Cellular IoT Security Whitepaper

Marvin Schirrmacher, Cellular IoT Security Consultant
März, 2021

Inhaltsverzeichnis

Einführung

grandcentrix entwickelt als Internet of Things Solution Provider Ende-zu-Ende Lösungen, mit denen Hersteller ihre Produkte vernetzen können. Dabei kommt vermehrt Mobilfunk zum Einsatz, der es Produktherstellern ermöglicht, ihre Geräte autark und ohne lokale Gateway-Infrastrukturen (wie WLAN-Router) ins Internet der Dinge zu bringen. Vor allem LPWAN-Technologien (Low Power Wide Area Network) wie Narrowband IoT oder LTE-M eignen sich für das Internet der Dinge.

Dies ermöglicht die Erschließung neuer (digitaler) Geschäftsmodelle, Kostenreduktion, Optimierung von Serviceprozessen und dem häufig erstmals direkten Kontakt zu Endkunden. Klassische Anwendungsfälle sind das Erfassen und Nutzbarmachen von Telemetriedaten sowie die Anpassung von Konfigurationswerten aus der Ferne.

Um den Eintritt in die Welt *cellular connected devices* leicht und kostengünstig zu gestalten, hat grandcentrix mit *Narrowband+* ein speziell auf die Bedürfnisse per Mobilfunk vernetzter IoT-Geräte angepasstes Service-Offering als Teil des *Cellular IoT* Portfolios entwickelt.

Dieses Dokument beschreibt die Sicherheitsarchitektur von *Cellular IoT* und *Narrowband+*. Es wird verdeutlicht, wie grandcentrix Sicherheitskonzepte einsetzt, um Kunden und ihre Produkte über die oft jahrelangen Lebenszyklen zu schützen. Bei diesen Sicherheitskonzepten handelt es sich sowohl um technische Lösungen als auch um organisatorische Prozesse und Vorgaben.

Kurzbeschreibung Cellular IoT

Die *Cellular IoT*-Familie stellt alle Komponenten bereit, die von Produktherstellern für die Verbindung zwischen Produkt und IT-Infrastruktur (z.B. Microsoft Azure) benötigt werden:

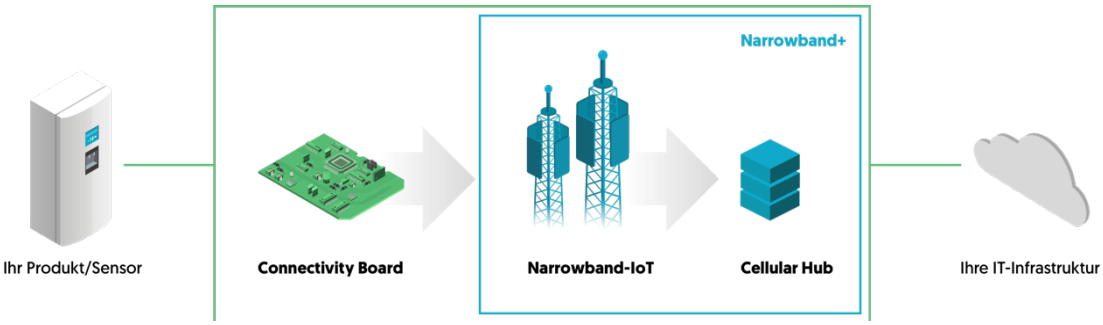

Abb. 1: Architekturskizze Cellular IoT

In das Produkt selbst wird ein *Connectivity Board* eingebaut und bildet somit eine Einheit mit dem eigentlichen Gerät. Es ist verantwortlich für die Kommunikation zwischen Sensoren und Aktoren des Geräts auf der einen und der Cloud auf der anderen Seite. Für volle Flexibilität nutzen wir einen erprobten und zertifizierten Hardware Blueprint als Basis des Connectivity Boards. Dieses beinhaltet ein Modem sowie eine industrielle SIM-Karte, mit deren Hilfe eine Verbindung in das Mobilfunknetz aufgebaut wird, um Daten in beide Richtungen zu übertragen. Hierfür kommt der SiP (System in Package) Nordic Semiconductor nRF9160 zum Einsatz, für welches grandcentrix ein SDK zur Verfügung stellt, um wiederkehrende Aufgaben in der Firmware-Entwicklung standardisiert durchführen zu können.

Unser Connectivity Board ist CE-zertifiziert und damit für den Einsatz in Europa zugelassen. Es ist möglich, aufbauend auf dem Blueprint ein eigenes Connectivity Board auf die eigenen Bedürfnisse (Firmware, Formfaktor, Hardware-Anschlüsse, etc.) anzupassen.

Die Übertragung der Daten erfolgt mittels Narrowband-IoT. NB-IoT ist ein von der 3GPP beschriebener Standard in Mobilfunknetzen. Da dieser Standard speziell auf eine effiziente Energiebilanz und hohe Verfügbarkeit ausgerichtet ist, kommt als Transportprotokoll UDP zum Einsatz. Bei der Vernetzung mit den gängigsten Cloud Service Providern wird hingegen oft nur TCP für die Registrierung und Kommunikation verwendet, so dass zur Anbindung von Geräten an die Cloud Services eine Protokollkonvertierung erforderlich ist.

Damit Geräte zuverlässig direkt mit der gewünschten Plattform in der Cloud kommunizieren können, übernimmt *Cellular Hub* diese Konvertierung. *Cellular Hub* ist ein von grandcentrix betriebener PaaS (Platform-as-a-service) und nimmt die Daten direkt aus dem Vodafone-Mobilfunknetz entgegen, bereitet sie für die Weiterverwendung auf und leitet sie konvertiert in das gewünschte Zielsystem weiter. Die Anbindung unterschiedlicher Kundensysteme erfolgt über standardisierte Schnittstellen (z.B. Azure IoT Hub, MQTT Broker).

Neben der Protokollkonvertierung ermöglicht *Cellular Hub* Aufgaben wie Device Management, SIM Management, das Ausspielen von Firmware Updates und die Integration in Produktions-, Logistik- und Fulfillment-Prozesse. Eine Datenspeicherung findet nicht statt.

Bei *Narrowband+* handelt es sich um eine vollständige Connectivity-Lösung, welches die Benutzung von Narrowband-IoT und *Cellular Hub* in über 30 Ländern für 1 Cent pro Tag pro aktiviertem Gerät ermöglicht. *Connectivity Boards* sind nicht in *Narrowband+* enthalten und müssen separat bestellt werden.

Sicherheitsmodell

Grundlage für die Absicherung von *Cellular IoT* bildet ein Sicherheitsmodell. Unter dem Begriff Sicherheitsmodell versteht man einen Rahmen für die Entscheidungsfindung während der Entwicklung. Bevor ein Sicherheitsmodell erstellt werden kann, werden schützenswerte Assets definiert.

Assets

Für die Implementierung von Sicherheitskonzepten ist es wichtig schützenswerte Assets zu identifizieren. Als Assets werden materielle und immaterielle Güter oder auch nichtfunktionale Eigenschaften verschiedener Komponenten betrachtet. Wenn alle schützenswerten Assets definiert sind, wird im nächsten Schritt ein Sicherheitskonzept erstellt, um das Gefährdungspotential zu minimieren.

Für *Cellular IoT* stehen folgende Assets im Fokus:

Asset	**Beispiele**
Kundendaten	Zahlungsinformationen, Namen, Passwörter
Kundenprodukte	Smart Products, Industrieanlagen
Endverbraucher	Nutzer der Smart Products
Connectivity Boards	Geräteinformationen (z.B. Geräteschlüssel), sichere Kommunikation, ggf. Batterielaufzeit
Connectivity SIMs	Aktivierung, Verwaltung, Zuordnung zu Kunden
Cellular Hub	Erreichbarkeit, Integrität, sichere Kommunikation
Cellular Infrastruktur	Zugriffe auf Systemkomponenten (z.B. Datenbanken), Logs, Passwörter

Annahmen

Ein Sicherheitsmodell enthält Annahmen, die uns dabei helfen, sicherheitsrelevante Entscheidungen während der Entwicklung zu treffen. Wenn beispielsweise eine Systemkomponente als vertrauenswürdig eingestuft wird, müssen keine defensiven Maßnahmen implementiert werden, um das Vertrauensverhältnis zu korrigieren. Im Folgenden werden Annahmen getroffen, welche bei der Erstellung von Sicherheitskonzepten berücksichtigt werden.

Annahme: Vertrauen in unsere Cloud-Plattform
grandcentrix pflegt ein Vertrauensverhältnis zu der Cloud Plattform *Microsoft Azure*. Dennoch werden Sicherheitskonzepte für unsere Cloud-Infrastruktur erstellt. Es wird davon ausgegangen, dass Microsoft keine schädlichen Aktivitäten ausübt, die unser Produkt und unsere Kunden gefährden.

Annahme: Vertrauen in unsere Hardware-Hersteller
grandcentrix hat ein Vertrauensverhältnis zu seinen Hardware-Lieferanten. Die Erwartungen sind, dass die Integrität unserer Hardware-Komponenten gewährleistet ist. Wir gehen nicht davon aus, dass Hardware-Hersteller die Sicherheit unseres Produktes aktiv gefährden.

Annahme: Unbekannte LTE-Infrastruktur
LTE-Infrastrukturen sind hochgradig komplex, da sie zahlreiche Standards implementieren, die unterschiedliche Sicherheitsniveaus garantieren. Zudem sind auch Roaming Partner Bestandteil dieser Infrastrukturen. Dies bedeutet, dass grandcentrix nicht die volle Hoheit über alle Komponenten einer LTE-Infrastruktur hat. Somit muss sichergestellt werden, dass Mechanismen angewendet werden, welche die Kommunikation zwischen *Connectivity Boards* bzw. Hardware des Kunden und dem *Cellular Hub* vor unbekannten Faktoren schützen.

Annahme: Unbeschränkten Zugriff auf *Connectivity Boards* oder Hardware des Kunden
grandcentrix akzeptiert das Risiko, dass *Connectivity Boards* und die Hardware eines Kunden in den Besitz unberechtigter Dritter (z.B. durch Diebstahl) gelangen. grandcentrix akzeptiert auch, dass ein potentieller Angreifer vollen Zugriff auf die Operationen und das Dateisystem eines IoT-Gerätes erlangen kann. Es wird angenommen, dass Angreifer

- Reverse Engineering von Software und Hardware betreiben,
- Software und Hardware modifizieren,
- die Kommunikation eines IoT-Gerätes analysieren und manipulieren.

Dies zu verhindern würde bedeuten, während des gesamten Produktlebenszyklus keine Schwachstelle in jeglicher Software- und Hardwarekomponente des Gerätes zuzulassen. Das kann jedoch nicht gewährleistet werden. Somit müssen Mechanismen geschaffen werden, die Kunden sowie Infrastruktur auch dann schützen, wenn ein Angreifer vollen Zugriffes auf ein einzelnes IoT-Gerät erhält.

Annahme: Potentielle Angreifer
Die *European Union Agency for Cybersecurity (ENISA)* hat verschiedene Gruppen von Angreifern definiert (ETL 2017). Angreifer können eine Bedrohung für unsere Kunden und unsere Plattform darstellen. Abhängig von der Gruppierung eines Angreifers, werden verschiedene Sicherheitskonzepte erarbeitet. Sicherheitsmechanismen gegen gezielte Angriffe staatlicher Akteure müssen anders gestaltet sein als breit angelegte Attacken sogenannter “Script Kiddies”.

Folgende Angreifer-Gruppen sieht grandcentrix als potentielle Bedrohung für Cellular IoT an:

Angreifer Gruppe	Mögliche Ziele
Endbenutzer	Informationen, Unterhaltung
Researcher	Informationen, Publicity
Hacker	Schaden, Unterhaltung
Insider (z.B. ehemalige Mitarbeiter)	Informationen, Rache
Cyber-Kriminelle	Finanzielle Bereicherung
Konkurrenten	Informationen, Wettbewerbsvorteile

Annahme: Produktlebenszeit von *Connectivity Boards*
grandcentrix nimmt an, dass *Connectivity Boards* eine Lebenszeit bis zu mehreren Jahrzehnten haben. Während dieser Zeit muss sichergestellt sein, dass potentielle Sicherheitslücken in der Software oder Firmware identifiziert und jederzeit behoben werden können.

Annahme: Vertrauen in uns
grandcentrix hat ein Vertrauensverhältnis zu seinen Kunden. grandcentrix trägt die Verantwortung dafür, dass

- Kundendaten geschützt sind,
- die Infrastruktur erreichbar und zuverlässig ist,
- kritische Operationen mit Sorgfalt durchgeführt werden.

Secure Software Development Life Cycle

Produkt-Teams bei grandcentrix arbeiten nach dem *Secure Software Development Life Cycle*. Hier werden Security Spezialisten bereits während der Planung einer Software- oder Hardwarekomponente integriert. In jedem Entwicklungsschritt finden verschiedene Aktivitäten statt, die eine sichere Entwicklung gewährleisten. Das ermöglicht, alle Anforderungen der **ISO 27001**, **IEC 62443** und **VDE Smart Home** zu erfüllen.

Requirements	Design	Implementation	Verification & Release	Maintenance
Thread Analysis	Security Concepts	Security Consulting	Code Reviews	Security Audit & Research
Definition of Done	Role Definitions	Improvements	Security Tests	Security Radar
Security Label			Final Approval	Patch Management

Requirements

Noch vor der Entwicklung einer Software- oder Hardwarekomponente entscheiden Security-Experten, ob die jeweilige Komponente als sicherheitskritisch eingestuft wird. Wenn dies der Fall ist, werden potentielle Bedrohungen analysiert und Möglichkeiten zur Absicherung einer Komponente evaluiert. Außerdem wird eine *Definition of Done* für die Komponente festgelegt, welche nach der Entwicklung verifiziert wird. Jedes Entwicklungspaket wird mit einem Security Label versehen. Mit Hilfe von Security Labels wird entschieden, welche Aktivitäten für die *Verification* vollzogen werden. Es kommen fünf verschiedene Security Labels zum Einsatz, welche die Kritikalität und den Einfluss eines Entwicklungspakets widerspiegeln.

Security Score	⚪	🟢	🟡	🟠	🔴
Beschreibung	Sicherheit nicht kontrollierbar	Keine Relevanz für Sicherheit	Potenzielle Relevanz für Sicherheit	Relevanz für Sicherheit	Hohe Relevanz für Sicherheit
Beispiel	Einsatz unbekannter Software eines Kunden	Änderung der Dokumentation	Verbesserung bestehender Software-Tests	Konfiguration eines Ingress Controllers	Implementierung der Authentifizierung von Kunden
Aktivitäten	Keine	Keine	Optional	Code Reviews	Code Reviews, Security Testing

Design

Nachdem eine Komponente analysiert wurde, erarbeiten Security-Experten konkrete Sicherheitskonzepte. Je nach Anwendungsfall werden Sicherheitskonzepte mit unterschiedlichen Sicherheitsniveaus erstellt. Für die Entwicklung wird ein Sicherheitskonzept ausgewählt, das sich mit unserem Sicherheitsmodell und unserer Organisationsstruktur am besten vereinen lässt. Gegebenenfalls müssen Rollen definiert werden, um ein Sicherheitskonzept zu realisieren. Beispielsweise kann festgelegt werden, welche Person Zugriff auf bestimmte Passwörter hat oder wem es gestattet, ist eine Firmware zu signieren.

Implementation

Während der Entwicklung einer Software- oder Hardwarekomponente stehen Security-Experten den Entwicklerteams zur Seite und helfen, Unklarheiten oder Problemen zu lösen. In diesem Schritt können auch Änderungen an einem Sicherheitskonzept vollzogen werden. Es kommt vor, dass Sicherheitskonzepte aufgrund technischer Gegebenheiten nicht vollständig abgebildet werden können. Beispielsweise kann ein ausgewählter Algorithmus zur Verschlüsselung nicht für die gegebene Hardware geeignet sein, da dieser zu viel Speicherplatz allokiert. Diese Art von Erkenntnissen fließen in die Entwicklung ein und werden zur Anpassung von Konzepten genutzt.

Verification & Release

Dieser Schritt ist für die Validierung der Security Requirements. Die wichtigsten Aktivitäten sind hier Code Reviews und Security Tests durch Security-Experten. Mit Hilfe von Code Reviews werden Implementierungsfehler oder Konfigurationsfehler von Komponenten aufgedeckt. Security Tests werden mit verschiedenen Tools und Skripten ausgeführt, um die Sicherheitsattribute einer Komponente zu validieren. Gefundene Sicherheitslücken werden dokumentiert und behoben. Wenn die Verification erfolgreich ist, wird die Komponente zum Release freigegeben.

Maintenance

Die Security-Experten von grandcentrix führen regelmäßige Security Audits für die Absicherung unserer Infrastruktur durch. Hierfür wird evaluiert, welche Personen Zugriff auf unsere Cloud Umgebung haben und wie Systemkomponenten geschützt sind. Außerdem wird die eingesetzte Software nach Sicherheitslücken gescannt. Wenn Sicherheitslücken gefunden werden, werden diese mit Hilfe von Patch Management-Prozessen behoben. Wenn Schwachstellen mit großem Einfluss aufgedeckt werden, werden diese bis zur Behebung unter Beobachtung gestellt. Hierfür pflegen wir eine Liste mit bekannten Schwachstellen – der sogenannte *Security Radar*.

Kommunikation

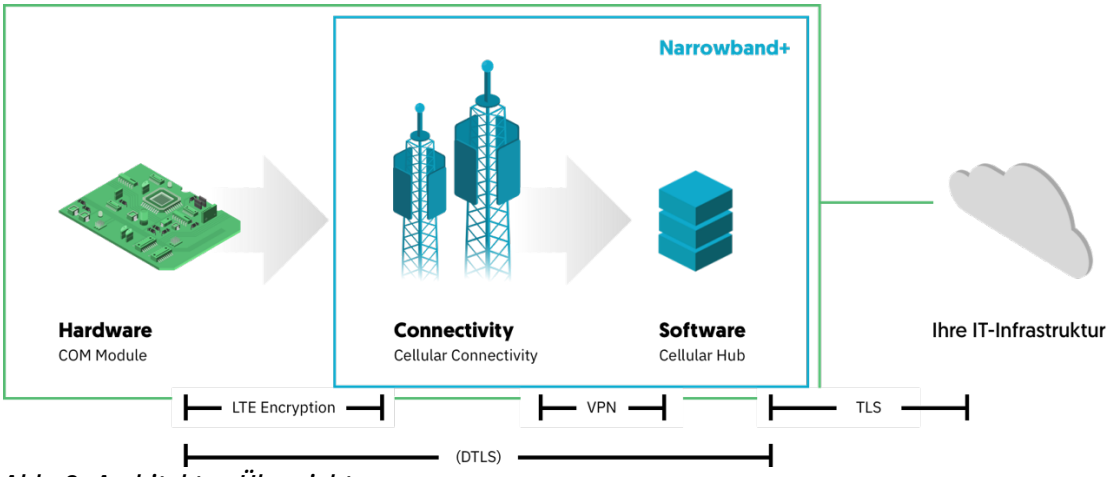

Abb. 2: Architektur-Übersicht

Connectivity Boards und IoT-Geräte unserer Kunden werden mit einer eingebetteten MFF2 SIM ausgestattet. Die SIM ermöglicht IoT-Geräten Zugang zu Vodafones globalen Narrowband-IoT- und LTE-M-Netzwerken. IoT-Geräte können nicht untereinander kommunizieren. Dies wird durch Vodafones LTE-Infrastruktur verhindert. Folglich können auch keine kompromittierten Geräte eine Verbindung zu anderen Geräten aufnehmen.

Die Kommunikation der IoT-Geräte wird über Funkmasten (*eNodeB*) an die *Vodafone Global M2M Platform* übertragen. Anschließend werden Nachrichten über ein Gateway (dem sogenannten Access Point) an *Cellular Hub* übertragen. Nachrichten werden mit dem IPSec Protokoll v3 verschlüsselt. *Cellular Hub* kann lediglich Nachrichten von IoT-Geräten unserer Kunden empfangen oder an diese senden. Vodafone verhindert, dass unbekannte IoT-Geräte eine Verbindung über Narrowband-IoT oder LTE-M mit dem *Cellular Hub* aufbauen können.

DTLS und TLS

Die Kommunikation zwischen *Connectivity Boards* und damit der Hardware eines Kunden und dem *Cellular Hub* ist durch Sicherheitsmechanismen verschiedener LTE-Spezifikationen und dem IPSec v3 Protokoll geschützt. Dennoch haben sich die Security-Experten von grandcentrix dafür entschieden, eine weitere Sicherheitsebene zu integrieren. Jegliche Kommunikation zwischen *Connectivity Boards* und dem *Cellular Hub* kann optional über das *DTLS 1.2 Protokoll* abgesichert werden.

DTLS ist eine Variante des weit verbreiteten TLS Protokolls, welches für sogenannte *Constrained Devices* optimiert wurde. Durch die Nutzung von DTLS über das UDP-Protokoll verbrauchen unsere Connectivity Boards weniger Energie und Rechenleistung.

DTLS bietet folgende Sicherheitsattribute:

- **Verschlüsselung**: Nachrichten sind verschlüsselt und können von keiner Instanz innerhalb der LTE-Infrastruktur eingesehen werden. Die Verschlüsselung ist für die geringe Rechenleistung der Connectivity Boards optimiert. Mit der Cipher Suite

ECDHE ECDSA with AES 128 GCM SHA256 basierend auf der elliptischen Kurve *secp256r1* kommen performante Algorithmen zum Einsatz.

- **Integritätsschutz**: Nachrichten können von keiner Instanz innerhalb der LTE-Infrastruktur manipuliert werden. Die Manipulation einer Nachricht wird von Connectivity Boards und dem Cellular Hub erkannt und die jeweilige Nachricht verworfen.
- **Schutz vor Replay Attacken**: Nachrichten können von keiner Instanz innerhalb der LTE-Infrastruktur aufgezeichnet und erneut versendet werden. Eine erneute Zustellung einer Nachricht wird von *Connectivity Boards* und *Cellular Hub* erkannt und verworfen.
- **Schutz vor DDos-Attacken**: DTLS verhindert IP Spoofing-Angriffe, indem Kommunikationspartner beweisen müssen, dass ihnen eine bestimmte IP-Adresse zugeordnet wurde. Dadurch können Angreifer keine Nachrichten an *Cellular Hub* mit gefälschten IP-Adressen senden. Somit wird verhindert, dass *Cellular Hub* auf Nachrichten reagiert, die gefälschte IP-Adressen enthalten. Würde *Cellular Hub* auf jede dieser Nachrichten antworten, könnte dieser durch eine Flut von Nachrichten lahmgelegt werden (vor allem wenn aufwändige Rechenoperationen angestoßen werden).
- **Identifizierung der Geräte**: Geräte lassen sich mit Hilfe von Zertifikaten (basierend auf *x509 v3*) eindeutig von *Cellular Hub* identifizieren. Bevor die Kommunikation zwischen *Connectivity Board* und *Cellular Hub* initiiert wird, findet ein *DTLS Handshake* statt. Wenn ein Zertifikat unbekannt oder gefälscht ist, wird die Anfrage abgelehnt. Zertifikate enthalten eine Hardware-Referenz auf ein *Connectivity Board*. Dadurch können Angreifer bei vollem Zugriff auf ein Gerät keine Nachrichten im Namen anderer Geräte senden. Der private Schlüssel eines *Connectivity Boards* ist auch grandcentrix unbekannt. Für die Erstellung der Zertifikate wurde eine eigene *Public-Key-Infrastruktur (PKI)* aufgesetzt. Die PKI wird bereits bei der Herstellung der *Connectivity Boards* eingesetzt, um Zertifikate als Vertrauensanker auf einem Gerät zu integrieren. Zertifikate werden in einem sicheren Speicher des Gerätes abgelegt. Das dazugehörige Schlüsselmaterial wird nur von einer sicheren Ausführungseinheit, der *Arm Trustzone*, behandelt.

Jegliche Kommunikation zwischen Cellular Hub und Kundensystemen wird durch das TLS Protokoll abgesichert. Je nach Kommunikationskanal wird hierfür TLS 1.2 oder TLS 1.3 verwendet. Diese Protokolle gewährleisten ähnliche Attribute wie die von DTLS.

Cellular Hub

Cellular Hub ist die Schnittstelle zwischen IoT-Geräten und der IT-Infrastruktur unserer Kunden. *Cellular Hub* stellt eine sicherheitskritische Komponente von *Cellular IoT* dar. Kunden verwalten über Cellular Hub ihre IoT-Geräte, senden und empfangen Nachrichten über sogenannte *Cloud Platform Adapter* oder provisionieren IoT-Geräte mit sensiblen Daten wie Firmwares und Schlüsselmaterial. Aus diesem Grund ist die Sicherheit des *Cellular Hub* von großer Bedeutung.

Cellular Hub wird in einer Container-Umgebung in der Microsoft Azure Cloud betrieben. Es ist Teil eines Kubernetes-Clusters, welches automatisiert die Erreichbarkeit und Verfügbarkeit des Systems sicherstellt. Quality Engineers führen regelmäßig Lasttests durch, um zu evaluieren, wie sich *Cellular Hub* unter starken Belastungen verhält. Die Absicherung des Kubernetes Clusters ist von großer Bedeutung, da unbefugter Zugriff auf die Kontrolleinheit des Clusters die Sicherheit des *Cellular Hub* gefährden könnte. Deshalb werden regelmäßig Security Audits durchgeführt, um die Zugriffe auf das Cluster zu überprüfen.

Für die Verwaltung kritischer Daten, wie Datenbank-Schlüssel, Zertifikate oder Passwörter, wird die Azure Key Vault eingesetzt. Dies ist ein Service von Microsoft Azure, der gewährleistet, dass sicherheitskritische Daten isoliert sind und vor unberechtigten Zugriffen geschützt werden.

Die Implementierung des Cellular Hubs basiert auf etablierten Open Source Libraries und Protokollen. Für jede Komponente, die als sicherheitskritisch eingestuft wird, führen wir ein Security Audit des Source Codes durch. Auch Implementierungen Dritter werden durch einen Security Audit geprüft, bevor diese in das Projekt integriert werden.

Connectivity Boards

Connectivity Boards werden mit einer eingebetteten *MFF2 SIM* geliefert, die Zugang zu Vodafones globalen Narrowband-IoT- und LTE-M-Netzwerken ermöglicht. Das *Connectivity Board* kommuniziert über das eingebettete LTE-Modem des *nRF9160* von *Nordic Semiconductor* mit dem *Cellular Hub*.

Einige unserer Kunden möchten die *Connectivity Boards* für mehrere Jahrzehnte einsetzen. Es kann vorkommen, dass die Software oder Firmware der *Connectivity Boards* Sicherheitslücken aufweist oder eingesetzte Algorithmen ausgetauscht werden müssen. Deshalb bieten grandcentrix signierte Firmware-over-the-Air (FOTA) Updates an.

Bereits während der Produktion werden *Connectivity Boards* mit öffentlichen Schlüsseln für die Validierung von Firmware Updates ausgestattet. Mit Hilfe dieser Schlüssel wird sichergestellt, dass nur vertrauenswürdige Software und Firmware auf unseren Geräten ausgeführt werden. Der Bootloader des *Connectivity Boards* führt die Firmware eines Gerätes nur dann aus, wenn die Signatur der Firmware validiert werden kann. Ein privater Schlüssel, welcher für die Signaturerstellung verwendet wird, ist in einem *Hardware Security Module (HSM)* hinterlegt. Somit hat keine Person direkten Zugriff auf den Signaturschlüssel. Die Signierung von Software und Firmware wird von Security-Experten geprüft und durchgeführt.

Neben den Schlüsseln für die Signaturprüfung wird jedes Connectivity Board mit individuellen x509 v3 Zertifikaten ausgestattet. Zertifikate stellen einen Vertrauensanker dar und ermöglichen, dass *Connectivity Boards* eindeutig von *Cellular Hub* identifiziert werden

können. Die Zertifikate werden aus unserer eigenen Public-Key-Infrastruktur (PKI) abgeleitet. Das sogenannte Root-Zertifikat wird auch in einem HSM hinterlegt.

Das *Connectivity Board* verfügt über einen *Arm Cortex-M33 Prozessor*. Dieser besitzt einen sicheren Speicherbereich für kritische Daten, wie Zertifikate oder Schlüsselmaterial. Außerdem stellt er eine isolierte Recheneinheit für kryptographische Operationen zur Verfügung - die *Arm TrustZone*. Die Arm TrustZone führt Verschlüsselungen und Signaturoperationen auf dem *Connectivity Board* aus.

Nachwort

Das Internet der Dinge wird zunehmend relevanter für Produkthersteller, Service-Anbieter und Anwender. Jedes IoT-Gerät verspricht Mehrwert für Nutzer, sowohl in Privathaushalten wie auch in Industrieanlagen. Mit der wachsenden Verbreitung von IoT-Geräten steigen auch die Optionen für potentielle Sicherheitslücken und konkrete Bedrohungen durch Ausfälle oder Angriffe. grandcentrix ist sich seiner besonderen Verantwortung als Hersteller und Entwicklungspartner für IoT-Produkte voll bewusst und leistet gewissenhaft seinen Beitrag zu einer sicheren Gegenwart und Zukunft. Dieses Dokument beschreibt die Komponenten und Sicherheitskonzepte, mit denen wir die Sicherheit von *Cellular IoT* verbessern.

Kontakt

grandcentrix GmbH
A Vodafone Company

Holzmarkt 1
50676 Köln
p. +49 221 67 78 60 -0
f. + 49 221 67 78 60 -99
e. hello@grandcentrix.net
www.grandcentrix.net

Glossar

Begriff	Definition
Arm Cortex-M33	Effizienter Prozessor für IoT Anwendungen.
Arm TrustZone	Isolierte Recheneinheit, die sicherheitsrelevante Operationen ausführen kann. Arm Trustzone ist Teil des Arm Cortex-M33.
Azure Key Vault	Service der Microsoft Azure Plattform für die sichere Speicherung von sensiblen Daten.
Cellular Hub	Von grandcentrix betriebener PaaS für Device Management, SIM Management, Rollout Support, Integration mit Azure IoT Hub und MQTT
Connectivity Board	CE-zertifizierte Hardware auf Basis unseres Blueprints für den Einsatz in Produkten, um eine Verbindung zum Mobilfunknetz herzustellen.
Datagram Transport Layer Security (DTLS)	Variante des TLS Protokolls, die für UDP optimiert ist.
Hardware Security Module (HSM)	Komponente zur Persistierung kritischer Daten.
IPSec v3	Protokoll für die Verschlüsselung von Nachrichten zwischen Cellular Hub und der Vodafone Global M2M Platform.
Long Term Evolution (LTE)	Mobilfunk Standard. Für Cellular IoT kommen folgende Spezifikationen zum Einsatz: Narrowband-IoT und LTE-M
LPWAN	Low Power Wide Area Network
MFF2 SIM	SIM-Karte optimiert für IoT-Geräte, welche auf der Hardware eingebettet ist.
Microsoft Azure	Cloud-Plattform von Microsoft
Nordic nRF9160	System-in-Package (SiP), das über ein LTE Modem verfügt.
Public-Key-Infrastruktur (PKI)	Komponente zur Ausstellung digitaler x509 v3 Zertifikate für Connectivity Boards.
Virtual Private Network (VPN)	Verschlüsselte Netzwerkverbindung zwischen Cellular Hub und der Vodafone Global M2M Platform.

Vodafone APN	Ein Access Point Name stellt ein Gateway dar, das die Kommunikation von IoT-Geräten der Vodafone Global M2M Platform mit dem Cellular Hub ermöglicht.
Vodafone Global M2M Platform	Zentrale IoT Plattform für SIM Management und Kommunikation.
x509 v3	Standard für Public-Key-Infrastrukturen und zur Erstellung digitaler Zertifikate.