Applicability of LTE Public Key Infrastructure based device authentication in Industrial Plants

Apala Ray*†, Johan Åkerberg*†, Mats Björkman†, Rolf Blom ‡, and Mikael Gidlund§
*ABB AB; Corporate Research
†Mälardalen University; School of Innovation, Design, and Technology
‡Swedish Institute of Computer Science
§Mid Sweden University

***Abstract*—The security in industrial automation domain using cryptography mechansims is being discussed in both industry and academia. An efficient key management system is required to support cryptography for both symmetric key and public/private key encryption. The key managment should ensure that the device is verified before distributing the initial key parameters to devices. The software/firmware used in the device comes from manufacturers, therefore the initial authenticity of the device can be easily verified with the help of manufacturers. Mobile telecommunication is an industrial segment where wireless devices are being used for a long time and the security of the wireless device management has been considered through a standard driven approach. Therefore, it is interesting to analyse the security authentication mechanisms used in mobile communication, specified in Long-Term-Evolution (LTE) standard. This paper analyses the initial device authentication using public key infrastructure in LTE standard, and discusses if, where and how the studied solutions can be tailored for device authenticity verification in industrial plant automation systems.**

***Index Terms*—Industrial Automation, Mobile telecommunication security, Gap Analysis, Public-Key Infrastructure**

I. Introduction

Industrial control systems, which include Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC), are typically used in process industries like pulp and paper, water and wastewater, food and beverages, mining etc. Since the last decade, the severity of cyber threats towards existing and future industrial systems has increased the security awareness in the industrial automation domain. The level of threat has increased as the industrial systems are being interconnected with the communication networks. The integration of wireless devices with industrial automation systems has also raised the device security challenges. The state of the art in industrial communication system security research is well captured in [1]. This provides a good overview of the state of industrial communication security. The National Institute of Standards and Technology (NIST) has provided recommendations on how to establish secure industrial control systems in [2]. An efficient key management is required to support cryptography. However, the cryptography and the key management cannot assure communication security if the device is not verified as trusted before the key distribution. The manufacturers provide the software/firmware for the device. From the manufacturing phase to the industrial plant oeprations, devices are handled by different personnel based on the roles. Therefore, there is a need to verify whether the device has been compromised since the time manufacturer has released the product/device. This can be done with the help of manufacturers and the rest of the key management can be done without the manufacturers once the device has been considered as trusted. The secure management of certificates in industrial sectors has been discussed in [3]. The challenges of having a certificate management in industrial control system has been well discussed in this paper. In [4], the mechanism to enable *plug and work* of devices in industrial environment reusing the internet of things approach has been discussed and conclusion was that the best method to bootstrap initial credentials can be done through manufacturer provided certificate and with a secure device identifier based on 802.1AR [5]. This imposes a tight constraint on manufacturers to provide devices with secure device identity. This also might increase the manufacturing effort and costs as the credential generation will be included during the production process.

Mobile telecommunication is an industrial segment where the wireless devices are being used for a long time. In the mobile telecommunication domain the security of wireless device management has been considered through a standard driven approach. In addition to this, the mobile communication domain has some similarities with industrial plants. For example, mobile telecommunication domain also involves embedded devices. Some of the devices, such as, home base stations, similar to field devices may come from different vendors etc. The fourth generation of mobile telecommunication technology, known as 4G, has been evolved and based on this technology 3GPP (Third Generation Partnership Project) LTE standard have been proposed. The new 3GPP LTE system is known as Evolved Packet System (EPS). The technical specifications on 3GPP networks system security architecture, authentication framework and Security of Home Node have been produced by the 3rd Generation Partnership Project (3GPP) [6]–[8]. In [9] the LTE security is explained in detail.

Motivation of this paper: The device authentication using certificates and universal subscriber module has been well discussed in LTE standard. Therefore, it will be interesting to learn how the device authentication is managed in LTE and if some of those approaches can be tailored for industrial automation plant. In [10], three different security scenarios

from mobile telecommunications domain and their deployment aspects have been assessed. The SIM card or certificate based solutions in mobile telecommunication industry require a lot of engineering either in manufacturer premises or in the industrial plant itself. A SIM card based solution requires individual mapping between the SIM card and the devices, which adds extra time consuming steps in the device configuration. In this work, we do not intend to one-to-one map every elements in the LTE standard with the industrial automation, rather we focus on how device authentication is managed in network elements, such as, base station, home base stations and relay nodes.

Contribution of this paper: The applicability assessment of public key infrastructure used in initial device authentication in LTE will help to assess how to use a public key infrastructure for initial device authentication in industrial plants. In this paper, we review the device authentication using public key infrastructure in LTE standard and understand in which area of industrial plants this can be applied and how it can be applied. Then we propose a concept on initial device authenticity verification for industrial plants.

In this paper, section 2 presents an overview of public key infrastructure usage in LTE network elements. Section 3 assesses the LTE public key infrastructure used for authentication from industrial plant point-of-view. Based on this assessment, a device authenticity verification using public key infrastructure for industrial plant is presented in section 4. Finally, the conclusions and future works are outlined in section 5.

II. Device authentication using public key infrastructure of LTE

In this section we present an overview of device authentication using public key infrastructure in base station, home base station and relay nodes. The manufacturers and the operators are two major roles involved in the LTE public key infrastructure. We will study how these roles are involved and how devices are authenticated based on this public key infrastructure.

A. Base Station Authentication

A base station is a network element which is responsible for radio transmission and reception in one or more cells to or from the user equipment. The base station in LTE is known as evolved base stations and denoted as eNodeB or eNB. Based on the coverage area, base stations can be categorized by (1) Macro cell which is wide area base station, (2) Micro cell which is medium range base station, (3) Pico cell which is local area base station and (4) Femto cell which is home base station. The base station discussed in this section is macro base station and an high level overview of authentication is shown in Figure 1. The security of base station is important and as per 3GPP standard, the base station should be authenticated by an operator based PKI. However, the software loaded in the base station should be authorized by both manufacturers and operators as manufacturers provide software for base station and operators set configuration parameters for those. In most of the cases, the base stations are placed in a physically secure place, however, in certain scenarios, the base station can also be located in a location which is not physically secured. The authentication for the base station to connect with the backhaul link of the operator network is based on the public key infrastructure with IKEv2 certificate based authentication. The enrolment of the base station requires both the manufacturers and the operators to have their own public key infrastructure with certification authority. The base station authenticates itself to the operator network during the enrolment procedure using a manufacturer provided public/private key pair installed in the base station before enrolment, a certificate on the base station identity and the public key signed by a manufacturer certification authority. Therefore, when the operators buy base stations from manufactures, they also receive the unique identity and the public key of the devices signed by a manufactures certification authority. Operators also need to install the root certificate of the manufacturer. This should be done in a trusted way, so that the certificates of the authorized manufacturers only have been installed in operator network.

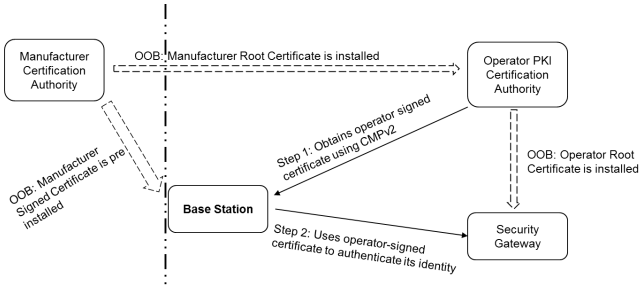

Figure 1. High Level View on Base Station Authentication

The base station authenticates its manufacture provided identity to the certification authority of operator and requests an operator signed certificate. The certification authority of operator generates the certificate and sends it to the base station. After authenticating the operator network certificate, the base station installs this certificate and then uses this operator-signed certificate to authenticate its identity to the security gateway of the operator network. The authentication of the operator network by the base station during enrolment would require either provisioning of the operator root certificate in the factory, or the installation of the operator root certificate on-site at installation time or some complex cross-signing relations between vendors and operators. Refer [9] and [8], for a comprehensive overview of certificate enrolment for base station.

B. Home Base Station Authentication

The home base station is a home version of base station with small-area or indoor coverage. The coverage of home base station is comparable to a wireless local area network (WLAN) access point. These home base stations are deployed within customer premises for efficient spectrum usage and customer specific deployments. These devices are sold in large

numbers and deployed in home environments. The security of these devices is important as they are deployed in customer premises. A customer can deploy home base station on a contract with the mobile operator and the home base station should be authenticated with the security gateway which controls the access to the core network of operators. The public key infrastructure is chosen for the authentication of home base stations. The authentication protocol IKEv2 (Internet Key Exchange) is used between the home base station and the security gateway. The mutual authentication between the home base station and the security gateway is based on certificates as shown in Figure 2. Each home base station will have a private/public key pair and a certificate binding the identity and other properties to the public key. The device certificate can be issued by the operator, manufacturer or by another party trusted by the operator. The advantage of using manufacturer provided device certificate is that the operator is not required to deploy a huge public key infrastructure for large number of home base stations. However, the security gateway will have the certificate from operator. The home base station will authenticate itself to the security gateway with its unique identity. The root certificate of the operator shall be pre-provisioned to the home base station.

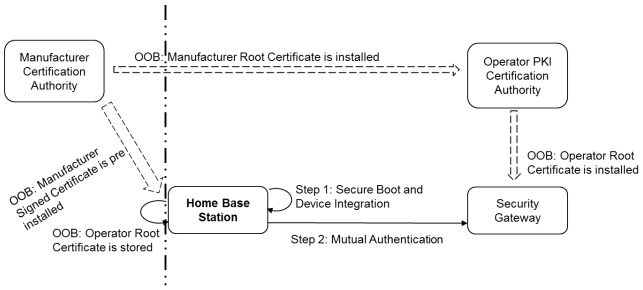

Figure 2. High Level View on Home Base Station Authentication

The security of home base station depends on a *Trusted Environment*. The *trusted environment* is the logical entity with a built-in root of trust. On power-up of the home base station or after hard reset, first the *trusted environment* itself is checked for integrity using the root of trust. Once the *trusted environment* has been started successfully, it proceeds to verify other software components of the home base station. The *trusted environment* also stores sensitive parameters which are used during operation of the home base station. The access to the private key which is used for device authentication is only given based on a positive device integrity result. In this scenario, the operator is not alone responsible for the home base station, as the manufacturer is responsible for device integrity when signing and providing the certificate.

Certain deployment scenarios require the separate authentication for the hosting party. Hosting party is the owner of the home base station who deploys the home base station in premises. This authentication is optional and is always preceded by a successful device authentication. The hosting party module stores the hosting party identity and the secret. This module is a removable token which is not physically bound to the home base station. The hosting party authentication uses the Authentication and Key Agreement (AKA) mechanism and the authentication is based on a permanent shared secret stored in the universal subscriber identity module (USIM) and the home location register. Refer [9] and [7], for a comprehensive overview of security of base station.

C. Relay Node Authentication

Relay nodes are base stations with added functionalities which enable operators to improve and extend the coverage area. Relay nodes are connected to the core network through the wireless link. Relay node can play a dual role, such as, the role of a user equipment and the role of a base station. When the relay node plays the role of a user equipment, the authentication is done using universal subscriber identity module (USIM). When a relay node connects to an operator network for the first time, it may follow the certificate enrolment mechanism similar to the base station and the home base station. To ensure mutual authentication between the USIM and relay node, either certificate or pre-shared keys on both sides can be used. Refer [9] and [11], for a comprehensive overview of relay node security.

III. Discussion on applicability of device authentication in industrial automation

This section summarizes the applicability of device authentication concepts in industrial automation domain as shown in Figure 3. In base station deployment, the authentication of the base station device is done by the public key infrastructure of the operator. However, to enrol the base station in the public key infrastructure of the operator, the manufacturer provided certificate is used. Manufacturer of the base station should generate the public/private key pair and sign the public key and the device identity with the certificate authority from the manufacturer. The operator also needs to install the root certificate of the manufacturer, so that it can use that certificate for verification. This needs an out-of-band trusted channel between the manufacturer and the operator. During the operational phase, the operator may need to update the public/private key pair of the base station. This can be done with the operator certificate. Therefore, the manufacture provided public/private key pair and the certificate may not be required once the device is enrolled in the operator network.

The base station can receive the certificate from operator when it is connected with the operator network. In industrial plant, there is an option of using configuration tool during commissioning phase. Therefore, the certificate from the operator can be put in a trusted way to the device using configuration tool once the device is authenticated using the manufacturer provided certificate. The unique identity and the public key of the device is used during the enrolment of the base station. The base station also provides a proof of possession for the private key which belongs to the public key to be certified.

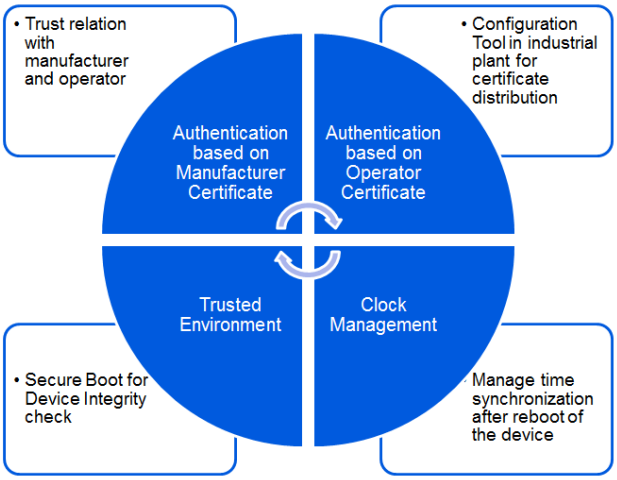

Figure 3. Summary of device authentication concepts applicability

The security of home base station is little different than the security of base station as the device authentication is done using the manufacturer provided certificate. This requires that the manufacturers need to pre-provision some data into the home base station. Therefore, the manufacturers and the operators need to trust each other from organization point of view. If manufacturers do not have a certification authority to sign the device certificate and used third party certification authority, then the operators also need to trust that third party. The root certificate which is used for the validation of the certificate of home base station need to be handed to each operator who are supporting the home base station. As in home base station, the certificate from manufacturers are used for authentication, the revocation of the certificates also need to be done from the manufacturers. This implies that the manufacturers will also be involved during the operational phase of home base station regarding certification revocation. It also requires that if the device is compromised or broken, then the device needs to be sent to the manufacturing unit for managing keys and certificates. Therefore the device management lifecycle requires a chain of trust till production. In industrial plants, there are generally different devices installed from different manufacturers and they might have different computation and functional capabilities. Hence, in our proposed device authentication framework we can limit the initial device authentication to the manufacturer provided certificate. Once the operator/plant has verified that the device is not tampered since it has produced from the manufacturing unit, the key management mechanism specific to the plant can be used.

The managing of clock inside the home base station is another aspect for certificate management. If the home base station does not have any continuous clock, then the current time should be saved in *trusted environment*. On subsequent power up, the home base station can use the last saved time directly. However, the operator needs to take care the validity period of the network side certificate. In industrial plant, if the certificate management is used during the operation phase of the plant, then it is also required to investigate the certificate validity times. If a validity time is set for a certificate, then how to update when the certificate expires for the device, is also an issue.

IV. Device Authenticity Verification framework for industrial automation - Overview

In this section, based on the applicability assessment of the LTE public infrastructure based authentication, we present a concept of device authenticity verification in industrial plants. This device authenticity verification is done before the devices are deployed within the plant environment. The role of the components which are used in the public key based device authentication are described along with their assumptions. The sequence of workflow phases and the involvement of the user are also described.

A. Objective of the Authenticity Verification Framework

The objective of this framework is to ensure that the devices which will be deployed inside the plant have not been tampered or compromised before they arrive inside the plant premise. This implies that the plant is required to have an infrastructure where devices can be verified. In industrial plants, generally configuration tools or commissioning devices are used to configure the device parameters. However, before the device is configured using commissioning devices, it is required to know the parameters on which the device can be verified. In our framework, we consider that the industrial plant is physically protected and only employees with valid approval are allowed to enter in the plant. This framework should be able to satisfy the following two goals, which we have identified as the major objectives to get fulfilled.

- The plant system should be able to verify the identity of the device which has been shipped from manufacturing unit.
- The plant system should be able to detect if the device has been tampered during the shipment.

B. System Components

The components which are involved in this verification framework are presented below.

- **Manufacturer of the Device:** Manufacturers produce the devices and install firmware in the device. The manufacturer is assumed to be trusted component in the framework.
- **Certificate Authority of Manufacturer:** The certificate authority is responsible for managing the initial certificate of a device. It is assumed that this certificate authority of manufacturer cannot be compromised.
- **Plant Security Manager:** The plant security manager is responsible for managing the security parameters required for the device communication, and it monitors the state of the security of the devices in a running plant. In our framework scope we have assumed that this security management component cannot be compromised.

- **Device:** This is the component which is verified before gaining access in the industrial network.
- **Commissioning Engineer:** This person is authorized to configure or commission devices prior to the operational phases or during maintenance phase.

C. Proposed Framework Concept

In this proposed concept we use the concept of secure boot-up and trust anchoring through manufacturer provided certificate as used in LTE standard. In this approach, the manufacturers need to share their root certificate with the plant system. The plant system uses this root certificate to verify the device certificate. When the device comes with the manufacturer provided certificate, then the initial authentication of device is simple as the identity of the device will be in the certificate. In addition to it, the device contains a secure and trusted environment which is used to install manufacturer credentials. However, once the operator/plant has verified that the device is not tampered since it has produced from the manufacturing unit, the key management mechanism specific to the plant can be used.

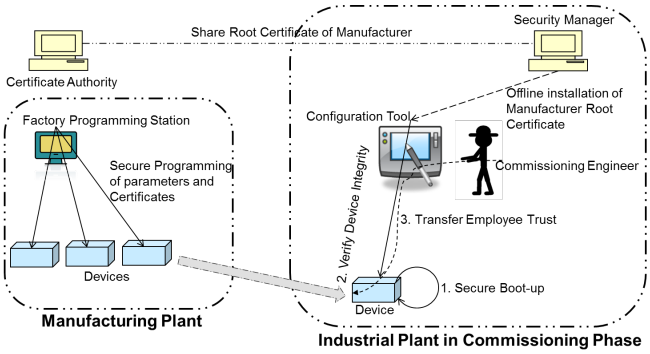

Figure 4. Overview of Proposed Device Authenticity Verification

Figure 4 presents an overview of the device authenticity verification using a secure boot-up and the certificate verification. The device contains a secure and trusted environment which is used to install manufacturer credentials. The trusted environment contains a 'root of trust' which stores the private key and the identity of the device. It also provides trusted functions and is used for secure boot process. Once the device is brought inside the industrial plant and powered up, the device checks its integrity using the root of trust. The verification of trusted environment follows the verification method used in LTE specification. Once the device passes the device integrity check, then it provides its manufacturer provided identity to the configuration tool or the commissioning device in the industrial plant. The security management component in industrial plant has already installed the certificate of manufacture. The security management component transfer this information to the configuration tool or the commissioning device for initial device authentication.

The message flow for an initial device authentication in an industrial plant is shown in Figure 5. The device generates the initial authentication request with its identity and signs the request with the manufacture provided private key. The configuration tool verifies the signature of the device identity. Once the verification is done, the configuration tool can verify the integrity of the device as the private key of the device in the trusted environment can be accessed only after a successful secure boot-up. Once the authenticity of the device has verified and it is found that the device has not been tampered since its production time, the concept of initial trust bootstrapping from employee trust [12] can be used for device deployment.

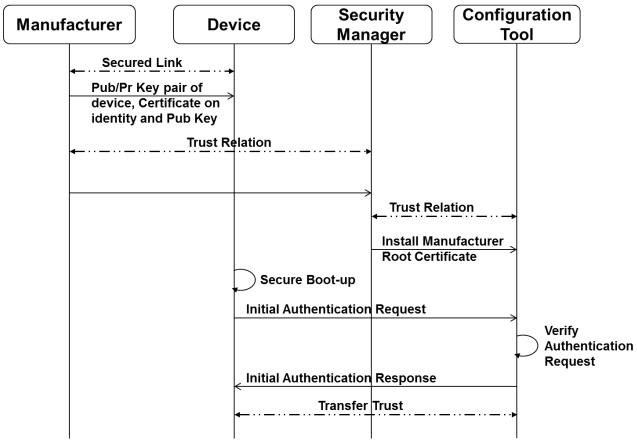

Figure 5. Message flow during initial device authentication

D. Discussion on the proposed initial authentication of the device

In this section, we will discuss whether the two objectives for the proposed concept of the initial authentication of the device are satisfied.

- The first objective is to verify the manufacturer provided identity. The configuration/commissioning tool used in industrial automation plant verifies the device certificate with the help of root certificate of manufacturer. The device certificate contains the manufacturer provided device identity which is signed by the manufacturer certificate authority.
- The second objective is to ensure that the devices which will be deployed inside the plant have not been tampered or compromised before they arrive inside the plant premise. The secure boot in the device provides capability of software and configuration integrity checking and authentication. Before the software is allowed to run on the processor, the firmware image is checked to make sure that it has not been altered or tampered with. The hash values of the firmware itself is signed with the private key of manufacturer and the public key is given in the device as part of the hardware root of trust. Therefore, if the firmware is modified or tampered with, then the device will not be able to get the private key of the device itself which is stored inside the trusted environment.

Therefore, the configuration/commissioning tool can verify the authenticity of the device, when the device sends the initial

authentication request signing with the private key of itself. The root certificate of the manufacturers is already transferred by an out-of-band channel to the plant security management component. Therefore, if any attacker tampers the device before it reaches the industrial plant premises, this can be easily detected. In addition to it, when the authenticity of the device is verified using the configuration tool, the employee can commission other parameters and transfer the trust of the employee itself. Later, the security management of the device can be done as per the security policy in the plant. In this initial authentication of the device, the integrity of the device firmware is checked with the help of manufacturer provided certificate.

Challenges: This proposed initial device verification framework is meant for future industrial devices. The automation plant should procure the devices from manufacturer where the manufacturers provide the device certificates along with trusted environment in the device. If the manufacturers are not providing the device certificate and the secure trusted environment then this framework cannot be used. In this framework, the industrial plant needs to have an out-of-band channel with manufacturers to receive the root certificate of manufacturer. In industrial plant, there might be devices from different manufacturers. This out-of-band channel with manufacturer to receive the root certificate should be managed carefully by the security management component in industrial automation plant. The devices also should be able to support secure boot process for this framework. In mobile telecommunication also there are devices that come from different vendors, but the devices follow the same set of standards. This is not the similar situation for industrial plants. Therefore, to accommodate some industrial devices which do not have any processing capabilities in secured framework is a real challenge in industrial automation plant.

V. Conclusions and Future Work

In this paper, we have explored the authentication of base stations, home base stations and relay nodes in mobile telecommunication industry. The authentication in LTE standard for mobile telecommunication industry is based on certificates or universal subscriber module. In this work we focus on the LTE public key infrastructure based device authentication mechanisms using certificates and secure environment. From the discussion, we found that the security of base stations and home base stations in mobile telecommunication depend on the secure provisioning of parameters in the secured environment from the manufacturing plant for telecommunication equipment. This concept is used in our proposed initial device authentication workflow as it is required to understand how and on what parameters the device can be considered as trusted. The manufacturer is the provider of the software in devices, therefore it will be useful to verify with manufacturers' certificate whether the device has been tampered with, since production of the device. The use of Trusted Environment of devices for device integrity validation is interesting area to consider as we also propose the initial device authentication once the secured boot-up happens through a trusted environment. Our proposed initial device authentication is for future industrial devices and require that the device should be provided with trusted environment and manufacturer provided certificates. Considering the heterogeneous characteristics of industrial plants, the devices may come from different manufacturers with different computation and functional capabilities. In mobile telecommunication also there are devices that come from different vendors, but that all follow the same set of standards. It will be beneficial for industrial plant security management if future industrial plant devices could also follow a set of standards. In our next work, we plan to explore the contact-less subscriber identity module cards standardized for M2M (machine-to-machine) applications. These could feasibly be installed in all new industrial devices, protecting new and future devices. However, this will not work for the installed base.

Acknowledgment

This work has been supported by the Swedish Knowledge Foundation (KKS) through ITS-EASY, Embedded Software and Systems Industrial Research School, affiliated with the School of Innovation, Design and Engineering (IDT) at Mälardalen University (MDH, Västerås, Sweden) as well as by the ABB Communication Research Area. This work is also partially funded by SSpiia project supported by Vinnova.

References

[1] M. Krotofil and D. Gollmann, "Industrial control systems security: What is happening?" in *Industrial Informatics (INDIN), 2013 11th IEEE International Conference on*, July 2013, pp. 670–675.

[2] K. A. Stouffer, J. J. A. Falco, and K. A. Scarfone, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, United States, Tech. Rep., 2011.

[3] S. Obermeier, R. Schierholz, H. Hadeli, R. R. Enderlein, A. Hristova, and T. Locher, "Secure management of certificates for industrial control systems," in *39th Annual Conference of the IEEE Industrial Electronics Society (IECON 2013)*, November 2013.

[4] K. Fischer and J. Gesner, "Security architecture elements for iot enabled automation networks," in *Emerging Technologies Factory Automation (ETFA), 2012 IEEE 17th Conference on*, Sept 2012, pp. 1–8.

[5] IEEE Standard for Local and metropolitan area networks, *Secure Device Identity*, 802.1AR-2009 Std., 2009.

[6] 3GPP, "3gpp system architecture evolution (sae); security architecture," 2013.

[7] ——, "Security of Home Node B (HNB) / Home evolved Node B (HeNB)," 2013.

[8] ——, "Network Domain Security (NDS); Authentication Framework (AF)," 2013.

[9] D. Forsberg, G. Horn, W. Moeller, and V. Niemi, *LTE Security: Second Edition*, 2nd ed., 2012.

[10] A. Ray, J. Åkerberg, M. Björkman, R. Blom, and M. Gidlund, "Technical report: An assessment of mobile telecommunication security framework for industrial automation," Tech. Rep., August 2014.

[11] 3GPP, "Feasibility study on LTE relay node security," 2011.

[12] A. Ray, J. Akerberg, M. Gidlund, and M. Bjorkman, "A solution for industrial device commissioning along with the initial trust establishment," in *Industrial Electronics Society, IECON 2013 - 39th Annual Conference of the IEEE*, Nov 2013, pp. 5570–5575.