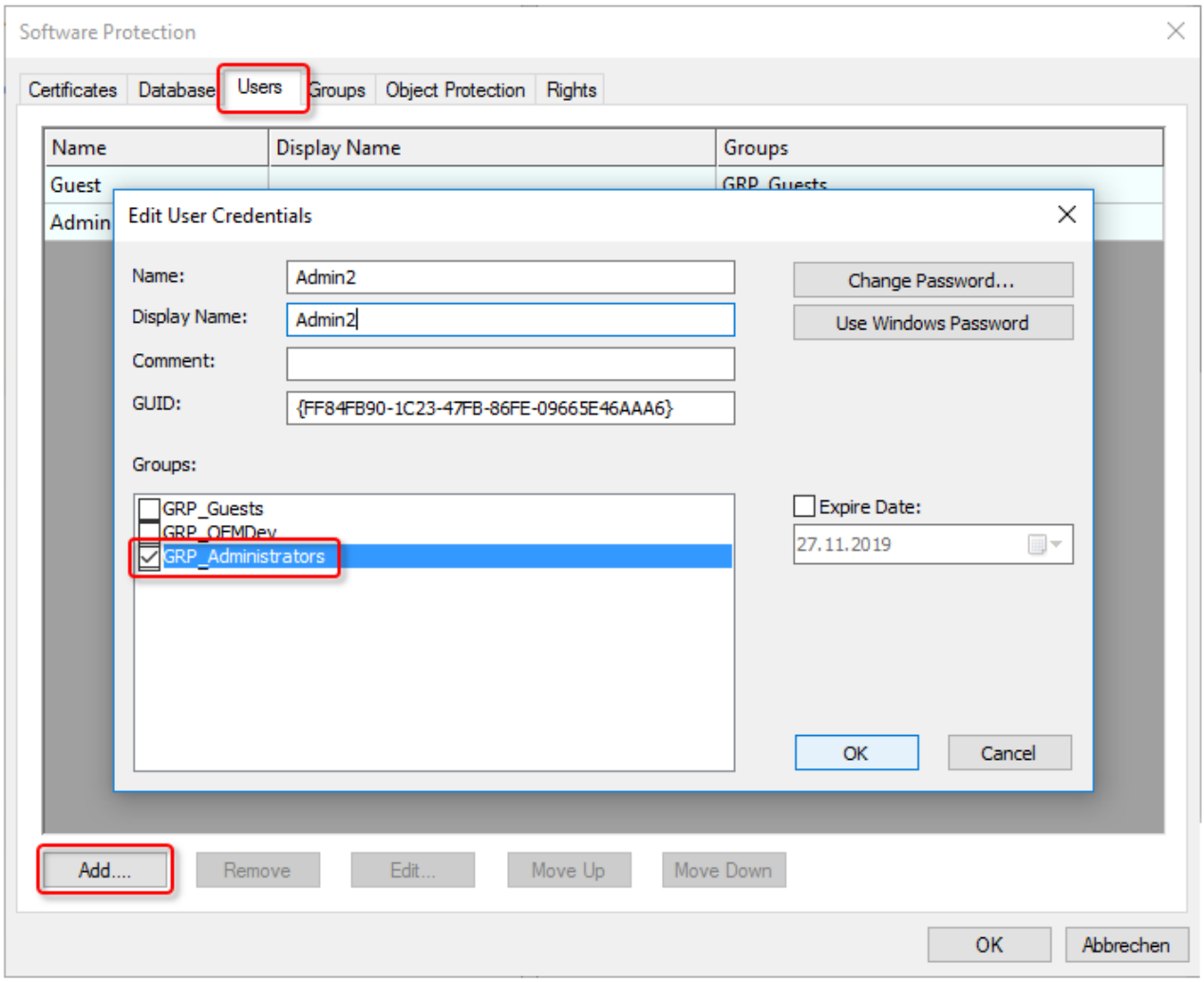
In der Konfigurationskonsole der Software Protection können weitere signierende Administratoren im Reiter **Database** angelegt werden.

Die gewünschte Datenbank muss ausgewählt sein; dann kann im Fensterbereich **Database Admin** ein neuer Administrator angelegt, oder ein bestehender gelöscht werden:



Neue editierende Datenbank-Administratoren anlegen

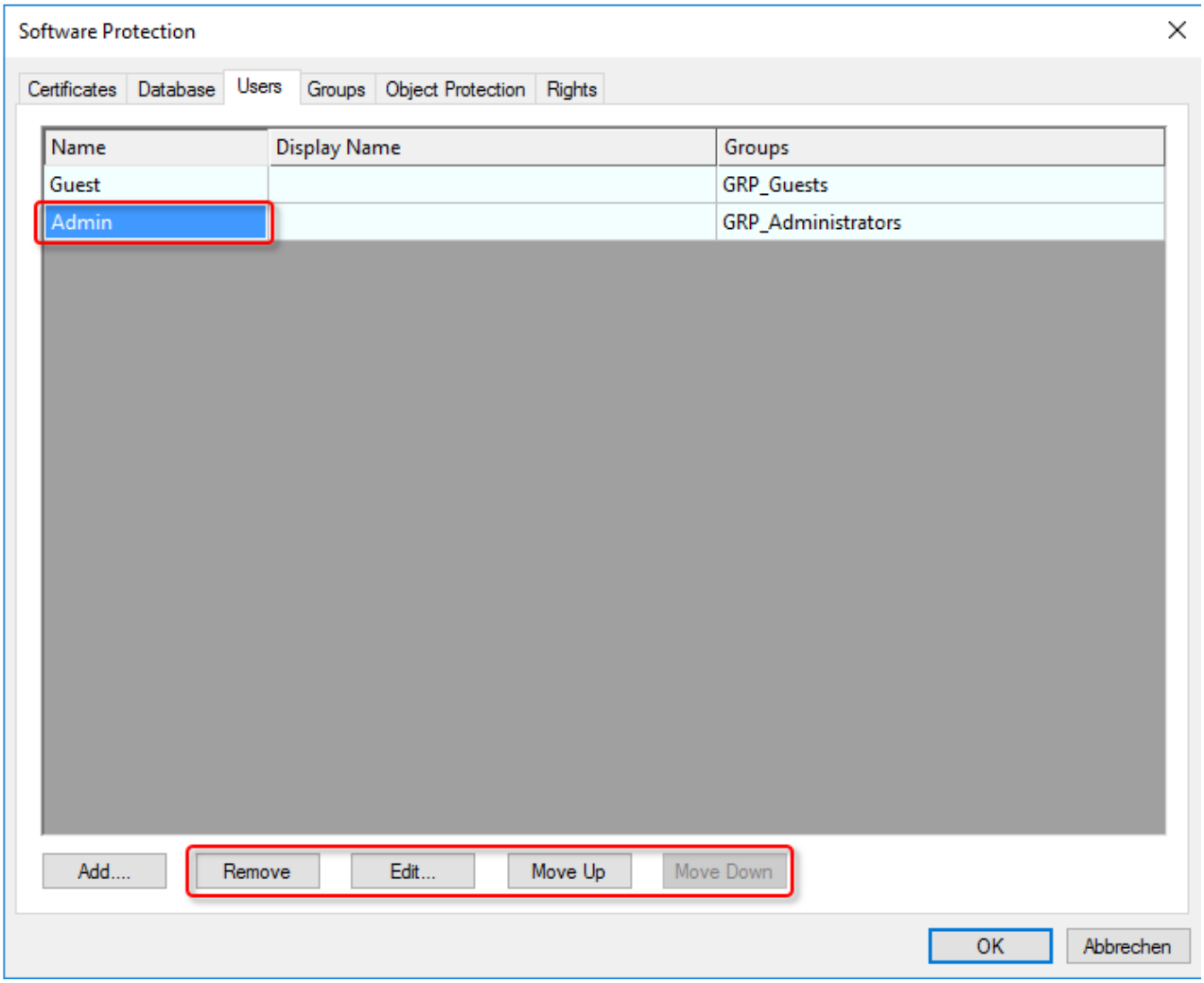
In der Konfigurationskonsole der Software Protection können weitere editierende Administratoren im Reiter **Users** angelegt werden:



Der neue Benutzer muss der Gruppe „GRP_Administrators“ zugeordnet werden.

Der Benutzer kann auch ein Windows Account (Domain User) sein; in dem Fall kann das zugehörige Windows Password zum automatischen Einloggen verwendet werden.

Nach Auswahl eines Benutzers kann dieser auch gelöscht, geändert oder in der Liste verschoben werden:



Es muss immer einen Benutzer mit Administrator-Rechten geben!

Wenn Sie keinen Benutzer mit Administrator-Rechten in der Benutzerdatenbank haben, können Sie keinerlei Änderungen mehr in der Datenbank vornehmen (auch keinen neuen Administrator hinzufügen!). Es muss daher immer mindestens einen Benutzer mit (editierenden) Administrator-Rechten geben! (Der signierende Administrator reicht nicht aus, da er keine Änderungen an der Benutzerdatenbank vornehmen darf.)

5.6.2 Trennung der Funktionen Datenbank-Administrator und Entwickler

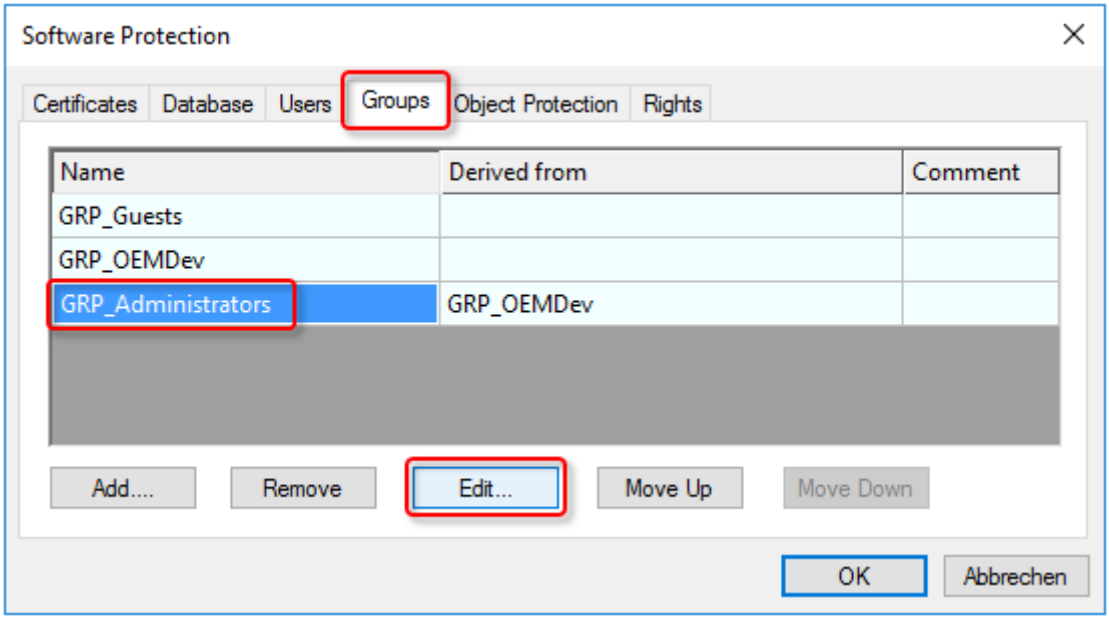
Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

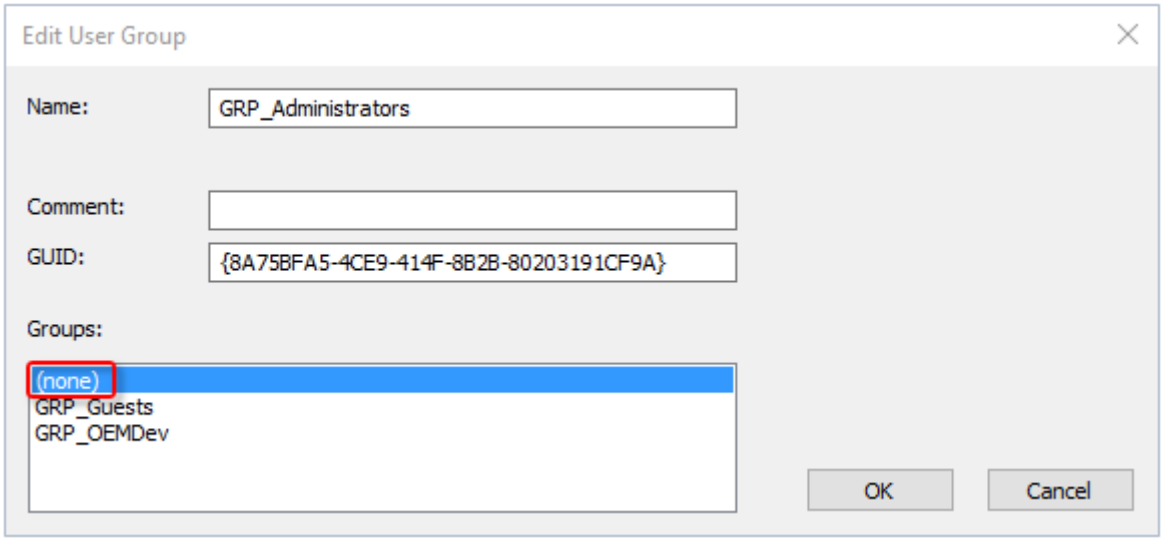
Standardmäßig erbt die Gruppe „GRP_Administrators“ auch die Rechte der Gruppe „GRP_OEMDev“ (Developers).

Soll der (editierende) Administrator der Benutzerdatenbank keine Rechte zum Ändern der TwinCAT Solution haben, muss nur die Zugehörigkeit der Gruppe „GRP_OEMDev“ bei der Gruppe „GRP_Administrators“ geändert werden.

Dazu in der Konfigurationskonsole der Software Protection im Tab **Groups** die Gruppe „GRP_Administrators“ auswählen und dann auf den Button **Edit** klicken:



Dann kann die gewünschte Gruppenzugehörigkeit (oder „None“ für keine) ausgewählt werden:



Nun kann ein (editierender) Administrator zwar noch die Benutzerdatenbank ändern, hat aber nicht mehr ebenfalls die Rechte der Gruppe „GRP_OEMDev“ (Developers).

5.6.3 Hinzufügen von Benutzern zu einer Gruppe

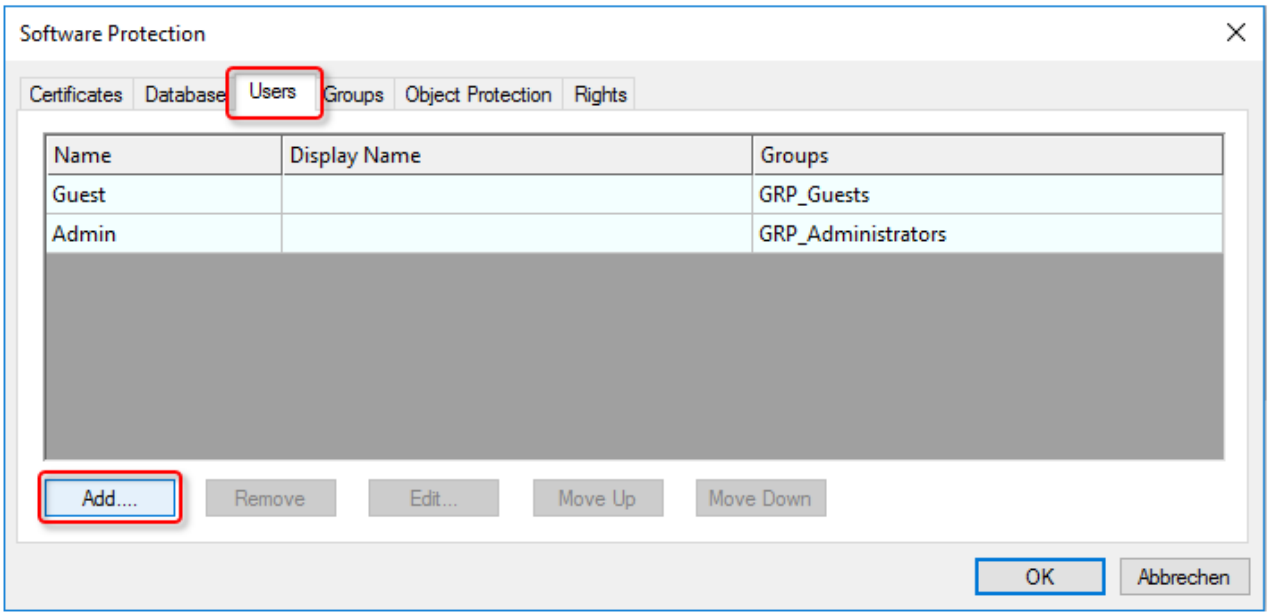
Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

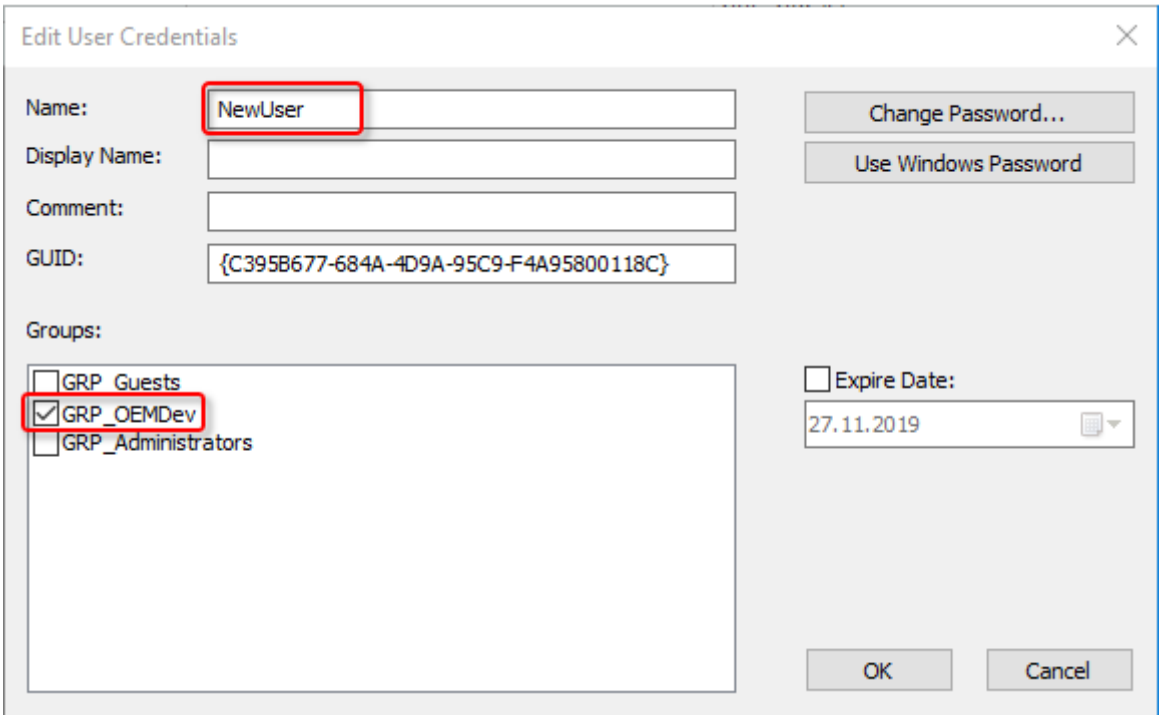
In diesem Beispiel wird ein Benutzer zur Gruppe „GRP_OEMDev“ hinzugefügt. Die Vorgehensweise gilt entsprechend auch für andere Gruppen.

Ein Benutzer kann auch Mitglied mehrerer Gruppen sein.

In der Konfigurationskonsole im Reiter **Users** auf den Button **Add…** klicken:



Nun kann ein neuer Benutzer angelegt und die gewünschte Gruppenzugehörigkeit eingestellt werden:



Der Benutzer kann auch ein Windows Account (Domain User) sein; in dem Fall kann das zugehörige Windows Password zum automatischen Einloggen verwendet werden.

Ab Build 4024.8

Benutzer können auch in sogenannten „Extensions [▶ 48]“ von Benutzerdatenbanken angelegt werden. Dieses ist hier [▶ 41] beschrieben.

Das Anlegen neuer und Anpassen von Benutzergruppen wird im Kapitel „Anlegen und Editieren von Benutzergruppen [▶ 62]“ erläutert.

5.6.4 Eigene Gruppenzugriffsberechtigungen definieren

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Download-Link: Planungstabelle für Gruppenrechte und Object Protection Level

Eine Excel-Tabelle zur einfachen Planung von Gruppenrechten und Zugriffsberechtigungsgruppensets (Object Protection Level) können Sie https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip herunterladen.

5.6.4.1 Einführung

Systemvoraussetzungen

Betriebssystem:

- Um alle Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist mindestens Windows 7 (bzw. dessen Embedded-Version) erforderlich. Windows XP und Windows CE (Windows Embedded Compact) unterstützen weder die Verschlüsselung der Boot-Datei noch OEM-Lizenzen.

TwinCAT-Version:

- Die beschriebenen Funktionalitäten erfordern mindestens TwinCAT 3.1 Build 4022.

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

Download-Link: Planungstabelle für Gruppenrechte und Object Protection Level

Eine Excel-Tabelle zur einfachen Planung von Gruppenrechten und Zugriffsberechtigungsgruppensets (Object Protection Level) können Sie https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip herunterladen.

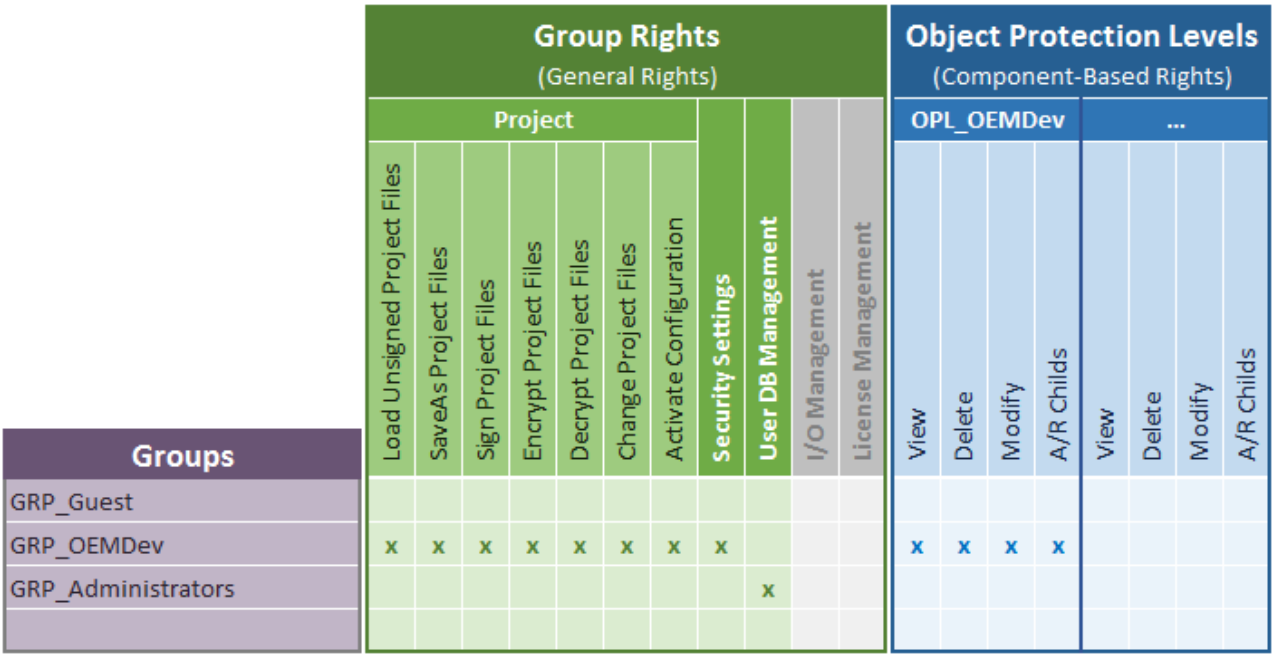
TwinCAT Benutzerzugriffsrechte

- Zugriffsrechte werden im TwinCAT 3 Engineering Gruppen zugewiesen.
- Benutzer können mehreren Gruppen zugewiesen werden.
- Gruppen können Mitglied **einer** anderen Gruppe sein.

Hinweis: Für eine bessere Übersicht wird empfohlen, Gruppen nicht einer anderen Gruppe zuzuordnen, sondern die Gruppe am besten komplett eigenständig mit Rechten zu versehen.

Rechte sind im TwinCAT 3 Engineering in zwei Hauptkategorien aufgeteilt:

1. Allgemeine Rechte im Projekt (z. B. das Recht, Dateien zu signieren). Diese sind Benutzergruppen einzeln zugeordnet, da sie immer für das gesamte Projekt gelten.
2. Komponenten-spezifische Rechte („View“, „Delete“, „Modify“ und „Add/Remove Children“).
   Da diese für verschiedene Komponenten eines Projekts je nach Gruppenzugehörigkeit unterschiedlich sein können, sind sie in einem „Rechte-Set“ organisiert, dass die einzelnen Rechte aller Gruppen unter einer Bezeichnung zusammenfasst.



Im Bild oben ausgegraute Rechte sind im aktuellen Stand „für zukünftige Verwendung“ vorgesehen und noch nicht implementiert.

Ein solches Rechte-Set wird als „Object Protection Level“ bezeichnet, und stellt eine Matrix aus den vorhandenen Gruppen und deren Rechten für ein Objekt dar. Mit einem Object Protection Level kann man einzelne Projektkomponenten komfortabel mit vorgefertigten Rechte-Sets für jeweils alle Gruppen auf einmal versehen, und muss diese nicht gruppenweise jeder Projektkomponente zuordnen.

Wenn sich die Objekte eines Projekts nicht bezüglich des Sets an Zugriffsrechten unterscheiden (einfachster Anwendungsfall), reicht die Definition und Nutzung eines einzigen Object Protection Level aus. Dieser wird dann allen Objekten des Projektes zugewiesen.

Im Beispiel oben darf die Gruppe Entwickler alles, außer Änderungen an der Datenbank zu machen, die Gruppe Administrator darf nur Änderungen an der Datenbank machen, und die Gruppe Guest darf gar nichts (nicht einmal das Projekt laden).

Beachten Sie dabei die Mitgliedschaft von Gruppen in anderen Gruppen!

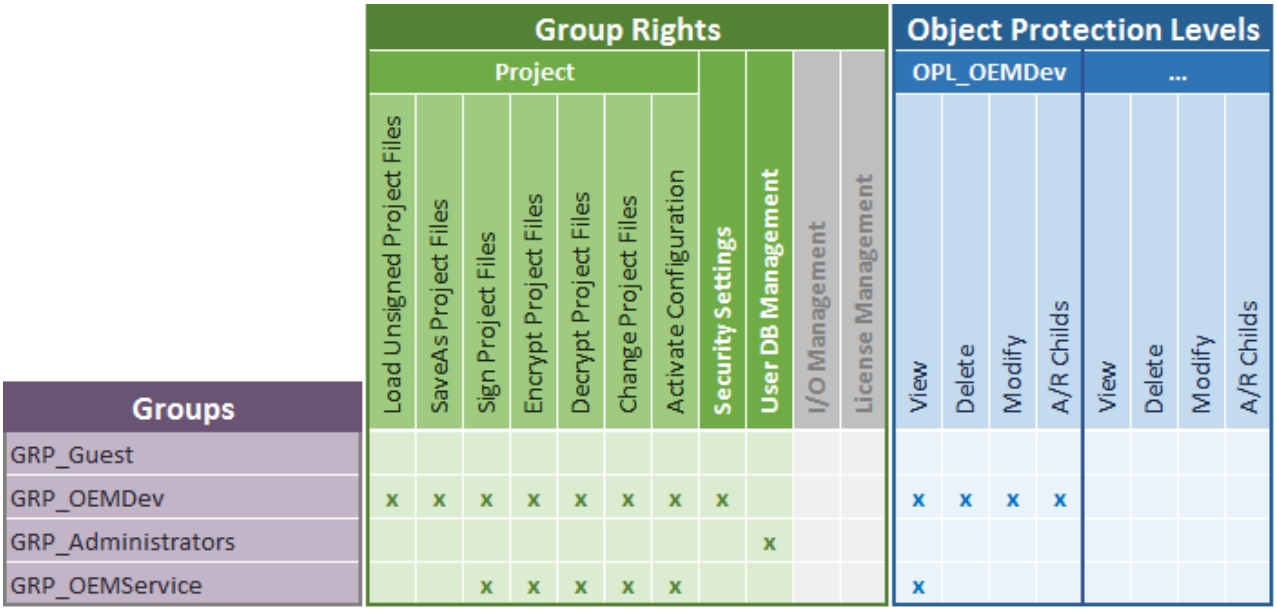
Beispiel 1

Im folgenden Beispiel soll eine neue Gruppe „GRP_OEMService“ hinzugefügt werden.

(Das Erstellen einer neuen Gruppe und die Zuweisung der Rechte ist hier [▶ 62] beschrieben.)

Die neue Gruppe darf alles sehen, aber nichts ändern, und darf das Projekt aktivieren.

Um das Projekt ansehen zu können, muss die Gruppe das Recht „Decrypt Project Files“ haben (sonst kann Visual Studio die verschlüsselten Teile des Projektes nicht laden).



Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	...: View	Delete	Modify	A/R Childs
GRP_Guest																			
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x				
GRP_Administrators									x										
GRP_OEMService			x	x	x	x	x					x							

Für das Aktivieren des Projektes ist es neben dem Recht „Activate Configuration“ erforderlich, die Projektdatei modifizieren zu können (da dort beim Aktivieren bestimmte Informationen hinterlegt werden), als auch das verschlüsselte Speichern dieser Änderungen. Daher sind noch die Rechte „Change Project File“ und „Encrypt Project Files“ erforderlich.

Bei den Komponenten-spezifischen Rechten ist nur „View“ notwendig.

Ein neuer Object Protection Level muss nicht erstellt werden, da dieses Rechte-Set immer für das gesamte Projekt gelten soll.

Beispiel 2

Im nächsten Beispiel soll die Gruppe „GRP_OEMService“ nur noch definierte Komponenten des Projektes ansehen können.

Dazu ist es erforderlich, ein neues Gruppenrechteset, also einen neuen Object Protection Level (OPL), anzulegen, um die jeweilige Rechtezuweisung für eine bestimmte Projektkomponente differenzieren zu können. Den neuen OPL nennen wir „OPL_OEMService“.

(Das Erstellen eines neuen Object Protection Levels ist hier [▶ 67] beschrieben.)

Das View-Recht für die Gruppe GRP_OEMService wird nun aus dem „OPL_OEMDev“ herausgenommen und im neuen „OPL_OEMService“ hinzugefügt:

Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	OPL_OEMService: View	Delete	Modify	A/R Childs
GRP_Guest																			
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x	x	x	x	x
GRP_Administrators									x										
GRP_OEMService			x	x	x	x	x									x			

Da die Gruppe „GRP_OEMDev“ auch im neuen „OPL_OEMService“ alles machen darf, wurden dort für diese Gruppe ebenfalls alle Rechte (View, Modify, …) eingetragen.

Beispiel 3

Im nächsten Beispiel soll die Gruppe GRP_OEMService zusätzlich bei bestimmten Projektkomponenten auch Änderungen vornehmen dürfen. (Sie darf allerdings (weiterhin) keine Projektkomponenten löschen oder hinzufügen.)

Dafür muss ein weiterer neuer Object Protection Level (OPL) angelegt werden. Wir nennen ihn „OPL_OEMServiceEdit“:

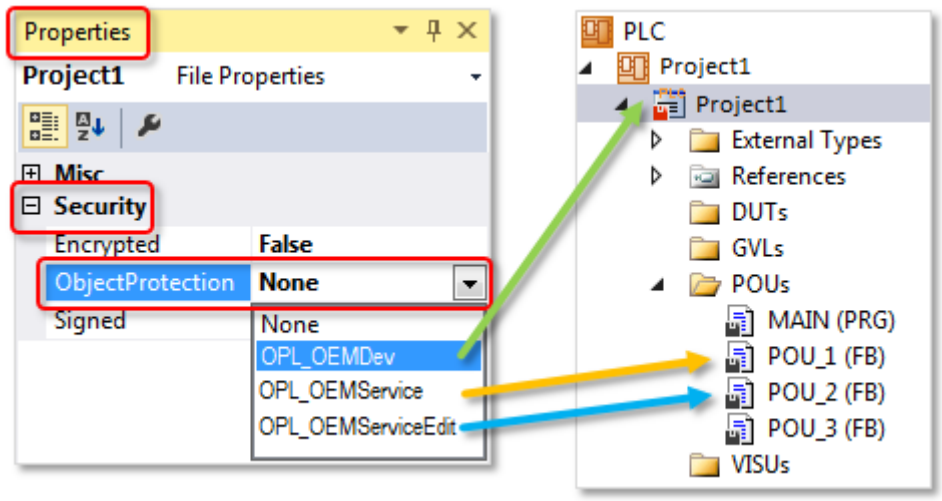
Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	OPL_OEMServAct: View	Delete	Modify	A/R Childs
GRP_Guest																			
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x				
GRP_Administrators									x										
GRP_OEMService	x		x	x	x	x	x											x	

Gegenüber OPL_OEMService kommt hier nur das Recht „Modify“ hinzu, der Rest ist identisch.

Projektkomponenten, die dem OPL_OEMServiceEdit zugeordnet werden, dürfen nun von Benutzern der Gruppe GRP_OEMService auch verändert werden.

Zuweisung der Object Protection Level im Projekt

Nun müssen wir die in den vorherigen Beispielen erstellten OPLs nur noch den Projektkomponenten zuweisen. (Wie die Zuweisung des OPLs genau im TwinCAT Engineering erfolgt, ist hier [▶ 71] beschrieben.)



OPL wird vererbt

Der der Wurzel des PLC-Projektes zugewiesene OPL wird in die darunter liegenden Knoten vererbt. Nur die Knoten, die eine andere Einstellung als die PLC Projekt-Wurzel benötigen, müssen individuell mit dem erforderlichen OPL konfiguriert werden.

Beispiel 4

Im folgenden Beispiel soll der Fall behandelt werden, dass der Servicemitarbeiter ein Projekt aktivieren, aber nicht einsehen darf.

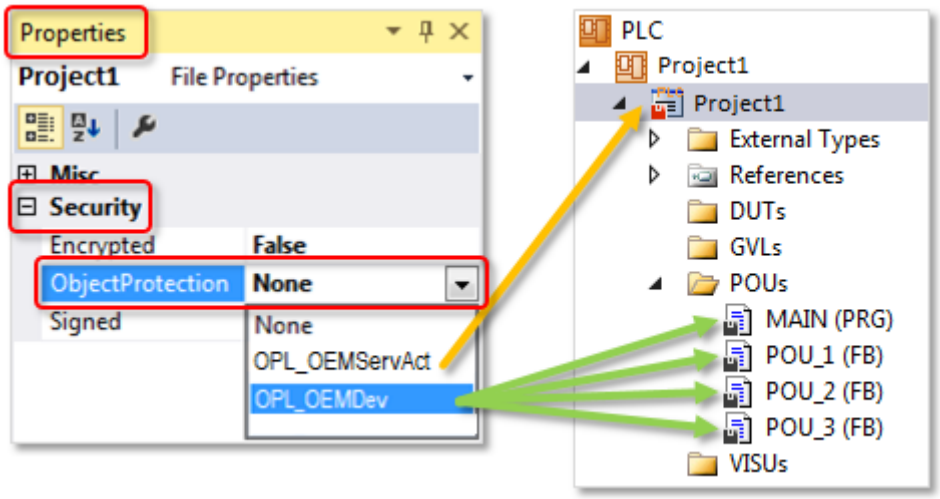
Da hier eine spezielle Rechtekonfiguration nur für den Root des PLC-Projektes erforderlich ist, benötigen wir hierfür einen eigenen Object Protection Level. Wir nennen ihn „OPL_OEMServAct“:

Groups	Group Rights: Project: Load Unsigned Project Files	SaveAs Project Files	Sign Project Files	Encrypt Project Files	Decrypt Project Files	Change Project Files	Activate Configuration	Security Settings	User DB Management	I/O Management	License Management	Object Protection Levels: OPL_OEMDev: View	Delete	Modify	A/R Childs	OPL_OEMServAct: View	Delete	Modify	A/R Childs
GRP_Guest																			
GRP_OEMDev	x	x	x	x	x	x	x	x				x	x	x	x				
GRP_Administrators									x										
GRP_OEMService	x		x	x	x	x	x											x	

Im Unterschied zum Beispiel 2 hat hier die Gruppe „GRP_OEMService“ nur Modify-, aber keine View-Rechte. „View“ ist nicht in „Modify“ enthalten.

Visual Studio benötigt das „Modify“-Recht für die Projektdatei, da dort bei der Aktivierung Änderungen erfolgen müssen.

Bei der Zuweisung der OPLs wird die Projektwurzel nun mit dem „OPL_OEMServAct“ versehen.



Da sich diese Eigenschaft aber an die unterhalb der Wurzel liegenden Projektkomponenten weitervererbt (sofern dort keine expliziten individuellen Einstellungen gemacht wurden), müssen die unterhalb der Wurzel liegenden Projektkomponenten gegebenenfalls einzeln manuell auf einen anderen OPL umgestellt werden. Die komfortable Vererbungsfunktion der PLC Wurzeleigenschaften kann dann in diesem Fall nicht verwendet werden.

Dokumente hierzu

https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip

5.6.4.2 Benutzer anlegen und editieren

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Mindestens einen Benutzer mit Administrator-Rechten

Um Änderungen in der Datenbank machen zu können, muss mindestens ein Benutzer der Datenbank der Administrator-Gruppe angehören. Legen Sie daher immer einen Benutzer mit Administratorrechten an.

Der beim Anlegen der User DB definierte „Database Admin“ wird ausschließlich zum Signieren der Datenbank verwendet. Dieser Account kann nicht zum Einloggen oder für Änderungen in der Datenbank genutzt werden.

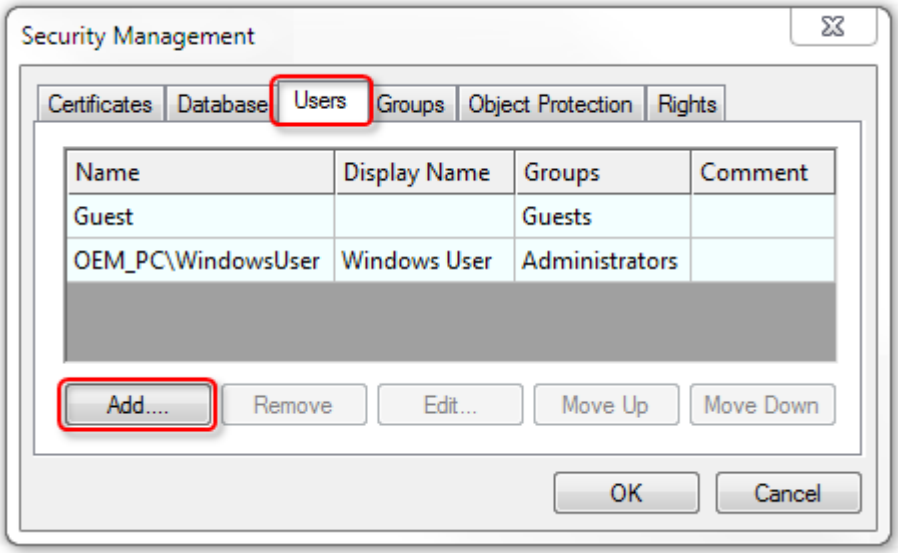
Anlegen und Editieren von Benutzern

In der Registerkarte **Users** des Software-Protection-Konfigurators können Sie die Einstellungen für existierende Benutzer ändern und neue Benutzer anlegen.

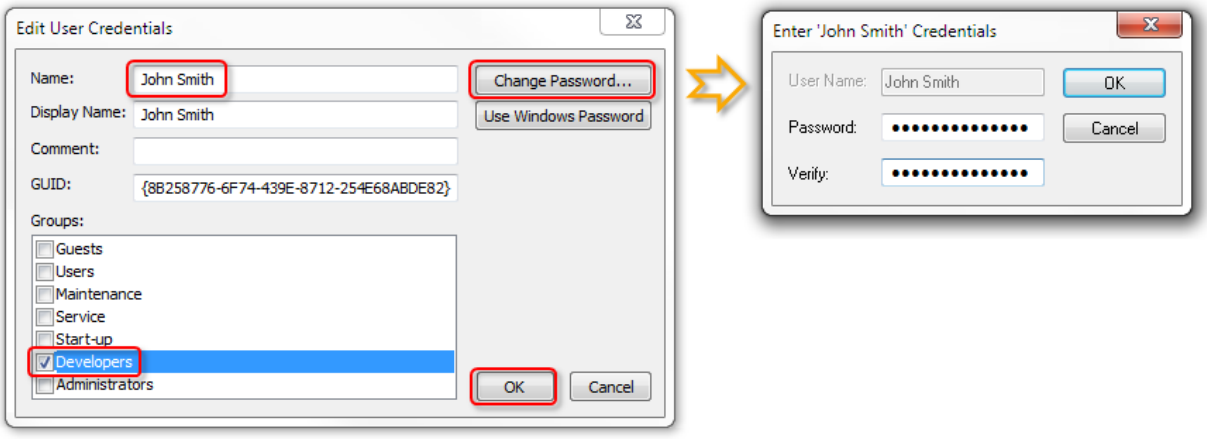
✓ Benutzerdatenbanken können nur angelegt oder editiert werden, wenn kein Projekt geöffnet ist. Schließen Sie eventuell geöffnete Projekte.

✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

1. Wählen Sie die Registerkarte **Users** aus.



2. Klicken Sie auf **Add**, um einen neuen Benutzer hinzuzufügen.
   ⇨ Der Dialog **Edit User Credentials** öffnet sich.
3. Geben Sie dem Benutzer einen Namen (**Name**) und weisen Sie ihn einer Benutzergruppe zu, indem Sie das entsprechende Auswahlkästchen aktivieren (**Groups**).
4. Bei einem Windows-Account kann die Authentifizierung automatisch über Windows erfolgen. Bei allen anderen Benutzern müssen Sie ein Passwort für diesen Benutzer festlegen. Klicken Sie dazu auf **Change Password**.
   ⇨ Ein Dialog zum Festlegen eines Passworts öffnet sich.
5. Vergeben Sie ein Passwort für den Benutzer, bestätigen Sie das Passwort durch eine wiederholte Eingabe.
6. Schließen Sie den Dialog mit **OK**.



   ⇨ Der neue Benutzer erscheint in der Übersicht.
7. Wenn Sie einen Eintrag bearbeiten möchten, markieren Sie den Benutzer in der Übersicht und klicken Sie auf **Edit**.
8. Schließen Sie den Dialog **Edit User Credentials** mit **OK**.

⇨ Ein neuer Benutzer ist im System angelegt.

Ab Build 4024.8:

Benutzer können auch in sogenannten „Extensions [▶ 48]“ von Benutzerdatenbanken angelegt werden. Dieses ist hier [▶ 41] beschrieben.

Erst mit dem Speichern und Signieren der Benutzerdatenbank werden alle Änderungen final übernommen und sind gültig

5.6.4.3 Benutzergruppen anlegen und editieren

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

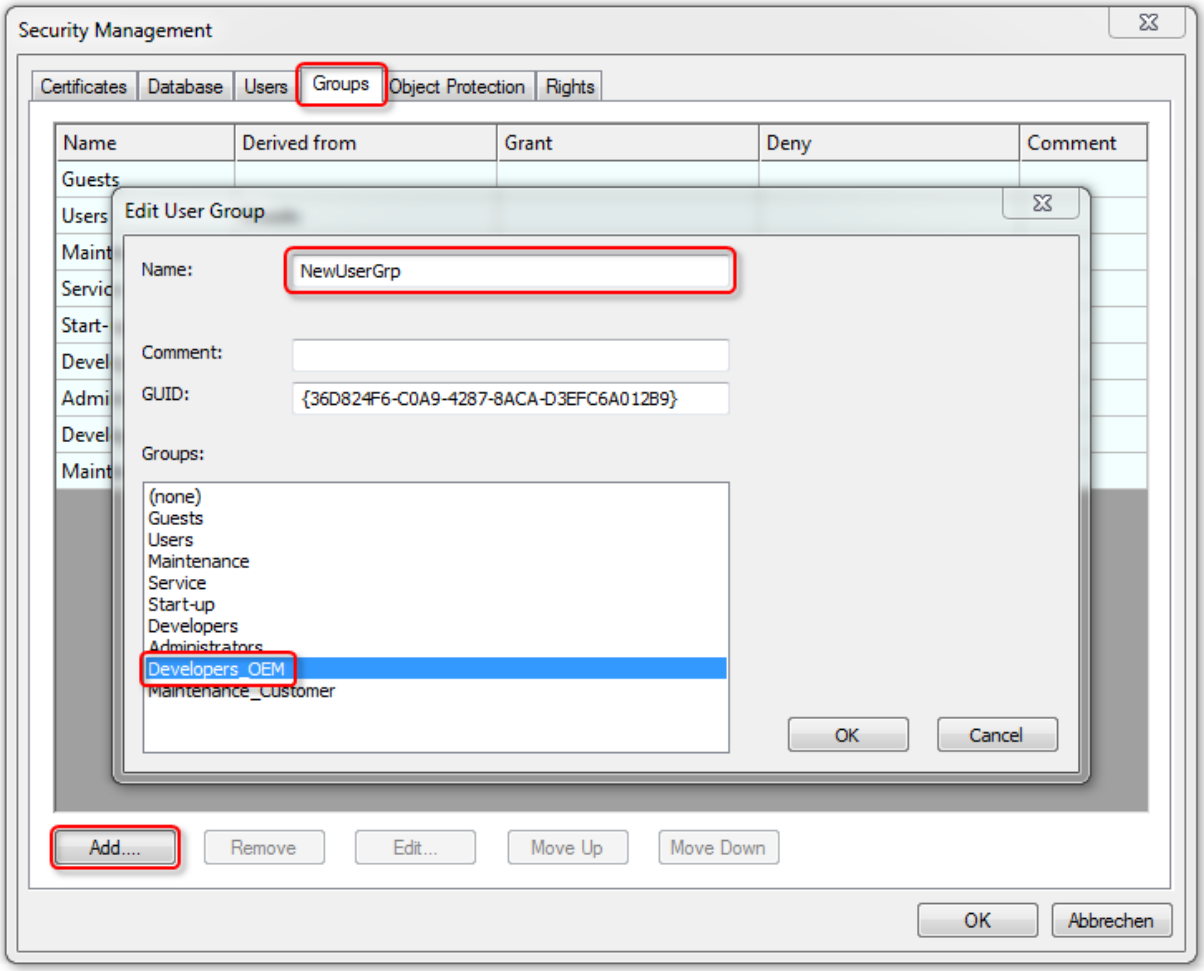
Anlegen und Editieren von Benutzergruppen

In der Registerkarte **Groups** des Software-Protection-Konfigurators können Sie die Basiseinstellungen für existierende Benutzergruppen ändern und neue Benutzergruppen anlegen.

Hinweis: Die Anpassung der einer Benutzergruppe zugewiesenen Rechte erfolgt im Tab „Rights“ und wird im nachfolgenden Kapitel [▶ 65] beschrieben.

✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

1. Wählen Sie die Registerkarte **Groups** aus.



2. Klicken Sie auf **Add**, um eine neue Gruppe anzulegen.
   ⇨ Der Dialog **Edit User Group** öffnet sich.
3. Geben Sie der Gruppe einen Namen (**Name**).
4. Wenn die Gruppe die Rechte einer anderen Gruppe erben soll, wählen Sie die entsprechende Gruppe im Bereich **Groups** aus.

5. Schließen Sie den Dialog mit **OK**.
   ⇨ Die neue Gruppe erscheint in der Übersicht.
6. Wenn Sie einen Eintrag bearbeiten möchten, markieren Sie die Benutzergruppe in der Übersicht und klicken Sie auf **Edit**.
7. Schließen Sie den Dialog **Edit User Group** mit **OK**.

⇨ Eine neue Benutzergruppe ist im System angelegt.

Erst mit dem Speichern und Signieren der Benutzerdatenbank werden alle Änderungen final übernommen und sind gültig

In der Registerkarte **Rights** können Sie Benutzergruppen Rechte zuweisen. Weitere Informationen finden Sie im Abschnitt Rechte von Benutzergruppen anpassen [▶ 65].

5.6.4.4 Zugriffsrechte von Benutzergruppen anpassen

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

In der Registerkarte **Rights** des Software-Protection-Konfigurators verwalten Sie die den Benutzergruppen zugewiesenen Rechte.

Download-Link: Planungstabelle für Gruppenrechte und Object Protection Level

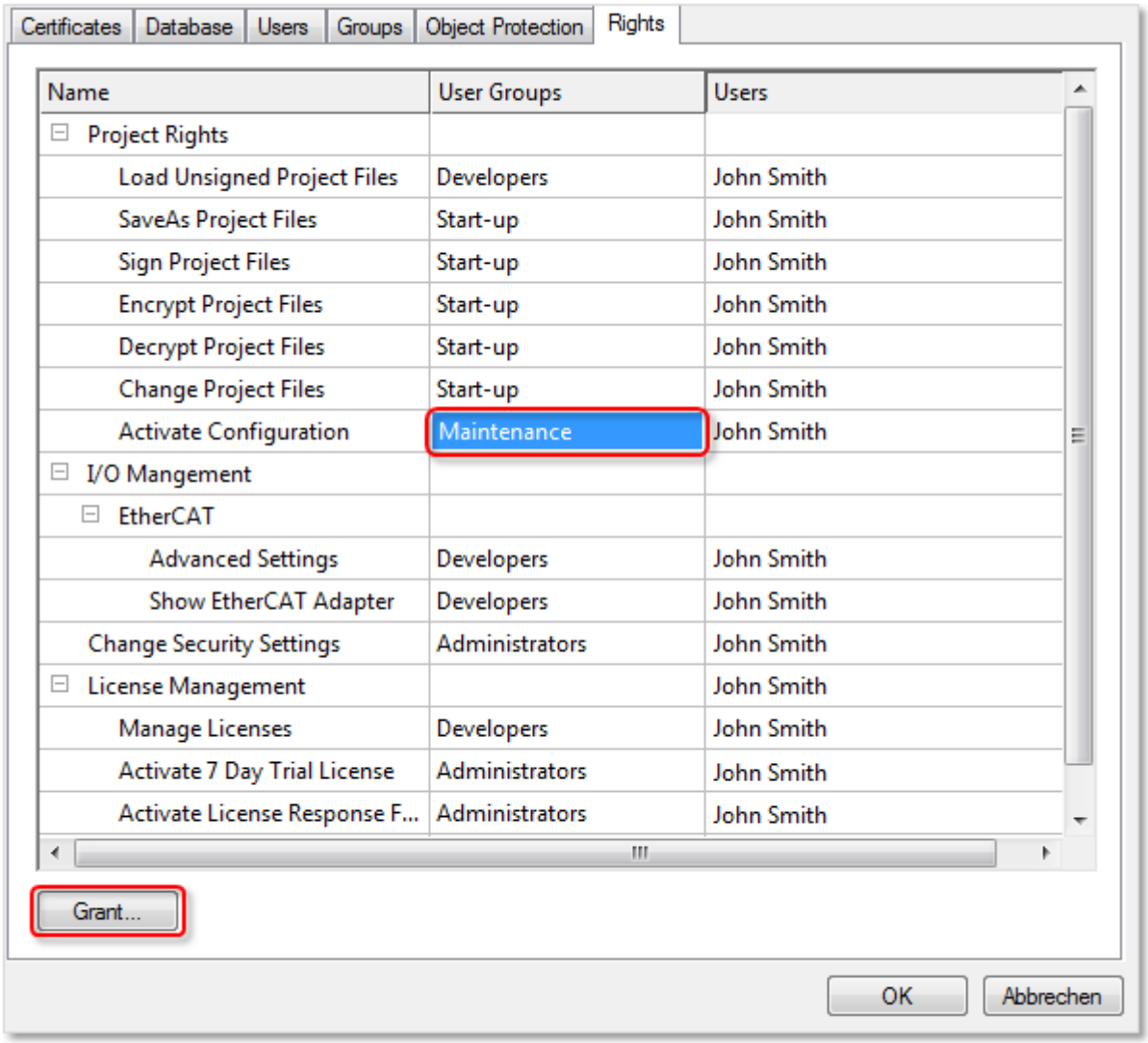
Eine Excel-Tabelle zur einfachen Planung von Gruppenrechten und Zugriffsberechtigungsgruppensets (Object Protection Level) können Sie https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip herunterladen.

✓ Benutzerdatenbanken können nur angelegt oder editiert werden, wenn kein Projekt geöffnet ist. Schließen Sie eventuell geöffnete Projekte.

✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

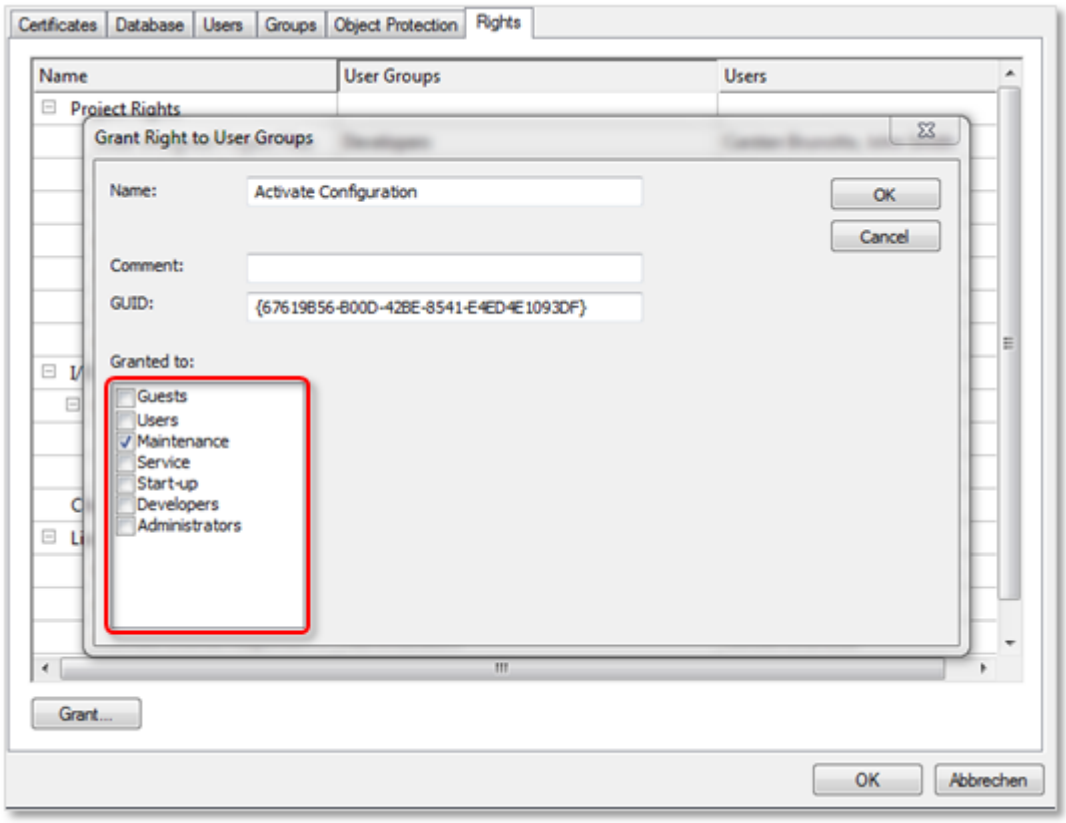
1. Wählen Sie die Registerkarte **Rights** aus.

2. Markieren Sie in der Spalte **UserGroups** die Zeile mit dem gewünschten Recht und klicken Sie auf die Schaltfläche **Grant**.



⇨ Der Dialog **Grant Right to User Groups** öffnet sich.

3. Wählen Sie über die Auswahlkästchen aus, welche Benutzergruppen dieses Recht haben sollen.



4. Klicken Sie auf **OK**.

⇨ Die Änderungen werden (temporär) übernommen.

Erst mit dem Speichern und Signieren der Benutzerdatenbank werden alle Änderungen final übernommen und sind gültig

5.6.4.5 Zugriffsberechtigungsgruppensets (Object Protection Level) anlegen und editieren

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Download-Link: Planungstabelle für Gruppenrechte und Object Protection Level

Eine Excel-Tabelle zur einfachen Planung von Gruppenrechten und Zugriffsberechtigungsgruppensets (Object Protection Level) können Sie https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip herunterladen.

✓ Benutzerdatenbanken können nur angelegt oder editiert werden, wenn kein Projekt geöffnet ist. Schließen Sie eventuell geöffnete Projekte.

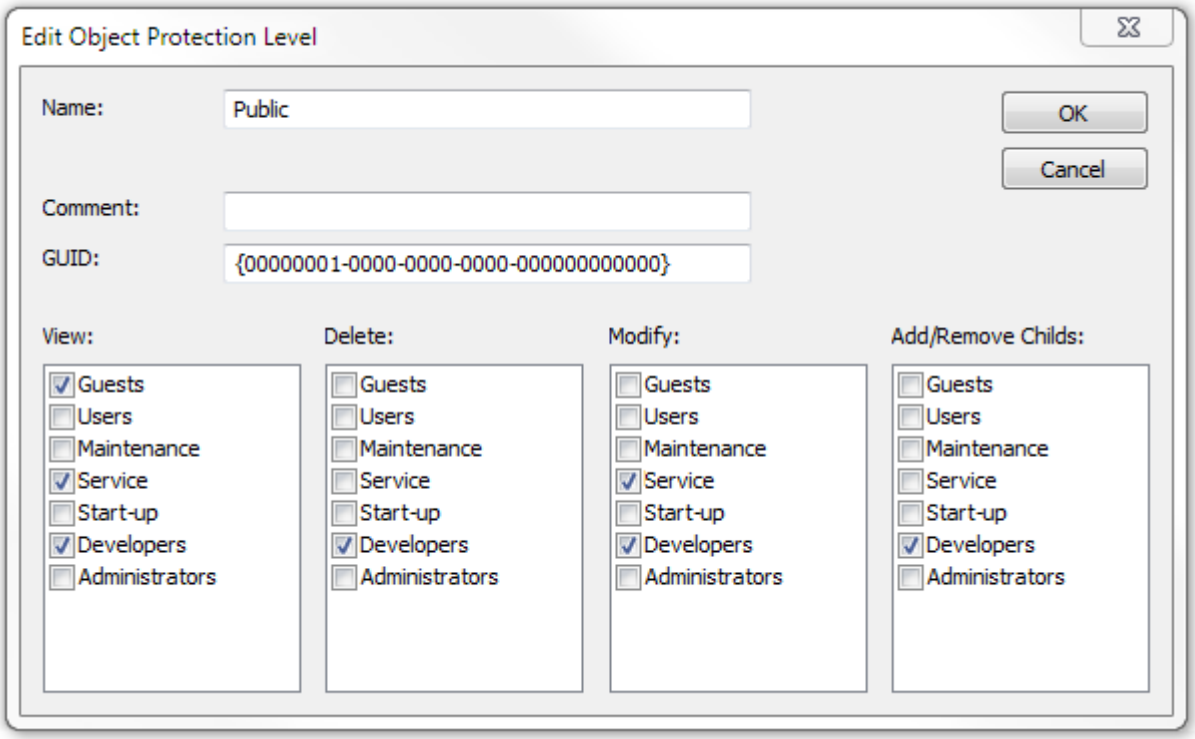
✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

1. Wählen Sie die Registerkarte **Object Protection** aus.
2. Klicken Sie auf **Add**.

⇨ Der Dialog **Edit Object Protection Level** öffnet sich.

3. Ordnen Sie allen im Security Management definierten Gruppen die Benutzerrechte für diesen spezifischen Object Protection Level einzeln zu, indem Sie die jeweiligen Auswahlkästchen aktivieren.

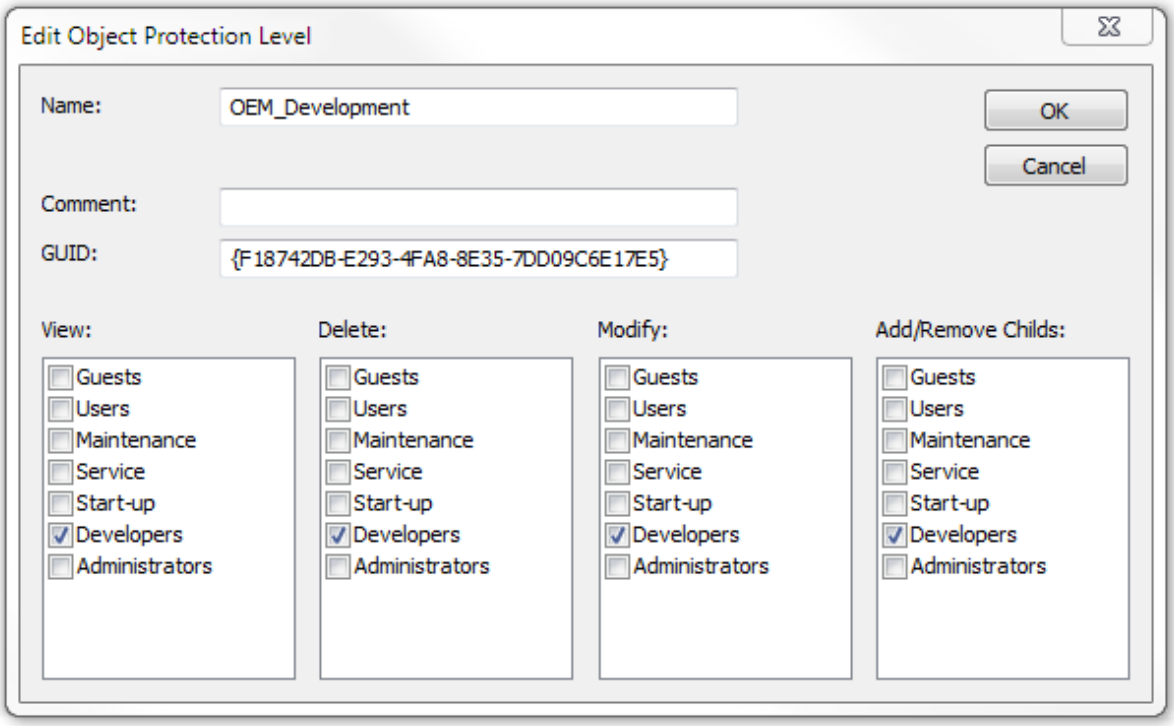
   Im folgenden Beispiel ist die Definition des Object Protection Levels „Public“ dargestellt:



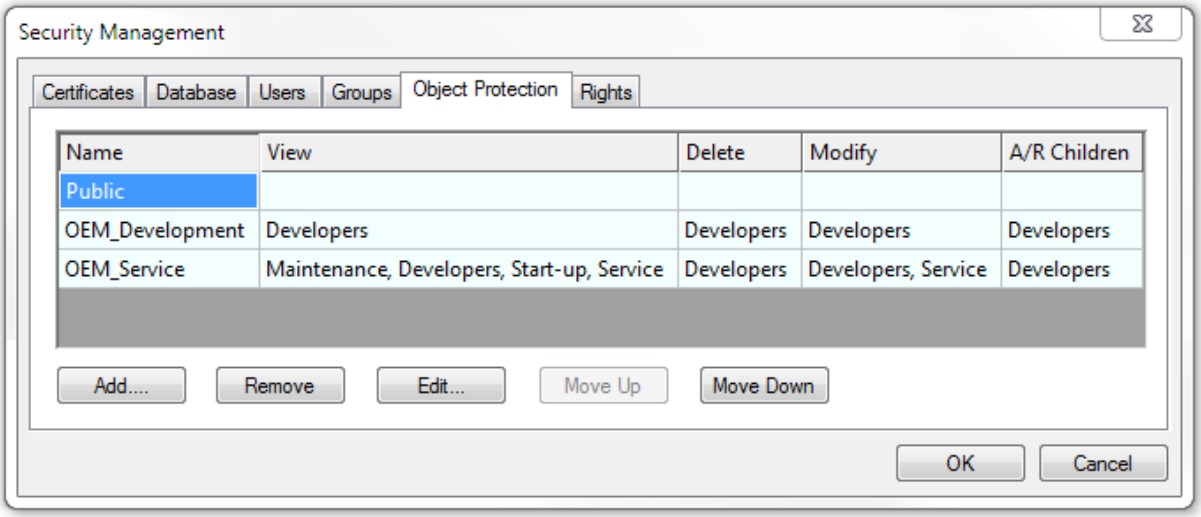
- Die Benutzergruppe „Guest“ kann ein mit diesem Object Protection Level versehenes TwinCAT-Objekt lesen, aber nicht verändern.
- Die Benutzergruppe „Service“ kann ein mit diesem Object Protection Level versehenes TwinCAT-Objekt lesen und verändern, aber nicht löschen.

- Die Benutzergruppe „Developers“ hat vollen Zugriff.

  Im folgenden Beispiel darf nur die Benutzergruppe „Developers“ auf das TwinCAT-Objekt zugreifen. Die restlichen Benutzergruppen haben keinerlei Rechte.



4. Bestätigen Sie den Dialog mit **OK**.
   ⇨ Der Object Protection Level mit den Benutzerrechten ist im System angelegt und wird in der Übersicht der Registerkarte **Objekt Protection** im Software-Protection-Konfigurator angezeigt.
5. Vergeben Sie dementsprechend für weitere Benutzergruppen die gewünschten Benutzerrechte in einem Object Protection Level.
6. Um einen Object Protection Level zu editieren, markieren Sie die gewünschte Spalte und klicken Sie auf **Edit**.



7. Um ein Object Protection Level zu entfernen, klicken Sie auf **Remove**.
8. Um die Position des ausgewählten Object Protection Level in der Übersicht zu verändern, klicken Sie auf **Move up** bzw. **Move down**.

Erst mit dem Speichern und Signieren der Benutzerdatenbank werden alle Änderungen final übernommen und sind gültig

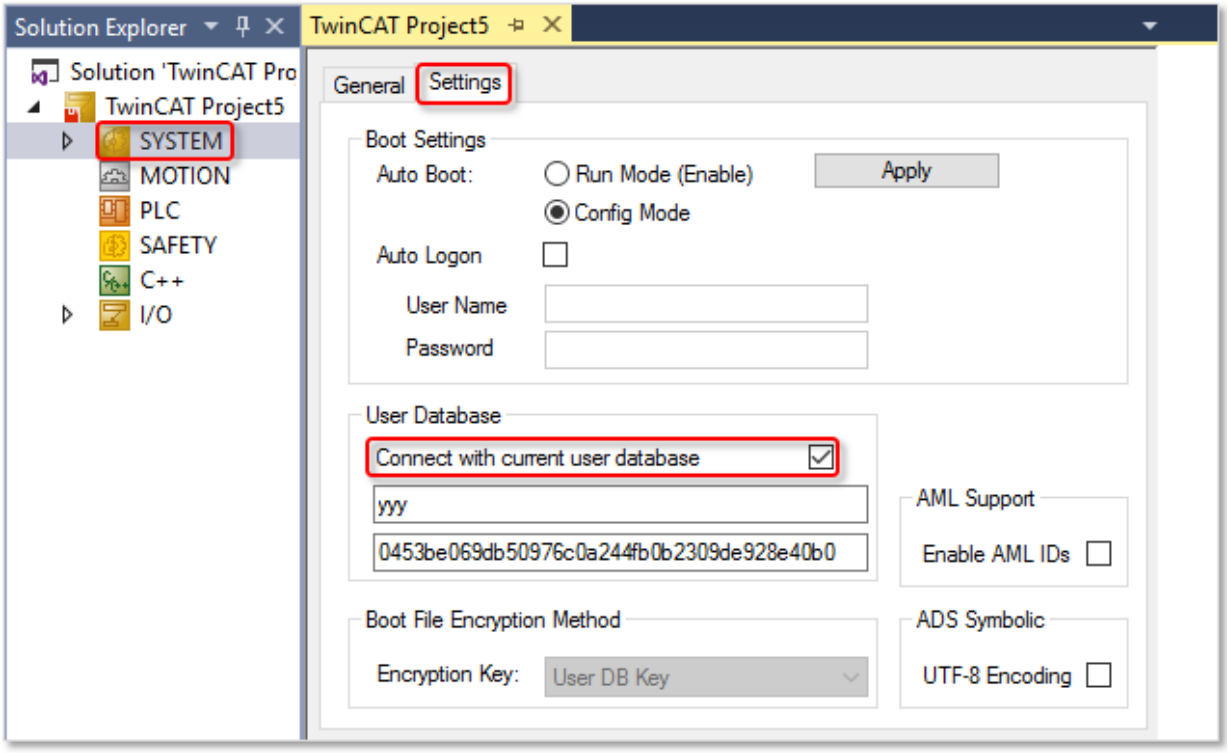
5.7 Benutzerdatenbank mit Projekt verbinden

Ein Projekt muss initial einmal manuell mit einer Benutzerdatenbank verbunden werden. Die Verknüpfung mit der Datenbank wird dann im Projekt gespeichert.

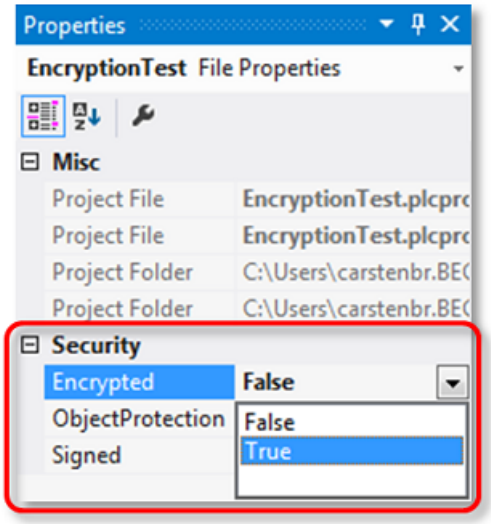
✓ Erstellen Sie immer erst eine Sicherungskopie Ihres Projektes, bevor Sie es mit einer Benutzerdatenbank verbinden.

✓ Eine Benutzerdatenbank ist angelegt und aktiviert. Ein TwinCAT-Projekt ist geöffnet.

1. Klicken Sie im TwinCAT-Projekt doppelt auf den SYSTEM-Knoten, um die Systemeinstellungen zu öffnen.
2. Öffnen Sie die Registerkarte **Settings**.
3. Aktivieren Sie im Bereich **User Database** das Auswahlkästchen **Connect with current user database**.



⇨ Das Projekt ist nun mit der Benutzerdatenbank verbunden. In den Eigenschaften (**Properties**) einer Projektkomponente wird der Bereich **Security** sichtbar.



5.8 Benutzerzugriffsberechtigungen im Projekt zuweisen

Download-Link: Planungstabelle für Gruppenrechte und Object Protection Level

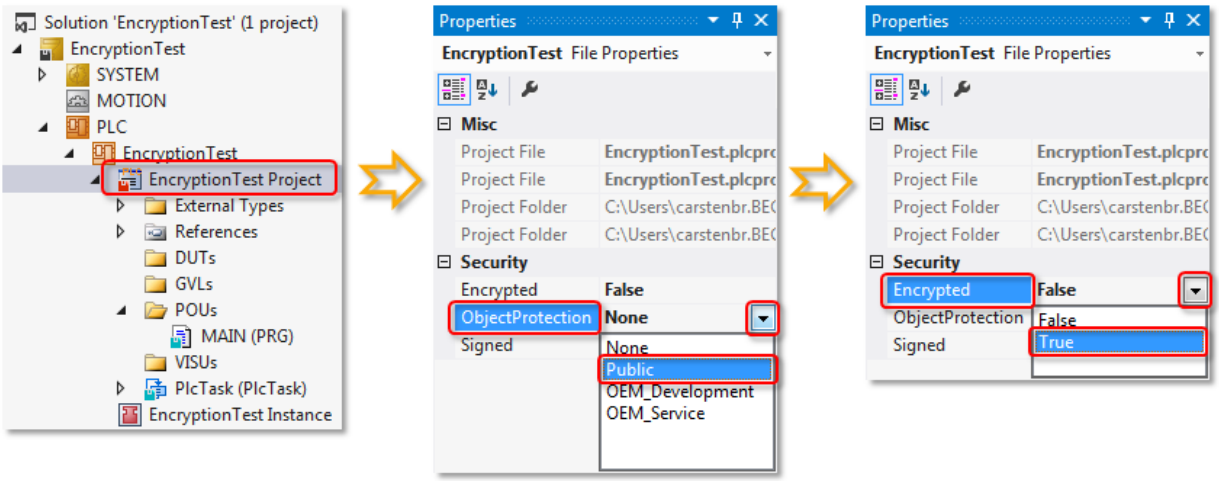
Eine Excel-Tabelle zur einfachen Planung von Gruppenrechten und Zugriffsberechtigungsgruppensets (Object Protection Level) können Sie https://infosys.beckhoff.com/content/1031/tc3_security_management/Resources/8882888971.zip herunterladen.

Die erstellten Object Protection Level [▶ 67] können Sie TwinCAT-Objekten zuweisen, z. B. einem SPS-Projekt.

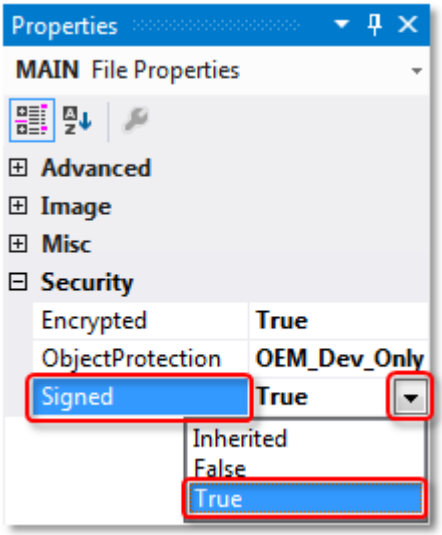
✓ Die Zugriffsberechtigungsgruppen sind definiert.

✓ Das Projekt ist mit einer Benutzerdatenbank verbunden.

1. Markieren Sie das SPS-Objekt im SPS-Projektbaum im Projektmappen-Explorer.
   ⇨ Die Ansicht **Properties** aktualisiert sich. (Wenn die Ansicht **Properties** nicht geöffnet ist, wählen Sie den Befehl **Properties Window** im Menü **View**, um diese zu öffnen.)
2. Wählen Sie aus der Drop-down-Liste der Eigenschaft **ObjectProtection** in der Kategorie **Security** das gewünschte Object Protection Level aus.

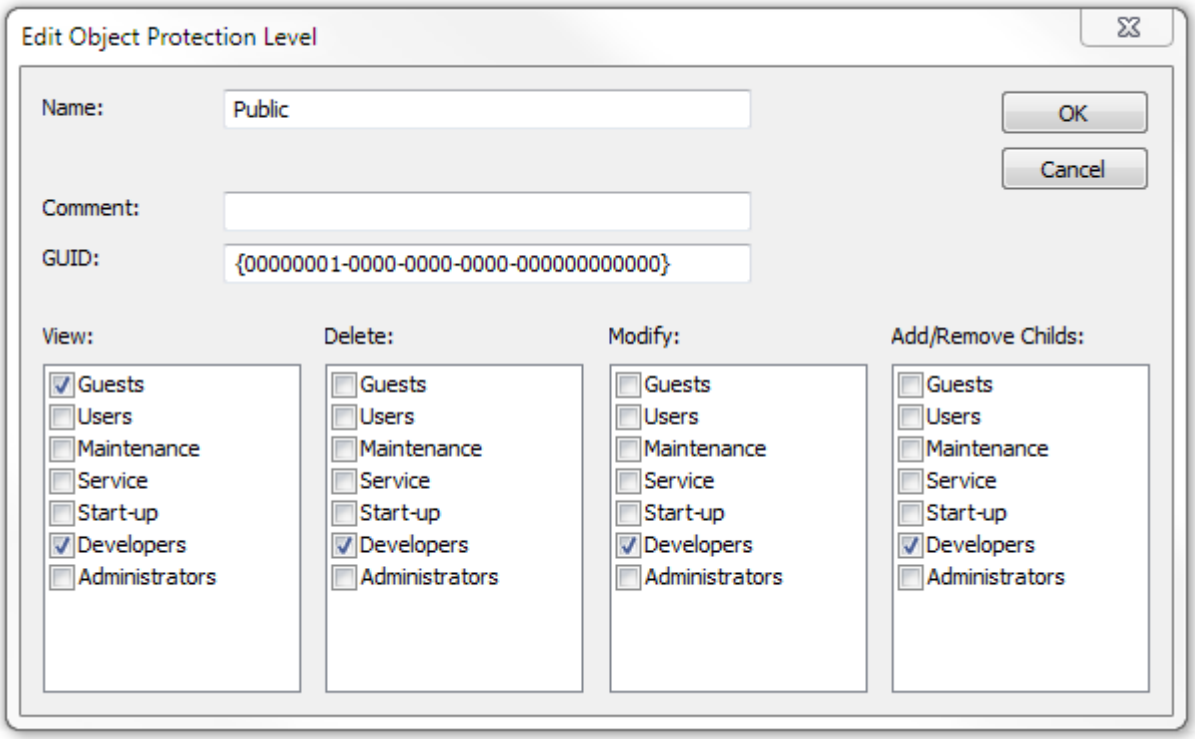


3. Setzen Sie dann den Wert der Eigenschaft **Encrypted** über die Drop-down-Liste auf TRUE. Diese Einstellung ist wichtig, um den Zugriff auf den Quellcode, z. B. über die Betriebssystemebene, zu verhindern.
4. Setzen Sie danach den Wert der Eigenschaft **Signed** über die Drop-down-Liste auf TRUE. Diese Einstellung ist wichtig, um einen unautorisierten Austausch der Objektdatei auf Betriebssystemebene gegen eine andere Datei gleichen Namens zu unterbinden.



⇨ Auf das SPS-Projekt können nun die Benutzergruppen zugreifen, die im Object Protection Level festgelegt worden sind. Mit dem Speichern des SPS-Projektes werden die Einstellungen übernommen.

Im Beispiel Object Protection Level „Public“:

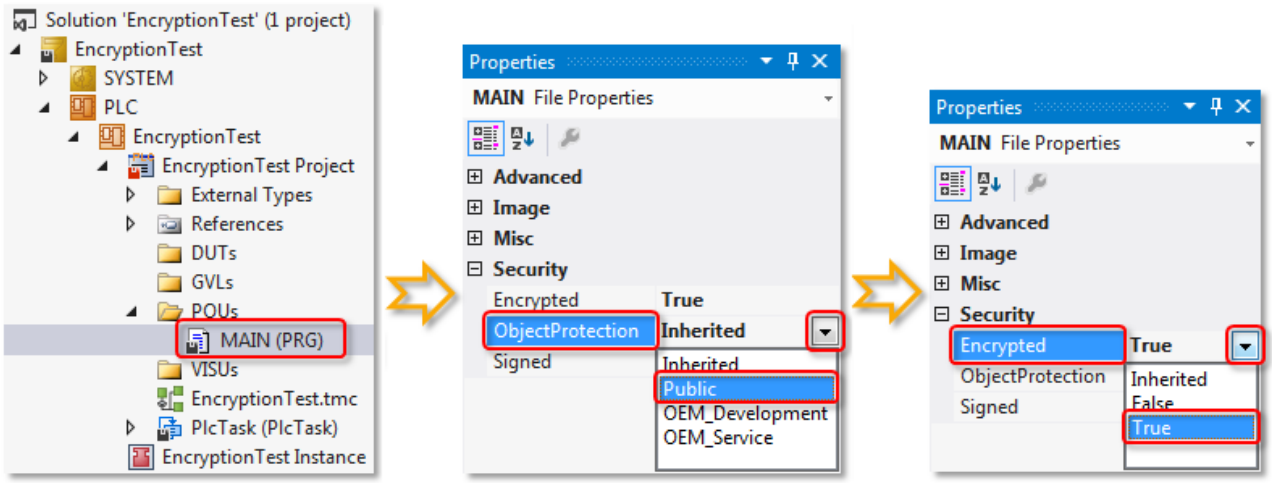


- Die Benutzergruppe „Guests“ kann lesend auf das SPS-Projekt zugreifen.
- Die Benutzergruppe „Developers“ hat vollen Zugriff.

(Für die restlichen Benutzergruppen sind hier keine Zugriffsrechte definiert worden, da sie im Beispielprojekt nicht genutzt werden.)

Die in der Wurzel des SPS-Projektes festgelegten Zugriffsrechte werden im SPS-Projektbaum automatisch an alle Unterelemente des SPS-Objektes weitervererbt, wenn diese die Eigenschaften **Object Protection Level** und **Encryption** haben.

Für jedes Unterelement kann aber auch eine eigene, individuelle Zuweisung des Object Protection Levels und der Verschlüsselung erfolgen. Dies stellen Sie in den Eigenschaften des Unterelements ein.



Auch hier müssen Sie für das Objekt die Wert der Eigenschaften **Encrypted** und **Signed** über die Drop-down-Listen auf TRUE setzen, um zum einen den Zugriff auf den Quellcode, z. B. über die Betriebssystemebene, zu verhindern und zum anderen einen unautorisierten Austausch der Objektdatei gegen eine andere Datei gleichen Namens zu unterbinden.

5.9 Distribution / Austausch von Benutzerdatenbanken

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Änderungen von Einstellungen einer Benutzerdatenbank nicht bei geöffnetem Projekt

Für eine Änderung der Einstellungen einer Benutzerdatenbank darf kein Projekt geöffnet sein.

Beachten Sie beim Arbeiten mit User DBs folgende Hinweise:

- Die User DB muss in der aktuellen TwinCAT-3-Version immer im Verzeichnis *c:\TwinCAT\3.1\CustomConfig\UserDBs* gespeichert werden.
- Eine User DB kann auf Dateiebene frei kopiert und eingefügt werden.
- Beim Anlegen einer User DB wird ein eineindeutiger User DB Key erzeugt, der diese Datenbank eindeutig identifiziert.
- Wenn ein Projekt mit einer User DB verknüpft wird, kann es nur mit einer User DB mit dem gleichen Namen und dem gleichen User DB Key geöffnet werden.
- Modifikationen des Inhalts einer User DB wirken sich nicht auf den User DB Key aus (dieser wird einmalig beim Erstellen der User DB generiert). Sie können also prinzipiell mit mehreren unterschiedlichen Versionen einer User DB arbeiten. Beispiel: Die „Inhouse“-Version einer User DB beinhaltet andere Benutzerkonten als die Version, die auf dem Steuerungsrechner zum Endkunden ausgeliefert wird. Damit kann der Endkunde nur eine festgelegte Auswahl an verfügbaren Benutzerkonten sehen und Sie können die verfügbaren Zugriffsmöglichkeiten auf der ausgelieferten Maschine gegenüber der „Inhouse“-Entwicklungsumgebung stark einschränken.
- Nach dem Erzeugen einer User DB wird das OEM-Zertifikat nicht mehr für das Arbeiten mit der User DB benötigt.
- Änderungen der User DB müssen von einem (signierenden) Administrator der User DB signiert werden. Die entsprechende Abfrage kommt automatisch nach Änderungen in der User DB beim Verlassen des Software-Protection-Konfigurators.

6 Einloggen / Auswahl eines Benutzerkontos

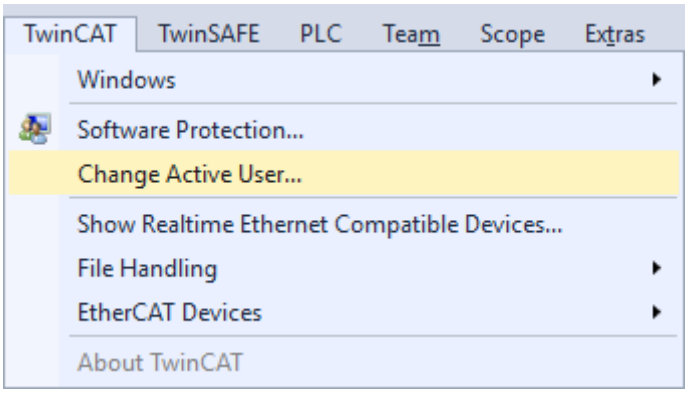
Betriebssystemzugriff nur für autorisierte Benutzer erlauben

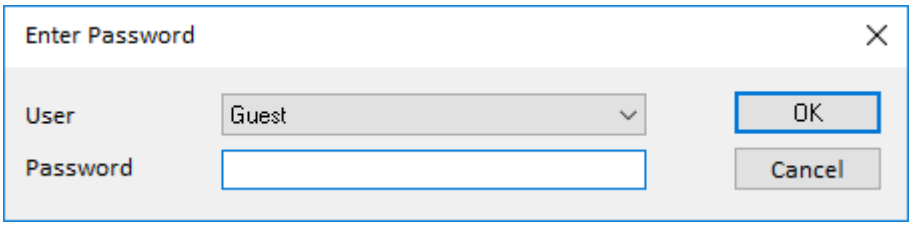
Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

Änderungen von Einstellungen einer Benutzerdatenbank nicht bei geöffnetem Projekt

Für eine Änderung der Einstellungen einer Benutzerdatenbank darf kein Projekt geöffnet sein.

Der Benutzer kann entweder über die Toolbar, oder über den Hauptmenüpunkt **TwinCAT -> Change Active User** geändert werden:





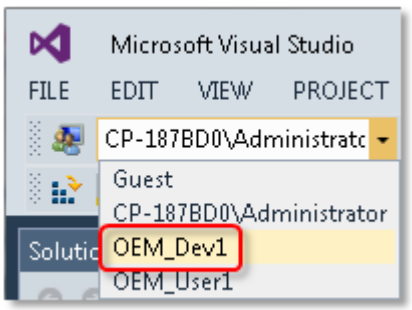
Die Änderung des Benutzers darf nur erfolgen, wenn kein Projekt geladen ist.

6.1 Build 4022

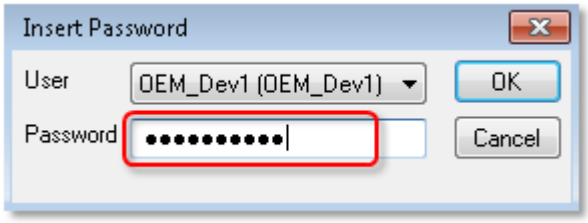
Ein Benutzerkonto können Sie einfach über das Auswahlfeld in der der Security-Management-Symbolleiste auswählen.

✓ Sie haben die Security-Management-Symbolleiste [▶ 11] geöffnet.

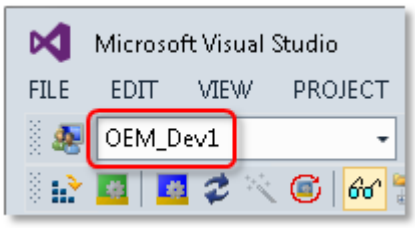
1. Wählen Sie aus der Drop-down-Liste das Benutzerkonto aus.



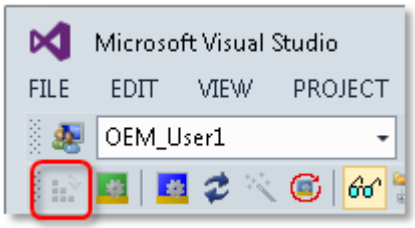
2. Wenn das Einloggen des Benutzers ein Passwort erfordert, öffnet sich ein Dialog zur Eingabe des Passworts. Geben Sie das Passwort ein. Wenn die Authentifizierung über den Windows User Account erfolgt, wird kein Passwort abgefragt, da die Authentifizierung bereits über das Einloggen bei Windows erfolgt ist.



⇨ Das ausgewählte Benutzerkonto wird in der Security-Management-Symbolleiste angezeigt.



Abhängig von den Rechten des Benutzerkontos können auch bestimmte TwinCAT-Menüpunkte ausgegraut und damit deaktiviert sein.



7 Grundschutz der PLC-Anwendungssoftware einrichten

Betriebssystemzugriff nur für autorisierte Benutzer erlauben

Der Inhalt der Benutzerdatenbank ist mit einer Signatur gegen Manipulationen geschützt. Die Namen von Gruppen, Object Protection Leveln und Benutzern sind nicht verschlüsselt und könnten ausgelesen werden. Der Zugriff auf den IPC sollte über das Betriebssystem auf autorisierte Nutzer eingeschränkt werden.

7.1 Verschlüsselung

Machen Sie eine unverschlüsselte Datensicherung vor dem Verschlüsseln!

Bevor sie ein Projekt verschlüsseln: Machen Sie immer eine Datensicherung des Projekts im unverschlüsselten Zustand!

TwinCAT 3 verwendet eine 256-Bit-AES-Verschlüsselung und setzt beim OEM-Zertifikat ein Verfahren mit Private und Public Key ein.

Voraussetzung für die Nutzung dieser Funktion: Ausstellung eines TwinCAT OEM Zertifikates [▶ 19]

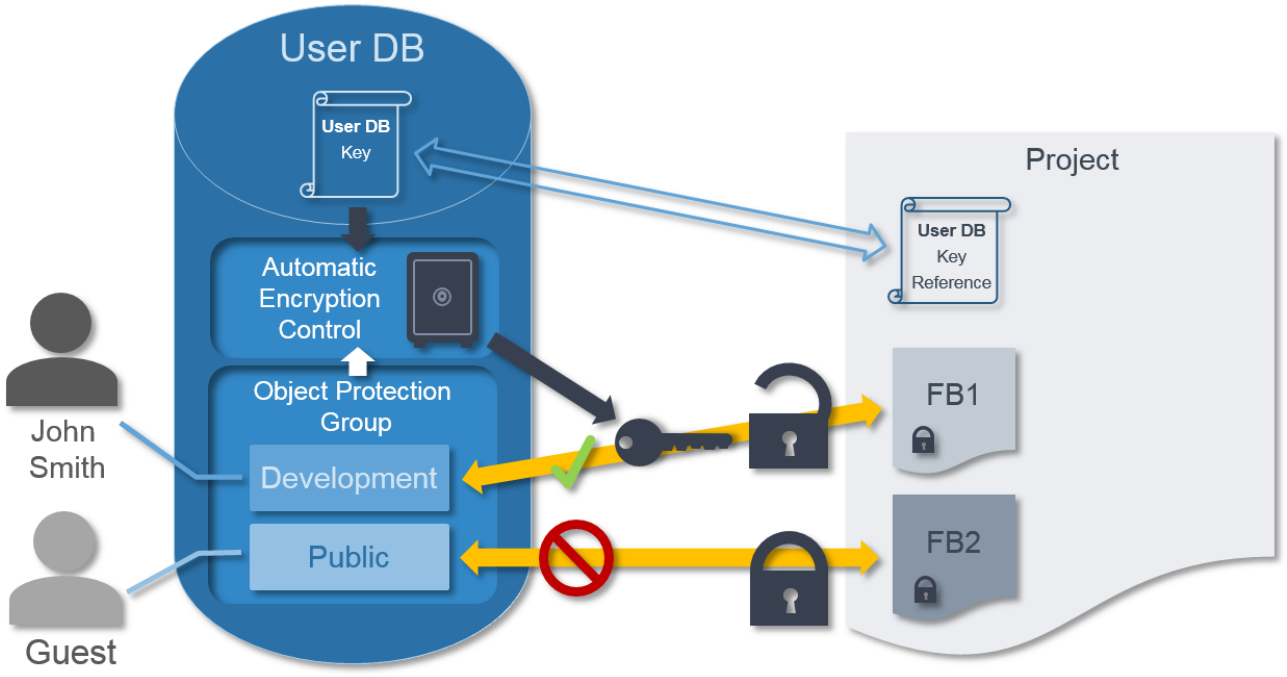
Folgende Objekte können Sie in TwinCAT verschlüsseln:

- PLC-Quellcode
- Projektdatei
- Boot-Projekt

Sicherer Schutz nur bei Verschlüsselung der Projektdatei

Die Projektdatei muss bei Einsatz der Verschlüsselung in jedem Fall mit verschlüsselt werden, da sie wichtige Informationen zu den Eigenschaften des Projekts enthält. Eine Manipulation dieser Informationen könnte eine sichere Verschlüsselung des Quellcodes verhindern.

Der für die Verschlüsselung verwendete Schlüssel ist in der Benutzerdatenbank gesichert. Die zugehörige Benutzerdatenbank muss daher immer auf dem Engineering-Rechner vorhanden sein. (Verzeichnis: *c:\Twincat\3.1\CustomConfig\userDBs*)



Für die Entschlüsselung des Boot-Projektes (=Binärdatei) ist die Benutzerdatenbank nicht erforderlich.

Systemvoraussetzungen

Betriebssystem:

- Um alle Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist mindestens Windows 7 (bzw. dessen Embedded-Version) erforderlich. Windows XP und Windows CE (Windows Embedded Compact) unterstützen weder die Verschlüsselung der Boot-Datei noch OEM-Lizenzen.

TwinCAT-Version:

- Die beschriebenen Funktionalitäten erfordern mindestens TwinCAT 3.1 Build 4022.

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

7.1.1 PLC-Quellcode verschlüsseln

Machen Sie eine unverschlüsselte Datensicherung vor dem Verschlüsseln!

Bevor sie ein Projekt verschlüsseln: Machen Sie immer eine Datensicherung des Projekts im unverschlüsselten Zustand!

Der Zugriff auf verschlüsselte Objekte wird über den Object Protection Level festgelegt. Daher müssen Sie neben der Verschlüsselung immer den gewünschte Object Protection Level für das TwinCAT-3-Objekt einstellen. Object Protection Level und Verschlüsselung können Sie einfach und komfortabel in den Eigenschaften (Properties) des jeweiligen TwinCAT-Objektes zuweisen, z. B. einem SPS-Projekt. Das Projekt muss dazu mit der Benutzerdatenbank verbunden sein. Im Abschnitt Benutzerzugriffsberechtigungen im Projekt zuweisen [▶ 71] wird die Verschlüsselung und die Festlegung von Object Protection Leveln beschrieben. Mit dem Speichern des Projektes werden die gemachten Einstellungen übernommen.

7.1.2 Projektdatei verschlüsseln

Sicherer Schutz nur bei Verschlüsselung der Projektdatei

Die Projektdatei muss bei Einsatz der Verschlüsselung in jedem Fall mit verschlüsselt werden, da sie wichtige Informationen zu den Eigenschaften des Projekts enthält. Eine Manipulation dieser Informationen könnte eine sichere Verschlüsselung des Quellcodes verhindern.

Machen Sie eine unverschlüsselte Datensicherung vor dem Verschlüsseln!

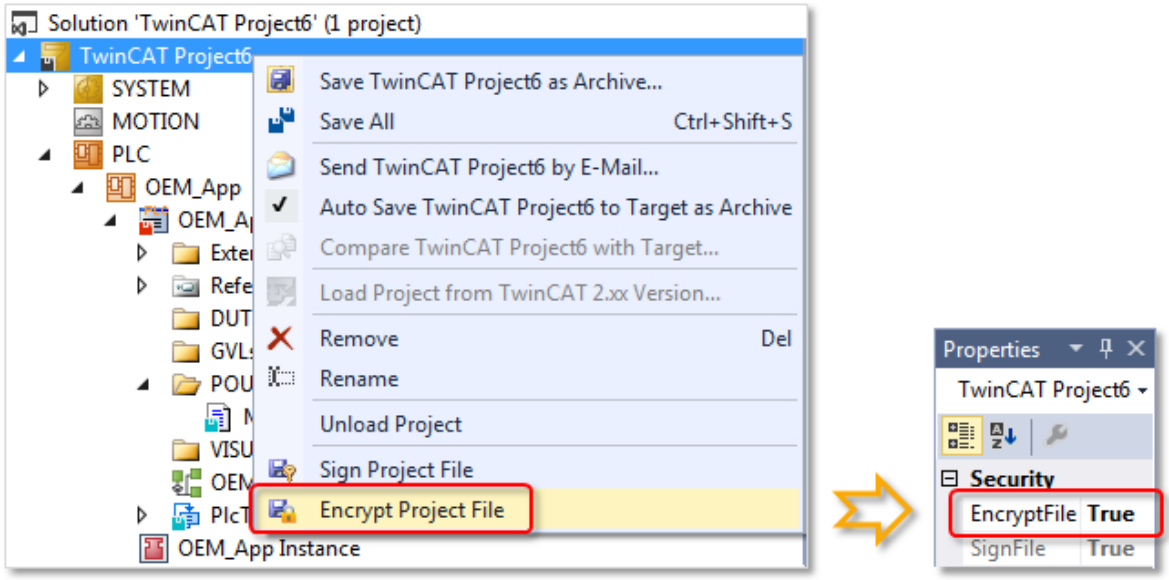
Bevor sie ein Projekt verschlüsseln: Machen Sie immer eine Datensicherung des Projekts im unverschlüsselten Zustand!

Die Verschlüsselung der Projektdatei stellen Sie über den TwinCAT-Projektknoten ein.

✓ Das Projekt ist mit einer Benutzerdatenbank verbunden.

1. Markieren Sie den TwinCAT-Projektknoten im Projektbaum im Projektmappen-Explorer.
2. Wählen Sie im Kontextmenü den Befehl **Encrypt Project File**.

⇨ In der Ansicht **Properties** wird der Wert der Eigenschaft **EncryptFile** in der Kategorie **Security** auf TRUE gesetzt.



⇨ Die Projektdatei ist verschlüsselt. Es beinhaltet Informationen zu den Komponenten der Lösung. Mit dem Einstellen der Verschlüsselung wird nur die Projektdatei selbst verschlüsselt. Die Verschlüsselung wird nicht auf die im Projekt enthaltenen Komponenten vererbt. Die Verschlüsselung muss bei allen (Haupt-) Komponenten des Projektes einzeln eingestellt werden.

Gilt nur für TwinCAT 3.1 Build 4024.0: Erstellung einer User DB erfordert Crypto Version 1

Die Erstellung einer Benutzerdatenbank [▶ 33] für die TwinCAT Software Protection darf in der TwinCAT-Version Build **4024.0** nur mit einem OEM-Zertifikat mit der Crypto Version 1 erfolgen!

7.1.3 Boot-Projekt verschlüsseln

Voraussetzung: Eine aktuelle Windows- oder TwinCAT/BSD-Version auf dem Zielsystem

Verschlüsselung wird von älteren Betriebssystemen, wie Windows NT, Windows CE / Windows Embedded Compact nicht unterstützt.

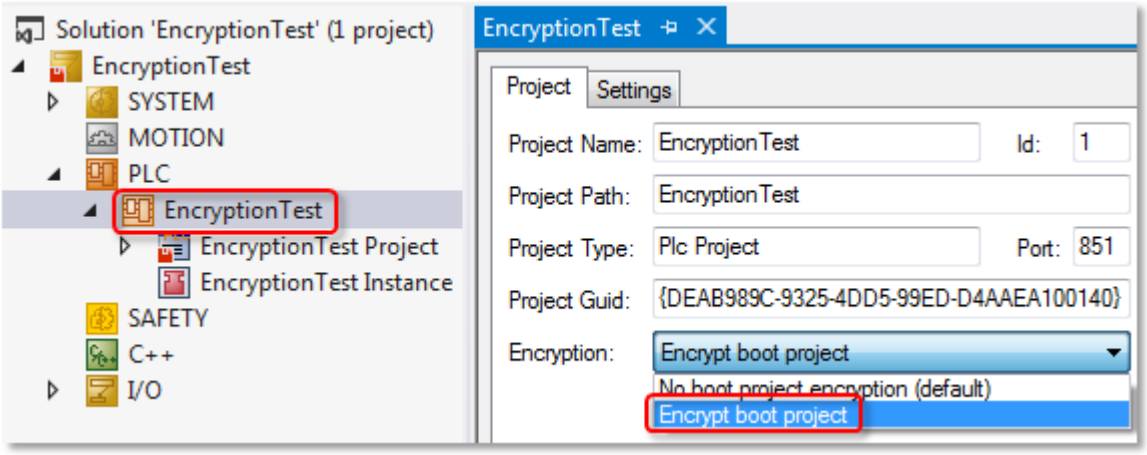
Die Verschlüsselung des Boot-Projekts (auf dem Target-System) stellen Sie im Wurzelknoten des SPS-Projekts ein.

✓ Im TwinCAT Engineering ist eine Benutzerdatenbank ausgewählt [▶ 39] (und gültig).

✓ Das Projekt muss mit der Benutzerdatenbank verbunden [▶ 70] sein, da für die Verschlüsselung Informationen aus der Benutzerdatenbank verwendet werden.

1. Klicken Sie doppelt auf das SPS-Projektobjekt im SPS-Projektbaum im Projektmappen-Explorer.
   ⇨ Die SPS-Projekteinstellungen werden in einem Editor geöffnet.

2. Wählen Sie in der Registerkarte **Project** in der Drop-down-Liste der Einstellung **Encryption** den Eintrag **Encrypt boot project** aus.

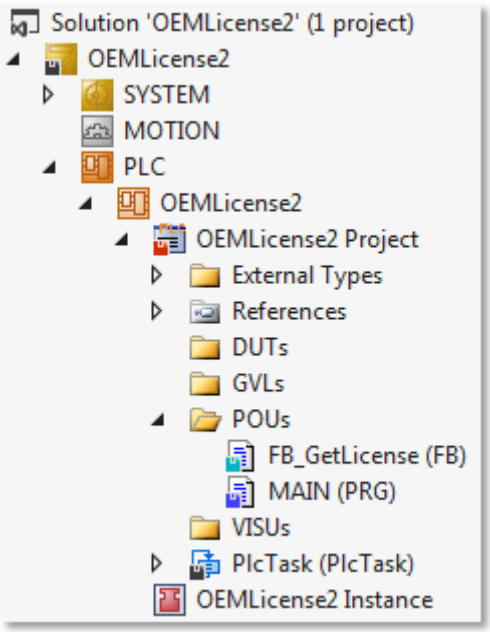


⇨ Das Boot-Projekt wird bei der Aktivierung für das Zielsystem verschlüsselt auf dem Zielsystem gespeichert.

Für die **Entschlüsselung** des Boot-Projekts auf dem **Zielsystem** ist weder eine Benutzerdatenbank noch ein OEM-Zertifikat erforderlich.

7.1.4 Anzeige des Objektschutzstatus

Den Status eines TwinCAT-Objektes erkennen Sie am Disketten-Symbol im Icon des Objektes im Projektbaum.



Zur Anzeige des Schutzstatus eines TwinCAT-Objektes wird die normale Statusanzeige eines TwinCAT-Objektes erweitert. In der nachfolgenden Tabelle sind die Symbole und ihre Bedeutungen aufgelistet.

Symbole des TwinCAT-Objektstatus

Symbol	Bedeutung
	Keine Änderungen
	Änderungen, nicht gespeichert
	Signiert
	Verschlüsselt

Regeln:

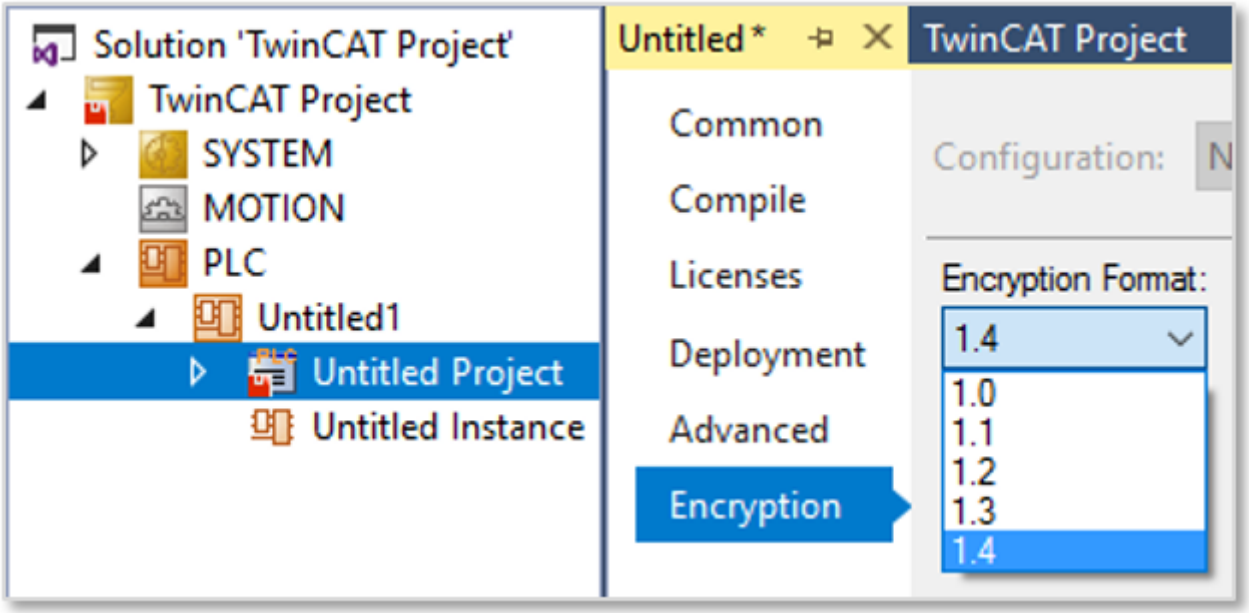
1. Türkis überschreibt Blau
2. Rot überschreibt alle anderen Farben

7.1.5 Anzeige der aktuellen Verschlüsselungsversion

Die aktuelle TwinCAT-Version setzt die aktuelle Verschlüsselungsversion ein. Beim TwinCAT Build 4022.x ist das zum Zeitpunkt der Erstellung dieser Dokumentation die Version 1.4.

Die Versionen 1.0-1.3 wurden bei den ersten Versionen (Build 4020.x) verwendet. Vom Einsatz dieser Verschlüsselungsversionen wird dringend abgeraten. Es sollte immer die neueste verfügbare Version verwendet werden.

Die aktuell verwendete Verschlüsselungsversion kann in den Properties eines Projektes eingesehen werden:



Falls es sich um ein älteres Projekt (mit Build 4020.x erstellt) handeln sollte, kann hier auch eine neuere Verschlüsselungsversion eingestellt werden.

Die aktuelle Verschlüsselungsversion steht nur im aktuellen TwinCAT 3-Build zur Verfügung! Die TwinCAT 3-Versionen Build 4020.x unterstützen z. B. nicht die Verschlüsselungsversion 1.4.

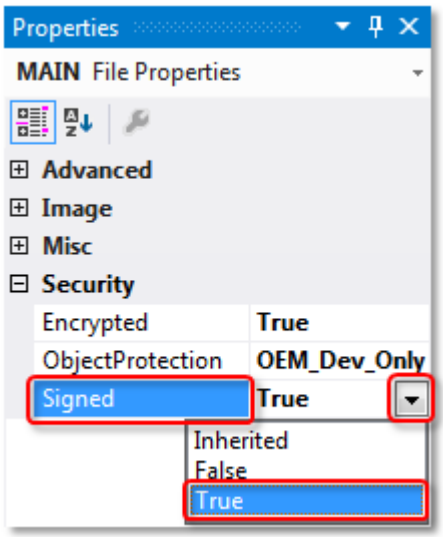
Voraussetzung für eine sichere Verschlüsselung ist der Einsatz einer aktuellen TwinCAT-Version mit der aktuellen Verschlüsselungsversion!

7.2 Dateien signieren (Schutz gegen unautorisierte Änderungen)

Durch das Signieren von Komponenten (Dateien) des Projektes stellen Sie sicher, dass einzelne Projektkomponenten nicht unautorisiert ausgetauscht werden können.

Signieren Sie auch die Projektdatei selbst, da dort die Information gespeichert ist, welche darunter liegenden Komponenten signiert sein müssen.

Wenn das Projekt mit einer Benutzerdatenbank verbunden ist, können Sie die Signierung in den Eigenschaften der jeweiligen Projektkomponente einstellen. Markieren Sie die Projektkomponente im Solution Explorer und setzen Sie in der Ansicht **Properties** den Wert der Eigenschaft **Signed** auf TRUE.



Systemvoraussetzungen

Betriebssystem:

- Um alle Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist mindestens Windows 7 (bzw. dessen Embedded-Version) erforderlich. Windows XP und Windows CE (Windows Embedded Compact) unterstützen weder die Verschlüsselung der Boot-Datei noch OEM-Lizenzen.

TwinCAT-Version:

- Die beschriebenen Funktionalitäten erfordern mindestens TwinCAT 3.1 Build 4022.

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

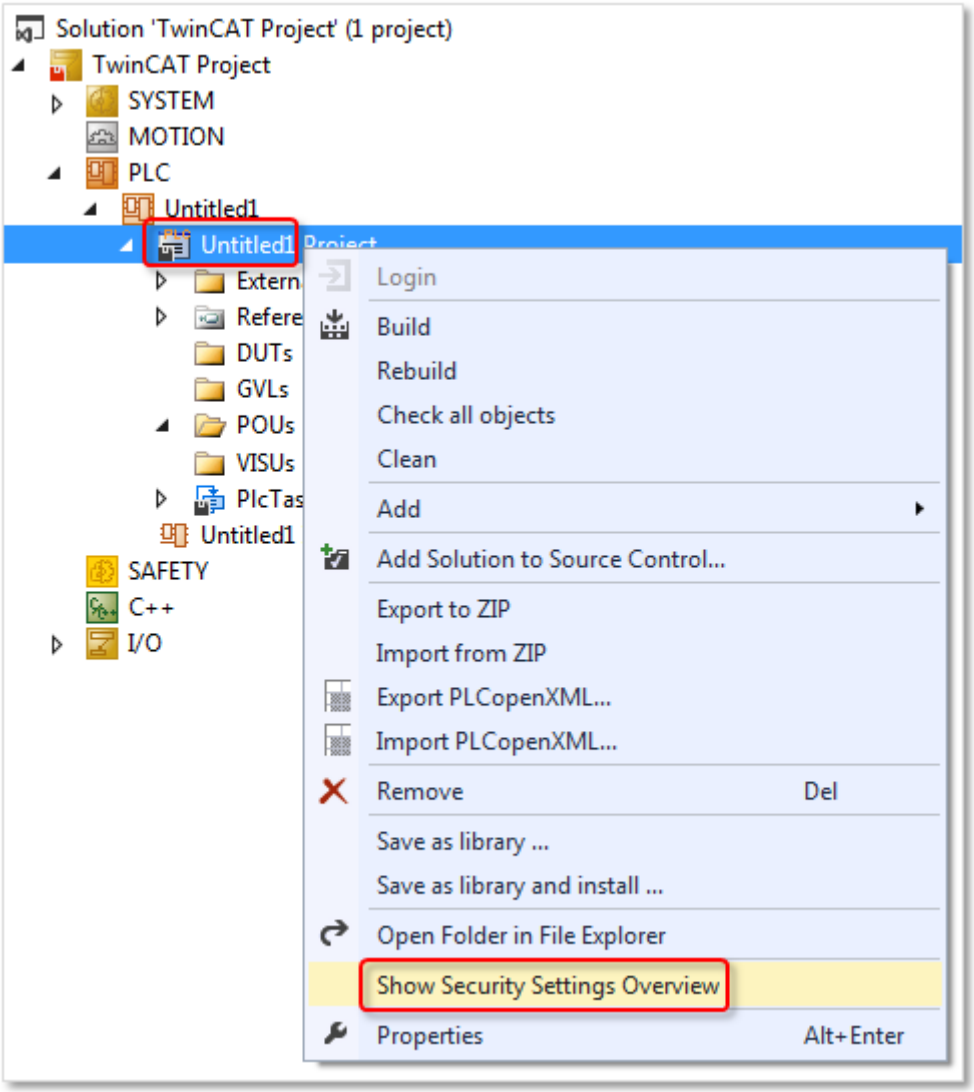
Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

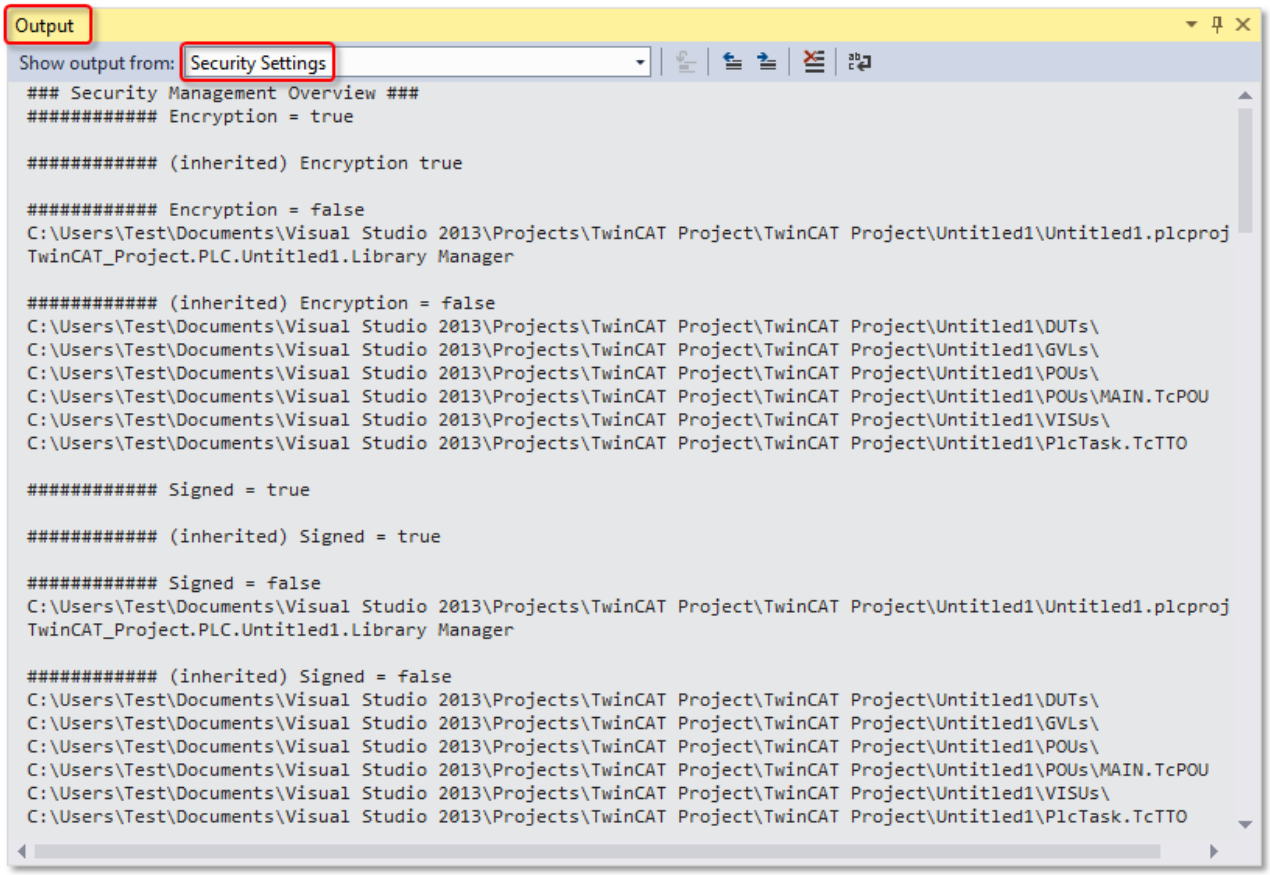
7.3 Übersicht der Softwareschutz-Einstellungen des PLC-Projektes anzeigen

Sie können sich die Einstellungen zum Schutz der PLC-Anwendungssoftware im Ausgabefenster der TwinCAT-3-Entwicklungsumgebung anzeigen lassen.

Markieren Sie im Projektmappen-Explorer den Wurzelknoten des SPS-Projekts und wählen Sie im Kontextmenü den Befehl **Show Security Settings Overview**.



Im Ausgabefenster wird eine Zusammenfassung der aktuellen Security-Einstellungen des Projektes angezeigt.


Output
Show output from: Security Settings
Security Management Overview
############ Encryption = true
############ (inherited) Encryption true
############ Encryption = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\Untitled1.plcproj
TwinCAT_Project.PLC.Untitled1.Library Manager
############ (inherited) Encryption = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\DUTs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\GVLs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\MAIN.TcPOU
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\VISUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\PlcTask.TcTTO
############ Signed = true
############ (inherited) Signed = true
############ Signed = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\Untitled1.plcproj
TwinCAT_Project.PLC.Untitled1.Library Manager
############ (inherited) Signed = false
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\DUTs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\GVLs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\POUs\MAIN.TcPOU
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\VISUs\
C:\Users\Test\Documents\Visual Studio 2013\Projects\TwinCAT Project\TwinCAT Project\Untitled1\PlcTask.TcTTO

8 Eigene OEM-Lizenzen ausstellen und nutzen

Mithilfe der TwinCAT 3 Lizenztechnologie kann eine SPS-Anwendung durch Bindung an eine Hardware (Beckhoff IPC oder TwinCAT-Dongle) vor Klonen geschützt werden. Außerdem können durch Erstellung sogenannter „Feature-Lizenzen“ Zusatzfunktionalitäten der Anwendung an Endkunden lizenziert werden.

Hier finden Sie dazu den Quickstart.

Systemvoraussetzungen

Betriebssystem:

- Um alle Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist mindestens Windows 7 (bzw. dessen Embedded-Version) erforderlich. Windows XP und Windows CE (Windows Embedded Compact) unterstützen weder die Verschlüsselung der Boot-Datei noch OEM-Lizenzen.

TC3 PLC Lib Tc2_Utiltities:

- Verwenden Sie mindestens Version 3.3.24 der TC3 PLC Lib Tc2_Utilities, da sie diverse Funktionen zum komfortablen Handling von TwinCAT-3-Lizenzen bietet. Sie ist zwingend erforderlich für die Nutzung von TwinCAT-3-Dongles für OEM-Applikationslizenzen. Die TC3 PLC Lib ist ab TwinCAT 3.1 Build 4022.16 enthalten.

TwinCAT-Version:

- Die beschriebenen Funktionalitäten erfordern mindestens TwinCAT 3.1 Build 4024.

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

Allgemeine Hinweise

Nutzung von OEM-Lizenzen = Bootprojekt verschlüsseln!

Denken Sie daran, dass die per FB_CheckLicense [▶ 93] abgefragte License-ID [▶ 86] im Binärcode mit einem Hex-Editor leicht gefunden und (mit einem gewissen Aufwand) manipuliert werden kann. Arbeiten Sie daher unbedingt mit einer Verschlüsselung des Bootprojektes [▶ 78] (am sichersten), oder verschleiern Sie zumindest die abgefragte License-ID im Quellcode bestmöglich.

- Für die Anwendungslizenzierung ist keine Benutzerdatenbank erforderlich.
- Die Lizenzvalidierung erfolgt durch die TwinCAT-3-Runtime (XAR). Die TwinCAT-3-Runtime muss also auf dem IPC installiert sein.
- Die Gültigkeit der Anwendungslizenz ist unabhängig von der Gültigkeitsdauer des OEM-Zertifikates. Die Anwendungslizenz bleibt also auch nach Ablauf der Gültigkeitsdauer des OEM-Zertifikates gültig.
- Die Nutzung von OEM-Applikationslizenzen erfordert immer einen TwinCAT-3-Dongle oder einen Beckhoff IPC.
- Bei IPCs mit einem Plattform-Level >= 90 (Nicht-Beckhoff-IPCs) muss aus Sicherheitsgründen immer ein TwinCAT-3-Dongle als „License Device“ verwendet werden!

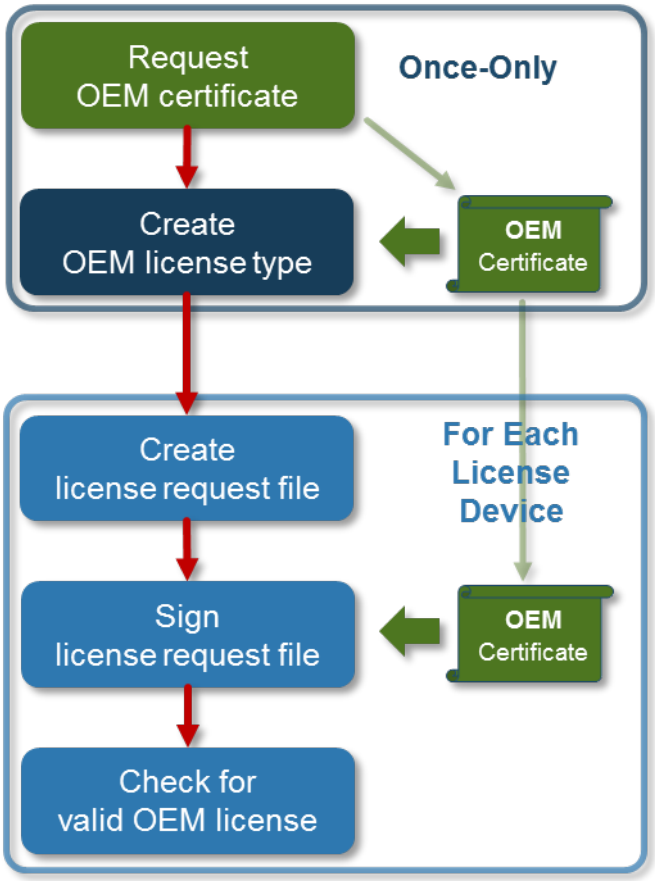
Voraussetzung für die Nutzung dieser Funktion: Ausstellung eines TwinCAT OEM Zertifikates [▶ 19]

Lizenzierungsprozess

Der Lizenzierungsprozess unterteilt sich in folgende Schritte:

1. Erstellen einer generellen Lizenzbeschreibungsdatei.
   Die Lizenzierungsbeschreibungsdatei dient zum Beschreiben und Auswählen eines spezifischen Lizenztyps im Laufe des Lizenzierungsprozesses. Sie enthält u.a. eine eindeutige License ID, die zur eindeutigen Identifikation dieses Lizenztyps dient.
2. Erstellen eines License Request Files für das gewünschte Zielsystem.

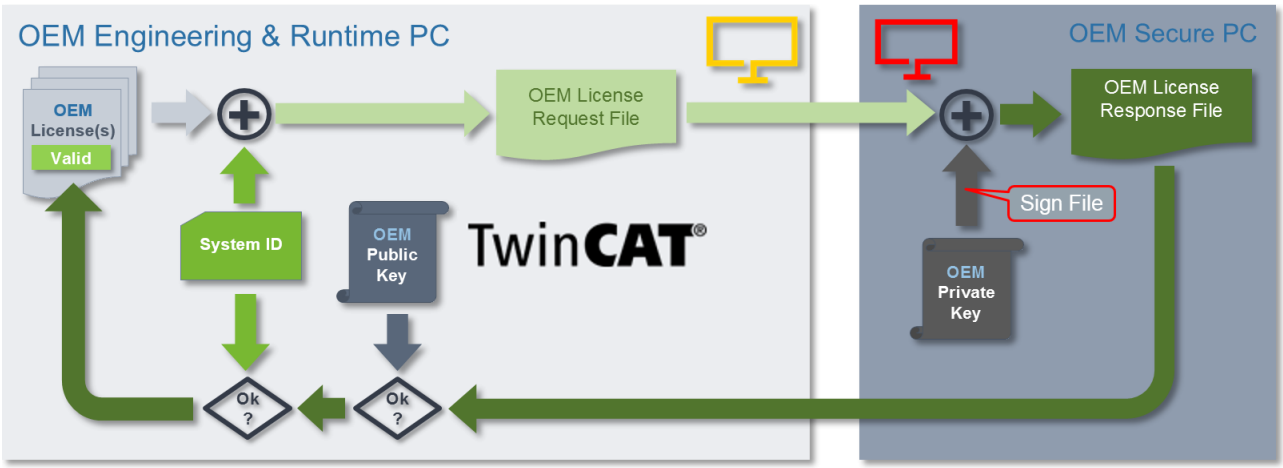
3. Signieren des License Request Files mit dem OEM-Zertifikat und damit Erzeugen eines License Response Files für das angegebene Zielsystem. Diese aktiviert dann auf dem jeweiligen Zielsystem die zugehörige OEM-Applikationslizenz.



Die Details des Lizenzierungsprozesses werden in den folgenden Abschnitten beschrieben.

8.1 OEM-Applikationslizenzen erstellen

Die folgende Grafik soll einen generellen Überblick über den Lizenzierungsprozess vermitteln:



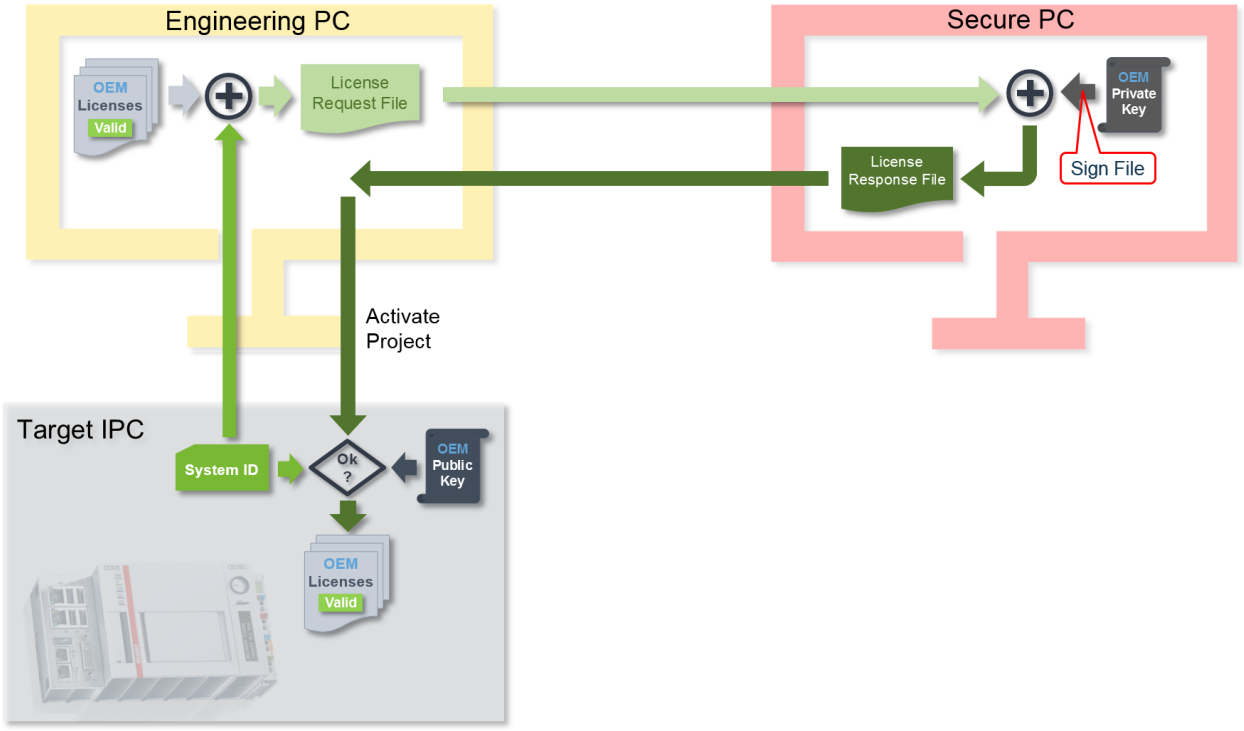
Der linke Teil der Grafik (hellgrauer Kasten) stellt weitgehend die Erstellung eines License Request Files für eine TwinCAT-3-Lizenz, bzw. deren Prüfung in der TwinCAT-3-Runtime dar.

Der rechte Teil der Grafik (dunkelgrauer Kasten) zeigt die Prozesse der Lizenzvergabe, die vom Beckhoff Lizenzserver übernommen werden.
Bei einer OEM-Applikationslizenz erfolgt dieser Teil, also die Ausstellung einer Lizenz, jedoch durch den OEM über eine Signierung mit dem OEM Private Key. Der Beckhoff Lizenzserver ist also nicht in den Prozess des Erstellens einer OEM-Applikationslizenz eingebunden.

OEM-Zertifikate nur in sicherer Umgebung verwenden

Da für das Ausstellen einer OEM-Applikationslizenz mit dem OEM-Zertifikat und dessen Passwort hantiert werden muss, führen Sie den Vorgang nur in einer gegenüber Schadsoftware abgeschotteten Umgebung (= gesicherter PC) durch, um z. B. das Abgreifen des Passwortes für den OEM Private Key durch Schadsoftware zu verhindern.

Wenn Steuerungsrechner und Engineering-Rechner separate Geräte sind, sieht der Prozessfluss wie folgt aus:



8.1.1 Vorbereitung des TwinCAT 3 Engineering

Das TwinCAT Engineering ist standardmäßig nicht für die Erstellung von OEM-Lizenzen vorkonfiguriert.

1. Erstellen Sie vorab folgende Verzeichnisse:
   - <TwinCAT_ROOT>\3.1\CustomConfig\Licenses
   - <TwinCAT_ROOT>\3.1\Components\Base\License
2. Kopieren Sie in das Verzeichnis *c:\TwinCAT\3.1\Components\Base\License* das Tool „CreateLicense.exe*“. Dieses Tool können Sie über den E-Mail-Alias tccertificate@beckhoff.com anfragen.

TwinCAT Root-Verzeichnis <TwinCAT_ROOT>

Bis einschließlich TwinCAT 3.1.4024: **C:\TwinCAT**
Ab TwinCAT 3.1.4026: **C:\ProgramData\Beckhoff\TwinCAT**

8.1.2 Lizenzbeschreibungsdatei für eine OEM-Applikationslizenz erstellen

Die Parameter des Typs einer TwinCAT-3-Lizenz werden in einer Lizenzbeschreibungsdatei im XML-Format mit der Extension .tmc festgelegt.

Eine Lizenzbeschreibungsdatei beinhaltet:

- eine eineindeutige „License ID“, die den Lizenztyp sicher identifizierbar macht
- die eineindeutige OEM-ID (aus dem OEM-Zertifikat)
- den OEM-Namen
- den Namen des Lizenztyps
- die Bestellnummer
- optional eine E-Mail-Adresse für die Zusendung des License Request Files per Email

```
<Vendor>
    <Name>SampleOEM Inc</Name>
</Vendor>
<Licenses>
    <License>
        <LicenseId>{CF1A625C-F2EC-477F-9008-65C305079F03}</LicenseId>
        <OemId OemName="SampleOEM Inc" OrderAddress="license@SampleOEM.com">{DB77E273-19F3-C4B6-2A2D-007613D67AA4}</OemId>
        <OrderNo>4711-0815</OrderNo>
        <DisplayName>Sample_License A1</DisplayName>
    </License>
</Licenses>
```

Über die OEM-ID kann die Lizenz einem spezifischen OEM zugeordnet werden. Nur dieser OEM (mit dieser OEM-ID in seinem OEM-Zertifikat) kann die Lizenz mit seinem OEM-Zertifikat signieren und damit gültig machen.

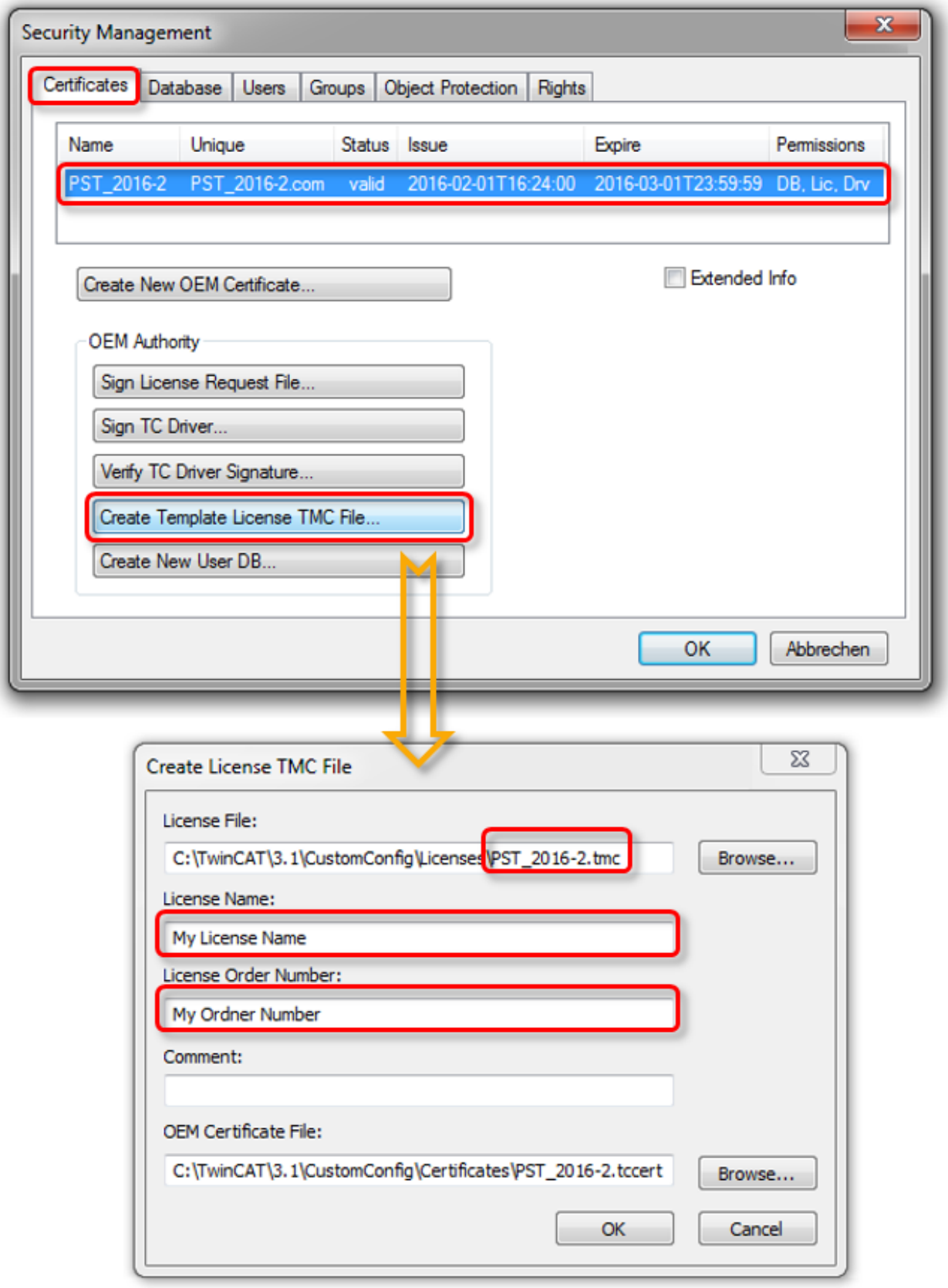
Eine OEM-Lizenzbeschreibungsdatei können Sie mit einem geeigneten Editor öffnen und verändern, wenn die XML-Struktur dabei nicht beschädigt wird.

Neue OEM-Lizenzbeschreibungsdatei angelegen

> **TwinCAT Root-Verzeichnis <TwinCAT_ROOT>**
>
> Bis einschließlich TwinCAT 3.1.4024: **C:\TwinCAT**
> Ab TwinCAT 3.1.4026: **C:\ProgramData\Beckhoff\TwinCAT**

✓ Der Software-Protection-Konfigurator [▶ 11] ist geöffnet.

1. Wählen Sie in der Registerkarte **Certificates** das OEM-Zertifikat aus, auf dessen Basis die OEM-Lizenzbeschreibungsdatei erstellt werden soll.
2. Klicken Sie auf **Create Template License TMC File**.
   ⇨ Der Dialog **Create Licenses TMC File** öffnet sich.
3. Geben Sie die Parameter für die OEM-Lizenzbeschreibungsdatei ein:
   - Speichern Sie die Lizenzbeschreibungsdatei im Ordner *<TwinCAT_ROOT>\3.1\CustomConfig\Licenses*, und starten Sie das TwinCAT 3 Engineering neu. Erst dann wird die Lizenzbeschreibungsdatei von TwinCAT 3 erkannt.
   - Geben Sie einen Lizenznamen und eine Lizenzbestellnummer ein.



4. Starten Sie das TwinCAT 3 Engineering neu, damit der neue Lizenztyp erkannt wird.

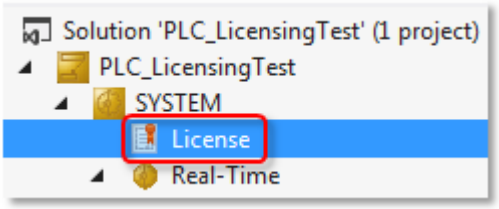
⇨ Die Lizenzbeschreibungsdatei ist erstellt.

8.1.3 License Request Files für eine OEM-Applikationslizenz erstellen

TwinCAT-3-Lizenzen für Nicht-Beckhoff-IPCs

Wenn Sie einen IPC von einem anderen Hersteller als Beckhoff einsetzen (TwinCAT-3-Plattform-Level >= 90), ist für die Lizenzierung von TwinCAT 3 immer ein TwinCAT-3-Lizenz-Dongle erforderlich.

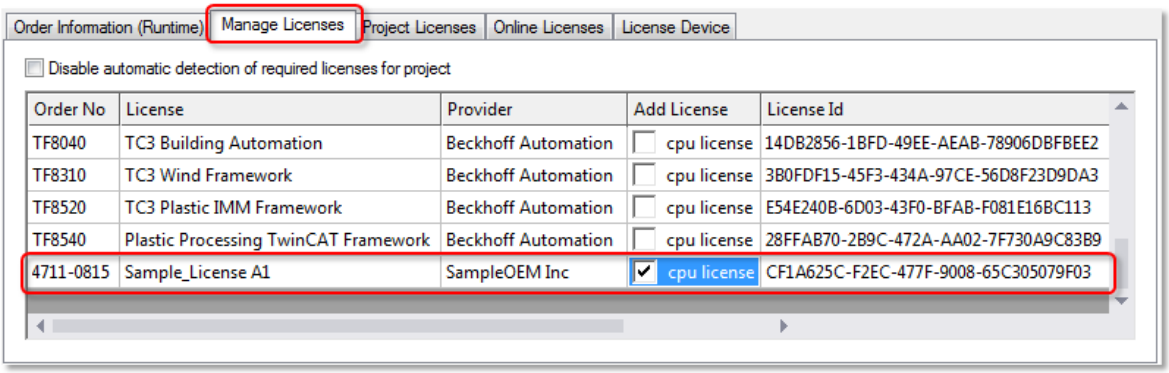
1. Klicken Sie doppelt auf den SYSTEM-Unterknoten **License** im TwinCAT-Projektbaum, um den TwinCAT 3 Lizenzmanager zu öffnen.



   ⇨ Die Lizenzeinstellungen öffnen sich in einem Editor.

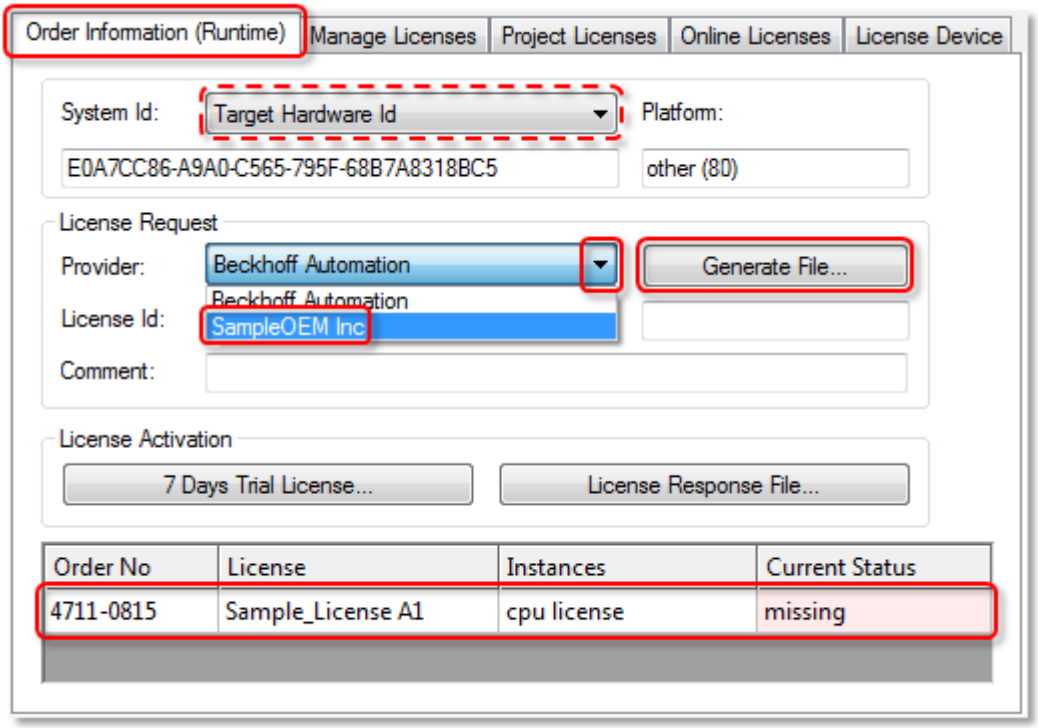
2. Öffnen Sie die Registerkarte **Manage Licenses** und bewegen Sie die Laufleiste des Listenfelds nach unten.

   ⇨ Am Ende der Liste finden Sie die neu erstellte OEM-Lizenz.



3. Aktivieren Sie das Auswahlkästchen der Lizenz.

4. Öffnen Sie die Registerkarte **Order Information**.



5. Optional können Sie bei **System ID** auch einen TwinCAT-3-Lizenz-Dongle als Lizenz-Hardware auswählen (gestrichelte Linie).
6. Stellen Sie als **Provider** den jeweiligen OEM ein. Sie dürfen nicht den Eintrag „Beckhoff“ auswählen, dieser gilt nur für TwinCAT-3-Lizenzen von Beckhoff.
   ⇨ In der Liste im unteren Bereich des Fensters muss die ausgewählte OEM-Lizenz aufgelistet und aktiv (= nicht ausgegraut) sein. Wenn die Lizenz ausgegraut ist, ist nicht der korrekte „Provider“ ausgewählt. Nur die als „aktiv“ gekennzeichneten Lizenzen werden in das License Request File übernommen.
7. Klicken Sie auf **Generate File**, um das License Request File (Endung: *.tclrq) zu erzeugen.
   ⇨ Der Standarddialog zum Speichern einer Datei öffnet sich.
8. Wählen Sie einen Speicherort aus und bestätigen Sie den Dialog.

⇨ Das Licence Request File für eine OEM-Applikationslizenz ist erstellt.

8.1.4 License Response Files für eine OEM-Applikationslizenz erstellen

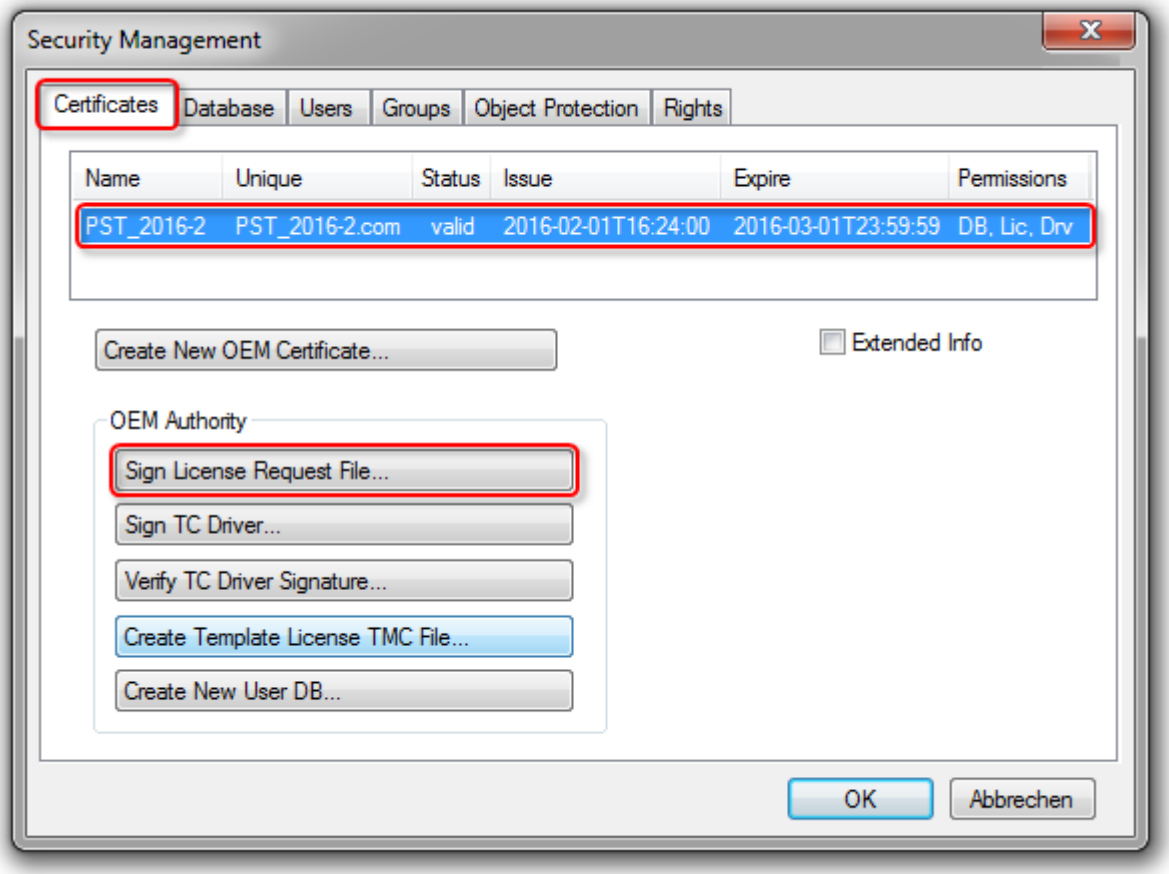
8.1.4.1 Manuelle Erstellung über das TwinCAT Engineering

OEM-Zertifikate nur in sicherer Umgebung verwenden

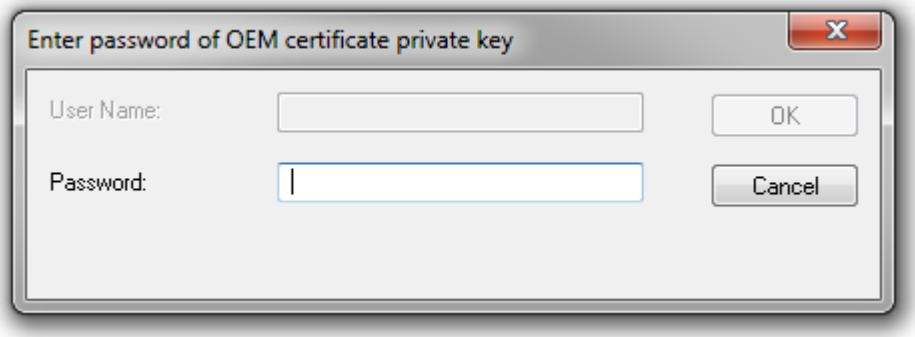
Da für das Ausstellen einer OEM-Applikationslizenz mit dem OEM-Zertifikat und dessen Passwort hantiert werden muss, führen Sie den Vorgang nur in einer gegenüber Schadsoftware abgeschotteten Umgebung (= gesicherter PC) durch, um z. B. das Abgreifen des Passwortes für den OEM Private Key durch Schadsoftware zu verhindern.

Das manuelle Signieren eines License Request Files, und damit das Erstellen eines License Response Files, nehmen Sie im TwinCAT Engineering im Software-Protection-Konfigurator [▶ 11] vor.

1. Wählen Sie in der Registerkarte **Certificates** das OEM-Zertifikat aus.



2. Klicken Sie auf **Sign License Request File**.
   ⇨ Ein Explorer-Fenster öffnet sich.
3. Wählen Sie das zu signierende License Request File (Endung: *.tclrq) aus.
   ⇨ Ein Dialog öffnet sich, in dem das Passwort abgefragt wird.



4. Geben Sie das Passwort ein und klicken Sie auf **OK**.

⇨ Die Signierung des License Request Files wird durchgeführt und das Ergebnis als License Response File (Endung: *.tclrs) gespeichert. Das License Response File muss nun wieder auf den Engineering-PC oder den Steuerungsrechner transferiert werden.

8.1.4.2 Automatisierte Erstellung über ein Kommandozeilentool

OEM-Zertifikate nur in sicherer Umgebung verwenden

Da für das Ausstellen einer OEM-Applikationslizenz mit dem OEM-Zertifikat und dessen Passwort hantiert werden muss, führen Sie den Vorgang nur in einer gegenüber Schadsoftware abgeschotteten Umgebung (= gesicherter PC) durch, um z. B. das Abgreifen des Passwortes für den OEM Private Key durch Schadsoftware zu verhindern.

TwinCAT Root-Verzeichnis <TwinCAT_ROOT>

Bis einschließlich TwinCAT 3.1.4024: **C:\TwinCAT**
Ab TwinCAT 3.1.4026: **C:\ProgramData\Beckhoff\TwinCAT**

Das TwinCAT 3 Engineering nutzt ein Kommandozeilentool (TcSignTool.exe) zum Ausstellen (Signieren) von OEM-Lizenzen. Dieses Tool kann auch aus einem Anwenderprogramm heraus zum automatisierten Ausstellen von OEM-Lizenzen aufgerufen werden.

TcSignTool.exe liegt in einer TwinCAT 3-Installation im Pfad <TwinCAT_ROOT>\3.1\sdk\Bin.

Aufrufparameter

tcsigntool licsign /f certificatefile [/p password] [/i issueTime] [/d validDays] [/q] licfile1 [licfile2]

- certificatefile: OEM Zertifikatsdatei
- password: Passwort für das OEM Zertifikat
- issueTime: Format yyyy-mm-ddThh:mm:ss (Default-Wert = aktuelle Zeit)
- validDays: Default-Wert = Unlimitiert
- licfile<n>: License Request oder Response Datei mit der Erweiterung '.tclrq' oder '.tclrs‘. License Request Dateien mit der Erweiterung '.tclrq' werden umbenannt in '.tclrs‘.
- /q Quiet Mode
- Rückgabewerte: 0 = Succeeded, 1 = Failed

8.1.5 License Response Files für eine OEM-Applikationslizenz importieren

TwinCAT-3-Lizenzen für Nicht-Beckhoff-IPCs

Wenn Sie einen IPC von einem anderen Hersteller als Beckhoff einsetzen (TwinCAT-3-Plattform-Level >= 90), ist für die Lizenzierung von TwinCAT 3 immer ein TwinCAT-3-Lizenz-Dongle erforderlich.

TwinCAT Root-Verzeichnis <TwinCAT_ROOT>

Bis einschließlich TwinCAT 3.1.4024: **C:\TwinCAT**
Ab TwinCAT 3.1.4026: **C:\ProgramData\Beckhoff\TwinCAT**

Die Aktivierung der OEM-Applikationslizenz erfolgt genauso wie bei einer TwinCAT-3-Standardlizenz. Der einfachste Weg, ein TwinCAT 3 Licence Response File in TwinCAT 3 zu aktivieren, ist der Import über den TwinCAT 3 Lizenzmanager. Weitere Informationen finden Sie in der Dokumentation „Lizenzierung“ im Abschnitt License Response Files importieren und aktivieren.

Sie können die Lizenzdatei aber auch direkt auf dem Zielsystem im Verzeichnis *<TwinCAT_ROOT>3.1\target\license* speichern.

Wie Sie die Lizenzdatei auf einem TwinCAT-3-Dongle ablegen, wird in der Dokumentation „Lizenzierung“ im Abschnitt Lizenzdateien manuell auf dem Dongle speichern beschrieben.

8.2 OEM-Applikationslizenzen auf einem Dongle ablegen

Um eine OEM-Applikationslizenz auf einem Lizenz-Dongle abzulegen (zu speichern), gibt es zwei Möglichkeiten, die im Bereich der TwinCAT-3-Lizenzierung beschrieben sind:

- Lizenzdateien manuell auf dem Dongle speichern
- SPS-Funktionsbausteine zur Speicherfunktion der Lizenz-Dongles

8.3 OEM-Applikationslizenz in einer SPS-Applikation abfragen

Nutzung von OEM-Lizenzen = Bootprojekt verschlüsseln!

Denken Sie daran, dass die per FB_CheckLicense [▶ 93] abgefragte License-ID [▶ 86] im Binärcode mit einem Hex-Editor leicht gefunden und (mit einem gewissen Aufwand) manipuliert werden kann. Arbeiten Sie daher unbedingt mit einer Verschlüsselung des Bootprojektes [▶ 78] (am sichersten), oder verschleiern Sie zumindest die abgefragte License-ID im Quellcode bestmöglich.

Die Lizenzüberprüfung im Aufstartprozess der TwinCAT Runtime erfolgt in zwei Schritten:

1. TwinCAT 3 liest zunächst die im System (auf der Festplatte) gespeicherten Lizenzdateien ein, überprüft deren Inhalt und erstellt eine interne Liste der gefundenen Lizenzen.
2. Die finale Überprüfung der Lizenzen erfolgt nach der Inbetriebnahme des EtherCAT-Busses, da erst dann alle erforderlichen Informationen zur Verfügung stehen. (Vorher kann z. B. das Vorhandensein einer EL6070 Lizenzklemme nicht verifiziert werden.)

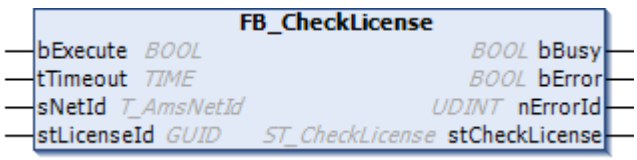
Das Ergebnis können Sie nach dem abgeschlossenen Aufstart mit dem Funktionsbaustein FB_CheckLicense abrufen.

Im laufenden Betrieb (nach dem Aufstart und der finalen Lizenzprüfung) wird der Status der Lizenzen von der TwinCAT Runtime ca. **alle zwei Minuten** erneut überprüft. Das sollte im PLC-Programm entsprechend berücksichtigt werden (also FB_CheckLicense z. B. nur alle 10 Sekunden aufrufen).

Hinweise:

- FB_CheckLicense liest lediglich den aktuell gespeicherten Lizenzstatus in der internen Tabelle, löst aber keine erneute Lizenzüberprüfung aus. Das Entfernen eines Dongles im laufenden Betrieb kann sich also erst nach bis zu ca. zwei Minuten beim Lizenzstatus der zugehörigen Lizenz bemerkbar machen.
- Tipp: Bei Bedarf können aktuell am System angeschlossene Dongle mit dem Funktionsbaustein FB_GetLicenseDongles ermittelt werden.
- Die Lizenzüberprüfung ist Teil des Aufstartprozesses der TwinCAT Runtime. Bedeutet also: Keine laufende Runtime = keine aktuellen Lizenzinformationen!

FB_CheckLicense



Der Funktionsbaustein ermittelt den TwinCAT-3-Lizenzstatus für eine gegebene Lizenz-ID.

Eingänge

```
VAR_INPUT
    bExecute    : BOOL;
    tTimeout    : TIME;
    sNetId      : T_AmsNetId;
    stLicenseId : GUID;
END_VAR
```

Name	Typ	Beschreibung
bExecute	BOOL	Über eine positive Flanke an diesem Eingang wird der Baustein aktiviert.
tTimeout	TIME	Timeout-Zeit, die bei Ausführung des Befehls nicht überschritten werden darf.
sNetId	T_AmsNetId	AmsNetId (AMS-Netzwerkkennung) des TwinCAT-Rechners, dessen Lizenzstatus ausgelesen werden soll. Für den lokalen Rechner kann auch ein Leerstring angegeben werden.
stLicenseId	GUID	Lizenz-ID

Ausgänge

```
VAR_OUTPUT
    bBusy          : BOOL;
    bError         : BOOL;
    nErrorId       : UDINT;
    stCheckLicense : ST_CheckLicense
END_VAR
```

Name	Typ	Beschreibung
bBusy	BOOL	TRUE, solange der Baustein aktiv ist.
bError	BOOL	TRUE, wenn bei der Ausführung des Kommandos ein Fehler auftritt.
nErrorId	UDINT	Liefert bei einem gesetzten bError-Ausgang die ADS-Fehlernummer.
stCheckLicense	ST_CheckLicense [▶ 94]	Struktur mit Lizenzdaten

STRUCT ST_CheckLicense

```
TYPE ST_CheckLicense :
STRUCT
    stLicenseId     : GUID;
    tExpirationTime : TIMESTRUCT;
    sExpirationTime : STRING(80);
    eResult         : E_LicenseHResult;
    nCount          : UDINT;
END_STRUCT
END_TYPE
```

Name	Beschreibung
stLicenseId	Lizenz-ID
tExpirationTime	Verfallsdatum
sExpirationTime	Verfallsdatum
eResult	Lizenzstatus (siehe E_LicenseHResult [▶ 94])
nCount	Anzahl der Instanzen für diese Lizenz (0=unbegrenzt)

ENUM E_LicenseHResult

```
TYPE E_LicenseHResult :
(
    //success
    E_LHR_LicenseOK                : DINT := 0,
    E_LHR_LicenseOK_Pending        : DINT := 16#203,
    E_LHR_LicenseOK_Demo           : DINT := 16#254,
    E_LHR_LicenseOK_OEM            : DINT := 16#255,
    //error
    E_LHR_LicenseNoFound           : DINT := DWORD_TO_DINT(16#98110700+16#24),
    E_LHR_LicenseExpired           : DINT := DWORD_TO_DINT(16#98110700+16#25),
    E_LHR_LicenseExceeded          : DINT := DWORD_TO_DINT(16#98110700+16#26),
    E_LHR_LicenseInvalid           : DINT := DWORD_TO_DINT(16#98110700+16#27),
    E_LHR_LicenseSystemIdInvalid   : DINT := DWORD_TO_DINT(16#98110700+16#28),
    E_LHR_LicenseNoTimeLimit       : DINT := DWORD_TO_DINT(16#98110700+16#29),
    E_LHR_LicenseTimeInFuture      : DINT := DWORD_TO_DINT(16#98110700+16#2A),
    E_LHR_LicenseTimePeriodToLong  : DINT := DWORD_TO_DINT(16#98110700+16#2B),
    E_LHR_DeviceException          : DINT := DWORD_TO_DINT(16#98110700+16#2C),
```

```
    E_LHR_LicenseDuplicated        : DINT := DWORD_TO_DINT(16#98110700+16#2D),
    E_LHR_SignatureInvalid         : DINT := DWORD_TO_DINT(16#98110700+16#2E),
    E_LHR_CertificateInvalid       : DINT := DWORD_TO_DINT(16#98110700+16#2F),
    E_LHR_LicenseOemNotFound       : DINT := DWORD_TO_DINT(16#98110700+16#30),
    E_LHR_LicenseRestricted        : DINT := DWORD_TO_DINT(16#98110700+16#31),
    E_LHR_LicenseDemoDenied        : DINT := DWORD_TO_DINT(16#98110700+16#32),
    E_LHR_LicensePlatformLevelInv  : DINT := DWORD_TO_DINT(16#98110700+16#33)
)DINT;
END_TYPE
```

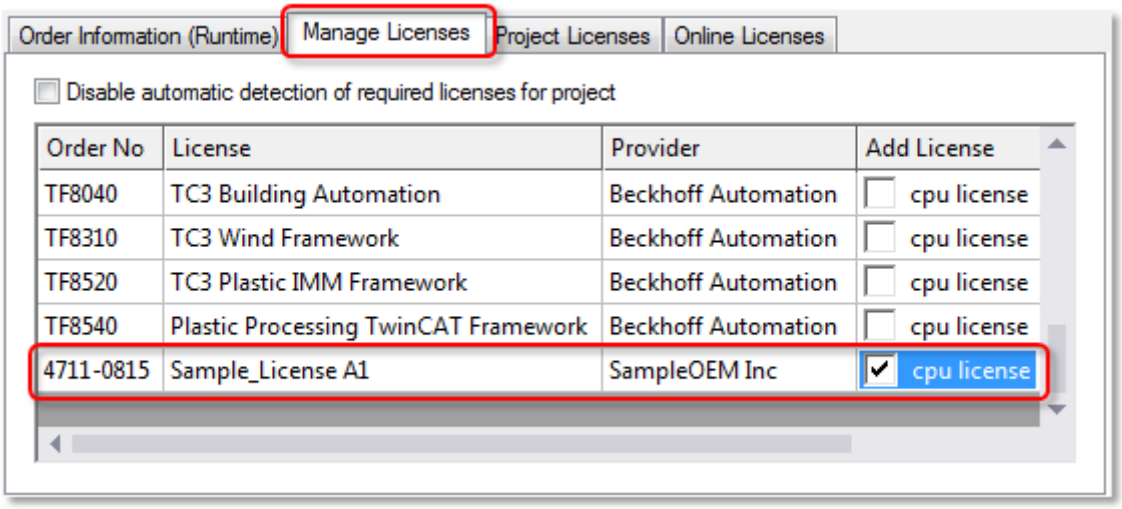
Wert	Bedeutung
E_LHR_LicenseOK	Lizenz ist gültig
E_LHR_LicenseOK_Pending	Validierung des Lizenzierungsgeräts (z. B. Lizenzklemme) notwendig
E_LHR_LicenseOK_Demo	Testlizenz ist gültig
E_LHR_LicenseOK_OEM	OEM-Lizenz ist gültig
E_LHR_LicenseNoFound	Fehlende Lizenz
E_LHR_LicenseExpired	Lizenz abgelaufen
E_LHR_LicenseExceeded	Lizenz hat zu wenig Instanzen
E_LHR_LicenseInvalid	Lizenz ist ungültig
E_LHR_LicenseSystemIdInvalid	Falsche System-ID für die Lizenz
E_LHR_LicenseNoTimeLimit	Lizenz nicht zeitlich begrenzt
E_LHR_LicenseTimeInFuture	Lizenzproblem: Ausstellungszeitpunkt in der Zukunft
E_LHR_LicenseTimePeriodToLong	Lizenz-Zeitraum zu lang
E_LHR_DeviceException	Exception beim Systemstart
E_LHR_LicenseDuplicated	Lizenzdaten mehrfach gelesen
E_LHR_SignatureInvalid	Ungültige Signatur
E_LHR_CertificateInvalid	Ungültiges Zertifikat
E_LHR_LicenseOemNotFound	OEM-Lizenz für unbekannten OEM
E_LHR_LicenseRestricted	Lizenz für das System ungültig
E_LHR_LicenseDemoDenied	Testlizenz nicht erlaubt
E_LHR_LicensePlatformLevelInv	Ungültiger Plattform-Level für die Lizenz

License ID der OEM-Lizenz ermitteln

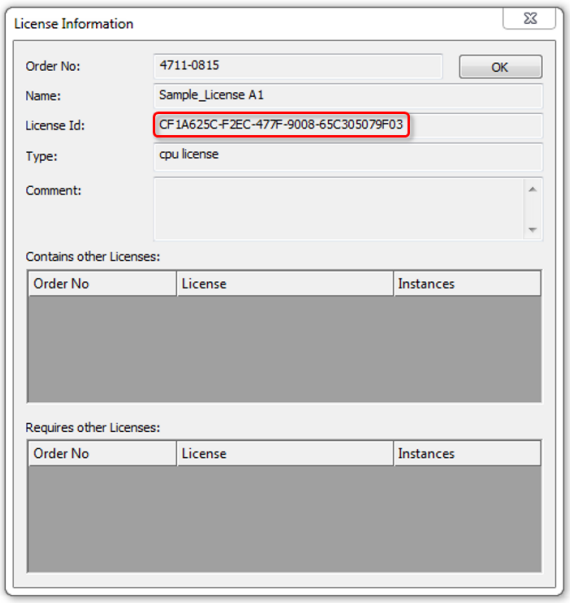
Die License ID der OEM-Lizenz können Sie der zugehörigen Lizenzbeschreibungsdatei oder dem Lizenzmanager entnehmen.

Lizenzbeschreibungsdatei:

Registerkarte "Manage Licenses" des Lizenzmanagers:



Mit einem Doppelklick auf die Zeile der Lizenz öffnet sich ein Fenster mit den Eigenschaften der Lizenz, u. a. der License ID:



Der OEM kann in seiner SPS-Applikation festlegen, wie auf das Vorhandensein bzw. Fehlen der OEM-Applikationslizenz reagiert werden soll. Möglich sind ein Programmabbruch oder auch das Freischalten eines Zusatzfeatures.

Systemvoraussetzungen

Betriebssystem:

- Um alle Funktionen zum Schutz der Anwendungssoftware nutzen zu können, ist mindestens Windows 7 (bzw. dessen Embedded-Version) erforderlich. Windows XP und Windows CE (Windows Embedded Compact) unterstützen weder die Verschlüsselung der Boot-Datei noch OEM-Lizenzen.

TC3 PLC Lib Tc2_Utiltities:

- Verwenden Sie mindestens Version 3.3.24 der TC3 PLC Lib Tc2_Utilities, da sie diverse Funktionen zum komfortablen Handling von TwinCAT-3-Lizenzen bietet. Sie ist zwingend erforderlich für die Nutzung von TwinCAT-3-Dongles für OEM-Applikationslizenzen. Die TC3 PLC Lib ist ab TwinCAT 3.1 Build 4022.16 enthalten.

TwinCAT-Version:

- Die beschriebenen Funktionalitäten erfordern mindestens TwinCAT 3.1 Build 4024.

Sicherer Schutz nur bei Verwendung der neuesten TwinCAT-3-Version

Verwenden Sie für einen sicheren Schutz (z. B. eine sichere Verschlüsselung) immer die neueste TwinCAT-3-Version. Diese bietet die höchste Sicherheit.

Verwenden Sie mindestens TwinCAT 3.1 Build 4024.x.
Verwenden Sie aus Sicherheitsgründen keine ältere Version!

Siehe auch: Dokumentation zur PLC-Bibliothek Tc2_Utilities , Abschnitt Lizenzierungsfunktionen

8.4 OEM SPS-Libraries mit einem Lizenzschutz versehen

OEM-Lizenz immer mit FB_CheckLicense abfragen!

Die unten beschriebene Methode kann als Ergänzung zur Abfrage mit FB_CheckLicense eingesetzt werden (nicht als alternative Methode).

Die Abfrage des Lizenzstatus muss immer mit FB_CheckLicense [▶ 93] erfolgen, da nur so die Ermittlung eines sicheren aktuellen Lizenzstatus möglich ist.

Dieser Lizenzcheck mit FB_CheckLicense ist völlig ausreichend; es ist nicht erforderlich (und wird daher auch nicht empfohlen), die License GUID zusätzlich in den Properties der selbst erstellten Library einzutragen.

Mit dem Eintrag der License GUID zusätzlich in den Properties der selbst erstellten Library ist der TwinCAT 3 Runtime bekannt, dass diese Lizenz für das Projekt erforderlich ist, und es erfolgt beim Start der Runtime eine **erste** Überprüfung dieser Lizenz.

Dieser erste Check erfolgt sehr früh in der Aufstartphase der TwinCAT Runtime. Der EtherCAT-Bus wird z. B. erst später im Aufstartprozess in Betrieb genommen; das Vorhandensein einer EL6070 Lizenzklemme kann also erst danach verifiziert werden.

Es ist daher sehr wichtig, in jedem Fall einen Lizenzcheck mit FB_CheckLicense durchzuführen, **nachdem** das komplette System aufgestartet (und somit der EtherCAT-Bus in Betrieb) ist.

Der Status aller Lizenzen wird von der TwinCAT Runtime (nach dem Aufstart) im laufenden Betrieb ca. **alle zwei Minuten** überprüft. Das sollte im PLC-Programm entsprechend berücksichtigt werden (also z. B. kein Aufruf von FB_CheckLicense in jedem SPS-Zyklus).

9 Anwendung gegen Klonen schützen

Siehe Eigene OEM-Lizenzen ausstellen und nutzen [▶ 84]

10 Support und Service

Beckhoff und seine weltweiten Partnerfirmen bieten einen umfassenden Support und Service, der eine schnelle und kompetente Unterstützung bei allen Fragen zu Beckhoff Produkten und Systemlösungen zur Verfügung stellt.

Downloadfinder

Unser Downloadfinder beinhaltet alle Dateien, die wir Ihnen zum Herunterladen anbieten. Sie finden dort Applikationsberichte, technische Dokumentationen, technische Zeichnungen, Konfigurationsdateien und vieles mehr.

Die Downloads sind in verschiedenen Formaten erhältlich.

Beckhoff Niederlassungen und Vertretungen

Wenden Sie sich bitte an Ihre Beckhoff Niederlassung oder Ihre Vertretung für den lokalen Support und Service zu Beckhoff Produkten!

Die Adressen der weltweiten Beckhoff Niederlassungen und Vertretungen entnehmen Sie bitte unserer Internetseite: www.beckhoff.com

Dort finden Sie auch weitere Dokumentationen zu Beckhoff Komponenten.

Beckhoff Support

Der Support bietet Ihnen einen umfangreichen technischen Support, der Sie nicht nur bei dem Einsatz einzelner Beckhoff Produkte, sondern auch bei weiteren umfassenden Dienstleistungen unterstützt:

- Support
- Planung, Programmierung und Inbetriebnahme komplexer Automatisierungssysteme
- umfangreiches Schulungsprogramm für Beckhoff Systemkomponenten

Hotline:	+49 5246 963-157
E-Mail:	support@beckhoff.com

Beckhoff Service

Das Beckhoff Service-Center unterstützt Sie rund um den After-Sales-Service:

- Vor-Ort-Service
- Reparaturservice
- Ersatzteilservice
- Hotline-Service

Hotline:	+49 5246 963-460
E-Mail:	service@beckhoff.com

Beckhoff Unternehmenszentrale

Beckhoff Automation GmbH & Co. KG

Hülshorstweg 20
33415 Verl
Deutschland

Telefon:	+49 5246 963-0
E-Mail:	info@beckhoff.com
Internet:	www.beckhoff.com

Trademark statements

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered trademarks of and licensed by Beckhoff Automation GmbH.

Third-party trademark statements

Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

Mehr Informationen:
www.beckhoff.com/te1000

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Deutschland
Telefon: +49 5246 9630
info@beckhoff.com
www.beckhoff.com