Security Architecture of Smart Metering Systems

Natasa Zivic, Christoph Ruland

Security Architecture of Smart Metering Systems

Natasa Zivic [1] and Christoph Ruland[1]

[1] University of Siegen, Institute for Data Communications Systems,
Hoelderlinstrasse 3, 57076 Siegen, Germany
{Natasa.Zivic, Christoph.Ruland}@uni-siegen.de

Abstract. The main goals of smart metering are the reduction of costs, energy and CO_2 by the provision of actual metering information to the providers and the customer. They allow for flexible possibilities to influence the customers' energy consumption behavior and to adapt dynamically the power generation and distribution to the requested energy by smart grids. Metering devices are under control of governmental organizations, which are responsible for the permanent correct delivery of metering data. The governmental organizations accept online metering, administration and even software download of regulated software only, if strong, lawful security requirements are fulfilled. This paper describes such a security system. It considers not only the security mechanisms of the metering devices, but also of the complete system hierarchy, which is planned for the communication system of smart metering. It supports also new use cases, which are caused by the liberalization of the energy and metering services markets.

Keywords: Smart Metering, Smart Grids, Liberalization of Energy and Metering Market, Power Line Communication, Security Requirements, Security Protocols, Public Key Infrastructure, Asymmetric and Symmetric Cryptography

1 Introduction

The liberalization of the telecommunication market in the last decade of the last century was followed by the liberalization of the energy market, which led to the liberalization of the metering market (in some countries). It meant the separation of generation, transport, distribution, selling and metering of energy, and the consumer mutated from a subscriber to a customer. Everyone is allowed to buy and to sell energy or to offer related services. The customer can choose the manufacturer of energy, the provider of energy, of the meters and of the metering services. The customer can even choose more than one provider, for example depending on the load profile, day and night. The customer is able to switch from one provider to another one as he wants. By this way, at one hand, the liberalization should strengthen the competition and save money. Online metering is a prerequisite for such possibilities.

At the other hand, the energy manufacturers and energy providers are interested to get actual information about the energy situation, so they can react instantly on the situation, how much energy of what source is consumed by the customers. Load profiles are required in industrial scenarios. That needs also a frequent online access to the metering devices. Additionally, the behavior of the consumers should be influ-

enced in such a way, that energy is saved. The consumer should have the permanent possibility to monitor the consumption. The politics want to strengthen the energy awareness of the society. At the end, the governmental department, which is responsible for the correctness of metering, wishes to have access to the meters to check the correctness of hard- and software. Under strong restrictions they allow software download of metrological software [1].

Many national laws have to be respected, when online metering is planned, which cover data protection and privacy, security, regulation of energy and telecommunication, as well as teleservices.

Other rules and guidelines have to be considered, which cover the metrological aspect. On the highest international level it is OIML, which issues the software requirements for Software Controlled Measuring Instruments [2], there exist the WELMEC group with software requirements [3] and software guides [4] for metering, and the (binding) European Metering Instruments Directive [6]. Last, but by far not least, laws and regulations on the national level have to be fulfilled, which are applied for the approval process of metering devices.

The structure of the paper is as follows: in chapter 2 the communication system structure of smart metering is explained, the type of exchanged information is characterized and the security requirements are derived. Chapter 3 presents the architecture of the security solutions, before the key management is described in Chapter 4. Chapter 5 handles use cases of the operation of the security system and chapter 6 concludes the paper.

2 Communication System of Smart Metering Devices

2.1 Structure of the Communication System

The source of metering data and the destination of commands regarding metering are the metering devices. New generations of meter devices are equipped with electronics, for example embedded systems, which allow them to store, process and to exchange information over networks. The communication module supports one of the older interfaces like IEC 1107 over RS 485, or Power Line Communication, LAN or GSM/GPRS. Electricity meters are mostly better equipped with electronic power, so they can work additionally as a master for water meters or gas meters using RS 485 interfaces or the M-Bus (optional wireless). Of course, it is also possible to run a water or gas meter independently on a electricity meter. Online metering itself and secure online metering is usually for a couple of years [7], but new communication concepts and new requirements have been developed recently.

The configuration of an electricity, gas and water meter is a typical scenario in a residential family house.

In apartment houses or office buildings there are clusters from 1 to hundreds of electricity, gas and water meters. For such larger scenarios the concept of a MUC has been specified [8]. MUC (Multi Utility Communication) acts as a concentrator in a building and supports communication to external entities, but also to the customers. The customer gains direct access from the apartment to the meters to get information

about the history and actual consumption of energy. The interface used for this access may be a LAN or via a PLC adapter (LAN-Interface/Power Line Communication). Additionally, consumption displays may be located in the rooms of the apartment to strengthen the awareness of power consumption and power saving.

Remark. The customer has also access to its metering information (combined with the billing data) stored in the database of the metering service provider, but this access is out of the scope of the smart metering communication system.

Power Line communication plays an important role in metering communication, because electricity meters are connected always physically by power lines and meters are located very often in basements, where no wireless communication is available. Power line communication is the cheapest method to connect electricity meters, and the other meters are mostly closed by.

Some MUCs (of one big building or more buildings in a street) are connected via Power Line Communication to a concentrator (CN), which could be located in the next transformer station. This concentrator supports wireless communication or DSL, for example, to the outside world: to the metering provider, to the data collection provider, to the power provider, to the metrological institute, etc. All of them have specific access rights to exchange information with the system components.

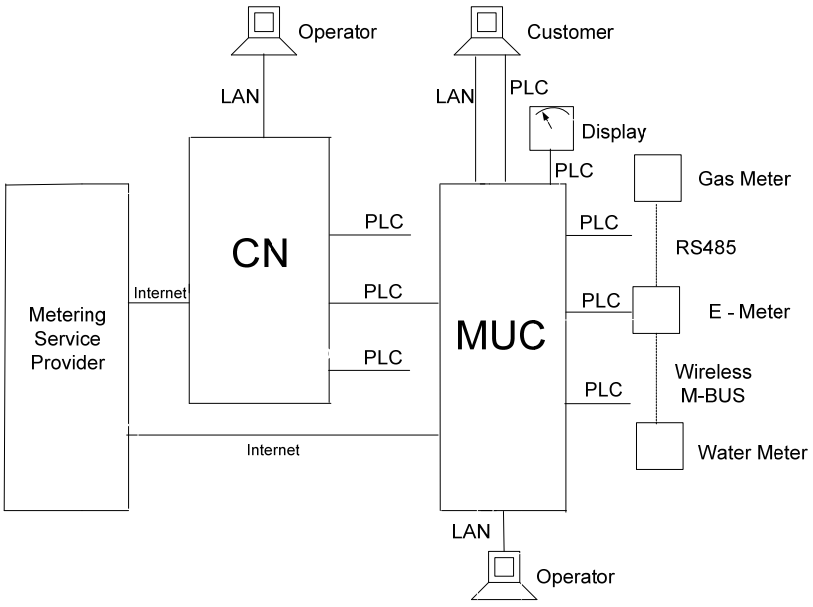

Fig. 1 Communication Architecture

TCP/IP or IP Telemetry Protocol is used between MUCs, concentrators and providers, but the metering devices communicate to the MUC by specific protocols, which are

introduced in the metering device industry, for example, DLMS, IEC 1107, M-Bus (wireless).

2.2 Data Traffic

The context of data, which is exchanged between the components of the metering communication system, has to be analyzed, before their security requirements can be specified.

Metering Data — Data of the meter of the consumption of energy, extended by timestamps, tariff information. They can contain single records, or a bulk of metering data over a certain time, load profiles, etc.

Metrological Parameters — Parameters with impact on the metrological part of the metering device may be set or modified by an entity, which is authorized by the governmental metrological institute, which is responsible for approval, calibration and examination of metering devices. Such parameters are: set of date and time, metering parameters, calibration, etc

Metrological Logbook — Each write access to or trial to modify (alert!) the metrological part is recorded in the metrological logbook, which can be read and reset only if authorized by the governmental metrological institute.

Table 1: Exchanged information (sent to/read from the device: →/←)

	Metering Device	MUC	Concentrator
Metrological Institute	Metrological Commands → Software Download → Metrological Logbook ←		
Energy Provider	Metering Data ←		
Metering Service Provider	Metering Data ← Non Metrological Commands →	Non-Metrological Commands →	Non-Metrological Commands →
Customer		Metering Data ←	
Manufacturer(s)	Non-Metrological Commands →	Non-Metrological Commands →	Non-Metrological Commands →
Local Operator(s)	Metrological and Non-Metrological Commands →	Non-Metrological Commands →	Non-Metrological Commands →
Consumption Indicator	Metering Data ←		

Metrological Software Download	Till recently the software Download of regulated software for updating software of the metrological part was not allowed. Now rules exist and conditions are specified, how this is possible in the future [1].
Non Metrological Parameters, Logbook, Software Download	Metering Devices are separated into a metrological and a non metrological part, which is under the responsibility of the manufacturer, provider, etc. The security requirements of the non metrological part (hard- and software) are specified by the manufacturer, not by the government.

2.3 Security requirements

For the types of data listed in table 1 are following security requirements mandatory.

Authentication of Data Origin and long term Non-Repudiation of Origin
are necessary for:

- Metering data
- Metrological Logbook
- Metrological commands
- Software Download into the metrological part of a metering device

The information needed for support of non repudiation of origin (Non Repudiation of Origin Token, for example specified in ISO 13888-2) has to be stored together with the information itself. It should be possible anytime for the authorized entities to verify the proof of origin. The non repudiation of origin is needed by the legal meaning of the metering information.

Authentication of Data Origin
has to be provided for the access to the metering information and to the non-metrological part of metering devices, to MUCs and concentrators and mutually for the exchange of information.

Confidentiality
is not required by metrological laws, but by the data protection law – as soon as the privacy of the people is concerned. Metering data themselves are considered as "pseudonymous", as long as they don´t allow a direct relation to a person, but very often a relation to a person or family can be established, so confidentiality of metering data is needed by privacy reasons.

Other reasons to use confidentiality for the data traffic are manufacturer´s product specific administrative information including the software download.

Access Control
As seen in chap. 2.1., there are many roles requesting access to metering devices and the components of the metering system:

It is necessary to execute access control for each function or action, which can be activated. For each function it has to be specified, which role is allowed to send a command. The access control has to be based on strong authentication.

3 Security Mechanisms and Protocols

In chap. 2 the communication scenario of smart metering under security aspects has been described. In this chapter a security solution is presented. The security mechanisms and protocols are chosen, which support the security requirements.

Non-Repudiation of Origin
Digital signatures are used together with a regulated (trusted, under law control) infrastructure similar to the requirements specified for qualified digital signatures of the Digital Signature Law. The private key has to be physically protected against reading and modification. The digital signature is generated at the source in a protected hardware environment and coded together with the (metering) information, which has to be sealed. The digital signature will stay together with the information for the lifetime of the information. The root of the PKI is based on the governmental metrological institute.

SML signatures are used for the integration of digital signatures into the data format used for end-to-end data exchange. SML signatures are very similar to XML signatures. SML (Smart Metering Language) is a special type of XML adapted for the needs of metering.

Authentication of Data Origin of Commands
Digital signatures are used based on a Certification Authority (Trusted Third Party) as anchor of the PKI. The security properties of storage and usage are specified by the metering service provider.

SML signatures are used for the integration of digital signatures into the data format used for end-to-end data exchange.

Confidentiality
Transport-oriented authentication of origin and confidentiality are provided by TSL/SSL on all communication channels, which use TCP/IP. A Certification Authority (Trusted Third Party) is used as anchor of the PKI.

Some connections don´t use TCP/IP because of the protocol overhead, so on Power Line Communication between the apartment (customer or the consumption display) and the MUC, or on the wireless M-Bus. Both communication technologies (PLC and wireless M-Bus) support symmetric cryptographic algorithms (AES), which are used for confidentiality.

Access Control
Access Control is given by access control tables for all of the commands. These include not only the execution of functions but also changes of access rights. The need of change of access rights are caused by the liberalization to change or sell the providers.

4 Key Management

4.1 Public Key Infrastructure

Energy Metering Device
Each Energy Meter (EM) generates its own asymmetric key system during the calibration process, the public key PK_{EM} is read out, certified by the calibration authority, $CERT_{EM}$ written into the metering device and published, for example in a LDAP server. The private key SK_{EM} is stored internally. These key systems are used for digital signatures providing long term non-repudiation (SML signatures, SML_{SIG}).

Concentrator and MUC
Each concentrator (CN) and MUC generates its own asymmetric key system, the public key PK_{CN}, rsp. PK_{MUC} is read out and certified by the manufacturer and published as $CERT_{CN}$, rsp. $CERT_{MUC}$. The private key SK_{CN}, rsp. SK_{MUC} is stored internally. These key systems and certificates are used for SSL/TSL communication.

Manufacturers
Each manufacturer (MFC) of MUC, concentrator and energy meter has an asyrmmetric key system. The public key PK_{MFC} is certified ($CERT_{MFC}$) by a Certification Authority (CA) and published. The private key SK_{MUC} is stored internally. These keys systems and certificates are used for SSL/TSL communication. CA owns also a public key system PK_{CA}, SK_{CA} , using the private key SK_{CA} to issue the certificates.

The manufacturer writes its own public key into the metering device, concentrator or MUC during production.

Provider of Metering Services
The provider of metering services should be divided in two departments: security management (SM) and operational management (OM).

The security management owns a public key system. The public key PK_{SM} is certified by CA and published ($CERT_{SM}$). The private key SK_{SM} is stored internally.

The security management generates public key systems (SK_{OPi}, PK_{OPi}) and issues certificates extended by role oriented access rights to the members of the operational management. These certificates $CERT_{OPi}$ are published and enable local and remote maintenance.

The private key of SM is also used for digital signatures of security relevant commands to the components.

Optionally the provider of metering devices can delegate the data collection service (DCS) to a third party. In this case DCS generates its own public key system (PK_{DCS} ,

SK_{DCS}) and will receive a certificate $CERT_{DCS}$ from the security management of the metering devices provider including the attribute of the right for data collection.

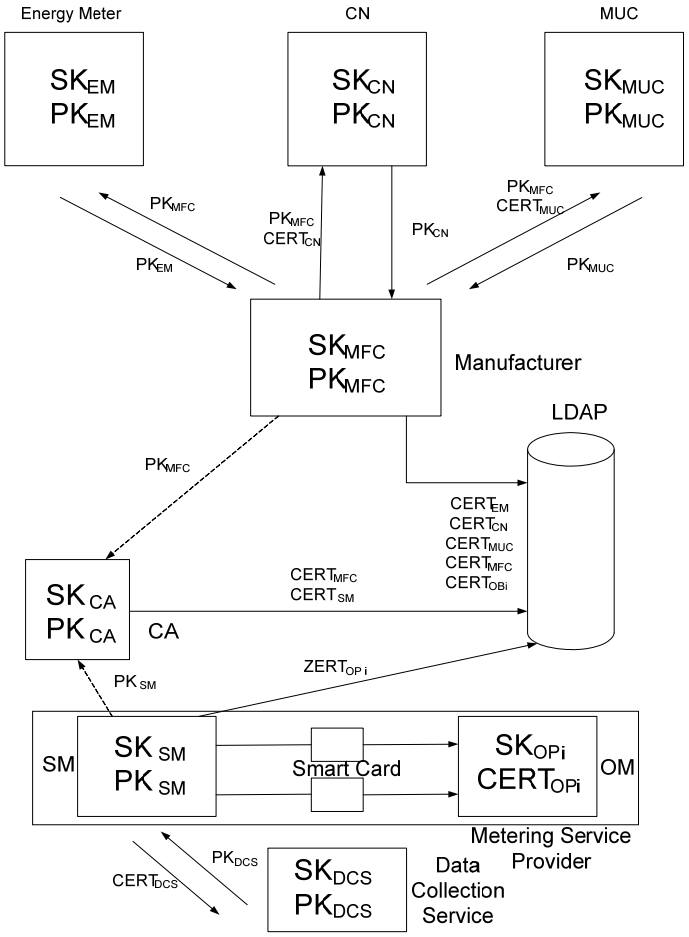

Fig. 2 Public Key Infrastructure

4.2 Symmetric Key Management

User
The user needs a password for access via LAN and TSL/SSL or via LAN/PLC by a PLC-Adapter to the MUC.

PLC-Adapter and MUC
A symmetric key is needed for PLC encryption ($KEY2_{PLC}$)

Wireless M-Bus
If metering devices, e.g. gas and water meters are connected by wireless M-Bus, they need symmetric keys for wireless M-Bus encryption and data integrity ($KEY_{M\text{-}Bus}$). The peer entity, e.g. the electricity meter or MUC, needs the same key as well.

Energy Consumption Display
The adapter of the energy consumption display (ECD) holds a symmetric key for PLC encryption ($KEY1_{PLC}$) as well as the MUC.

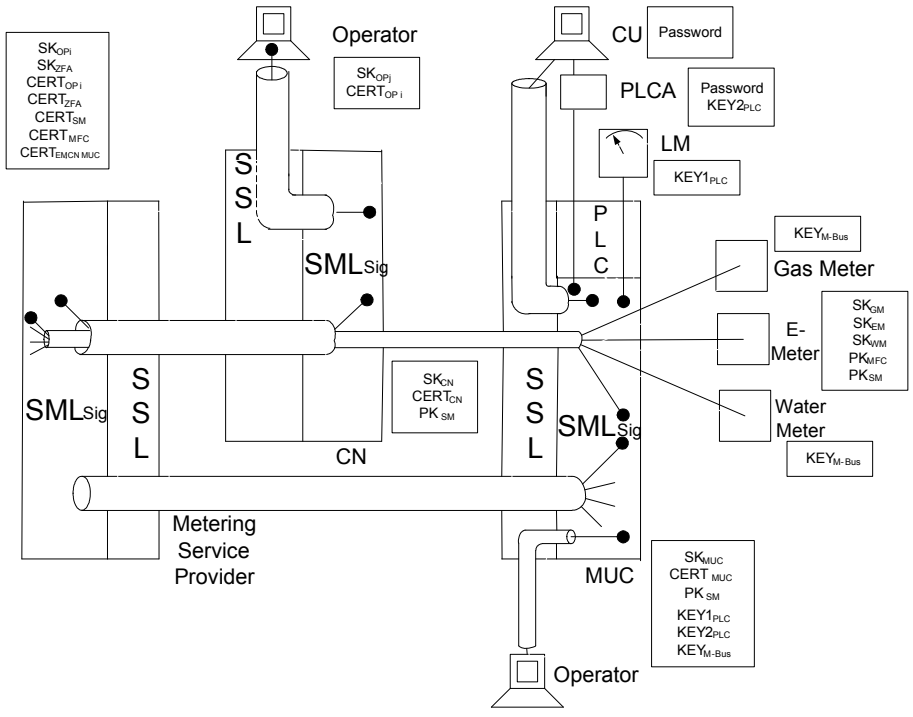

Fig. 3 Distributed Keys after Initialization without negotiated SSL/TSL keys

4.3 Initialization

During initialization the components get all the certificates, which they need for verification of authentication to perform access control and for SSL/TSL online from the Authentication Directory, for example a LDAP Server.
The symmetric keys have to be installed locally.

If the Initialization is finished and operation is in process, the components have those keys and credentials, which are presented in Fig. 3.

5 Use Cases

- Reading of metering data
  Reading is done using Pull method. The reading command is signed by the entity and verified by the MUC including checking the authorization. The metering (SML) data are digitally signed by the meter inside the meter using the private key. The MUC transmits the data via SSL/TSL and TCP/IP to a concentrator or the Metering Service Provider.
  If the metering device is not able to generate digital signatures, the metering data are transmitted from the metering device to the MUC using symmetric encryption, and the digital signature is generated by the MUC.

- Maintenance
  An operator establishes a SSL/TLS connection to MUC or CN using an asymmetric key system with exchange of certificates. If commands should be executed on the metering device, they have to be signed digitally by the operator. The certificate is sent to the metering device. For verification of the certificate the metering device uses the public key of the Metering Service Provider, which has been loaded after installation. The Metering Service provider issues the certificates of the maintenance operators.

- Replacement/Repair of metering instruments devices
  If a metering device has to be replaced, the memory is completely erased internally, and a new installation is performed as described in chap. 4.1 and 4.3.

The liberalization of the energy and metering service market enables the participants of the market to choose and to change their contract partners. Therefore there are new use cases, which have to be supported:

- Change of Metering Service Provider
  If a Metering Service Provider surrenders metering devices to another Metering Service Provider, the operator of the first metering service provider sends the certificate of the second metering service provider to the MUCs. The new public key overwrites the old one. New addresses are set in the components by using maintenance commands.

If the first metering service provider hesitates to admit access to the new metering service provider, the manufacturer is also able to delete the public key and access rights of the former metering service provider. Therefore the metering devices know the public key of the manufacturer since production time.

- Download of Metrological Software
  There are different digital signatures, which have to be verified before new metrological software is accepted and executed by a metering device. The manufacturer sends new software to the metrological institute, which checks the correctness and approves the software. The object code of the new software is signed by the metrological institute and returned to the manufacturer. The manufacturer signs the software additionally and distributes it to the metering service provider for distribution to the metering devices. The metering devices verify the authorization of the metering service provider by checking the digital signature of the maintenance command, then the digital signature of the manufacturer is verified and, finally, the digital signature of the metrological institute. A powerful software version management has to be used. If the new software can´t be executed successfully, a mechanism restarts the preceding version. Therefore the metering devices must be able to store two or three software images and require an operating system. The metering service provider, manufacturer and metrological institutes are always permitted to check the version and correctness of the running software. The metering device can calculate a checksum of the software, sign this checksum and send it to the requesting entity. The security mechanism for the download of metrological software requires higher security levels than other transactions.

If the functionality of the Metering Service Provider is divided in different parts, and some of them are delegated to other providers, for example Metering Data Collection, additional use cases will happen and have to be supported.

6 Summary

The liberalization of the energy and metering services markets need new communication systems for smart metering devices and a security architecture, which satisfies all legal requirements and the requirements of the providers and customers. The communications system has been described, the exchanged information has been analyzed for their security needs, and a security architecture has been proposed, which covers all use cases. The focus was on the key management, which supports the security mechanisms and protocols. A special requirement of the key management is the possible change of the stakeholders caused by the liberalization of the markets.

References

1. Hick, S., Ruland, C.: Security Aspects for Secure Download of Regulated Software, Trustbus 2007, LNCS 4657, pp. 219 – 227, Springer Verlag, Berlin
2. International Organization of Legal Metrology: General Requirements for Software Controlled Measuring Instruments, OIML TC 5 / SC 2 – Committee Draft OIML CD 1, May 2007, http://www.oiml.org
3. WELMEC 7.1 (issue 2): Development of Software Requirements, May 2005, http.//www.welmec.org/publications/7-1.pdf
4. WELMEC 7.2 (issue 1): Software Guide (Measuring Instruments Directive 2004/22/EC, May 2005, http.//www.welmec.org/publications/7-2en.pdf
5. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:135:0001:0080:EN:PDF
6. MID-Software: Software Requirements and Validation Guide, Version 1., European Growth Network , http://www.lne.fr/fr/metrologie_legale/documents/MIDSW_1.00.pdf
7. Lo Iacono, L., Ruland, C., Zisky, N.: Secure Transfer of Measurement Data in Open Systems, Computer Standards & Interfaces, Vol, 28, pp. 311-326
8. Multi Utility Communication (MUC), Version 1.0, 8/2009, VDE, http://www.vde.de/de/fnn/arbeitsgebiete/messwesen/documents/FNN_LH-MUC_1-0_2009-08-05.pdf