Security Service for the Rollout of Security Credentials in Ubiquitous Industrial Automation Environments

Rainer Falk, Steffen Fries
Siemens AG
Corporate Technology
Germany
{rainer.falk; steffen.fries}@siemens.com

Abstract— **Industrial control networks, e.g., for factory, process or energy automation and smart metering, are increasingly based on IT communication technologies like Ethernet, IP, and Web-Services. Security measures as authentication or cryptographic VPNs are used to protect communication links to supervising control stations and for remote service. While standard communication technologies have been used at the supervision level for some time, they will increasingly be used down to the field level comprising a huge number of field level control devices, sensors and actuators. These may be installed in largely distributed, uncontrolled areas. IT security measures are needed to protect the exchange of control commands and monitoring information between these field level devices and towards control stations. The efficient and secure distribution of required security credentials is challenging This paper describes a service for managing security credentials for ubiquitous field level devices (sensors, actuators) in an industrial automation environment.**

Keywords – Ubiquitous Security, Industrial Communication, Energy Automation, Sensor Actuator Network

I. Introduction

Standard communication technologies as Ethernet, the IP protocol, and Web-Services are increasingly used in industrial environments such as automation systems for energy distribution, building, factory and process automation, or for smart metering. This trend will extend down the automation pyramid to field level devices including even individual sensors and actuators. These numerous field level devices being widely distributed form an ubiquitous automation environment. Integrated security mechanisms have to be supported by a huge number of pervasive devices. Extremely easy commissioning and integrated security functionality are required to make the technology suitable for industrial applications. Automated Plug&Work mechanisms especially supporting security configuration are needed also to support agile automation concepts in which the production environment is flexibly adapted to changing needs. Moreover, security configuration has to take into account that automation environments may be geographically far-flung.

This paper describes challenges, side conditions and approaches for a security service enabling the efficient rollout of security credentials in ubiquitous industrial automation environments. This service comprises technical as well as organizational means. It allows field level components to be configured with the required set of security parameters to protect the device itself and its communication. In particular the preconfiguration of security credentials during the manufacturing process is considered as one way of supporting a secure configuration as part of device installation.

The remainder of this paper is structured as follows. Section II provides a motivation for security configuration processes based on existing security applications in automation networks. Section III describes a security service for the rollout of security credentials covering the whole security parameter lifecycle, which is the discussed in the context of the product life cycle of ubiquitous industrial field devices. Section IV afterwards describes different supported approaches for key distribution, applicable to industrial environments, while Section V describes an exemplary setup of the security service, where one service instantiation is used during device manufacturing, and a second one during device installation and operation. Section VI summarizes the findings and gives an outlook to future work.

II. Automation Systems Security

Typical automation systems are built in a hierarchical way as shown in Figure 1. It shows typical layers of an automation pyramid. On the lowest level there are sensors and actors that are connected to field devices. Specialized field buses are expected to be increasingly replaced by standard communication technology as Ethernet and IP. These field devices are actuated by controllers, e.g., a programmable logic controller PLC, which may be interconnected using industrial real-time

Ethernet protocols as, e.g., ProfiNet (cf. [10]). On the top are interconnections to supervisory systems and enterprise resource planning systems.

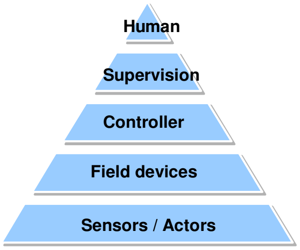


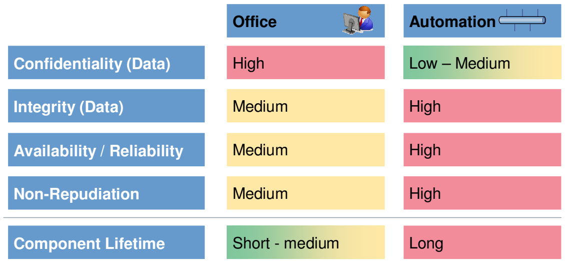
Figure 1: Automation Pyramid

Today, security in industrial automation is commonly applied by isolating cells on controller level using security gateways. Internally, the automation network is assumed to be closed and communication is not further cryptographically secured. In the future it is expected that devices down the automation pyramid including sensors and actors will feature integrated security functionality. This has already been discussed in the context of funded projects like the European funded project “Virtual Automation Networks – VAN” (cf. [1]) enabling secured communication between automation cells or devices in automation cells of different production lines. In contrast, energy automation already uses IP connectivity down to the field level.

Security mechanisms to be supported in automation communication comprise well-known security services:

- **Authentication**: The property that the claimed identity of an entity is correct.
- **Authorization**: The process of giving someone permission to do or have something.
- **Integrity**: The property that information has not been altered in an unauthorized manner.
- **Confidentiality**: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.
- **Availability**: The degree to which a component is operable (non-cryptographically service).

In contrast to office networks, automation networks have different requirements to security services as shown in the Figure 2.



	Office	Automation
Confidentiality (Data)	High	Low – Medium
Integrity (Data)	Medium	High
Availability / Reliability	Medium	High
Non-Repudiation	Medium	High
Component Lifetime	Short - medium	Long

Figure 2: Comparison Office/Industrial Security Requirements

The determination of security needs reveals the high importance of integrity and availability within automation networks. Also non-repudiation is often important so that e.g. reliable information about production is available or to provide billing-relevant information that can be relied upon. These security needs are quite different to typical priorities in office networks, see Figure 2.. A particular design consideration is the long component life time (several decades, depending on industry). All of the stated security services, independent of the application area, have one in common. They all need some type of security credential (which may be symmetrical or asymmetrical), where they can build upon. Thus, the process to efficiently install required security credentials on a huge number of devices will provide a big challenge. Its solution is a prerequisite to the successful adoption of integrated security mechanisms.

To better motivate the need for security credentials or more generally security parameters, the following subsections outline concrete examples for security in automation communication.

A. *Example 1: Energy Automation*

IEC 61850 provides a standard for communication in the domain of energy automation. It addresses the data exchange on process level, field level, and station level. Today, IEC 61850 is mainly used for reporting status and sampled value information from Intelligent Electronic Devices (IED) to a substation automation controller as well as for command transport from a substation automation controller to IEDs. It also covers the communication between IEDs instead of dedicated wires.

The following Figure 3 gives an example for a typical IEC 61850 communication scenario.

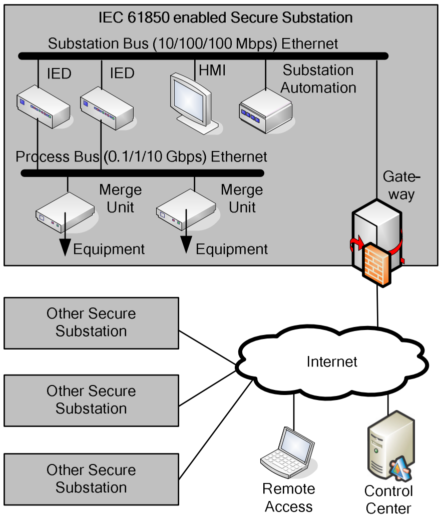


Figure 3: Typical Energy Automation Scenario

ISBN: 978-1-61208-105-2

This scenario obviously requires security services to protect the communicated control data. For energy automation the necessary security services are defined in IEC 62351. It defines explicit measures for communication using TCP and also serial protocols which are used directly in substation automation as well as in adjacent communication supporting energy automation, e.g., inter-control center communication. IEC 62351 addresses the general security requirements stated above. Currently the standard comprises eight parts that are in different state of completion.

While part 1 and 2 are more general and provide information about considered threat scenarios and the definition of terms, part 3 to 6 are directly related to energy automation protocols like IEC 61850 (IEC 62351 Part 6) and IEC 60870-5-x (IEC 62351 Part 5) and their mappings to protocols like TCP/IP (IEC 62351 Part 3) and MMS (IEC 62351 Part 4). These parts utilize symmetric as well as asymmetric cryptographic functions to secure the payload and the communication link. Moreover, the existing security protocol Transport Layer Security (TLS), which has been successfully used in other technical areas and industrial applications, is directly applied. Here, IEC 62351 specifies cipher suites (the allowed combination of authentication, integrity protection and encryption algorithms) and also states requirements to the certificates to be used with TLS.

Besides TCP/IP, IEC 62351 Part 5 relates to the specialties of serial communication. Here security measures are defined to especially protect the integrity of the connections based on pre-shared keys. This part also specifies the key management necessary for the security measures.

IEC 62351 Part 7 describes security related data objects for end-to-end network and system management and also security problem detection. These data objects support the secure control of dedicated parts of the energy automation network.

Part 8 of the standard is currently in definition and addresses the integration of role-based access control mechanisms into the whole domain of power systems based on ID-certificates, attribute certificates, or software tokens. This is necessary as in protection systems and in control centers authorization as well as stringent traceability is required. One usage example is the verification of the authorization and accomplishment of a dedicated switching action.

As it can be seen from the description above, IEC 62351 utilizes security credentials, e.g., in the context of the transport layer (using TLS or serial communication) but also on application layer for role-based access control. Crucial to the application of security credentials is the general credential handling comprising generation, provisioning, revocation, and especially the initial distribution to all participating entities. This is currently underspecified, but has been acknowledged by standardization as important. As the standard is extensible, it is expected that there will be a new part, describing credential handling in the context of IEC 62351 services.

B. *Example: Wireless Sensor Networks*

Wireless sensor networks consist of sensors (and actors) that communicate using short range wireless communication based on 802.15.4, Bluetooth, ZigBee or wireless HART. Important industrial use cases are machine and plant monitoring, asset tracking, and metering [8]. As the wireless communication can easily be intercepted and manipulated, a cryptographic protection is a must. Therefore, the sensors/actuator nodes have to be configured with a join key that allows to securely join a wireless network and to set-up required security associations. The join key is typically a secret key that is used to authenticate towards a security manager. The security manager authenticates the nodes and provides required session keys. The join keys are configured when the sensor network is installed, but it would also be possible to provide sensor nodes that have been pre-configured during manufacturing.

C. *Example: Product Authentication*

To identify products, in particular replacement parts, and to verify the claimed identity, electronic authentication mechanisms can be integrated directly into the components. This allows an automation system to automatically identify installed components and verify whether they are genuine (anti counterfeiting). Further information can be stored along the product life cycle [9]. An electronic authentication module being part of the product provides a cryptographic authentication function.

III. Security Service for the Credential Rollout

The rollout of security credentials describes the process of the initial setup of security credentials (e.g., keys, certificates) and related configuration information (permissions, policies). The result is a trust anchor enabling the further deployment of configuration information, services and communication.

The main functionalities of the security service for the credential roll-out for ubiquitous industrial field level devices are:

- Credential generation, certification, and archival,
- Credential distribution to field level devices,
- Credential life cycle management.

The security service can be adapted to different application-scenario-specific requirements through configurable policies. This ensures that the credential management is compliant with relevant requirements of the automation operator. The security service is exposed towards a user as for example a worker installing a field level or an employee in the field level device manufacture only in a way that ensures that the security service is used easily while ensuring compliance with defined security policies.

Security credentials are, like other type of data or equipment, part of a lifecycle. They are created, applied, and destroyed and need to satisfy a certain security policy. The typical life cycle of security credentials is depicted in Figure 4.

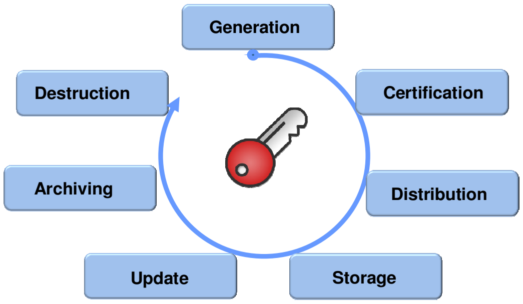
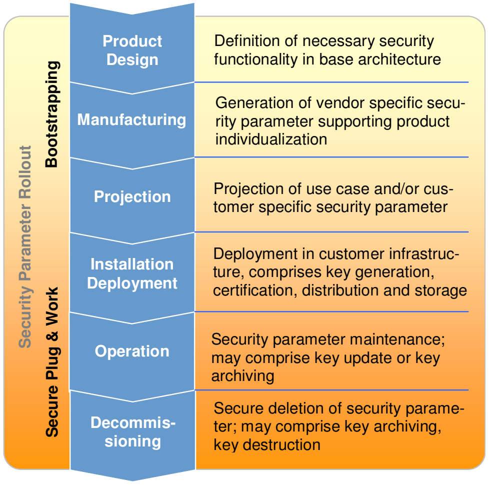


Figure 4: Security Parameter Life Cycle

The following list explains the single stages in the life cycle that are realized by the credential rollout service:

- **Key Generation**: Device keys can be created on the device itself. For example, in case of asymmetric key pairs, the device may generate the key material and a Certificate Signing Request (CSR), which is sent to a Certification Authority. Alternatively, keys may be created externally (e.g., a trust center, an engineering station, or an administrators laptop) and installed on the target device (off-device key generation).
- **Key Certification**: Typically done for asymmetric keys through a certificate authority. Depending on the key generation, this can be part of the key generation in a trust center or may be done on information sent in a CSR.
- **Key Distribution**: In case of off-device key generation, the device key has to be installed on the target device. This can be performed offline, e.g. the key is installed to the target entity during a manufacturing step, or online requiring communication with a security server (out-of band using a separate communication channel or in-band as part of a service communication).
- **Key Storage**: The private/secret device key can be stored in secured memory (e.g., flash) or in a separate hardware module (e.g., smart card or a trusted platform module).
- **Key Update**: Session key update does not belong to the describe process of security parameter rollout as it is typically performed by the security protocol used, based on a given security policy. Cryptographic keys have a dedicated lifetime, e.g., user certificates typically have a lifetime of 2 years, while server certificates are limited to 1 year.
- **Key Archiving**: Typically long term (secure or private) keys are archived to enable access to encrypted data. A use case is given by an employee leaving a company. While encryption keys are archived, signature/authentication keys need not to be archived as it is sufficient to archive corresponding public key / certificate.
- **Key Destruction**: Session keys are destructed (deleted) as soon as the session has ended. Long term keys are deleted, after keys have been renewed. This can be the case after the lifetime of the key has ended regularly, or if the key has been compromised.

The security parameter lifecycle has to be aligned with the product lifecycle, whereas the product may be a single component or a complete automation system.



Product Design	Definition of necessary security functionality in base architecture
Manufacturing	Generation of vendor specific security parameter supporting product individualization
Projection	Projection of use case and/or customer specific security parameter
Installation Deployment	Deployment in customer infrastructure, comprises key generation, certification, distribution and storage
Operation	Security parameter maintenance; may comprise key update or key archiving
Decommissioning	Secure deletion of security parameter; may comprise key archiving, key destruction

Figure 5: Security Parameter Rollout in the Product Life Cycle

Figure 5 shows main phases along the product life cycle:

- **Manufacturing**: This phase concerns the production of the hardware, possibly including a dedicated hardware security module, and the programming of the flash memory by the manufacturer. The product is individualized during manufacturing by programming a fixed device identifier (e.g. serial number).
- **Project Planning (Projection)**: During the project planning phase, a certain industrial installation is

planned. The used components, their (security) configuration and interconnection are defined.

- **Installation**: During the installation phase, the equipment is physically installed, configured and tested according to the project plan.
- **Operation**: During the operation phase, the devices are in regular operation mode. It is interrupted by maintenance and repair phases, which may comprise security parameter updates due to the normal key management lifecycle or complete device exchange.
- **Decommissioning**: Finally, the devices are decommissioned, i.e., they are put out of operation. Installed security parameter need to be deleted before leaving the customer premises.

As shown, security parameters are used in different phases of the product lifetime and are applied as:

- short term or session parameter (e.g., for integrity or confidentiality protection of an administrative action)
- long term or permanent parameter (e.g., for authentication)

Besides the pure key material, an efficient and secure solution requires well defined organizational processes for the life-time management of security credentials, standardized (and preferably certified) software and hardware components, a protected environment, etc.

It is useful to distinguish different phases of the security rollout:

- **Bootstrapping** concerns device-specific credentials installed as part of manufacturing. These are not bound to a specific usage environment of the product but may be used as a trust anchor for the next phase.
- **Secure Plug&Work** describes the process of installing a device in its intended usage environment. The installed credentials are specific to this usage as defined by the project plans.

These different phases pose quite different requirements on the handling of security credentials:

- During the bootstrapping phase, a manufacturer creates and installs credentials for a huge number of devices in a uniform way. The challenge is to define processes that allow handling the huge number of security credentials cost-efficiently, in a uniform way. This comprises the in-factory handling and also the distribution of the device connected parameter to the end customer.
- During Plug&Work the installation personal has to be supported so that they can install and commission devices very easily according to the project planning documentation. Here an individual device has to be brought to operation. As a huge number of devices have to be installed in a typical industrial plant, it is important to limit the effort to install a single device while configuring it according to its role in the project plans.

IV. Key Generation and Distribution

The security service for the rollout of security credentials is an important functionality to create, distribute and manage credentials for ubiquitous industrial field level devices. The differences of different application field require some flexibility concerning the deployment and operation of the security service. This Section describes supported options to distribute cryptographic keys to target field level devices..

Cryptographic keys may be generated by the security service itself, e.g. within a trusted hardware security module including a physical random generator. The created keys are then installed on the target device. This has to happen in a secure environment, e.g. a manufacturing plant. Alternatively, the secret/private keys are created on the field level device itself and the security service certifies the public key by a digital certificate.

The rollout of security parameter may be distinguished based on the credential distribution methods into:

- Offline parameter distribution
- In-band parameter distribution
- Out-of-band parameter distribution

None of the stated methods does necessarily require a cryptographic key already in place to support the bootstrapping. Obviously, there are technical variations for each of the categories. The following list provides a short characterization of the method and also provides some examples for each category:

- **Offline parameter distribution:** Performed using dedicated engineering tools directly connected to the device or via a separate network before the device is brought to operation (see Figure 6).

  This requires a (mobile or fixed) engineering station in the offline network having all parameter sets for the devices to be bootstrapped available. Besides the example given in Figure 6 another approach is the application of a token to transport the cryptographic parameter to the target device. This approach is supported for instance in the setup of common WLAN routers using Wi-Fi simple configuration. A further example is given by application of SIM (Subscriber Identity Modules) cards in mobile devices, were the SIM card, carrying all necessary security parameter, can be distributed independently of the actual mobile device.

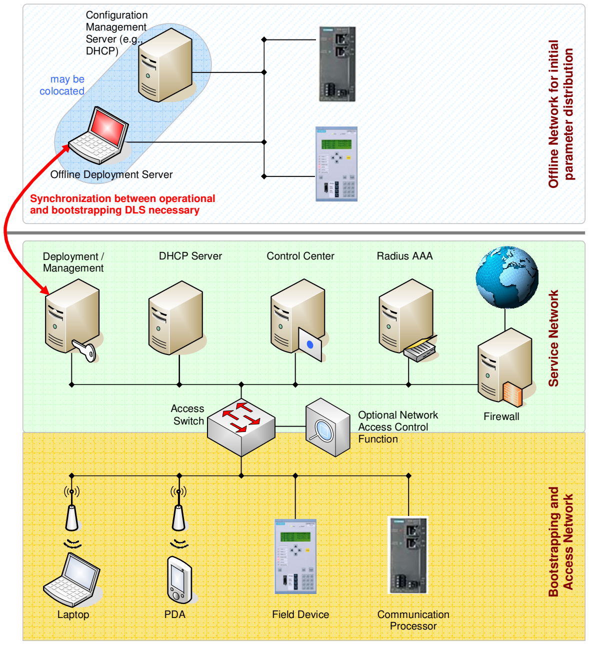

Configuration Management Server (e.g. DHCP)
may be colocated
Offline Deployment Server
Synchronization between operational and bootstrapping DLS necessary
Offline Network for initial parameter distribution
Deployment / Management
DHCP Server
Control Center
Radius AAA
Service Network
Access Switch
Optional Network Access Control Function
Firewall
Laptop
PDA
Field Device
Communication Processor
Bootstrapping and Access Network

Figure 6: Offline Key Distribution

- **Out-of-band parameter distribution:** A separate logical or physical communication channel used to configure security parameter (see Figure 7). It basically resembles the offline distribution approach using an online connection instead of a separate physical network. As stated before, devices may already possess a cryptographic credential, which can be provided by the device manufacturer.

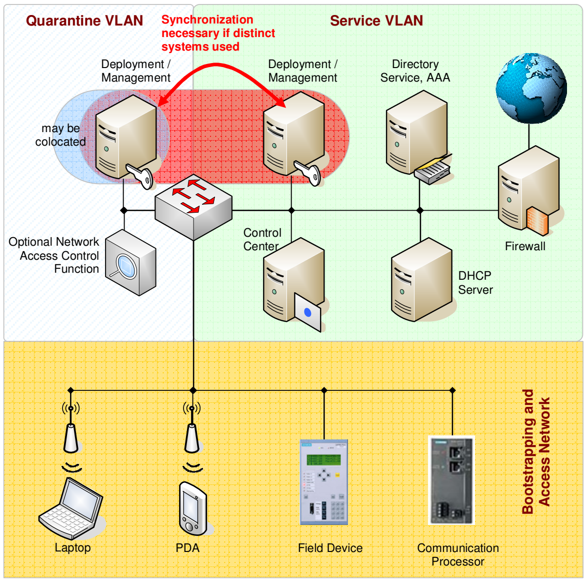


Figure 7: Out-of-Band Key Distribution

Figure 7 shows the application of a quarantine VLAN for the distribution of security credentials. This can be compared with today's methods of Network Access Control (NAC) by putting the connecting device into a dedicated logical environment to check it's compatibility to a local security policy before providing access to the Intranet. The security parameter bootstrapping may even be combined with this functionality.

- **In-band parameter distribution:** Distribution using the same communication channels as used during regular operation (see Figure 8). This may be based on a pre-configured device identifier (like the MAC address), manufacturer installed security credentials or even a liaison device.

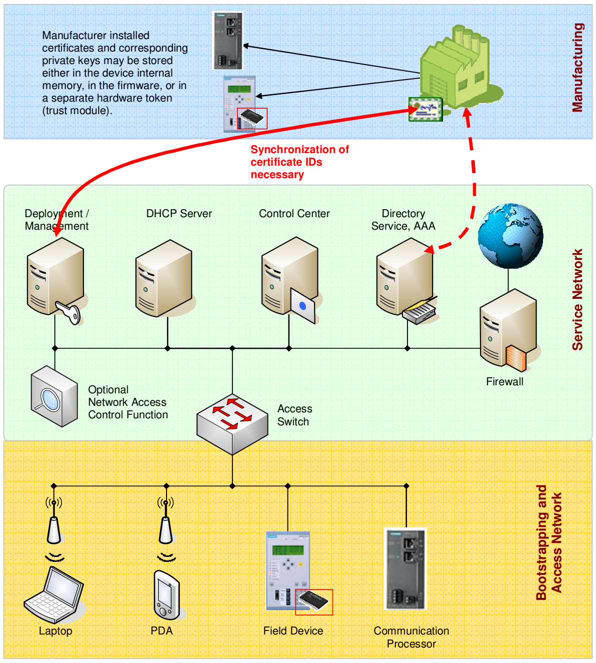

Manufacturer installed certificates and corresponding private keys may be stored either in the device internal memory, in the firmware, or in a separate hardware token (trust module).
Manufacturing
Synchronization of certificate IDs necessary
Deployment / Management
DHCP Server
Control Center
Directory Service, AAA
Service Network
Firewall
Optional Network Access Control Function
Access Switch
Laptop
PDA
Field Device
Communication Processor
Bootstrapping and Access Network

Figure 8: In-Band Key Distribution

Figure 8 shows an example using manufacturer installed security credentials to protect the distribution of customer specific key material.

A further variant of in-band parameter distribution is supported by the application of a liaison device, which is already in possession of a service technician. Here, the security credentials on the liaison device can be "borrowed" for the bootstrapping of the target security parameter by using near-field communication, an approach that is currently being standardized by 3GPP.

V. Use Case Example

The designed security service for the rollout of security credentials to ubiquitous industrial field level devices provides the flexibility to be adapted to different requirements. This Section describes a preferred variant based on device authentication credentials pre-installed during manufacturing. These allow the device to be identified and authenticated in its respective target environment. This secure device authentication is the trust basis for an automated bootstrapping of credentials within the target installation environment.

The following requirements respectively. side conditions of a typical industrial environment are respected:

- Before field level devices are installed, a detailed projection plan is defined. The projection plan defines the configuration for each component of the automation system. This information is useful as information in the expected devices and their interconnection needs to be available before the actual installation is performed.
- It should be possible that the installation is performed by personal not having an IT or even a security background.
- It must be possible that the correct installation according to the projection documents is proven to support a security audit trail.

The designed security service for the credential management for ubiquitous industrial field level devices achieves these objectives by the following design: When a field level device establishes network connectivity within the target environment for the first time, it authenticates towards a bootstrapping service using pre-installed device authentication credentials. The bootstrapping service checks whether the device is authorized and provides the target device configuration based on automation plant project planning data.

Devices are pre-configured by the manufacturer with a unique device key. This key is certified by a digital certificate. It allows installation personal to work only with device types and serial numbers, while not being exposed to cryptographic keys or certificates. The device manufacturer uses a corresponding security service that issues and manages device authentication credentials during manufacture that are valid for the product life time, independently on where the device is installed. The private device keys are created in a batch process to be installed within the manufacturing environment. The corresponding device certificate including the public device key is archived.

During installation, the device can be unambiguously and securely identified using the pre-configured device key. Using this initial device key, an installation-specific (customer-specific) device key is deployed in-band. The device and its configuration are registered in a configuration database. The automation system owner uses a second instantiation of the security service that issues and manages device credentials valid within the respective automation environment. The credentials are valid within the specific installation environment. The device keys can be, depending on respective policy, created on the field level device itself, or they are created during projection phase and installed on the respective target field level device during the setup. Optionally, after installation has been completed and the automation system is turned to operation, an automatic key update can be performed, so that the keys used during operation are not known by the installation personal. This re-keying is supported by the second security service. Similarly, such a key update can be performed as part of service, so that service personal does not get access to keys used during operation of the automation system.

VI. Conclusion and Outlook

While the problem of key distribution is as old as IT security, the increasing introduction of security mechanisms in industrial environments requires solutions that are adapted to the specific application field. This paper presented a security service for the rollout of security credentials to ubiquitous industrial field level devices. Both technical and organizational requirements have been described.

Currently, work is ongoing in the context of the European funded research project IoT@Work (Internet of Things at Work), service is worked out in more detail and is validated by prototypes.

References

[1] Homepage EU Project Virtual Automation Networks, http://www.van-eu.eu/

[2] RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, T. Dierks, E Rescorla, August 2008

[3] ISO-IEC 61850, Part 1: Introduction and Overview, May 2003

[4] ISO-IEC 61850, Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, May 2004

[5] ISO-IEC 62351, Part 4: Communication Network and System Security – Profiles Including MMS, October 2006

[6] ISO-IEC 62351, Part 5: Security for IEC 60870 and Derivatives, February 2007

[7] ISO-IEC 62351, Part 6: Security for IEC 61850, October 2006

[8] Rainer Falk, Hans-Joachim Hof, Ulrike Meyer, Christoph Niedermeier, Rudolf Sollacher, and Norbert Vicari: “From Academia to the Field: Wireless Sensor Networks for Industrial Use”, 7th GI/ITG KuVS Fachgespräch „Drahtlose Sensornetze“, Berlin, 25-26 Sep. 2008.

[9] Rainer Falk, Andreas Koepf, Hermann Seuschek, and Ming-Yuh Huang, Mingyan Li: Simulating a Multi-Domain RFID System for Replacement Part Tracking, Third International Conference on Emerging Security Information, Systems and Technologies SECURWARE 2009, Athens/Glyfada, Greece, 18-23 June 2009.

[10] Profinet, http://www.profibus.com/technology/profinet/

ISBN: 978-1-61208-105-2