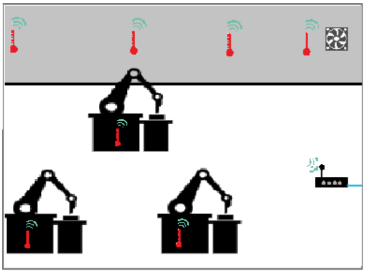
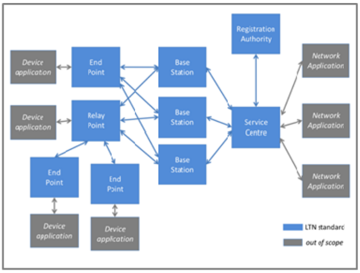
Fraunhofer IIS

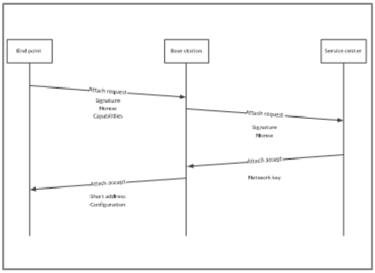
FRAUNHOFER INSTITUTE FOR INTEGRATED CIRCUITS IIS

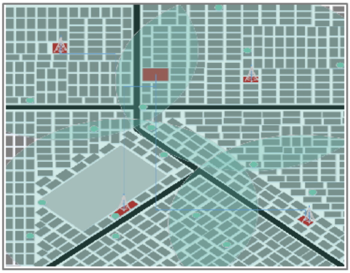
MIOTY™ – SECURTIY GUIDELINE

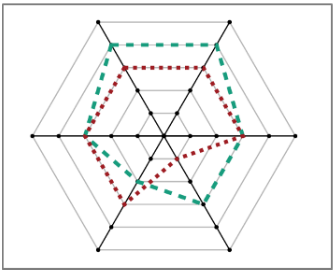
USE-CASES, REFERENCE-ARCHITECTURES AND RECOMMENDATIONS

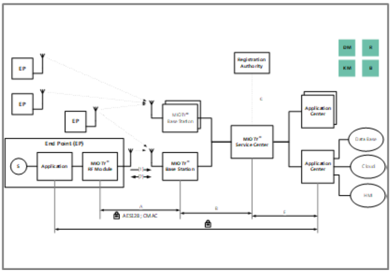












Published by
Fraunhofer Institute for Integrated Circuits IIS, Nuremberg

Editorial team
Distributed Systems and Security Division
Authors: Lukas Rothe, Moritz Loske

Version: v1.1

Layout and production
Distributed Systems and Security Division: Marketing and Communication

MIOTY™ (My IoT) is a Low Power Wide Area Networks (LPWAN) solution dedicated for large-scale, private IoT Networks. It delivers industry-grade connectivity that satisfies the most demanding (Industrial) IoT requirements, addressing critical communication challenges of power efficiency, coverage, cost and scalability.

Security is an important aspect of every communication system. Based on the security measures and requirements defined in the ETSI standards TS103357 and TS103358, this Security Guide offers holistic proposals and guidance for the secure implementation and design of a MIOTY™ communication infrastructure. By means of two exemplary use cases different realizations of the recommended security concepts, tailored to the application´s needs, are illustrated.

Table of Contents

1 Introduction

The Internet of Things (IoT) is a conglomerate of a large number of distinct Cyber Physical Systems (CPS). This number will expand tremendously from around 15 billion installed IoT devices in 2015 up to estimably 30 billion devices, accompanied by more than 600 zettabytes produced data per year by 2020 [1]. Quantities of this magnitude require dedicated technologies to facilitate device management and orderly communication.

MIOTY™ is a low power wide area network (LPWAN) solution dedicated for large-scale private IoT networks. The MIOTY technology delivers industry-grade connectivity for Industrial IoT applications, with a focus on low power consumption, maximum spectrum efficiency and unrivaled network capacity and scalability.

The IoT represents a fusion of the real and digital worlds. Due to the linkage of these two formerly independent worlds, cyber-attacks can have a tremendous impact in everyday or commercial life. Previous attacks and their damaging impact show the importance of cyber-security in industrial IoT applications. It is therefore necessary to pay close attention to the security mechanisms of the MIOTY™ technology.

This Security Guide is aimed at system integrators, manufacturers and MIOTY™ infrastructure providers who deal with the security aspects of the entire MIOTY™ architecture.

1.1 Definition of Cyber-Security

Cyber-Security deals with all aspects of security in the information and communications technology. The field of action of the classic IT security is extended to the whole cyber space. It comprises all information technology related to the Internet and similar networks, connected computing devices, the collection of tools, policies, processes, and the totality of transmitted and/or stored and processed information, applications and services.

Cyber-Security strives to ensure the attainment and maintenance of the security properties of the organization and user´s assets against relevant security risks in the cyber environment. [2, 3]

1.2 Cyber Security Challenges of IoT Systems

In comparison to classical IT-Systems, IoT Systems have to deal with various challenges and limitations in resources. With regard to the MIOTY™ technology, those factors are:

- Limited computing power
- Limited energy supply
- Limited bandwidth for communication
- Often one-directional communication
- Harsh and constrained environments.
- Networks with devices from varying manufacturers
- Waking hours, sleep mode

IoT poses its own requirements in terms of cyber security. Due to the aforementioned constraints, traditional protocols and cryptographic methods cannot be used. Hence, efficient standards and protocols for key exchanges and lightweight cryptographic methods are required in order to provide authenticity and to reach a certain level of confidentiality and integrity.

IoT devices are more commonly used in security critical applications within industrial or governmental context. Flaws in just one device within the network can cause successful attacks and allow cyber criminals to infiltrate the network. One major and unsolved problem is that many devices are not frequently provided with the latest firmware updates in order to close potential vulnerabilities, due to limited access. The distribution of updates is therefore another challenge that has to be faced. The protection objectives for IoT systems, and subsequently a MIOTY™ infrastructure, are elaborated in the next chapter.

2 Protection Objectives in IoT-Systems

The overall protection goals of classic IT-security are confidentiality, integrity, authenticity, availability and non-repudiation [2][4]. These objectives can be applied to IoT-Systems as well, but in order to meet the specific security requirements of interconnected IoT devices the goals need to be extended by the realization of key management and the quality of the connection. These two criteria are critical when it comes to a secure communication within resource limited network of IoT devices. These objectives of protection in IoT-Systems are explained below in more detail.

Security is an intangible and tough-to-measure objective. While internationally accepted standards, like IEC 62443 and Common Criteria (CC), exist, they are often criticized for being too formalized and time-consuming. We will therefor use a simple matrix to consider both the given security features and the security requirements of an application in regards to the aforementioned protection objectives. By comparing these evaluations, security gaps are detected from which additional security measures are derived.

2.1 Confidentiality

Confidentiality (Conf.) is roughly equivalent to privacy. Confidentially can be ensured by measures that are designed to prevent sensitive information from reaching the wrong people or instances, while making sure that the right people or instances can read the information. Usually achieved by encryption/decryption.

2.2 Integrity

Integrity (Int.) means the maintenance of trustworthiness of data during its entire life cycle. Data must not be changed in transit. Therefore, measures must be taken to ensure that unauthorized people or instances cannot manipulate data. This can be achieved by cryptographic checksums, e.g. based on hash functions (HMAC).

2.3 Authenticity

Authenticity (Auth.) is the property that ensures that the identity of a subject or resource is the identity claimed. Authenticity applies to individuals (users), but also to any other entity (applications, processes, systems, etc.). It is an identification, i.e. the recognition of a name indicating an entity without the slightest doubt. Authenticity is e.g. guaranteed by certificates. Cipher-based Message Authentication Codes (CMAC) provide both integrity and authenticity.

2.4 Non-Repudiation

Nonrepudiation (Non-Rep.) is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a communication cannot deny that they transmitted specific data packages. Usually achieved by using digital signatures based on Rivest–Shamir–Adleman (RSA) or Elliptic Curve (EC) cryptographic algorithms.

2.5 Key Management

Key Management (KM) means the secure management of cryptographic keys. This includes the generation, the exchange as well as the storage of cryptographic keys. Further it includes the cryptographic protocol design, key servers and other relevant protocols to manage the secure key handling. Using a crypto system in a secure way, requires a proper key exchange. Without a secure way of handshaking the keys, the whole encryption and decryption of messages may be considered to be unsecure.

2.6 Quality of connection

Quality of Connection (QoC) is an indicator for the availability of a communication technology. Industrial IoT networks rely on a wide range of different communication technologies both wired and wireless. A reliable communication requires a certain Quality of Connection. Therefor the medium of transmission and the individual frequency band (for the case of a wireless technology) will be taken into account in order to assess the QoC.

3 Security defined in ETSI Standard

MIOTY™ is based on the European Telecommunications Standards Institute (ETSI) standards for Low Throughput Networks (LTN). Important for this guide are the standards TS103357: *Protocols for radio interface A* [5] and TS103358: *LTN Architecture* [6]. Regarding the security of LTN networks these standards specify basic security measures and requirements for the wireless communication itself, as well as for the architecture of the communication system and subsequent communication interfaces. These, partly optional, security features are explained in the following sections.

3.1 Architecture

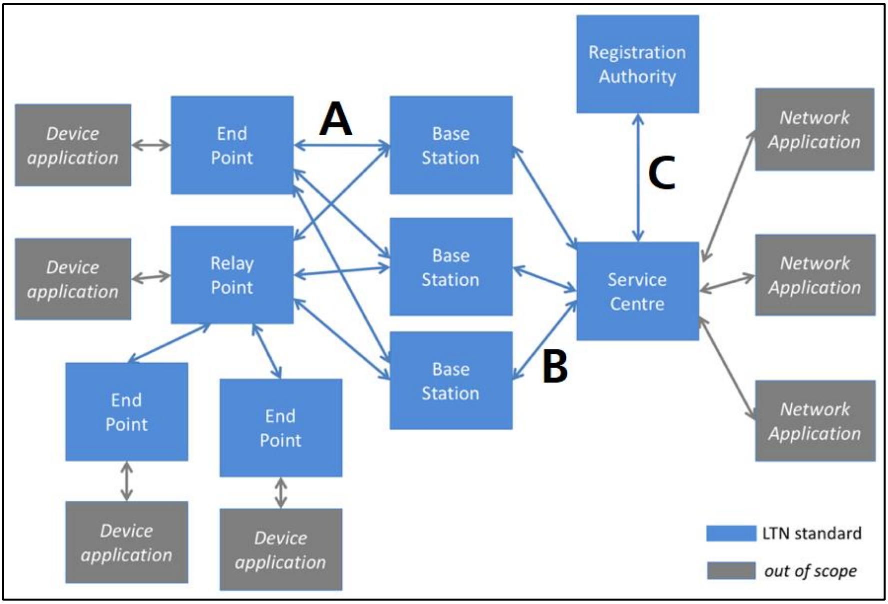


Figure 1: The architecture of an ETSI LTN system [6]

The proposed architecture of a LTN communication system can be seen in Figure 1. It spans the entire communication path from the devices to the application over several entities. These entities, or function blocks, do not necessarily correspond to distinct devices in practical applications.

3.2 Functional Units

The following functional units are defined in ETSI LTN Standard:

3.2.1 End Points

End Points (EP) obtain the data from the device application, encrypt it with their secret key and transmit it to the Base Station(s).

The ETSI LTN standard specifies two types of End Points, designated as **class A** devices and **class Z** devices.

Class Z

Class Z devices represent the simpler form of End Points. They have only uplink communication implemented, meaning they can send packages but are unable to receive any communication. Configuration and security measures can therefore not be executed via the radio communication.

Class A

Class A devices on the other hand are capable of up- and downlink communication. Thus, they can transmit and receive packages, enabling over-the-air configuration. Their communication encryption provides higher security per default, as shown in Section 3.4.

3.2.2 Relay Points

Relay Points relay the transmissions from End Points to the Base Stations, if they are out of reach otherwise.

3.2.3 Base Stations

Base Stations (BS) decrypt the received packages from the End Points and pass the data on to the Service Centre. They can also send communication from the Service Centre to the End Points. Base Stations need to store cryptographic keys of their attached devices.

3.2.4 Service Centre

The **Service Centre** (SC) manages the LTN system, requiring it to store cryptographic keys and application data. It attaches End Points to Base Stations by providing the Base Stations with the required cryptographic keys. The Service Centre also receives the data from the Base Stations and forwards it to their respective Network Applications.

3.2.5 Registration Authority

The **Registration Authority** (RA) holds all cryptographic keys. It delivers them on demand to the Service Centre.

3.3 Communication Interfaces

The communication paths between the individual components are also labeled. Communication between End Points and Base Stations goes over the **Interface A**, **Interface B** describes the communication between the Base Stations and the Service Centre and **Interface C** is connecting the Registration Authority and the Service Centre. Interface D, not pictured, between different Service Centers will not be considered in this guide.

This architecture aims to minimize unauthorized access to communication keys if a device is compromised. Each device holds only the keys necessary for its application. Base Stations and especially the Service Centre, as the central unit of the network, pose targets for attackers to obtain several keys at once and need enhanced security measures.

Interface	Connection	Description
A	End Point <-> Base Station	Mainly data transmission from the EP. Configuration data from the BS possible, depending on the End Point type.
B	Base Station <-> Service Centre	Data Transmission to the SC; configuration data and cryptographic keys from the SC to the BS.
C	Service Centre <-> Registration Authority	Used by the SC to request cryptographic keys from the RA for new EPs or Relay Points.
D	Service Centre <-> Service Centre	Optional communication interface to support roaming over networks.

ETSI also defines security measures and requirements for the communication interfaces A and B as stated below. The other communication interfaces between system components have no specified security requirements.

3.3.1 Interface A

Interface A is the primary air interface of the LTN, connecting the End Points to the Base Stations. It is almost exclusively used to transmit the application data from the End Points. The Base Station can also send configuration data over the interface, if class A devices are employed. The **Network Encryption** of Interface A is realized with the aid of a **Network key**.

Each End Point possesses its own cryptographic key, with which its communication is encrypted. The procedure used is the symmetric, block-wise advanced encryption standard with 128 bit keys (**AES128**), which is currently considered to be secure [7].

To verify the integrity, a cypher-based Message Authentication Code (CMAC) may be used, which signs the content of the message using the secret key mentioned above.

3.3.2 Interface B

The interface between Base Stations and the Service Centre, Interface B, is mainly used to relay the End Points' data to the Service Centre. Additionally, configuration data and cryptographic keys for the respective End Points is sent over this interface by the Service Centre. The security of the interface is considered briefly with the statement, that it "shall be secured, using IP-based encryption technology or equivalent" [6].

3.3.3 Interface C

Interface C connects the Registration Authority and the Service Centre. The SC can send a device's credentials to the RA, which answers them with the respective cryptographic keys.

3.3.4 Interface D

The optional Interface D is used for roaming purposes. It acts as the communication interface between Service Centres of the same LTN family. Security should be provided by using IP-secured links.

3.4 Key Transmission

There are two ways defined by the ETSI standard, how an End Point´s key is transmitted to the correct Base Station, depending on the capabilities of the End Point.

Class Z devices are unable to receive any commands, and thus need to be assigned to a Base Station beforehand. Figure 2 shows, how the Service Centre sends the required information, including the cryptographic key, to the Base Station. Since the End Point has only one encryption key, it is possible for a Base Station to decrypt all prior and later communication. The authenticity of received packages from an End Point is also not verifiable, if its key has been leaked, as mentioned in Section 3.3.1.

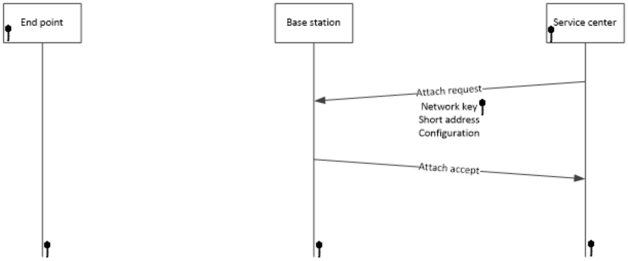


Figure 2: Key transmission for class Z devices [5]

Class A devices on the other hand are capable of two-way communication. As shown in Figure 3, they therefor request an attachment to a Base Station. The Base Station then uses the transmitted information to request the key from the Service Centre. Afterwards it can accept the request from the End Point. This protocol furthermore utilizes session keys, generated by the End Point and the Service Centre from the secret key and the random Nonce. Session keys are generated uniquely for every session and Base Station, thus preventing the decryption of earlier or later communication from the End Point with an obtained key. If a session key is compromised, the End Point and the Service Centre can generate a new one to secure further communication.

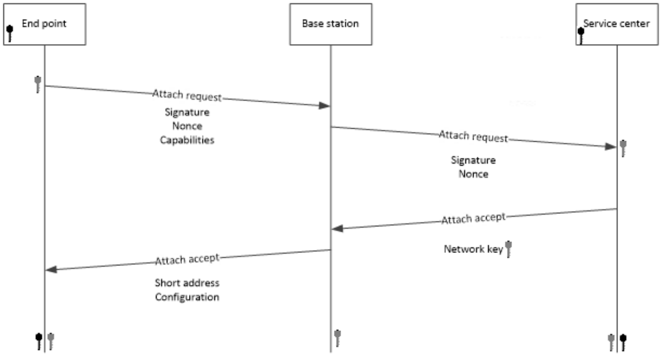


Figure 3: Key transmission for class A devices [5]

3.5 Security Evaluation

An evaluation of the radio communication in standard TS103357 with Telegram Splitting Method regarding the security objectives presented in Chapter 2 can be seen in Figure 4. The key management of the ETSI standard raises some concerns, which are discussed in the following.

The algorithm of AES is a symmetric-key algorithm. Such algorithms use one key for both encryption and decryption. Therefore both parties need to be in possession of the same key. This raises security concerns, as every Base Station that was in contact with an End Point obtains its key. This enables the Base Station, or malicious attackers who managed to compromise a Base Station, to decrypt any communication of the End Point. Both previous and later communication from the End Point with different Base Stations can be decrypted with this key, voiding its confidentiality. Such malicious parties can also encrypt packages with the End Point's key to pose as the End Point. This way they can inject malicious data into an application, since the encryption is seen as a proof for the authenticity of a message.

Class Z devices should consequentially be deployed in applications with fixed architecture, which do not require reconfiguration or key updates.

Class A devices mitigate this problem by generating a session key from their secret key, which is described in Section 3.4.

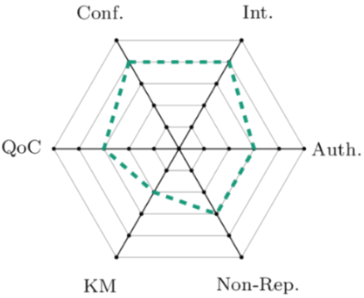


Figure 4: Security evaluation of the MIOTY™ radio interface

4 MIOTY™ Security guidance

The MIOTY™ network is a LPWAN technology that implements the ETSI LTN standards. The entire MIOTY™ technology, however, consists of more than just the aspects specified by the ETSI standards.

As the standard only states basic security measures and minimum security requirements, additional security measures are required to secure the entire MIOTY™ infrastructure. The aforementioned security features of the ETSI standard deal almost exclusively with the communication between an end point and the base station. Several critical topics, such as the predistribution of keys, physical security and subsequent communication paths, are not covered.

This chapter therefore describes the adapted MIOTY™ reference architecture and proposes different methods for the introduction of cryptographic keys to the devices and the respectively responsible authorities and gives general guidance and advice.

Possible security implementations are explained by means of two reference use-cases in Chapter 0. Based on the evaluation of their security requirements the general architecture will be adapted for them and security measures proposed to close potential security gaps.

4.1 General Reference Architecture

The MIOTY™ architecture, seen in Figure 5, is an implementation of the ETSI architecture. It has been modified with additional components, interfaces and task blocks.

Task blocks, shown in the top right corner of Figure 5, define important tasks of the network architecture, which are not bound to one specific entity in the communication system. They are instead assigned to one or more units depending on the application´s requirements and other design parameters, e.g. the key distribution method (see Section 4.2).

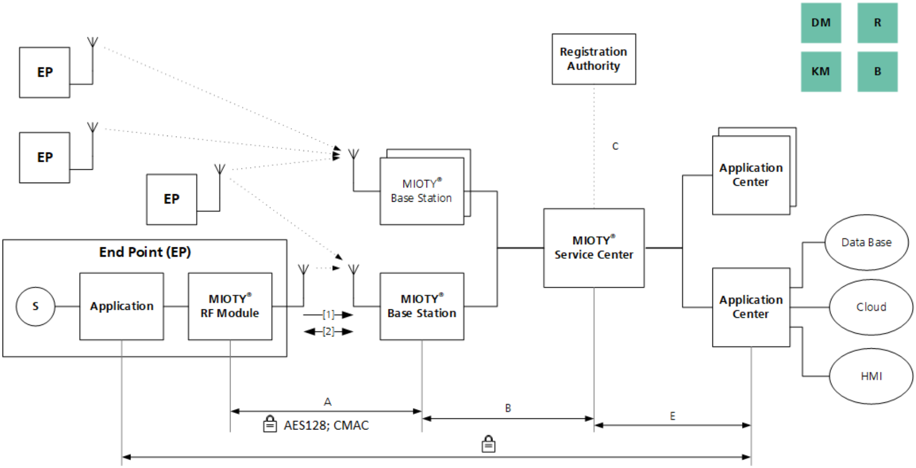


Figure 5: The general MIOTY™ architecture

End Points (Sensor Nodes), Base Stations and the Service Center do not differ in their role from the ETSI standard. The Registration Authority in this MIOTY™ architecture is responsible for the unique IDs of the End Points, key management is not necessarily its task. This function should be realized by the MIOTY™ Alliance. The architecture has been expanded by the **Application Center**. Each end customer is provided with one such Application Center as the in-network destination of their data. From there, customers can route their data to their application or applications.

Not pictured is the ETSI standard’s Interface C, connecting the Service Center and the Registration Authority, as it is not required in this general architecture. It might however be implemented depending on the key management. The addition of the Application Center has created a new interface, **Interface E**, between it and the Service Center.

Abbr.	Unit	Description	Connected Interfaces
EP	End Point	E.g. a sensor, captures data and transmits it over the air	A
BS	Base Station	Receives the data of EPs in the area and transmits it to the SC	A,B
SC	Service Center	Central unit of the MIOTY™ network. Relays the data to the ACs and keys to the BSs	B,C,E
AC	Application Center	Allows users to retrieve their data, can also provide management tools	E
RA	Registration Authority	Ensures unique IDs of End Points, might provide their keys alongside.	C

There are four task blocks defined for this architecture which are given to the devices of a MIOTY™ infrastructure depending on the requirements and specific architecture of the application:

- **Device Management (DM):** This task encompasses the introduction and decommissioning of devices and their assignment to Application Centers.
- **Routing (R):** Routing describes the delivery of data packets to their respective Applications.
- **Key Management (KM):** A device tasked with Key Management holds some or all keys, which are used within the network. The device needs to distribute those keys to communication partners when needed.
- **Billing (B):** It is necessary for billing to account for the number of packages from each customer. This process needs to be transparent for all involved parties to prevent fraud.

4.2 Cryptographic Key Management

Both the network key and the application key need to be handled carefully. We therefor present three different variants for key generation and key pre-distribution with their individual benefits and drawbacks. The valid choice depends on the parameters of the application. In each case it lies upon the executing party to securely generate cryptographic keys and introduce them onto the respective End Points.

Printed Keys

The manufacturer generates the keys and prints them, possibly in the form of a barcode or QR-code, on a label of the device. During setup, the keys can be scanned to admit them to the respective instances. This approach favors usability and ease-of-use, as no additional architecture is required. Attention should be payed, that the label is either peeled off from the End Point, or the End Point is mounted in a way, that makes reading the label impossible.

Central Key Authority

A second approach is the installation of a central MIOTY™ key server. Manufacturers, after installing the keys on the device, transmit them to the key server, where they can be requested from with the device ID. This method unifies key introduction across manufacturers, allowing for a simplified setup of heterogeneous MIOTY™ nodes. One drawback is the required internet connection. Also, if not secured properly, a digital break-in could compromise large numbers of MIOTY™ networks. The process of requesting keys also needs protection mechanisms.

Local Key Generation

To ensure, that no other party, manufacturer or otherwise, could be in possession of a device´s key, users themselves could generate the keys. Therefore, manufacturers would need to include an interface to flash cryptographic keys onto the device. When implemented properly, this approach guarantees the highest security level at the expense of usability.

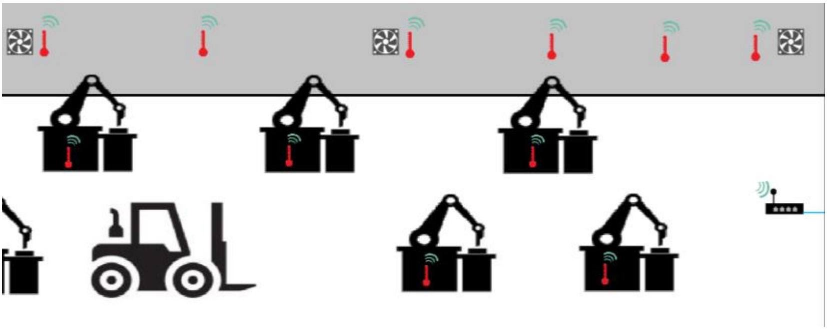
4.3 General Security Measures

The security of the MIOTY™ communication was increased by making the CMAC of packages in Interface A mandatory. It is furthermore strongly encouraged to use **Application Encryption**. A second key, the **Application key** is introduced for this purpose. It encrypts the data in the Sensor Node before the Network key is used. The decryption with the Application key then happens in the Application Center. The privacy of the data is additionally secured this way, as the data is never available unencrypted on its way through the MIOTY™ network. The encryption algorithm is not specified to allow customized implementation, we will simply use AES128 with CMAC, as used for network encryption.

After a reset, Base Stations will resynchronize with the Service Center to register and obtain the needed keys. It is therefore not necessary to permanently store cryptographic keys. Network and session keys on Base Stations are thus only held in the main memory, to further protect them. Attackers can thus only be compromised on live systems and not be read out from stolen or salvaged Base Stations. To prevent keys from finding their way onto the hard disk, paging should be disabled.

5 Reference Cases

5.1 Use-Case 1: Private basic MIOTY™ network in the Industrial IoT



5.1.1 Use-Case Description/Story

Type	Private	Manufacturer-operated, on premise
Area	Small	Factory premise
Customers	One	Manufacturer
Roaming	No	Stationary sensors
End Points	Z	Simple Sensors

A manufacturer wants to introduce predictive maintenance in one of his factories as a pilot project. This use-case addresses the influence of environmental parameters, such as humidity, temperature and air pressure, on the product quality and rate of machine failures. Therefore, a neural network shall be trained by processing production data in combination with ambient sensor readings to predict such failures. It can then preemptively advise local maintenance services to adjust air conditioning or replace machine party before they break. This process should reduce downtime in the factory while increasing the product quality, thus leading to a higher output of products with a better quality.

This system will in part be realized with a MIOTY™ infrastructure. While the production data, i.e. output, machinery failures and defective products, reaches the neural network over already established communication infrastructure, the sensor data is collected via MIOTY. Several hundreds of small, wireless, battery-powered sensors are placed across the factory, affixed to walls and machinery, measuring the aforementioned environmental parameters. Those sensor readings are transmitted every minute with the MIOTY™ protocol to one of several base stations in the factory. And from there relayed to a central unit, which combines the Service Center and the Application Center. A down-link communication from the base stations to the sensor nodes is not planned, so class Z devices are sufficient.

All devices of the MIOTY™ network are installed and maintained by an external contractor, ownership however belongs to the manufacturer.

From the base stations, the data is tagged with the current time and relayed over the Service Center to a data center off-site, where the sensor data is processed in combination with the production data by the neural network and process optimization takes place.

5.1.2 Interface Security Requirements

Confidentiality: The readings of ambient sensors do not require special secrecy. Since both data and infrastructure belong to the same company, there is also no need for additional encryption for the path taken by the data after the base station. Hence a confidentiality rating of **3**.

Integrity: The correctness of the transmitted data is very important to the process. The devices therefor need to be protected against malicious access, both physical and digital. The needed integrity level is **3**.

Authenticity: Authenticity is an important security goal to correctly connect the digital values to physical machines. The required authenticity is **3**.

Non-Repudiation: The non-repudiation of messages plays no special role in this unidirectional network with only one owning party. A rating of **1** is therefor given for non-repudiation.

Key Management: It is necessary for this use case to introduce new sensors or replace old ones in a fast and simple way. The key management system must be able to easily provide the key of any new device to the respective instances. The needed key management is rated at **3**.

Quality of Connection: The wireless connection of the network is a possible target for jamming or denial of service attacks to disable the predictive maintenance process, causing financial and material damages. Real-time communication to the second is not needed. A quality of connection rating of **3** is given.

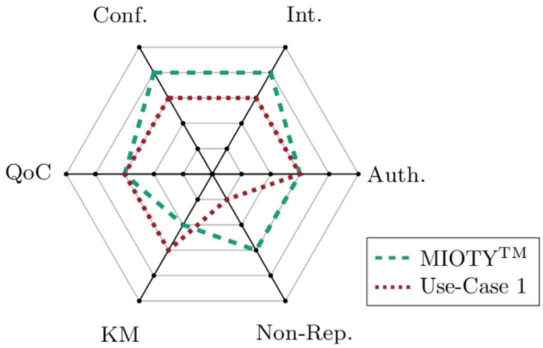


Figure 6: Security requirements of the first use-case weighted against the MIOTY™ air communication.

For interface A most requirements are satisfied with the general MIOTY security measures, as seen in Figure 6. Only the key management needs a dedicated measure to elevate the security to the required level. This is due to the fact, that key introduction and storage is not described in the standard. The other interfaces of the MIOTY™ network need to be realized in a way that satisfies the application´s security requirements.

5.1.3 Security Processes

Device Management

Device Management is simple for this use-case. New devices are registered at the central unit, where they can also be deregistered. Since the network is small with only a few Base Stations, it is feasible to distribute all keys to every Base Station.

Routing

No special routing within the MIOTY™ network is necessary, since only one Service Center and Application Center exist. The Application Center needs to forward the received data to the respective applications.

Key-Management

Since this application is not highly critical, the use of printed keys (see Section 4.2) should suffice. Application encryption is not required, since all data belongs to the manufacturer and there is no privacy in need of protection. During the initial setup the technician should scan the printed codes and enter them, together with location tags to the central unit. This should allow the Service Center to correctly distribute the keys to the Base Stations. The interface for these scanners on the central unit should be secured equally to other connections. To minimize the impact of a successful attack on a Base Station, cryptographic keys should be immediately discarded by Base Stations, if an End Point is detached.

Billing

Billing is not necessary, as the entire network is owned and operated by one company.

5.1.4 Secured System architecture

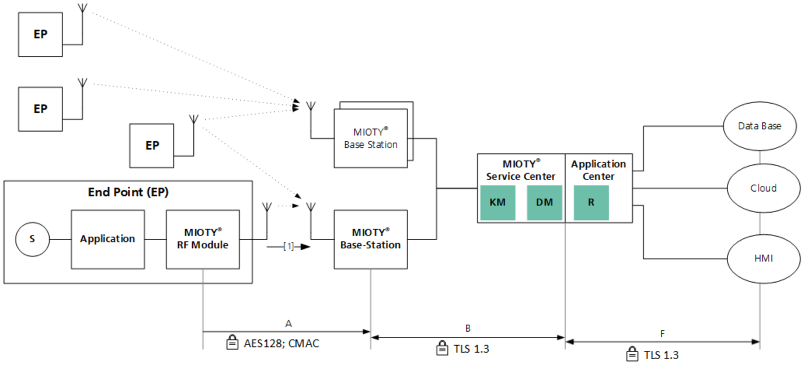


Figure 7: Recommended architecture of the first use-case

The proposed architecture is displayed in Figure 7. The slim scale of the on premise MIOTY™ network and system enables a combination of the Service Center and the Application Center in one device. The Registration Authority is also not included, as this is a closed private network. This approach simplifies the architecture and eliminates Interface C and Interface E, thus decreasing the number of security concerns and possible attack surfaces.

Assigning the tasks in this network is comparatively straightforward due to the simplicity of the use-case. Device Management is realized in the Service Center. The only Routing necessary is the routing of the data to the application, which is done by the Application Center. Key Management is also realized in the Service Center. For internal billing, the billing task could be assigned to the Application Center, but billing will not be considered going forward.

To secure the Interface B, between Base Stations and the Service Center, we propose the use of a certificate-based protocol using TLS 1.3 or higher. As neither the Service Center nor the Base Stations suffer from the harsh computational limitations of the End Devices, implementation of such security mechanisms should pose no problem. While normally out of scope of a MIOTY™ network, we will also consider **Interface F**, connecting the Application Center to the different applications, as it is part of the infrastructure in this architecture. Interface F should use, similar to Interface B, standard IP-based techniques, implementing certificates and TLS 1.3 or higher. While these technologies are not applicable to interface A, due to its constrained nature, the devices communicating over interface F can handle the computing complexity.

5.1.5 Security Guidance

This section describes measures to secure the MIOTY™ system and emphasizes important security considerations.

All MIOTY™ devices need to be compliant with the IT security rules of the company and should be audited accordingly (penetration testing). The Base Stations and backend devices should also use a secure operating system and reviewed programming libraries. All systems should be kept up-to-date by regularly installing updates to patch any vulnerabilities as fast as possible.

To keep attack surfaces small, network access to all system components should be kept to a minimum. Besides the defined interfaces, only controlled configuration and maintenance access, for firmware updates or the like, should be present. All devices should be kept secure from physical access by unauthorized persons. This protection is already partly realized, as the entire infrastructure is on the manufacturer´s premises.

End Points

End Points should be affixed to their locations in such a way, that physical manipulation is made difficult. Removing or relocating them should be made impossible without great effort and interfaces, such as debug interfaces, should be inaccessible. It should also be made impossible for passerby to read the printed keys. This can be achieved by i.e. removing the labels or mounting the devices in a way, which makes the labels unreadable.

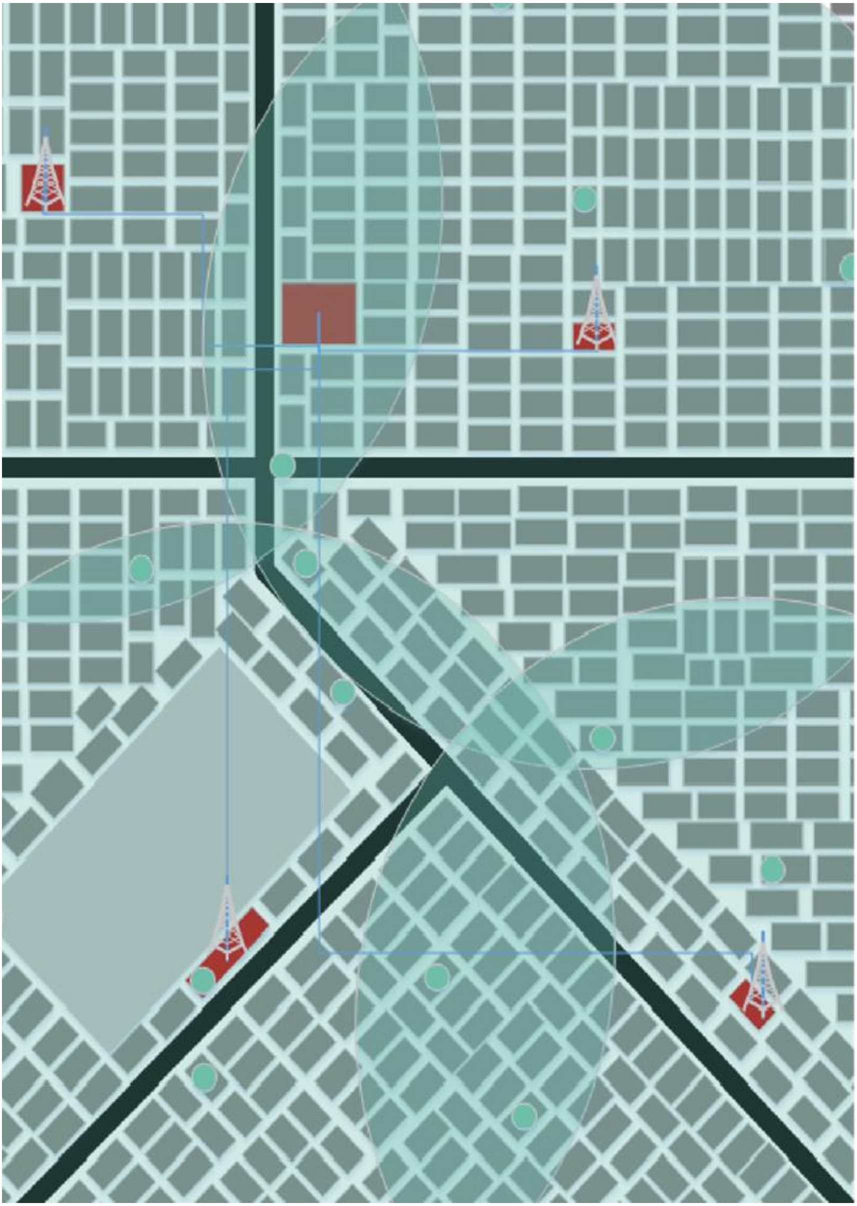
Base Stations

Base Stations represent a worthwhile target for attackers, as they contain numerous keys and the unencrypted data. Physical access to the Base Stations should therefore be restricted. Network-access over the maintenance network should also be sufficiently secured.

Service Center/Application Center

The Service Center/Application Center is the central piece of the MIOTY™ network and therefore should be paid special attention to. Physical access to this device should for that reason be restricted to necessary personnel. Network-access should also be thoroughly secured. The ways to access the device which should be kept in mind include the MIOTY™ interfaces, maintenance access, the connection for the key scanners and all other connection capabilities, e.g. USB slots.

5.2 Use-Case 2: Public MIOTY™ network for Smart City



5.2.1 Use-Case Description/Story

Type	Public	Infrastructure, partly publicly accessible
Area	Large	City area
Customers	Several	Utility company and others
Roaming	Yes	End Points on vehicles
End Points	Z (and A)	Depends on the customers' needs

An electric **utility company** wants to better monitor their facilities. Therefor they want to gather data from both inside and outside of the buildings. Sensors inside the facilities should monitor transformers and other parts of their grid system to detect and prevent arising power surges. On the outside, weather conditions, such as sunshine, wind or rainfall, should be detected to gauge coming changes in energy generation and consumption. This architecture will be implemented as a MIOTY™ network. The wireless sensor nodes are installed at the facilities by in-house technicians; partly indoors, for grid sensors, and partly outdoors, for environmental sensors. Some sensors will also be fitted on vehicles, which necessitates a roaming mechanism. Those unidirectional sensors periodically transmit their sensor readings to the MIOTY™ base stations, which are integrated in selected facilities, positioned for maximum coverage within the city. After receiving the data packages from the sensors, the base station sends them to a local data center. This data center, which also belongs to the electric utility company, analyses the data. The resulting changes to the grid are distributed via the control system already in place.

The company additionally opens this city-spanning network to other companies, acting as a **network provider**, in a second step. This enables **customers** to gather data with their own MIOTY™ sensors and access the data without having to set up an entire infrastructure. The utility company does not control the End Points in this case, it only relays the data to the respective companies.

Other companies register their own nodes, which can be mobile across the city area, with the provider. Their transmitted data packages will then be relayed to the data center by the base stations. There, the owning company is given access to their data. A possible billing model is a registration fee and a fee based on the transmitted data volume. Bi-directional communication will not be offered initially, but the process of relaying messages over the infrastructure to the nodes might be implemented in the future.

5.2.2 Interface Security Requirements

Confidentiality: While the environmental sensor data does not require dedicated protection, the facility data should be kept secret. The electricity provider´s data never leaves the owned network, so later encryption is not necessarily required for them. Customers however should additionally encrypt their data to protect it against access from within the infrastructure provider. Hence a confidentiality rating of **4**.

Integrity: The data integrity plays an important role for the process. The spread over a wide city area also makes the physical integrity of the devices a concern, more so since several devices are located outdoors. It is additionally not possible to compensate anomalous sensor readings with the readings of neighboring sensors, as the distance between them is too large. The needed integrity level is **4**.

Authenticity: The authenticity of the data is very important for the company´s application. When providing their MIOTY™ network as an infrastructure for other parties, authenticity becomes even more important. The required authenticity is **3**.

Non-Repudiation: When employing a billing system with a per-message cost, it is important to ensure that both parties, the provider and the customers, can neither deny sent messages nor claim additional transmissions. A rating of **3** is therefor given for non-repudiation.

Key Management: The addition of new End Points should be a simple process. The devices of potentially several distinct customers makes the easy and secure introduction of new keys into the network important. Additionally, customers might need a way to introduce application keys beforehand. The handoff of a mobile node from one base station to another also needs to be handled properly. The required key management is rated at **4**.

Quality of Connection: The quality of connection is important for the transmitted data. The wide distribution of the nodes makes it hard to disrupt several transmissions at once. While most applications in this use-case do not need real-time communication, as the serve to aggregate data over time, some events could require very fast transmission (e.g. recognizing and compensating power surges). A quality of connection rating of **3** is given.

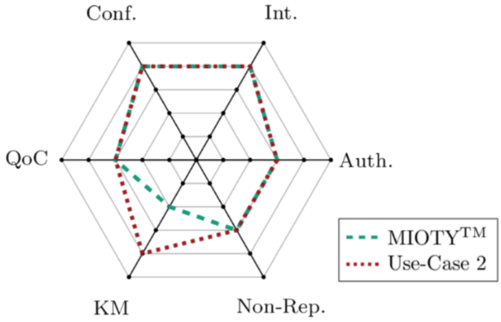


Figure 8: Security requirements of the second use-case

Figure 8 shows, how interface A satisfies the stated requirements. The field of key management again needs additional protective effort to secure the displayed MIOTY™ system. This will be realized with dedicated key introduction and storage measures. All other interfaces should also be implemented with these requirements in mind.

Since most categories are fulfilled exactly, there is a need to keep a close eye on them. If any requirements are tightened, e.g. due to changes in the application, it is necessary to evaluate the interfaces again.

5.2.3 Architectural Design Pattern

When deciding on the architecture, a decision needs to be made, if the dataflow from the Service Center to the Application Centers should be done via pushing or polling. This decision depends on several factors, most notably the scale and focus of the network. We will lay out both approaches and then provide guidance for the decision.

Push

In a push architecture, a mapping of End Points to customers is stored on the Service Center, which send incoming data packages to their respective Application Center. While the data content is not open to other parties in this case, application encryption should still be employed to encrypt the data against the network provider.

This method increases the performance of the network as no long storage of packets is necessary.

Poll

In the second approach, the Service Center makes all data packages available to every Application Center in the network. It is then the responsibility of the Application Centers to regularly poll the Service Center data and filter their packages out. Customers can not access each other’s data due to the Application encryption.

This enhances the privacy of the customers, as the Service Center does not hold the mapping of End Points to Application Centers.

Decision Guidance

Both approaches come with their advantages and drawbacks.

Push performs better in bigger networks, as the data does not need to be stored until all Application Centers have requested it and each Application Center has to only process its own data, not the entire data volume of the network.

Network analysis or security breaches of the Service Center however can allow malicious parties to deduce a mapping of End Points to their owners, which can have privacy implications.

With polling, the connection of End Points and customers can only be found on the Service Center during the registration of new End Points. In case of errors or attacks it is hence not possible to leak a significant amount of End Point to customer relations. Surveillance of Interface E also gives no indicators, which End Points belong to which customer, as every Application Center requests the same data.

This protection has several costs. Since each customer can view all data, application encryption should be mandatory and unencrypted meta-data should be kept at a minimum (End Point ID, timestamp). Application Centers need more capacities to process and filter the entire data of the MIOTY™ network. Depending on the network’s scale, the polling process might not be feasible.

For this use-case we will exemplify a push architecture, as the network is sufficiently large. The network provider might also want to provide additional meta data to the customers, e.g. signal strength to determine suitable Base Stations, which would lead to complications in a poll architecture.

5.2.4 Security Processes

Device Management

The registration and deregistration of devices is done by the customer. They can send the IDs of devices to the Service Center via their Application

Center to add or remove End Points. To distribute the respective keys as little as possible, an interface should be provided for customers to select the Base Station cells necessary for the End Point.

Key-Management

The introduction of keys is more complex compared to the previous use-case. Two general options, how keys are brought into the network, are conceivable. Either a central key server, maintained by the MIOTY™ alliance, holds all the keys, or customers can introduce them. The involvement of several parties (network provider, customers) makes application encryption a must. To ensure the secrecy of the application key, and to increase usability, we therefore consider customer-introduced keys for this use-case. Customers thus can decide individually, if they want to use printed keys or self-generated keys for network and application encryption. Both keys are entered into the Application Center, with the network key being transmitted to the Service Center. The Service Center then distributes the keys to the chosen Base Stations.

Routing

Routing is done by the Service Center, which distributes the packages to their respective Application centers.

Billing

The last security relevant process is the billing procedure. If the network provider charges a fixed amount, it is not necessary to include the billing process into the network. We assume a per-message billing, which necessitates assigning the billing task to a unit in the network. To minimize the risk of leaking personal information, the association of devices with the customer information should be done in only one, secured environment. This instance, the Trust Center, is described in the next section.

5.2.5 Secured System architecture

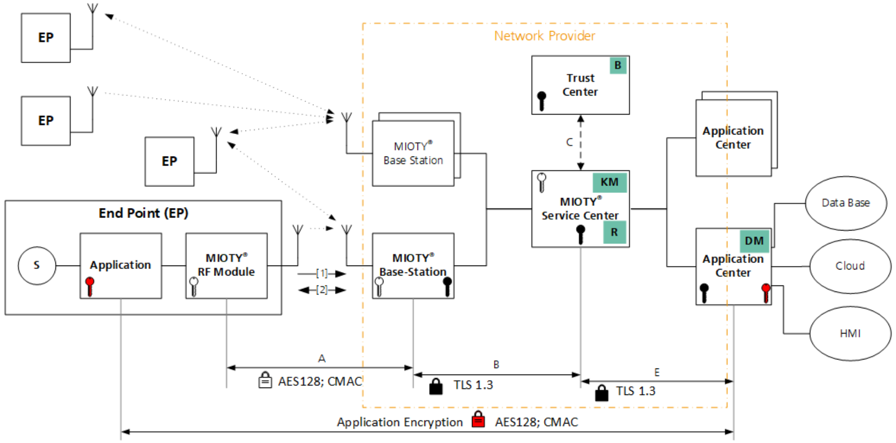


Figure 9: Recommended architecture of the second use-case

The proposed architecture for this use-case can be seen in Figure 9. In this architecture, each network unit is represented by a distinct device. The Registration Authority is not part of the network. A new unit, the Trust Center, has been added to fulfill partly similar responsibilities. The functionality of the Application Centers are realized on customer's devices to ensure the confidentiality of the application key. For this, they are provided with a software. After installation, the software then enables the customer to store their application key(s), register new End Points at the Service Center and receive their data.

The trust center exclusively holds the personal information of customers and their owned devices. To best protect the privacy of the customers and ensure compliance with the DSGVO, this information is held nowhere else in the network. The Service Center regularly sends the Trust Center information on which End Point has sent how many messages. The trust Center is then able to match the device IDs to the customers and bill them accordingly.

The task blocks are distributed according to the aforementioned processes. The introduction and removal of End Points to and from the network is done by the customers in the Application Center. Routing is done by the Service Center. Key Management is also realized by the Service Center, based on the customer's chosen Base Stations. Billing, as explained, is done by the Trust Center.

Interface A and the application encryption are implemented as described in the standard. Interfaces B, C and E are again secured between Base Stations and the Service Center, we propose the use of a certificate-based protocol using TLS 1.3. The certificates can either be generated by an external root authority, or self-signed by creating a root authority in the trust center.

5.2.6 Security guidance

Analogous to the first use-case, all MIOTY™ devices need to be compliant with the IT security rules of the company and should be audited accordingly (penetration testing). The Base Stations and backend devices should also use a secure operating system and reviewed programming libraries. All systems should be kept up-to-date by regularly installing updates to patch any vulnerabilities as fast as possible.

To keep attack surfaces small, network access to all system components should be kept to a minimum. Besides the defined interfaces, only controlled configuration and maintenance access should be present to enable firmware updates or the like. All devices should be kept as safe from physical access by unauthorized persons as possible.

1) The utility company's **End Points** should again be affixed to their locations in such a way, that physical manipulation is made difficult. Removing or relocating them should be made impossible without great effort and interfaces, such as USB-ports, should be inaccessible. It should also be made impossible for passerby to read the printed keys, if present. The security

of customer’s **End Points** lies in the respective customer’s responsibility, but it is advisable to publish guidelines similar to this one for customers.

2) **Base Stations** represent a worthwhile target for attackers, as they contain numerous keys. Physical access to the Base Stations should therefore be restricted. Network-access over the maintenance network should also be sufficiently secured. If it is not possible to set up all Base Stations in secure buildings to ensure coverage over the city area, additional security measures need to be taken. Emergency shutdowns in case of an intrusion as well as hard disk encryption and trusted platform modules (TPM) should be utilized to protect sensible data, especially the certificates, in case of theft of the Base Station.

3) The **Service Center** is the central piece of the MIOTY™ network and therefore should be paid special attention to. Physical access to this device should for that reason be restricted to necessary personnel. Network-access should also be thoroughly secured. The ways to access the device which should be kept in mind include the MIOTY™ interfaces, maintenance access, the connection for the key scanners and all other connection capabilities, e.g. USB slots.

4) The **Trust Center** realizes highly critical security mechanisms and therefore needs to be secured the same way as the Service Center. Due to the presence of personal information it is important to keep the number of authorized personnel as small as possible.

5) **Application Centers** are installed on customer devices. This makes the integrity of the device hard to maintain for the network provider. The Application Center software should thus employ checks of its correct installation and its communication should be monitored closely for anomalies by the Service Center. Updates should be regularly deployed and their installation required to patch vulnerabilities. Additionally, a security guide for the customers on how to protect their computer containing the Application Center could be published to increase security on their side.

6 Final Statement

Security is an important aspect of a system’s architecture, especially for critical infrastructure. Since the ETSI standard provide only basic measures to secure an entire communication infrastructure, additional measures were defined for MIOTY™. How these security measures and subsequent security processes can be implemented was shown in two use-cases.

These two use-cases represent both ends in terms of the complexity of MIOTY™ infrastructures. We thus gave reference implementations and models for security measures, from which the security design of real-life applications can be deduced. Use-cases, whose complexity lies between the two stated use-cases, require a mix of those security measures depending on the application. It is also important to re-evaluate the security requirements of an MIOTY™ system, should its circumstances or applications change. Such security solutions and concepts can be provided by the Fraunhofer IIS.

References

[1] IBM Institute for Business Value, “Internet of threats: Securing the Internet of Things for industrial and utility companies - BenchmarkInsights@IBV,” *BenchmarkInsights@IBV,* https://public.dhe.ibm.com/common/ssi/ecm/62/en/62013962usen/internet_of_threats_benchmarkinsightsibv.pdf, 2018.

[2] T. Scheible, *IT-Sicherheit Grundlagen: Schutzziele.* [Online] Available: https://cyber-security-lab.de/it-sicherheit-grundlagen-schutzziele/.

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI - Cyber-Sicherheit.* [Online] Available: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html. Accessed on: Sep. 29 2016.

[4] C. Eckert, *IT-Sicherheit: Konzepte - Verfahren - Protokolle,* 7th ed. München: Oldenbourg, 2012.

[5] *TS 103 357 - V1.1.1 - Short Range Devices; Low Throughput Networks (LTN); Protocols for radio interface A*, 2018.

[6] *TS 103 358 - V1.1.1 - Short Range Devices; Low Throughput Networks (LTN) Architecture; LTN Architecture*, 2018.

[7] *Announcing the advanced encryption standard (AES).*, 2001.

Glossary

Abbr.	Term	Description
AC	Application Center	Functional unit
AES	Advanced Encryption Standard	Cryptographic algorithm
Auth.	Authenticity	Protection goal
B	Billing	Task block
BS	Base Station	Functional unit
CC	Common Criteria	IT security standard
CMAC	cypher-based Message Authentication Code	Cryptographic signature
Conf.	Confidentiality	Protection goal
CPS	Cyber-physical system	Small IoT device
DM	Device management	Task block
EC	Elliptic curve	Cryptographic algorithm
EP	End Point	Functional unit
ETSI	European Telecommunications Standards Institute	Standards-defining organization
Int.	Integrity	Protection goal
IoT	Internet of Things	Conglomerate of interconnected devices

Abbr.	Term	Description
KM	Key management	Protection goal and task block
LPWAN	Low-power wide-area network	Network category
LTN	Low-throughput network	Network category
Non-Rep.	Non-repudiation	Protection goal
R	Routing	Task block
RA	Registration Authority	Functional unit
RSA	Rivest–Shamir–Adleman	Cryptographic algorithm
QoC	Quality of Connection	Protection goal
SC	Service Center	Functional unit
TPM	Trusted Platform Module	Secure hardware module