FULL-STACK IOT PORTFOLIO
SICHERHEITSARCHITEKTUR

Kurzfassung

Das Full-Stack-Angebot von Q-loud enthält eine umfassende Sicherheitsarchitektur. Sie ist Bestandteil jeder Q-loud IoT-Lösung und wirkt nach dem Defense-in-Depth-Prinzip gleich an mehreren Stellen. Die IoT-Plattform selbst wird als verteilte Architektur in drei geografisch getrennten Rechenzentren der Stufe Tier 3+ redundant und ausfallsicher betrieben. Alle Module, Sensoren und Aktoren von Q-loud verfügen über eine Verschlüsselung auf Microcontrollere-bene. Mit 868 MHz Funk übertragen die Geräte ihre Daten mit dem Q-loud Sensorprotokoll an das Q-loud Gateway. Dieses prüft auf der einen Seite die Sensordaten auf ihre Richtigkeit und baut auf der anderen Seite einen https Tunnel zur Q-loud IoT-Plattform auf. Erst dort werden die Datenpakete jedes einzelnen Sensors oder Aktors individuell geprüft, entschlüsselt und verarbeitet.
Diese Komplettlösung bietet größtmögliche Sicherheit in der Vernetzung von Geräten und bietet bei Hardwareintegration, Datenübertragung, IoT-Plattform, sowie Hard- und Softwarekom-ponenten wirksame Sicherheitsmechanismen. Kunden der Q-loud realisieren so Security-by-Design-Lösungen ohne selbst eigenes Know-How aufbauen zu müssen. Im Ergebnis heißt das höchste Sicherheit bei innovativen Produkten ohne Kompromisse in der Time-to-Market.

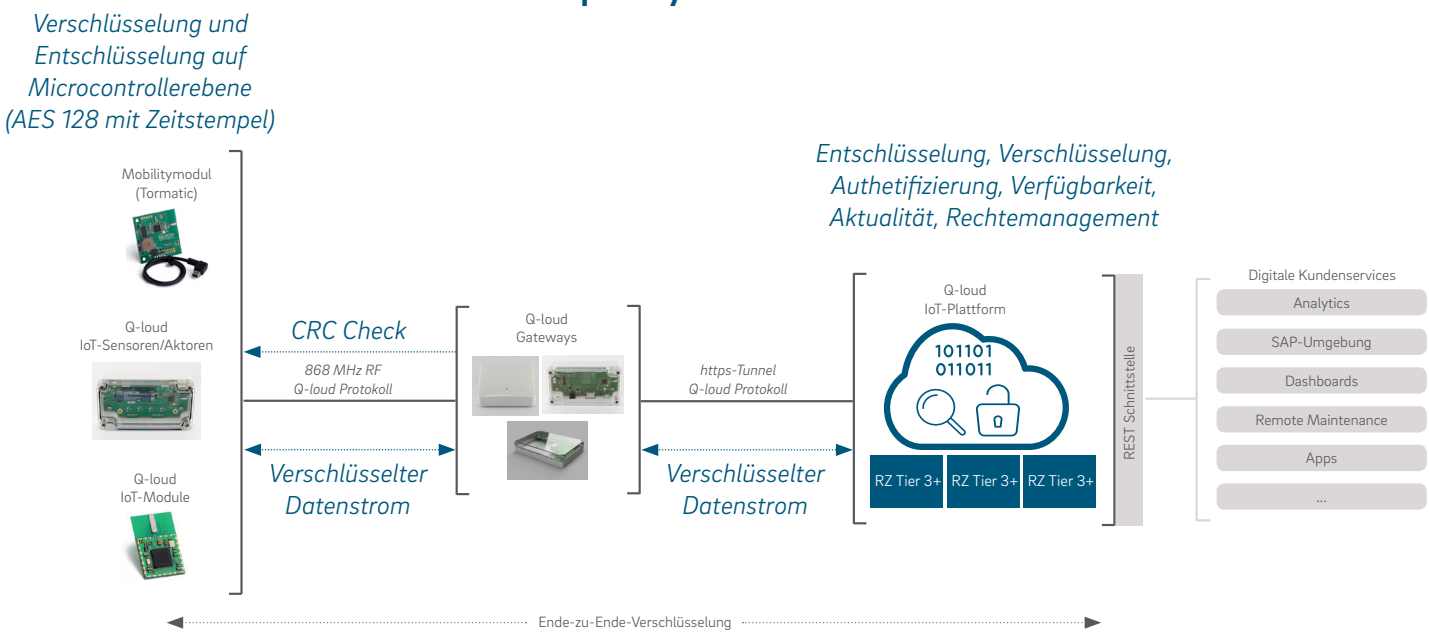
Sicherheitsziele.

Vertraulichkeit

Sowohl Sensordaten als auch Schaltbefehle an Aktoren werden grundsätzlich verschlüsselt übertragen und so das Mitlesen von Sensor-Daten und das einschleusen unbefugter Schaltbefehle verhindert. Hierzu verwendet Q-loud die Blockchiffre AES mit einer Schlüssellänge von 128 Bit. Dabei sind die notwendigen Schlüssel für jeden Sensor individuell, sodass im unwahrscheinlichen Falle eines erfolgreichen Angriffs nur ein einzelner Sensor und nicht das gesamte Ecosystem kompromittiert wird. Die Schlüssel werden zudem bei der Produktion der Sensoren und Aktoren auf Micro-controllerebene vorinstalliert. So entfällt die Einrichtung durch den Benutzer und die damit verbundenen Risiken einer Fehlbedienung oder bewussten Preisgabe des Schlüssels.

Um die Menge an verschlüsselten Daten mit Hilfe eines einzigen Schlüssels so gering wie möglich zu halten, werden die vorinstallier-ten Schlüssel nicht zur eigentlichen Verschlüsselung der Nutzdaten verwendet sondern in spezifizierten zeitlichen Abständen neue Schlüssel generiert. Dies erhöht zudem die Sicherheit: Sollte ein Angreifer in den Besitz eines Schlüssels gelangen, ist dieser nur eine kurze Zeit gültig.

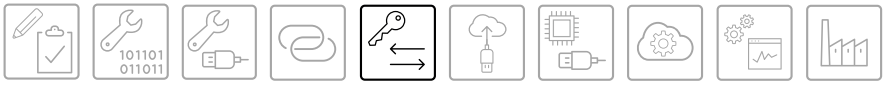
Defense-in-Depth-Systemarchitektur der Q-loud



Kontakt:
hello@qsc.de
0221-669 84 11
www.q-loud.de

Q-loud
Ein Unternehmen der QSC AG

FULL-STACK IOT PORTFOLIO
SICHERHEITSARCHITEKTUR



Authentizität
Fehlerhaft übertragene oder von unbefugten Dritten erzeugte Daten werden vom System erkannt und verworfen. So wird sichergestellt, dass keine manipulierten Sensor-Daten ins System eingeschleust werden können.

Hierzu wird zwischen Sensor und Q-loud Gateway zunächst ein CRC-Check durchgeführt, um Übertragungsfehler zu erkennen. Ist der CRC-Check negativ, sendet der Sensor das Datenpaket erneut.

Darüber hinaus schreibt das Q-loud Sensorprotokoll ein Auffüllen des letzten AES-Blocks mit Null-Bytes vor, sodass dieses Padding auf der IoT-Plattform geprüft und so die Authentizität der Daten bestätigt werden kann. Das Einschleusen von gefälschten Sensor-Daten, ist somit nahezu ausgeschlossen.

Aktualität
Bei sogenannten Replay-Attacken werden bereits übertragene Sensor- oder Aktordaten ein zweites Mal in das System eingebracht. Um dies auszuschließen, ist ein Zeitstempel fester Bestandteil der Daten-Pakete, die mit dem Q-loud Protokoll übertragen werden. Um diese Zeitinformation kryptografisch an jedes Daten-Paket zu binden ist der Zeitstempel fester Bestandteil der AES Verschlüsselung. Daher setzt das Q-loud Protokoll AES im sogenannten Counter Mode ein. Dadurch ist es Angreifern nahezu unmöglich einmal aufgezeichnete Sensor-Daten unter einem anderen Zeitstempel ins System einzuschleusen.

Ein weiterer positiver Nebeneffekt des AES-CTR Modes: Jedes verschlüsselt übertragene Nutzdatum sieht anders aus, sodass es Angreifern nicht möglich ist unveränderte Daten wieder zu erkennen und so zu interpretieren.

Verfügbarkeit
Jeder Service wird an seiner Verfügbarkeitsrate gemessen. Der redundante Aufbau der Q-loud IoT-Plattform als Cloud-Service garantiert höchste Verfügbarkeit unabhängig von der anliegenden Last. Denn die verteilte Architektur bewirkt zum einen, dass Daten von Sensoren und Aktoren jederzeit zuverlässig übertragen werden und zum anderen, dass selbst bei Komplettausfall eines Rechenzentrums der Service ohne negative Auswirkungen zur Verfügung steht.

Weitere Sicherheitsaspekte

Autorisierung und Rechtemanagement
Aufbauend auf den gesicherten Kommunikationsmöglichkeiten des Q-loud Protokolls, bietet die Plattform ein fein granulares User-Management-System, dass es den Besitzern von Sensoren und Aktoren erlaubt, Zugriffsrechte für Dritte zu definieren. Somit können sowohl Leserechte für bestimmte Sensoren als auch Schreibrechte für ausgewählte Aktoren erteilt und entzogen werden.

Sicheres Ansteuern von Aktoren
Neben der sicheren Übertragung von Sensor-Daten wurde das Q-loud Protokoll auch für das sichere Ansteuern von Aktoren konzipiert. So dient die Verschlüsselung jeglicher Kommunikation auch der Geheimhaltung aller Aktor-Kommandos. Angreifern ist es somit nicht möglich die eigentlichen Steuer-Kommandos mitzulesen. Auch das Wiedererkennen von Kommandos ist aufgrund des eingesetzten AES-CTR Modes nicht möglich.

Kontakt:
hello@qsc.de
0221-669 84 11
www.q-loud.de

Q-loud
Ein Unternehmen der QSC AG