AWS IoT Core Client SL

Die Bibliothek ‚AWS IoT Core Client SL' ermöglicht den Austausch von Nachrichten über den Amazon Service ‚AWS IoT Core'.

Produktbeschreibung

‚AWS IoT Core' ist eine verwaltende Cloud-Plattform von Amazon, mit der verbundene Geräte einfach und sicher mit Cloud-Anwendungen und anderen Geräten zusammenarbeiten können. Die Bibliothek ‚AWS IoT Core Client SL' stellt Funktionsbausteine zum Senden und Empfangen von Nachrichten zur Verfügung. Die Kommunikation erfolgt dabei verschlüsselt über das Protokoll MQTT. Nachrichten werden im AWS Umfeld typischerweise im JSON Format übertragen. Zum Parsen und Erzeugen von JSON Dateien kann die Bibliothek ‚JSON Utilities' verwendet werden.

Folgende Funktionsbausteine sind in er Bibliothek enthalten:

- `AWSIoTClient`: Funktionsbaustein zum Herstellen einer Verbindung zu ‚AWS IoT Core'
- `AWSIoTPublish`: Funktionsbaustein zum Veröffentlichen von Nachrichten (Publish)
- `AWSIoTSubscribe`: Funktionsbaustein zum Abbonieren eines Topics (Subscribe)
- `AWSIoTGetDeviceShadow`: Funktionsbaustein zum Lesen des ‚Device Shadows'
- `AWSIoTUpdateDeviceShadow`: Funktionsbaustein zum Aktualisieren von ‚Device Shadow' Daten
- `AWSIoTSubscribeDeviceShadow`: Funktionsbaustein zum Abonnieren von ‚Device Shadow' Änderungen

Unterstützte Funktionen

- Publish/Subscribe von Nachrichten auf Basis von MQTT V3.1.1
- TLS Verschlüsselung
- Authentifizierung via Clientzertifikat
- Unterstützung von ‚Qualitiy of Service': 0 und 1 (QoS0, QoS1)
- Datentyp Topics: `WSTRING`
- Maximale Größe eines Topics: 1024
- Die maximale Packetgröße und Payloadgröße ist über eine Parameterliste konfigurierbar
- Multitask- und Multicore-Unterstützung
- Unterstützung von ‚Last Will' Nachrichten (QoS0, QoS1)
- Unterstützung von Wildcards (# und +)

Bei der Installation wird das Beispielprojekt ‚AWS IoT Core Client SL Example.project' in das Zielverzeichnis installiert. Die Applikation `AWSDeviceShadow` demonstriert das Schreiben und Lesen des ‚Device Shadows'. Die Applikation `AWSPubSub` zeigt wie Nachrichten über die enthaltenen Funktionsbausteine veröffentlicht und abonniert werden können. Die Applikation `AWS_JSON_DeviceSchadow` zeigt die Updatemöglichkeit des ‚Device Shadows' mit Hilfe des JSONBuilders.

Die MQTT-Parameter können durch Hinzufügen der Bibliothek ‚MQTT Client SL' auf Toplevel im Library Manager geändert werden.

Installation eines Clientzertifikates

Die Authentifizierung eines Gerätes bei AWS IoT Core erfolgt über Clientzertifikate. Das Clientzertifikat kann über die ‚AWS Management Console' via Certificate Signing Request (CSR) erzeugt und heruntergeladen werden. Das Zertifikat kann anschließend auf dem entsprechenden Gerät installiert werden.

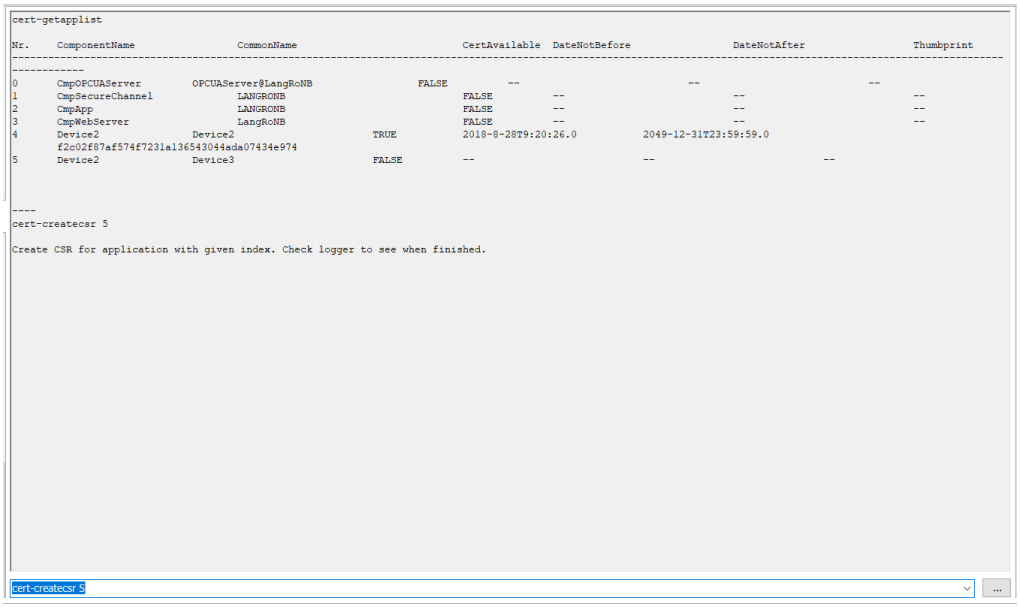
Zur Durchführung der weiteren Schritte muss das CODESYS Package ‚CODESYS Security Agent' und ‚OpenSSL' auf dem PC installiert werden.

Download Links:

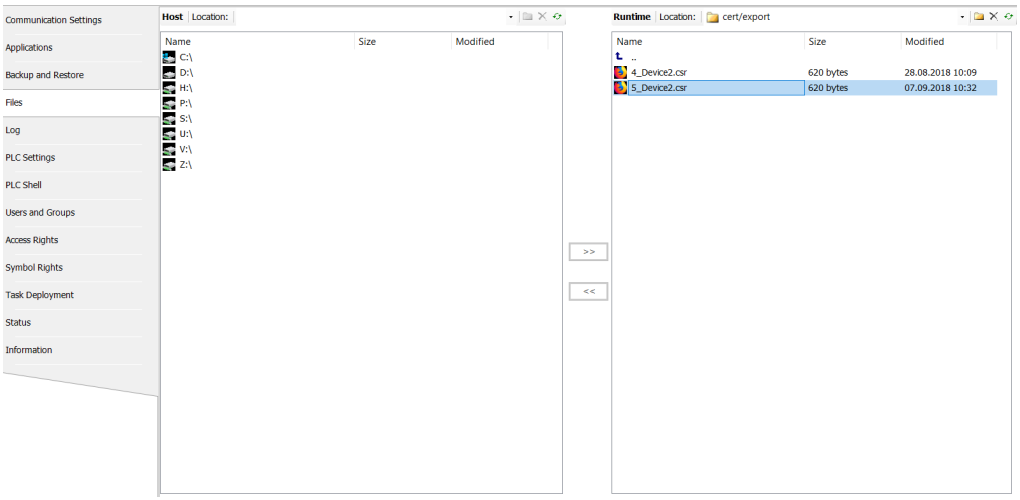
- CODESYS Security Agent: https://store.codesys.com/codesys-security-agent.html
- OpenSSL: https://www.openssl.org

Schritte zum Erstellen und Importieren eines Clientzertifikates:

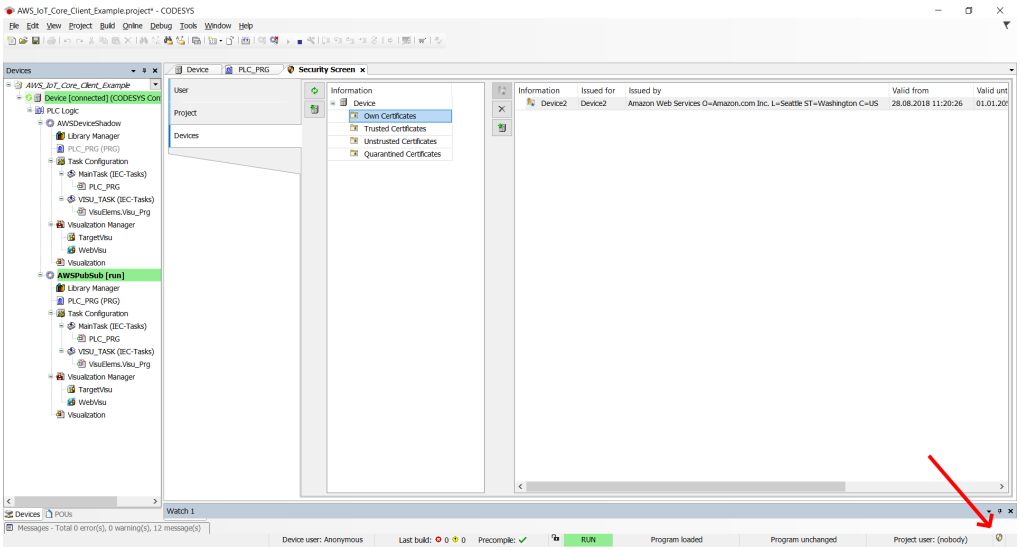
1. Gerät in ‚AWS IoT Core' anlegen, siehe https://docs.aws.amazon.com/iot/latest/developerguide/register-device.html
2. Beispielprojekt, Applikation `AWSPubSub` öffnen
3. Endpoint auf den Eingang `AWSIoTClient.sHostname` setzen (z.B. xxxxxxxxxxxxxx.iot.yyyyyyyy.amazonaws.com)
4. Gerätenamen (Name of thing) auf den Eingang `AWSIoTClient.sClient` setzen. Der Eingang `AWSIoTClient.sCertCNPrefix` sollte verwendet werden, wenn die ClientId mit dem Hostnamen identisch ist. Dies verhindert das Laden eines falschen Zertifikats (z.B. vom WebServer). Beispiel: `sCertCNPrefix := 'AWSClient'`, `sClientId := 'MyHostname'` => Der Common Name (CN) des Zertifikats lautet AWSClient@MyHostname
5. Projekt downloaden und starten
6. PLC Shell öffnen (Device -> PLC Shell)
7. `cert-getapplist` eingeben -> Es wird eine Komponente mit dem angegebenen Gerätenamen und einer `Nummer` angezeigt.
8. `cert-createcsr <Nummer>` eingeben, `Nummer` von Schritt 7 verwenden. Das Erzeugen der CSR Datei kann einige Sekunden dauern, im Device Log (Device -> Log) wird nach dem Generieren eine entsprechende Meldung ausgegeben.



1. (Device -> Files) öffnen, CSR-Datei vom Verzeichnis `cert/export` auf das lokale Filesystem kopieren



1. Momentan wird das Format der exportierten CSR Datei noch nicht von AWS unterstützt. Bis das Problem behoben ist muss die Datei via OpenSSL konvertiert werden. Zum Konvertieren des Formats folgenden Befehl ausführen:
   `openssl.exe req -in YOUR.csr -inform der -out YOUR.csr`
2. Mit der Datei `YOUR.crt` kann jetzt über die AWS Management Console (‚Create with CSR') ein Zertifikat erzeugt werden. (siehe: https://docs.aws.amazon.com/iot/latest/developerguide/create-device-certificate.html)
3. Zertifikat und Root-Zertifikat herunterladen
4. Security Screen -> Devices, Zertifikat unter ‚Own Certificats' installieren, Root-Zertifikat unter ‚Trusted Certificates' installieren



1. Menu: Online -> Reset Cold, Projekt starten
2. Ausgang `AWSIoTClient.xConnectedToBroker` sollte auf TRUE stehen -> Verbindung wurde hergestellt

Allgemeine Informationen

Lieferant:

CODESYS GmbH
Memminger Straße 151
87439 Kempten
Deutschland

Support:

Technischer Support ist bei diesem Produkt nicht enthalten. Um technischen Support zu erhalten, erwerben Sie bitte ein CODESYS Support Ticket.

https://support.codesys.com

Artikelname:

AWS IoT Core Client SL

Artikelnummer:

Vertrieb/Bezugsquelle:

CODESYS Store
https://store.codesys.com

Lieferumfang:

CODESYS Package

Systemvoraussetzungen und Einschränkungen

Programmiersystem	CODESYS Development System V3.5.15.0 oder höher
Laufzeitsystem	CODESYS Control V3.5.15.0 oder höher
Unterstützte Plattformen/ Geräte	Hinweis: Verwenden Sie das Projekt ‚Device Reader', um die von der Steuerung unterstützten Funktionen zu ermitteln. ‚Device Reader' ist kostenlos im CODESYS Store erhältlich.
Zusätzliche Anforderungen	AWS Account (AWS IoT Core)
Einschränkungen	-
Lizenzierung	Lizenzaktivierung optional auf dem CODESYS Key oder dem Soft Key (Soft Key: kostenloser Bestandteil der CODESYS Controls) Die Lizenzierung über Soft Key ist strikt an eine Hardware gebunden. Hinweis: Ohne Lizenz läuft die Software 30 Minuten im Demo-Modus.
Erforderliches Zubehör	-

Bitte beachten Sie: Technische Änderungen, Druckfehler und Irrtümer vorbehalten. Es gilt der Inhalt der aktuellen Online-Version dieses Dokuments.

Erstellungsdatum: 21.08.2023