Cellular IoT Security Whitepaper

Marvin Schirrmacher, Cellular IoT Security Consultant
March, 2021

Contents

Introduction

As an “Internet of Things” solution provider, grandcentrix develops end-to-end solutions that enable manufacturers to network their products. Increasingly, mobile communications are being used to enable product manufacturers to bring their devices into the Internet of Things (IoT) autonomously and without local gateway infrastructures (such as WLAN routers). Low Power Wide Area Network technologies (LPWAN) such as Narrowband IoT or LTE-M are particularly suitable for the Internet of Things.

This enables the development of new (digital) business models that facilitate cost reduction, and optimize service processes and direct contact with end customers, often for the first time. Classic examples for applications are the collection and utilization of telemetry data and the remote adjustment of configuration values.

To make the entry into the world of *cellular connected devices* easy and cost-effective, grandcentrix has developed *Narrowband+*, a service specifically adapted to the needs of cellular connected IoT devices as part of the *Cellular IoT* portfolio.

This document describes the security architecture of *Cellular IoT* and *Narrowband+*. It illustrates how grandcentrix deploys security concepts to protect customers and their products over lifecycles that often span years. These security concepts are both technical solutions and organizational processes and specifications.

Short Description of Cellular IoT

The *Cellular IoT* family provides all components required by product manufacturers for the connection between product and IT infrastructure (e.g., Microsoft Azure):

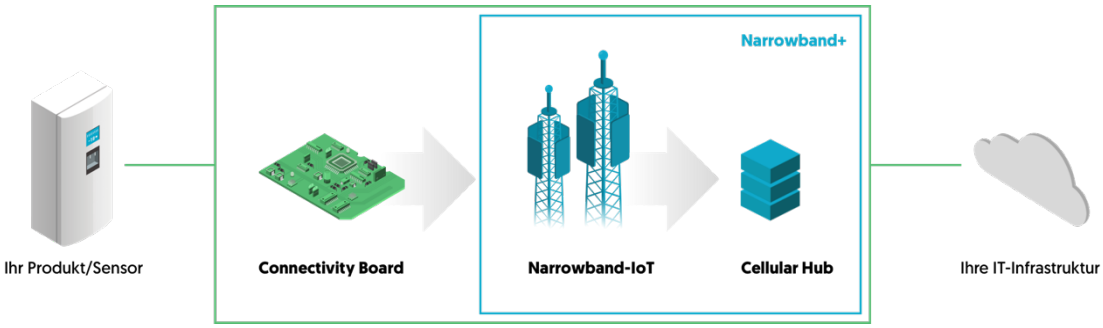

Fig. 1: Architectural sketch of Cellular IoT

A *Connectivity Board* is built into the product itself and thus forms a unit with the actual device. It is responsible for both the communication between sensors and actuators of the device and the cloud. For full flexibility, we use a proven and certified hardware blueprint as the basis for the connectivity board. This includes a modem as well as an industrial SIM card, which is used to establish a connection to the mobile network in order to transfer data in both directions. For this purpose, the SiP (System in Package) Nordic Semiconductor nRF9160 is used, for which grandcentrix provides an SDK to perform the recurring tasks of firmware development in a standardized way.

Our *Connectivity Board* is CE certified and therefore approved for use in Europe. Based on the blueprint, it is possible to customize your own *Connectivity Board* to your own needs (firmware, form factor, hardware connections, etc.).

Data is transmitted using Narrowband IoT. NB-IoT is a standard in mobile networks described by 3GPP. Because this standard is specifically designed for efficient energy balance and high availability, UDP is used as the transport protocol. Networking with the most common cloud service providers, on the other hand, often uses only TCP for registration and communication, and thus a protocol conversion is required to connect devices to the cloud services.

To enable devices to reliably communicate directly with the desired cloud platform, the *Cellular Hub* handles this conversion. The *Cellular Hub* is a PaaS (Platform-as-a-Service) operated by grandcentrix; it receives the data directly from the Vodafone mobile network, prepares it for further use, and forwards it converted to the desired target system. Different customer systems are connected via standardized interfaces (e.g., Azure IoT Hub, MQTT Broker).

In addition to protocol conversion, the *Cellular Hub* enables tasks such as device management, SIM management, the distribution of firmware updates and integration into production, logistics, and fulfillment processes. There is no data storage.

Narrowband+ is a complete connectivity solution that enables the use of Narrowband IoT and the *Cellular Hub* in over 30 countries for 1 cent per day per activated device. *Connectivity Boards* are not included in *Narrowband+* and must be ordered separately.

Security Model

The basis for securing *Cellular IoT* is a security model. The term security model refers to a framework for decision making during development. Before a security model can be created, assets worth protecting are defined.

Assets

For the implementation of security concepts, it is important to identify assets that are worth protecting. Assets are considered to be tangible and intangible goods or even non-functional properties of various components. Once all assets worth protecting have been defined, the next step is to create a security concept to minimize the potential risk.

For *Cellular IoT*, the focus is on the following assets:

Asset	Examples
Customer data	Payment information, names, passwords
Customer products	Smart Products, industrial equipment
End users	Users of smart products
Connectivity Boards	Device information (e.g., device key), secure communication, battery life, if applicable
Connectivity SIMs	Activation, management, assignment to customers
Cellular Hub	Accessibility, integrity, secure communication
Cellular infrastructure	Access to system components (e.g., databases), logs, passwords

Assumptions

A security model contains assumptions that help us make security-related decisions during development. For example, if a system component is deemed trustworthy, no defensive measures need to be implemented to correct the trust relationship. The following are assumptions that are considered when creating security concepts.

Assumption: Trust in our cloud platform
grandcentrix maintains a trust relationship with the cloud platform Microsoft Azure. Nevertheless, security concepts are created for our cloud infrastructure. It is assumed that Microsoft does not perform any harmful activities that endanger our product and our customers.

Assumption: Trust in our hardware manufacturers
grandcentrix has a relationship of trust with its hardware suppliers. The expectation is that the integrity of our hardware components is assured. We do not assume that hardware manufacturers actively compromise the security of our product.

Assumption: Unknown LTE infrastructure
LTE infrastructures are highly complex, implementing numerous standards that guarantee different levels of security. In addition, roaming partners are also part of these infrastructures. This means that grandcentrix does not have full sovereignty over all components of an LTE infrastructure. It must therefore be ensured that mechanisms are applied that protect the communication between *Connectivity Boards* or hardware of the customer and the *Cellular Hub* from unknown factors.

Assumption: Unrestricted access to *Connectivity Boards* or customer hardware
grandcentrix accepts the risk that *Connectivity Boards* and a customer's hardware may come into the possession of unauthorized third parties (e.g., through theft). grandcentrix also accepts that a potential attacker may gain full access to the operations and file system of an IoT device. It is assumed that attackers will:

- reverse engineer software and hardware,
- modify software and hardware,
- analyze and manipulate the communications of an IoT device.

Preventing this would mean not allowing any vulnerability in any software and hardware component of the device during the entire product lifecycle. However, this cannot be guaranteed. And for this reason, mechanisms must be created to protect customers as well as infrastructure even if an attacker gains full access to a single IoT device.

Assumption: Potential attackers
The *European Union Agency for Cybersecurity* (ENISA) has defined different groups of attackers (ETL 2017). Attackers can pose a threat to our customers and our platform. Depending on the grouping of an attacker, different security concepts are developed. Security mechanisms against targeted attacks by state actors must be designed differently than broad attacks by so-called “script kiddies”.

grandcentrix sees the following attacker groups as potential threats to Cellular IoT:

Attacker Group	Potential Targets
End users	Information, entertainment
Researchers	Information, publicity
Hackers	Damage, entertainment
Insiders (for example, former employees)	Information, revenge
Cyber criminals	Financial gain
Competitors	Information, competitive advantage

Assumption: Product lifetime of *Connectivity Boards*
grandcentrix assumes that *Connectivity Boards* have a lifetime of up to several decades. During this time, it must be ensured that potential security vulnerabilities in the software or firmware can be identified and fixed at any time.

Assumption: Trust in us
grandcentrix has a relationship of trust with its customers. grandcentrix is responsible for ensuring that:

- customer data is protected,
- the infrastructure is accessible and reliable,
- critical operations are performed with care.

Secure Software Development Life Cycle

Product teams at grandcentrix work according to the *Secure Software Development Life Cycle*. Here, security specialists are already integrated into the planning of a software or hardware component. At each stage of development, various activities take place to ensure secure development. This makes it possible to meet all requirements of **ISO 27001, IEC 62443** and **VDE Smart Home**.

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

Even before a software or hardware component is developed, security experts decide whether the component in question is classified as security-critical. If this is the case, potential threats are analyzed and options for securing a component are evaluated. A *Definition of Done* is also established for the component, which is verified after development. Each development package is assigned a security label. Security labels are used to decide which activities are performed for *verification*. Five different security labels are used, which reflect the criticality and impact of a development package.

Security Score	⚪	🟢	🟡	🟠	🔴
Description	Safety uncontrollable	No relevance to security	Potential relevance to security	Relevance to security	Of high relevance to security
Example	Use of a customer's unknown software	Modification of documents	Improving existing software tests	Configuring an ingress controller	Implementing customer authentication
Activities	None	None	Optional	Code reviews	Code Reviews, Security Testing

Design

After a component has been analyzed, security experts develop concrete security concepts. Depending on its intended use, security concepts with different security levels are created. A security concept is selected for development that harmonizes best with our security model and organizational structure. If necessary, roles must be defined in order to implement a security concept. For example, a specific person can be appointed who has access to certain passwords or who is allowed to sign firmware.

Implementation

During the development of a software or hardware component, security experts assist the development teams and help to solve ambiguities or problems. Changes to a security concept can also be made during this stage. Occasionally, security concepts cannot be fully mapped due to technical circumstances. For example, a selected algorithm for encryption may not be suitable for the given hardware because it allocates too much memory. These kinds of findings are incorporated into the development process and are used to adapt concepts.

Verification & Release

This stage concerns the validation of the security requirements. The most important activities here are code reviews and security tests by security experts. Code reviews are used to detect implementation errors or configuration errors of components. Security tests are executed using various tools and scripts to validate the security attributes of a component. Any security vulnerabilities found are documented and fixed. If the verification is successful, the component is released.

Maintenance

grandcentrix security experts perform regular security audits to ensure the security of our infrastructure. This involves evaluating which people have access to our cloud environment and how system components are protected. In addition, the software used is scanned for security vulnerabilities. If security vulnerabilities are found, they are fixed using patch management processes. If vulnerabilities with a major impact are uncovered, they are placed under observation until they are fixed. For this purpose, we maintain a list of known vulnerabilities: the so-called *Security Radar*.

Communication

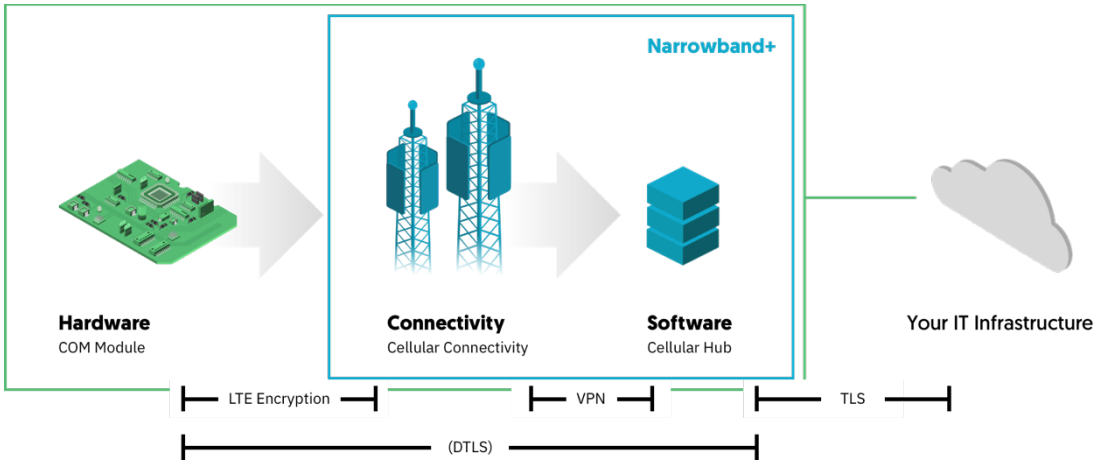

Fig. 2: Architectural overview

Connectivity Boards and the IoT devices of our customers are equipped with an embedded MFF2 SIM. The SIM enables IoT devices to access Vodafone's global narrowband IoT and LTE-M networks. IoT devices cannot communicate with each other. This is prevented by Vodafone's LTE infrastructure. Consequently, compromised devices cannot connect to other devices.

IoT device communications are transmitted to the *Vodafone Global M2M Platform* via radio masts (*eNodeB*). Messages are then transmitted to the *Cellular Hub* via a gateway (the so-called access point). Messages are encrypted using the IPSec protocol v3. The *Cellular Hub* can only receive messages from or send messages to our customers' IoT devices. Vodafone prevents unknown IoT devices from connecting to the *Cellular Hub* via narrowband IoT or LTE-M.

DTLS and TLS

Communication between *Connectivity Boards* and thus a customer's hardware and the *Cellular Hub* is protected by security mechanisms of various LTE specifications and the IPSec v3 protocol. Nevertheless, the security experts at grandcentrix have decided to integrate another layer of security. Any communication between *Connectivity Boards* and the *Cellular Hub* can be optionally secured using the DTLS 1.2 protocol.

DTLS is a variant of the widely used TLS protocol that has been optimized for so-called *Constrained Devices*. By using DTLS via the UDP protocol, our connectivity boards consume less energy and computing power.

DTLS provides the following security attributes:

- **Encryption**: Messages are encrypted and cannot be viewed by any entity within the LTE infrastructure. Encryption is optimized for the low processing power of the *Connectivity Boards*. High-performance algorithms are used with the cipher suite ECDHE ECDSA with AES 128 GCM SHA256 based on the elliptic curve secp256r1.

- **Integrity protection:** Messages cannot be manipulated by any entity within the LTE infrastructure. The *Connectivity Boards* and the *Cellular Hub* detect the manipulation of a message and the respective message is then discarded.
- **Replay-attack protection:** Messages cannot be recorded and re-sent by any instance within the LTE infrastructure. The *Connectivity Boards* and the *Cellular Hub* detect the redelivery of a message and discard it.
- **Protection against DDos attacks**: DTLS prevents IP spoofing attacks by requiring communication partners to prove that they have been assigned a specific IP address. Attackers thus cannot send messages to the *Cellular Hub* with fake IP addresses. This prevents the *Cellular Hub* from responding to messages that contain fake IP addresses. If the *Cellular Hub* were to respond to each of these messages, it could be paralyzed by a flood of messages (especially if complex computational operations are initiated).
- **Identification of devices:** Devices can be uniquely identified by the *Cellular Hub* using certificates (based on *x509 v3*). Before communication between the *Connectivity Board* and the *Cellular Hub* is initiated, a *DTLS Handshake* takes place. If a certificate is unknown or forged, the request is rejected. Certificates contain a hardware reference to a *Connectivity Board*. This prevents attackers, even with full access to a device, from sending messages on behalf of other devices. The private key of a *Connectivity Board* remains unknown even to grandcentrix. A separate *Public Key Infrastructure (PKI)* has been set up to create the certificates. The PKI is already being used in the manufacture of the *Connectivity Boards* in order to integrate certificates as a trust anchor on a device. Certificates are securely stored on the device. The associated key material is handled only by a secure execution unit, the *Arm Trustzone*.

All communication between the *Cellular Hub* and the customers' systems is protected by the TLS protocol. Depending on the communication channel, TLS 1.2 or TLS 1.3 is used for this purpose. These protocols ensure similar attributes as those of DTLS.

The Cellular Hub

The *Cellular Hub* is the interface between IoT devices and our customers' IT infrastructure. The *Cellular Hub* is a security-critical component of the Cellular IoT. Customers use the *Cellular Hub* to manage their IoT devices, send and receive messages via so-called *Cloud Platform Adapters* or provision IoT devices with sensitive data such as firmware and key material. For this reason, the security of the *Cellular Hub* is of great importance.

The *Cellular Hub* is run in a container environment in the Microsoft Azure cloud. It is part of a Kubernetes cluster that ensures the automated accessibility and availability of the system. Quality engineers regularly perform load tests to evaluate how the *Cellular Hub* behaves under heavy loads. Securing the Kubernetes cluster is of great importance, as unauthorized access to the cluster's control unit could also compromise the security of the *Cellular Hub*. Therefore, security audits are performed regularly to verify access to the cluster.

Azure Key Vault is used to manage critical data, such as database keys, certificates, and passwords. This is a Microsoft Azure service that ensures that security-critical data is isolated and protected from unauthorized access.

The *Cellular Hub* implementation is based on established open-source libraries and protocols. For each component that is classified as security-critical, we perform a security audit of the source code. Third-party implementations are also subjected to a security audit before they are integrated into the project.

Connectivity Boards

Connectivity Boards are supplied with an embedded MFF2 SIM that provides access to Vodafone's global narrowband IoT and LTE-M networks. The *Connectivity Board* communicates with the *Cellular Hub* via Nordic Semiconductor's nRF9160 embedded LTE modem.

Some of our customers intend to use the *Connectivity Boards* for several decades. It may happen that the software or firmware of the *Connectivity Boards* has security gaps or that the algorithms used have to be replaced. Therefore, grandcentrix offers signed Firmware-over-the-Air (FOTA) updates.

Already during production, *Connectivity Boards* are equipped with public keys for the validation of firmware updates. These keys ensure that only trusted software and firmware are executed on our devices. The bootloader of the *Connectivity Board* only executes a device's firmware if the firmware's signature can be validated. A private key, which is used for signature generation, is stored in a *Hardware Security Module* (HSM). This means that no person has direct access to the signature key. The signing of software and firmware is checked and performed by security experts.

In addition to the keys for signature verification, each *Connectivity Board* is equipped with individual x509 v3 certificates. Certificates provide a trust anchor and enable *Connectivity Boards* to be uniquely identified by the *Cellular Hub*. The certificates are derived from our own public key infrastructure (PKI). The so-called root certificate is also stored in an HSM.

The *Connectivity Board* has an Arm Cortex-M33 processor. This has a secure storage area for critical data, such as certificates or key material. It also provides an isolated computing unit

for cryptographic operations - the *Arm TrustZone*. The *Arm TrustZone* performs encryption and signature operations on the *Connectivity Board*.

Afterword

The Internet of Things is becoming increasingly relevant to product manufacturers, service providers, and users. Every IoT device promises to add value for users, both in homes and in industrial facilities. With the growing proliferation of IoT devices, the options for potential security vulnerabilities and concrete threats from failures or attacks also increase. grandcentrix is fully aware of its special responsibility as a manufacturer and development partner for IoT products, and conscientiously contributes to a secure present and future. This document describes the components and security concepts we use to improve the security of Cellular IoT.

Contact

grandcentrix GmbH
A Vodafone Company

Holzmarkt 1
50676 Cologne
Phone: +49 221 67 78 60 -0
Fax: + 49 221 67 78 60 -99
e. hello@grandcentrix.net
www.grandcentrix.net

Glossary

Term	Definition
Arm Cortex-M33	Efficient processor for IoT applications.
Arm TrustZone	Isolated computing unit that can perform security-related operations. Arm Trustzone is part of the Cortex-M33 arm.
Azure Key Vault	Service of the Microsoft Azure platform for the secure storage of sensitive data.
Cellular Hub	Grandcentrix-powered PaaS for device management, SIM management, rollout support, and integration with Azure IoT Hub, and MQTT
Connectivity Board	CE-certified hardware based on our blueprint for use in products to connect to the mobile network.
Datagram Transport Layer Security (DTLS)	A variant of the TLS protocol optimized for UDP.
Hardware Security Module (HSM)	Components for persistence of critical data.
IPSec v3	Protocol for encrypting messages between the Cellular Hub and the Vodafone Global M2M Platform.
Long Term Evolution (LTE)	Mobile phone standard. Cellular IoT uses the following specifications: Narrowband-IoT and LTE-M.
LPWAN	Low Power Wide Area Network
MFF2 SIM	SIM-Card optimized for IoT devices embedded on the hardware.
Microsoft Azure	Microsoft Cloud Platform
Nordic nRF9160	System-in-Package (SiP), which has an LTE modem.
Public-Key-Infrastructure (PKI)	Component issuing digital x509 v3 certificates for connectivity boards.
Virtual Private Network (VPN)	Encrypted network connection between the Cellular Hub and the Vodafone Global M2M Platform.
Vodafone APN	An Access Point Name is a gateway that enables IoT devices from the Vodafone Global M2M Platform to communicate with the Cellular Hub.

Vodafone Global M2M Platform	Central IoT platform for SIM management and communication.
x509 v3	Standard for public key infrastructures and for creating digital certificates.