SSL/TLS/HTTPS

Sichere Kommunikation zwischen Komponenten

Version 5.12

Handbuch

	Dokument: Handbuch- SSL/TLS/HTTPS Sichere Kommunikation zwischen Komponenten
	Freigabedatum: 03.05.2023
	Dokumentversion: 1.1
	Autor: FORCAM GmbH

FB_8-41 ERSTELLT AM: 03.05.23 GEÄNDERT AM: 03.05.2023 VERSION: V1
FREIGEGEBEN DURCH: HEAD OF TTE AUTOR: TECHNICAL WRITER VERTRAULICHKEITSSTUFE: ÖFFENTLICH

Inhaltsverzeichnis

1 Über dieses Handbuch

Dieses Handbuch beschreibt die Voraussetzungen und die Konfiguration für die SSL-Verschlüsselung der Kommunikation in und mit FORCE MES FLEX (vorher FORCE IIoT, im Folgenden nur noch MES FLEX genannt) sowie die Erstellung bzw. Bereitstellung der dafür notwendigen Zertifikate.

⚠ Dieses Handbuch basiert auf der Version 5.12.14. Die genannten Funktionen stehen möglicherweise in früheren IIoT-Versionen nicht zur Verfügung.

ⓘ Aus Gründen der besseren Lesbarkeit wird im Text verallgemeinernd das generische Maskulinum verwendet. Diese Formulierungen umfassen jedoch gleichermaßen alle Geschlechter und sprechen alle gleichberechtigt an.

1.1 Zielgruppe und Vorkenntnisse

Das Handbuch setzt Kenntnisse im Umgang mit FORCAM FORCE IIOT voraus.-Sollten Sie dazu keine oder wenige Kenntnisse haben, nehmen Sie sich die Zeit, sich mit den Grundlagen vertraut zu machen.

ⓘ Wir empfehlen Ihnen die Nutzung unserer Academy: **https://forcam.com/academie/**
Die FORCAM Academy bietet das Wissen zum effektiven Einsatz der Methoden für die digitale Transformation und der Technologien für die Smart Factory.
Unser Institutsteam begleitet Sie auf Basis von Lean Manufacturing und TPM-Methoden, Veränderungen im Unternehmen einzuleiten und die Technologien richtig einzusetzen.

2 Sichere Netzwerkkommunikation

Damit die einzelnen Funktionen und Komponenten der MES FLEX genutzt werden können, müssen die Komponenten sowohl untereinander als auch mit externen Anwendungen im Unternehmensnetzwerkes kommunizieren. Ohne entsprechende Absicherung kann die gesamte über ein Computernetzwerk gesendete Kommunikation abgefangen, gelesen oder geändert werden.
Zum Sicherstellen der Kommunikation innerhalb eines Netzwerkes empfiehlt sich die Verwendung des SSL-Protokolls.

ⓘ TLS steht für Transport Layer Security und ist das Nachfolgeprotokoll von SSL. Beide sind Verschlüsselungsprotokolle für die Transportschicht des Internets.

2.1 Kommunikation über SSL/TLS

SSL (Secure Socket Layer) und TLS (Transport Layer Security) sind branchenübliche Standard-Sicherheitstechnologien, die zum Einrichten einer verschlüsselten Verbindung zwischen einem Webserver und einem Webclient (z. B. einem Webbrowser) verwendet werden. Es sind Verschlüsselungsprotokolle für die Transportschicht des Internets. Sie sorgen für eine sichere Netzwerkkommunikation, indem der Server authentifiziert und dadurch Privatsphäre und Integrität aller übertragenen Daten sichergestellt werden.

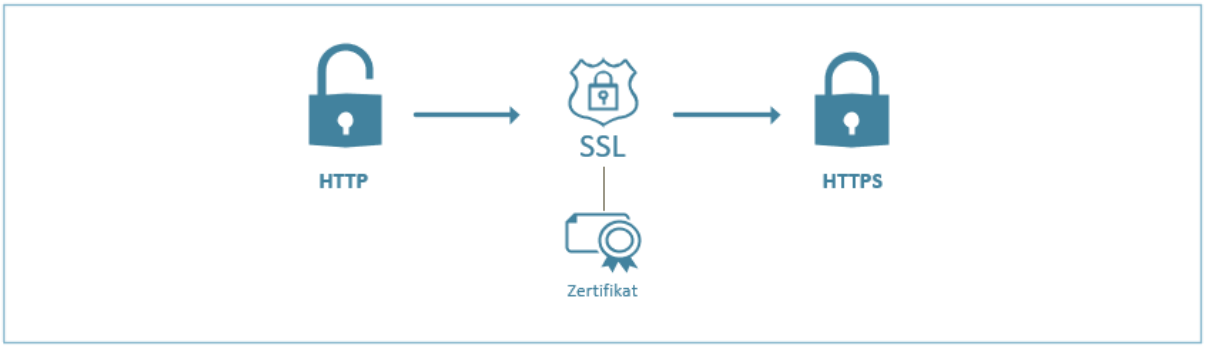

Bild 1: Übersicht – Verschlüsselung über SSL

Wenn die Kommunikation über diese verschlüsselte Transportschicht erfolgt, wird an den Protokollnamen ein „s“ angehängt: Aus http wird https, aus imap wird imaps usw.
Wenn eine Website über https kommunizieren will (wie die allermeisten Internetseiten heutzutage), ist ein sogenanntes SSL-Zertifikat erforderlich.

2.2 Zertifikate

Um eine SSL/TLS-Verbindung zwischen einem Webserver und einem Client zu erstellen, benötigt der Webserver ein Zertifikat. Das ist eine digitale Datei, die Informationen zur Identität des Webservers enthält. Sie enthält außerdem die Verschlüsselungstechnik, die verwendet wird, wenn ein sicherer Kanal zwischen dem Webserver und dem Client hergestellt wird. Ein Zertifikat muss vom Besitzer der Website (Domäne) erstellt und digital signiert werden.

Je nach Vertrauenswürdigkeit werden drei verschiedene Typen von Zertifikaten unterschieden, die in den folgenden Kapiteln näher beschrieben werden:

- **CA-signierte Zertifikate**
  Diese besitzen die größte Vertrauenswürdigkeit, da diese durch unabhängige Stelle nachgewiesen wurde.
- **Selbstsignierte Zertifikate innerhalb der eigenen Domäne**
  Dabei agiert ein Windows-Server als Stammzertifizierungsstelle (CA).
- **Selbstsignierte Zertifikate**
  Diese können vom Benutzer selbst erstellt werden und sind nur für Testzwecke zu verwenden.

ⓘ Kapitel 2.2.4 enthält eine Übersicht über die verschiedenen Zertifikatstypen und die empfohlenen Einsatzbereiche für die MES FLEX.

2.2.1 CA-signierte Zertifikate

ⓘ Allgemeine FORCAM-Empfehlung für Produktivsysteme. Unbedingt notwendig für Web-Kommunikation über das Internet.

Ein SSL-Zertifikat kann außer durch den Besitzer der Website auch durch eine **unabhängige Zertifizierungsstelle** (Independent Certificate Authority, CA) signiert werden. Eine CA ist ein vertrauenswürdiger Drittanbieter, der die Authentizität einer Website bestätigt. Wenn eine Website vertrauenswürdig ist, fügt die CA dem selbstsignierten SSL-Zertifikat dieser Website eine eigene **digitale Signatur** hinzu. Auf diese Weise wird Webclients garantiert, dass die Identität der Website überprüft wurde.
Beim Verwenden eines SSL-Zertifikats, das von einer bekannten CA ausgestellt wurde, findet die sichere Kommunikation zwischen dem Server und dem Webclient automatisch statt. Im Webbrowser wird keine Warnmeldung angezeigt, da die Website durch die CA überprüft wurde.

Für Produktionssysteme sollten immer diese von einer Zertifizierungsstelle signierten Zertifikate verwendet werden, insbesondere dann, wenn Benutzer außerhalb der Organisation mit den Browser-Clients auf den MES FLEX-Server zugreifen. Wenn der Server sich beispielsweise nicht hinter einer Firewall befindet und über das Internet aufgerufen werden kann, garantiert die Verwendung eines CA-signierten Zertifikats den Clients außerhalb der Organisation, dass die Identität der Website von einer unabhängigen Stelle überprüft wurde.

2.2.2 Selbstsignierte Zertifikate in einer Domäne

ⓘ Empfehlung FORCAM innerhalb der eigenen Domäne

Innerhalb einer Windows-Domäne kann auf einem Windows-Server eine Rolle **Active Directory-Zertifikatdienste (AD CS)** als Enterprise Stammzertifizierungsstelle (CA) installiert werden.
Dadurch kann auf dem Server ein Stammzertifikat erstellt werden, **welches für die gesamte Domäne valide ist**.

Dieses Stammzertifikat kann anschließend auch an die einzelnen Clients innerhalb derselben Domäne ausgerollt werden.

Ein selbstsigniertes Zertifikat, welches unter Einsatz des Stammzertifikats erstellt wurde, gilt somit für die Verbindung der Clients zum Server innerhalb der eigenen Domäne (MES FLEX-Systems) als vertrauenswürdig.

2.2.3 Selbstsignierte Zertifikate

⚠ **Keine FORCAM-Empfehlung: Nicht in produktiven FORCE IIOT/MES FLEX Systemen einsetzen.**

Ein selbstsigniertes Zertifikat ist ein SSL-Zertifikat, das nur vom Besitzer der Website signiert wurde. Selbstsignierte Zertifikate werden gelegentlich in Websites verwendet, die nur Benutzern im internen Netzwerk (LAN) der Organisation zur Verfügung stehen.

Wenn ein Webclient (z.B. ein Web-Browser) mit Hilfe eines selbstsignierten SSL-Zertifikats eine Verbindung zu einer Website herstellt, wird in einer Warnung angezeigt, dass die Website nicht als vertrauenswürdige Website verifiziert werden konnte. Informationen zum Unterdrücken von Warnungen von selbstsignierten Zertifikaten können abhängig vom Browser Typ eingestellt werden.

2.2.4 Übersicht: Zertifikate und Einsatzgebiete

Zertifikatstyp	Einsatzgebiet	Zentrale Merkmale
CA-Signiertes Zertifikat	Produktivsysteme mit und ohne Web-Kommunikation Unbedingt notwendig, wenn Force Clients über das Internet angebunden sind	– Die Vertrauenswürdigkeit wird durch CA-Zertifizierung nachgewiesen (Unabhängige vertrauenswürdige Organisation) – Keine Warnmeldung im Browser, automatisch sichere Kommunikation
Selbstsigniertes Zertifikat in der eigenen Domäne	Produktionssysteme, bei denen die Client-Server-Kommunikation nur innerhalb der eigenen Domäne stattfindet	– Vom eigenen Windows-Server erstellte Stammzertifikate gelten für die gesamte Domäne – Vertrauenswürdigkeit innerhalb des eigenen Netzwerks (MES-FLEX-Systems) garantiert
Selbstsignierte Zertifikate	Testsysteme	– -Netzwerkkommunikation (LAN) ausschließlich innerhalb der Organisation sichergestellt (nicht über das Internet)

2.3 Keystore

Ein Keystore ist ein Repository von Zertifikaten. Der Keystore enthält die Zertifikate, um eine sichere Datenübertrag mit TLS und Public-Key-Infrastructure (PKI) zu gewährleisten. Weiterhin werden dort das öffentliche Zertifikat des Services und der dazugehörige private Schlüssel hinterlegt. FFSetup übernimmt bei Neuinstallation bzw. Update der MES FLEX das Management der Zertifikate im Keystore (siehe Kapitel 4.1 und 4.2).

3 Voraussetzungen auf Kundenseite

3.1 Bereitstellung von Zertifikaten

ⓘ **Mitwirkungspflicht des Kunden**:

- Bereitstellung von Zertifikat(en) für MES FLEX
- Aktualisierung von Zertifikat(en) - valide Laufzeit

Die interne IT-Abteilung des Kunden muss ein gültiges Zertifikat für die MES FLEX zur Verfügung stellen. Sollte kein internes Knowhow vorhanden sein, kann ein externer Dienstleister mit der Bereitstellung beauftragt werden.

Folgende Anforderungen gelten an Zertifikate für die MES FLEX:

Allgemeine Anforderungen

Folgende allgemeine Anforderungen gelten bei der Zertifikatserstellung:

- Das SSL-Zertifikat wurde vom Besitzer der Website erstellt und digital signiert. Die signierende Zertifizierungsstelle (CA) muss von den MES-FLEX-Clients als vertrauenswürdig akzeptiert werden.
- Die verwendeten Hostnamen liegen in der Domaine des Kunden und sind DNS-auflösbar.
- Für jede MES-FLEX Instanz wird ein eigenes Zertifikat erstellt.

Technische Anforderungen

Das generierte Zertifikat muss folgende technische Anforderungen erfüllen:

Tabelle 2: Technische Anforderungen an das MES FLEX-Zertifikat

Hostname (DNS)	Im Zertifikat ist der verwendete Hostname hinterlegt (d.h., Server, auf dem MES Flex installiert ist).
Subject Alternative Name (SAN)	„FQDN“ (Fully-Qualified-Domain Name) muss enthalten sein.
Laufzeit des Zertifikats	Jedes Zertifikat ist mit einem Ablaufdatum in der Zukunft (max. 1 Jahr) versehen.
Verwendungszweck	Das Zertifikat ist zum Einsatz für einen Webserver ausgelegt.
Mindestschlüssellänge	Für RSA = 2048 Bit Für ECDSA = 256 Bit
Hash-Algorithmus	SHA-256 oder neuer
Dateiformat	Dateiformat „PKCS #12“ und Dateiendung „pfx“ Die Zertifikatsdateien sollten im Format PKCS #12 vorliegen. Um Kompatibilitätsprobleme zu vermeiden, muss gemäß Systemanforderungen eine aktuelle Java 11-Version verwendet werden.
Passwort	Das Passwort für die Zertifikatsdateien muss FORCAM zur Verfügung gestellt werden.

4 Konfiguration

4.1 Neuinstallation (FFSetup)

Durch die Installation mit FFSetup wird die SSL/HTTPS Konfiguration für die Anwendung erstellt.

4.1.1 Port-Konfiguration

Für folgende Komponenten und Dienste werden bei der Installation in der Properties-Datei (common.properties) vorgegebene Ports eingetragen:

Standardkomponenten:

- Shopfloor Terminal (SFT)
- Workbench
- NewOffice

Zusätzliche Services:

- ffauth
- fferp
- ffwebservices

ⓣ **Beispiel**:
Für die Workbench wird ein „Private Port“ 15080 für das HTTP-Protokoll definiert und ein „Public Port 15443“ für das HTTPS-Protokoll.

Die vorgegebenen Ports sind die Standard-Konfiguration der MES FLEX.
Änderungen an den Standard-Einstellungen werden in der Datei “customized.properties” gespeichert (siehe Kap.4.3). Damit stehen die Einstellungen für FFSetup bei einem Update zur Verfügung.

⚠ Bei Änderungen an der Standardkonfiguration muss sichergestellt sein, dass die eingestellten Ports die gleichen Eigenschaften besitzen (siehe Screenshots zu den einzelnen Access-Typen unten).

Server Access Ports

Das folgende Bild zeigt die Ports der Dienste die erreichbar und offen sind.

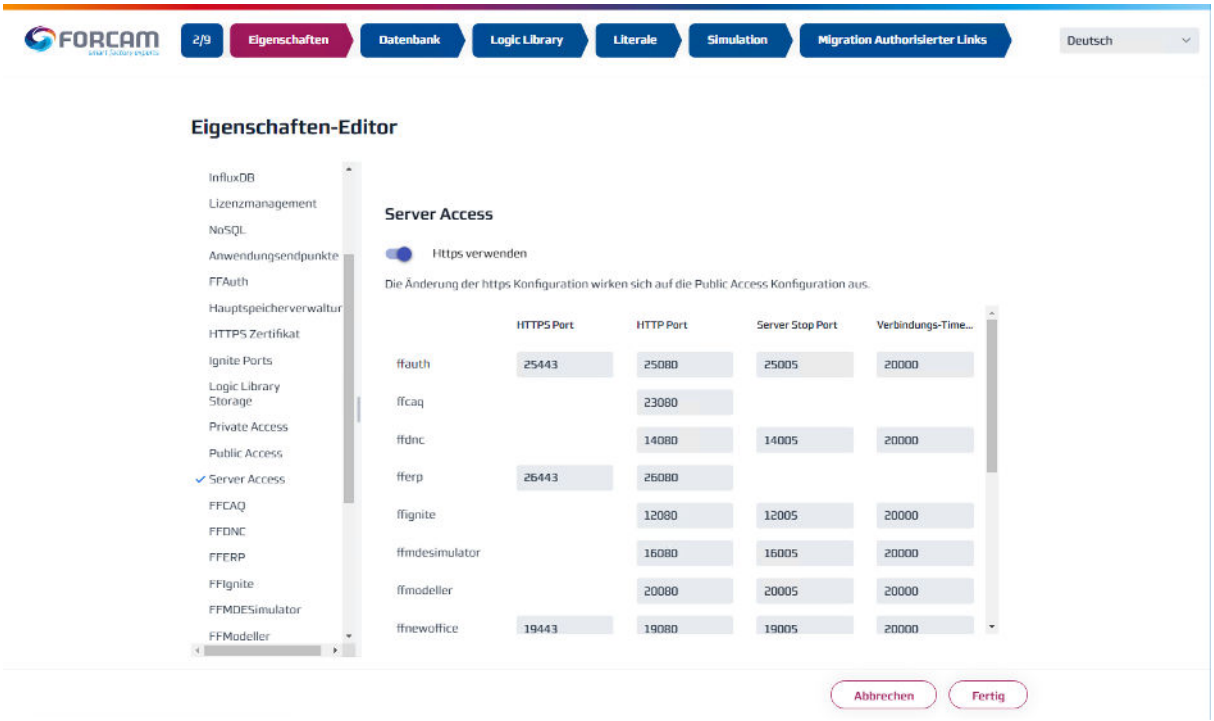

Bild 2: Server Access (Standard-Konfiguration für Tomcat)

Private Access Ports

Diese Ports dienen zur Kommunikation zwischen den Diensten.

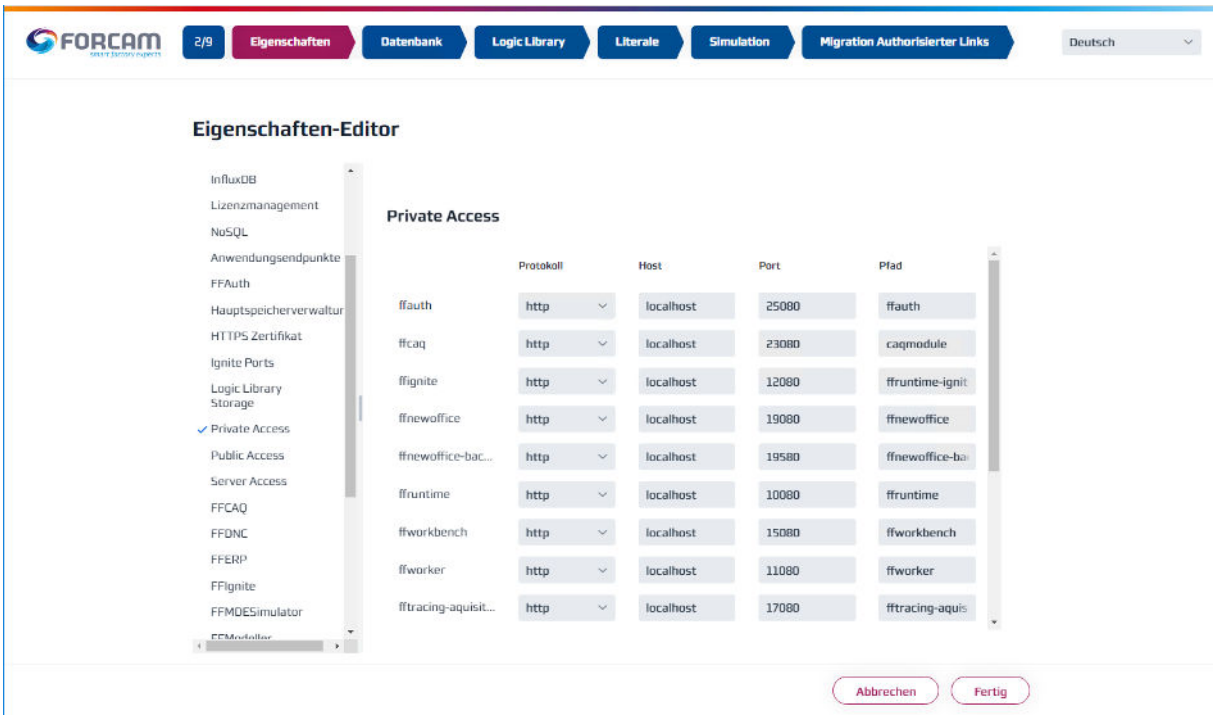

Bild 3: Private Access Ports (Standard-Konfiguration)

Public Access Ports

Diese Ports dienen zur Kommunikation der Clients (Workbench, New Office, SFT) mit dem Server.

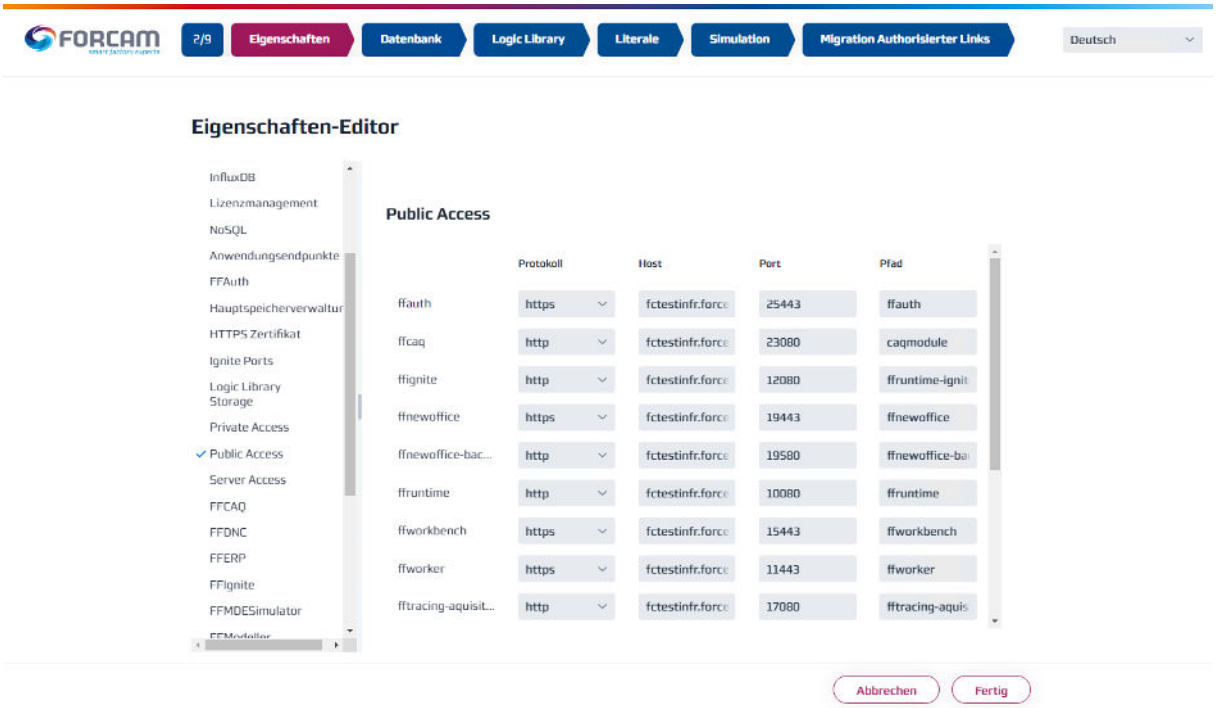

Bild 4: Private Access Ports (Standard-Konfiguration)

4.1.2 HTTPS-Zertifikat

Nach dem Starten von FFSetup kann im Eigenschaften-Editor die Seite **HTTPS-Zertifikat** aufgerufen werden.
Bei einer Neuinstallation kann entweder ein vorhandenes Zertifikat hochgeladen oder ein neues (selbstsigniertes) Zertifikat generiert werden.

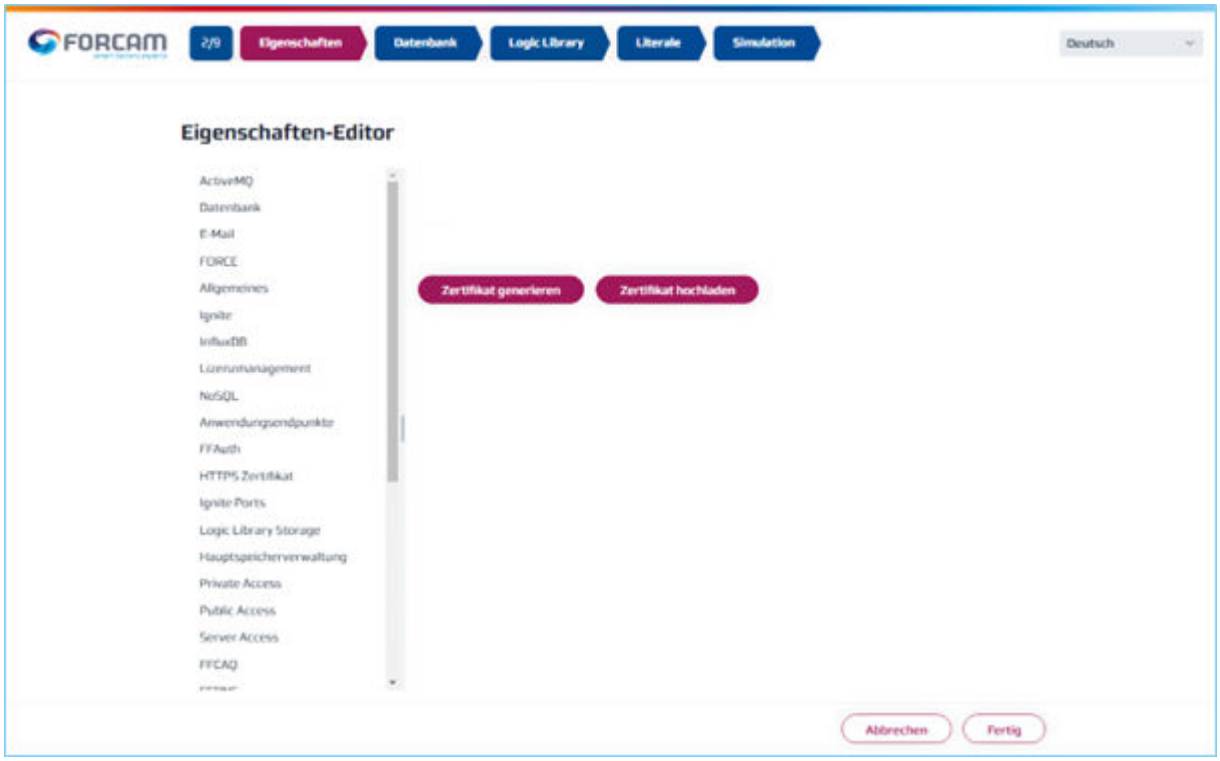

Bild 5: FFSetup: Zertifikat generieren oder hochladen

Zertifikat generieren

⚠ Nicht bei produktiven MES FLEX-Systemen einsetzen. Die Herkunft von selbstsignierten Zertifikaten wird nicht durch eine unabhängige Zertifizierungsstelle verifiziert (siehe Kapitel 2.2.3.Selbstsignierte Zertifikate

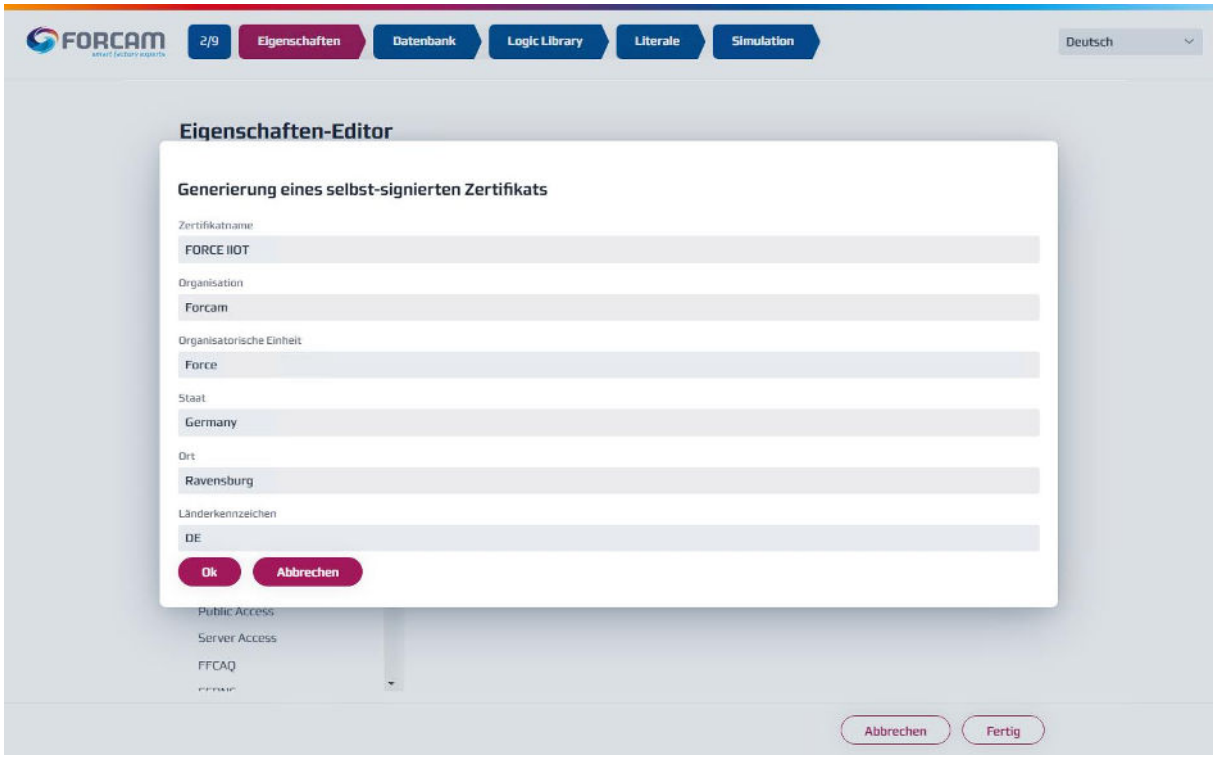

Bild 6: Selbstsigniertes Zertifikat generieren (Beispiel)

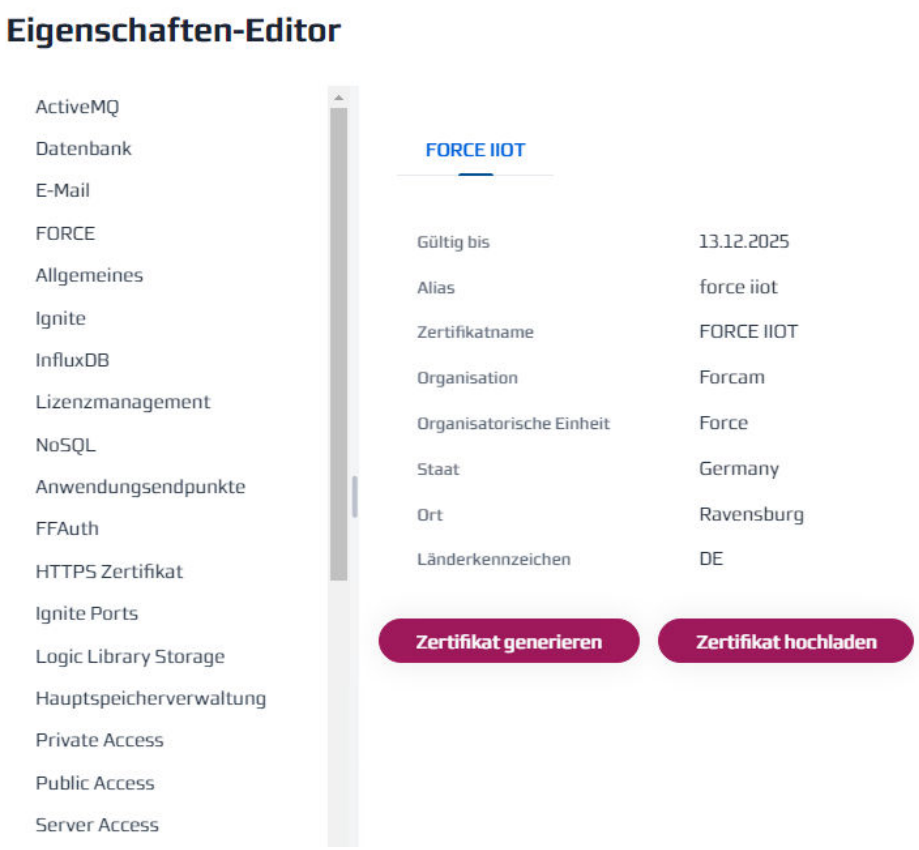

Bild 7: Generiertes Zertifikat (Beispiel)

Zertifikat hochladen

⚠ Der verwendete Hostname (Vollqualifizierter Domänenname/Full Qualified Domain Name) muss identisch mit dem Common Name (CN) beim Zertifikat sein. Siehe Kapitel 3.1 zu weiteren Bedingungen an das Zertifikat.

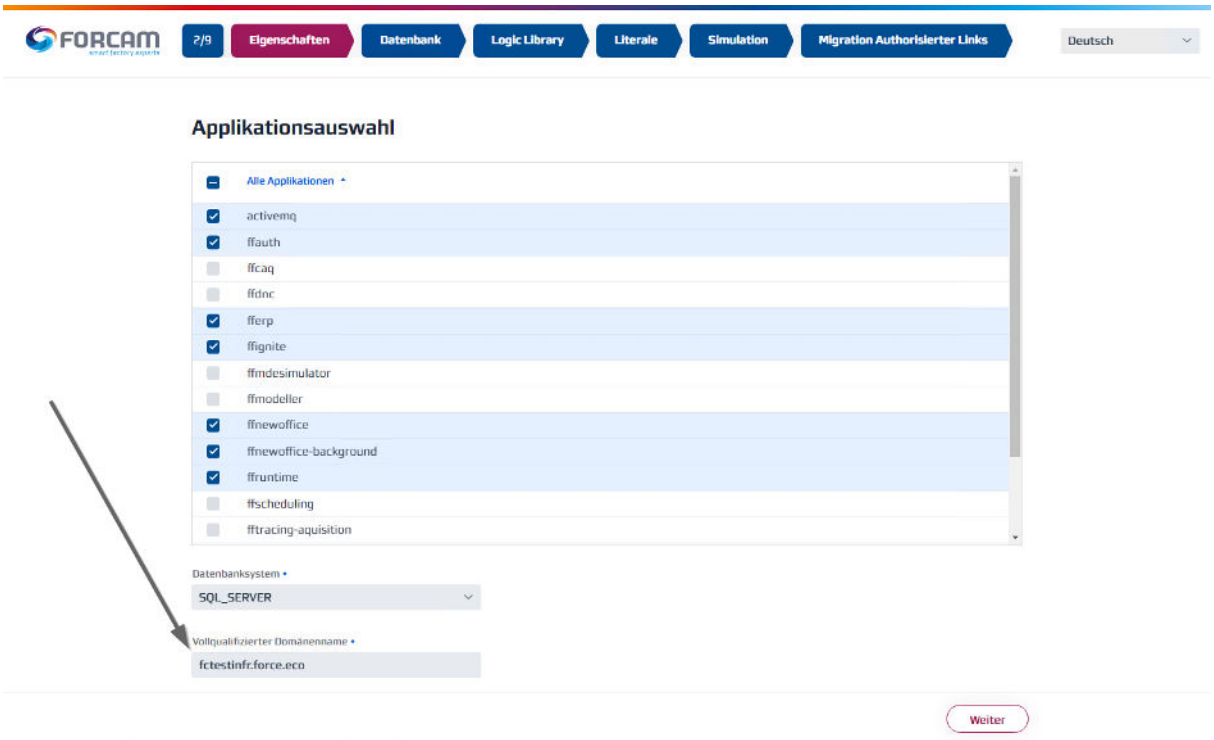

Bild 8: Vollqualifizierter Domänenname

Im Dialog kann das valide Zertifikat hochgeladen werden.

⚠ Anforderungen an Zertifikate der MES FLEX beachten (siehe Kap. 3.1).

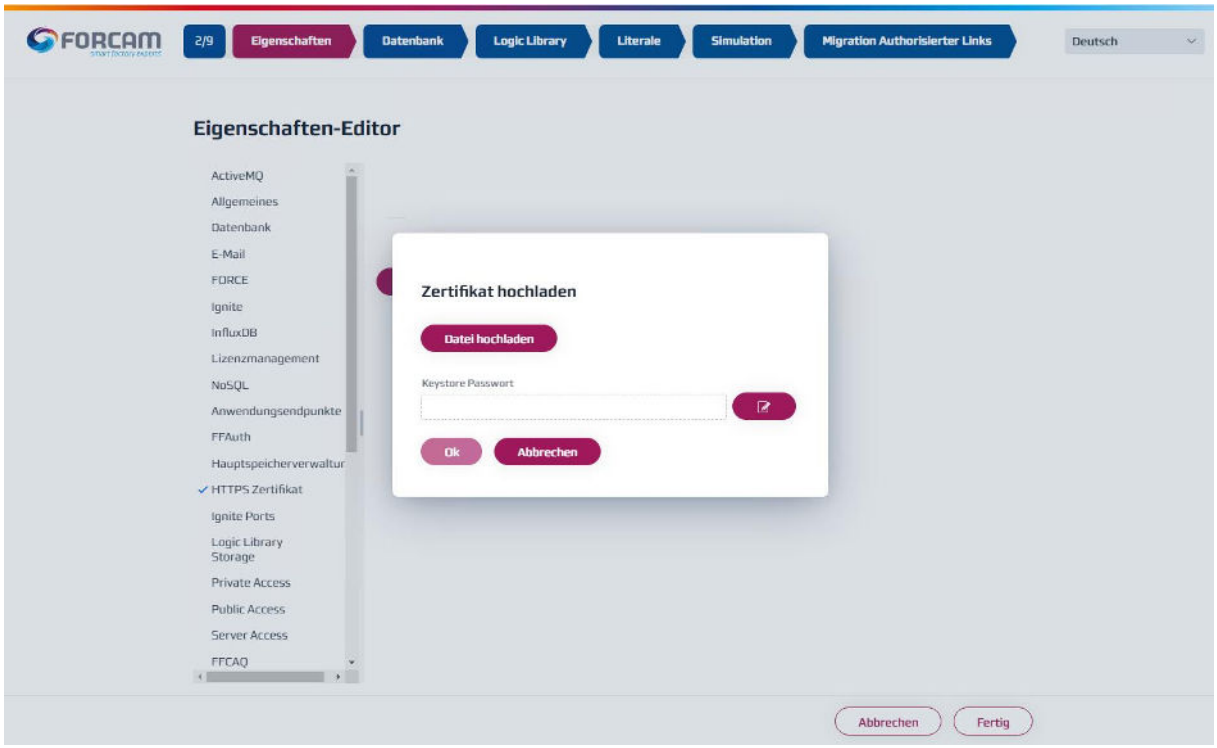

Bild 9: Zertifikat hochladen

Das hochgeladene Zertifikat wird im Eigenschaften-Editor angezeigt:

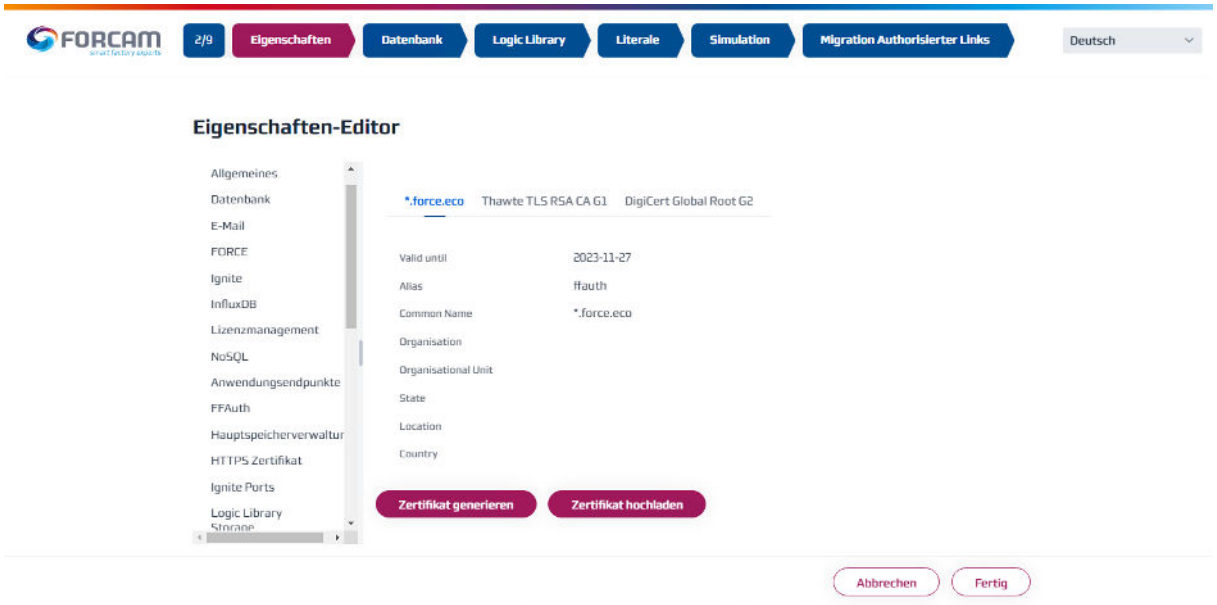

Bild 10: FFSetup: Vorhandende Zertifikate

4.2 Update mit FFSetup

Bei einem Update durch FFSetup wird das bestehende Zertifikat beibehalten:

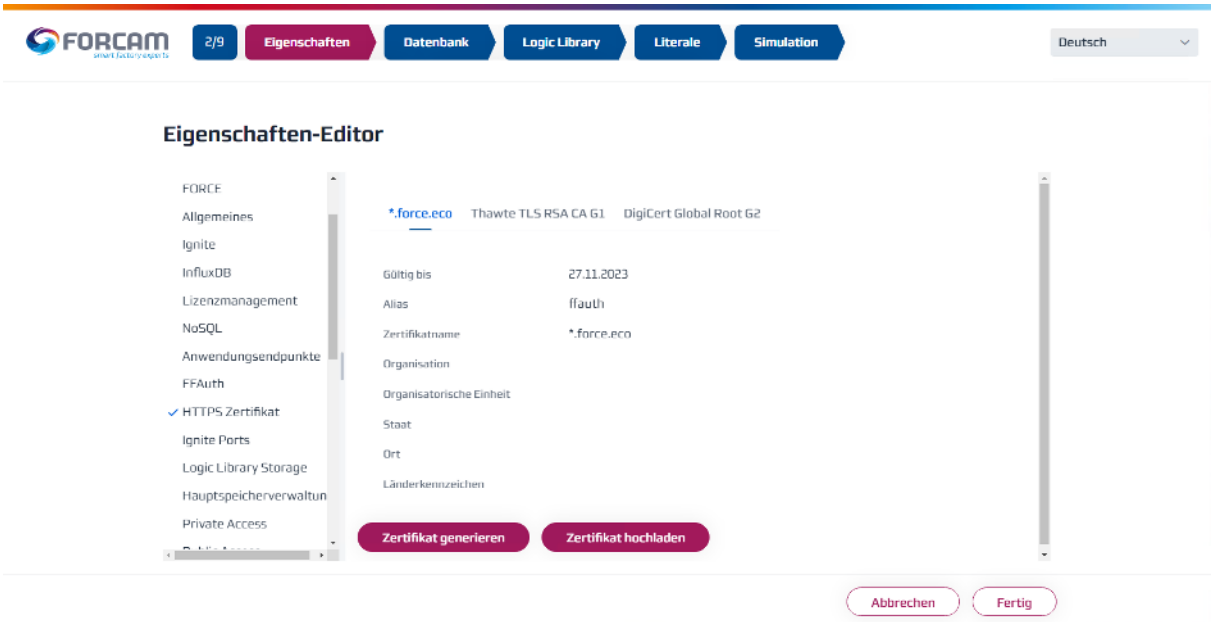

Bild 11: FFSetup Update: Aktuell verwendetes Zertifikat

ⓘ Änderungen an den Standard-Einstellungen werden in der Datei “customized.properties” gespeichert (siehe Kap.4.3). Damit stehen die Einstellungen für FFSetup bei einem Update zur Verfügung.

4.3 Verzeichnisse und Dateien

Folgende Verzeichnisse und Dateien sind für die SSL-Konfiguration relevant:

Inhalte/Datei	Pfad und Hinweise
Zertifikat	D:\ForcamForce\app\config\.keystore
Properties	D:\ForcamForce\app\config
Common Properties	D:\ForcamForce\app\config\common.properties Beispiel (Auszug): *…* *#https* *https.enabled=true* *…* *#keystore* *keystore.password=FQNLul6Qk68h+htMlJbOXlLh1RYnA=* *keystore.path=E:\ForcamForce\app\config\.keystore* *…* *#ssl* *ssl.certificate=MIILbACCBagwggWkAgEAMIIFnQY……* *…* *#ffworkbench* *ffworkbench.private.host=localhost* *ffworkbench.private.path=ffworkbench* *ffworkbench.private.port=15080* *ffworkbench.private.protocol=http* *ffworkbench.public.host=SERVERNAME* *ffworkbench.public.path=ffworkbench* *ffworkbench.public.port=15443* *ffworkbench.public.protocol=https* …
Customized Properties	D:\ForcamForce\app\config\customized.properties Hier werden Änderungen an den Standard-Einstellungen gespeichert. Damit stehen die Einstellungen für FFSetup bei einem Update zur Verfügung. Beispiel (Auszug): *#common* *…* *common.keystore.password=9p424LmjSrwoOdERiVlHgYrvUuM=* *common.keystore.path=F:\ForcamForce\app\config\.keystore*
Konfiguration Tomcat	Die „server.xml“ werden bei der Installation generiert (Im Schritt „Application Installation)

	D:\ForcamForce\app\ffworkbench-tomcat\server.xml Beispiel (Auszug): *<!--- HTTPS connector -->* *<Connector port="15443"* *…* *sslProtocol="TLS"* *keystoreFile="E:\ForcamForce\app\config\.keystore"* *keystorePass="FQNLul6Qk682zx5iRmsMlJbOXlLh1RYnA="*

5 Einschränkungen bei der Verschlüsselung

Für folgende Dienste werden die Kommunikationsendpunkte in der MES FLEX nicht verschlüsselt:

- Message Broker (ActiveMQ)

6 Anhang

6.1 Dokument-Konventionen

Tabelle 3: Verwendete Schriftarten, Formatierungen und Zeichen

Konvention	Beschreibung
Fettschrift	Die Bezeichnungen von Schaltflächen und Optionen sind fettgeschrieben.
Kursivschrift	Hervorgehobene Wörter sind kursivgeschrieben.
Pfad	Jeder angegebene **Pfad** ist auf FORCE MES LITE bezogen. In Klammern ist das jeweilige Modul aufgeführt.
Werte/Mengen	Werte/ Mengen, die nicht näher spezifiziert sind (z.B. durch Zusätze wie Soll/Ist), beziehen sich auf erfasste Daten.
Icons	Bei einer Funktion, die über ein Icon dargestellt ist, wird auf das Icon als Objekt referiert.
Alternativer Handlungsschritt	Alternative Handlungsschritte sind durch Oder getrennt.
Unterschritte einer Handlung	Unterschritte einer Handlung sind eingerückt und tragen einheitliche Symbole pro Handlungsebene. Die Reihenfolge der Ebene ist: 1. a. i. 1. usw.
Handlungsresultat	Handlungsresultate sind durch ➔ gekennzeichnet.
Voraussetzungen	Voraussetzungen sind durch ✓ gekennzeichnet.
Warnungen	Warnungen sind durch ⚠ gekennzeichnet.
Hinweis	Hinweise sind durch ⓘ gekennzeichnet.
Tipps	Tipps sind durch ⓣ gekennzeichnet.

6.2 Abkürzungen und Begriffe

Tabelle 4: Abkürzungen und Begriffe

Abkürzung/Begriff	Beschreibung
SSL	Secure Socket Layer Verschlüsselungsprotokoll für die Transportschicht des Internets. Die Datenströme zwischen Client und Server werden verschlüsselt.
TLS	Transport Layer Security Verschlüsselungsprotokoll für die Transportschicht des Internets. Die Datenströme zwischen Client und Server werden verschlüsselt. TLS ist das Nachfolgeprotokoll von SSL.
SFT	Shopfloor Terminal
CA	Certificate Authority
Keystore	Repository von Zertifikaten

6.3 Abbildungsverzeichnis