Selma – Technology and Applications

Thomas Schaub, Landis+Gyr, Switzerland

Abstract: In the liberalized energy market measured consumption data forms the basis for all contracts between the market participants. In the past, precision of the measurement was the most critical criterion a meter had to fulfil. Today precision is taken for granted. In addition, the market requires a secure and traceable data exchange process from the meter to the bill. In the paper we present the Selma concept (secure electronic measurement data exchange). Selma provides a comprehensive security architecture supporting the authentication of measuring data, secure data access and the certification of software.

1 Introduction

Selma stands for „secure electronic measurment data exchange". Selma represents a comprehensive security concept adapted to the needs of liberalised energy (electricity, gas, water, heat) markets. Selma considers the complete metering process chain – from calibration , installation, to measurement and billing.

The Selma security architecture considers the following "boundary conditions":

- existing international standards for communication and security;
- economic conditions in the metering environment (low lifecycle costs, communication channels with limited capacity);
- regulatory conditions in the metering environment (country specific approval and calibration processes).

The Selma solution is modular and scalable. With Selma customised, cost-efficient security solutions can be built. Due to the consequent use of standards interoperability is achieved enabling system integration at minimal costs.

2 The three security modules of Selma

Figure 1 shows the three security modules of Selma.

Authentication of measuring data:
Classic correspondence: signed document

The metering device adds an electronic signature to the measurement data. The signature stays with the data during its entire lifetime. Due to the signature it can be proven anytime that the data is original, that the data originates from a well defined meter and that it was measured at a specified point of time. The market participants can check their bills by verifying the signature.

Secured channels:
Classic correspondence: sealed envelope.
A digital signature is added to the communication services. With that the client accessing the metering device as well as the metering device itself is identified. The metering device grants access to pre-defined clients providing pre-defined sets of data. With the help of this module

even insecure channels can be used for security-critical interactions (e.g. clock setting, parameter download, SW download). This module enables the use of the Internet for measuring data acquisition and meter park management.

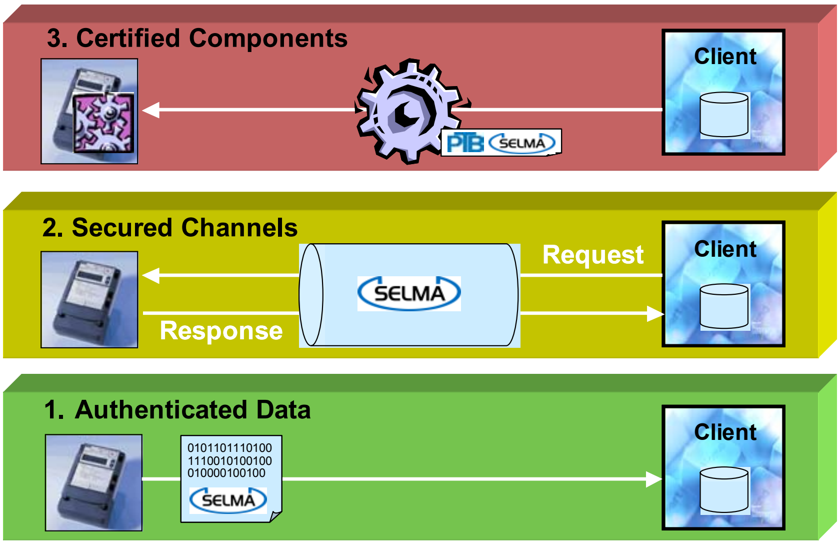

Figure 1: The three application modules of Selma

Certified device components:
Classical correspondence: registration mark
New parameter sets or new software versions are certified and signed by the corresponding certification authorities. On the other side, the measuring device verifies the signature. Only parameter sets, or software versions, with the valid signature are accepted. This module forms the basis for „in-field" re-configuration. Costly dismounting and re-certification can be avoided. With the help of this security module meter maintenance can be substantially simplified.

3 The security technology

The signature method shown if figure 2 forms the basis for all security modules. The data to be sent (e.g. the measurement data) is compressed to a fixed number of bytes using a standard algorithm - the so-called hash-value. The signature is calculated by encrypting the hash-value using the *private key.* The signature is then transmitted together with the original data. It should be noted that the original data is not altered by the signature. Therefore it is still possible to interpret the data on the receiver's side with the existing communication means, by just ignoring the signature. (This fact substantially facilitates the stepwise introduction of signed data into an existing system environment).

On the receiver's side the received signature is decrypted and compared with the calculated hash-value. If the two values are equal, the signature is declared as valid, and the data is accepted as authentic.

It has to be noted that the described „asymmetric" ciphering method uses a different key for encryption than for decryption. In addition, knowing the decryption key does not help to find the encryption key. For signature applications the encryption key is kept secret (private key), whereas the decryption key is made public (public key). With that the *generation* of the signature is only possible for the authorised, whereas the *verification* of the signature can be performed by anybody.

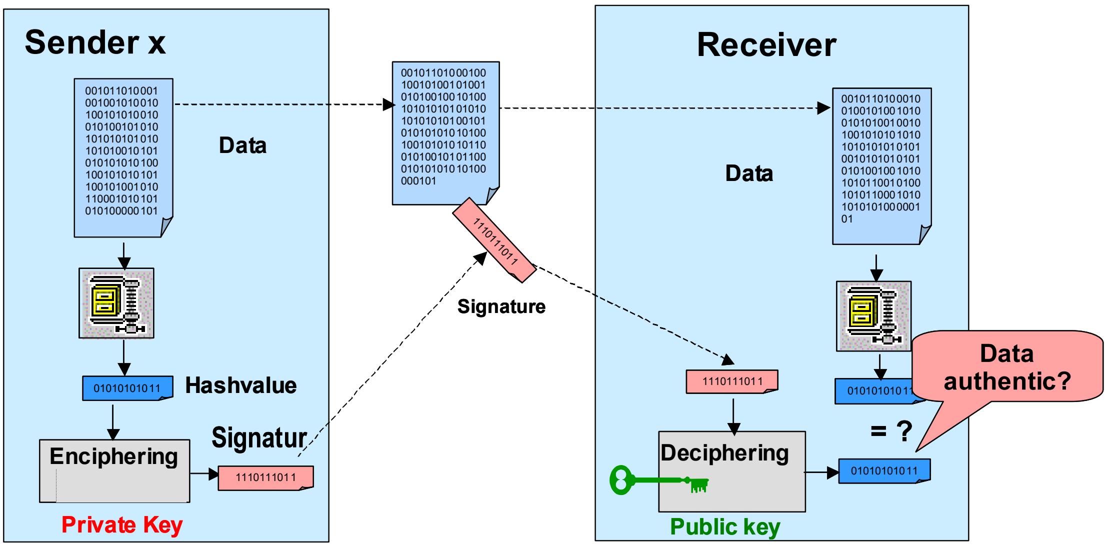

Figure 2: Security through signature technology

A critical issue is the distribution of the public keys. The keys must be certified by a trustworthy body (SigCA, Signature Certification Agency). The key-exchange is based on key certificates signed by the certification body. The security concept of Selma specifies the key exchange in detail by building on the existing infrastructure of approval and certification bodies.

4 Applications

In the following paragraphs the application of the Selma modules is illustrated with two examples.

4.1 Authentication of measurement data in the system environment

The measurement data is divided into so-called „daily profiles“. “Daily profiles” are load profiles according to VDEW2.1 (comp. [1]), divided into daily units. Each daily unit is signed separately by the measuring device. Additional information (meter number, meter point identification, measurement date and other measurement parameters) is added in order to make the daily data units unambiguously interpretable at any point of time. Selma defines the “daily profiles” and other data models in great detail (comp. [3]). For that purpose the same standardised description language is used as in the DLMS standard (comp. [2]). With that the Selma data models can be easily transferred to international standards.

According to figure 3 „signed daily profiles“ are transmitted via the existing communication channels to the data acquisition system and archived. In addition, the measuring data is packed into an internet compatible XML file. The XML file is then offered to end-customer via an existing internet server. The customer can validate the authenticity of her measuring data and cross-check it with the bill.

The Selma concept allows the use of existing infrastructure on the one hand, on the other hand it opens the doors for new technology. Selma is particularly suited in conjunction with internet technologies.

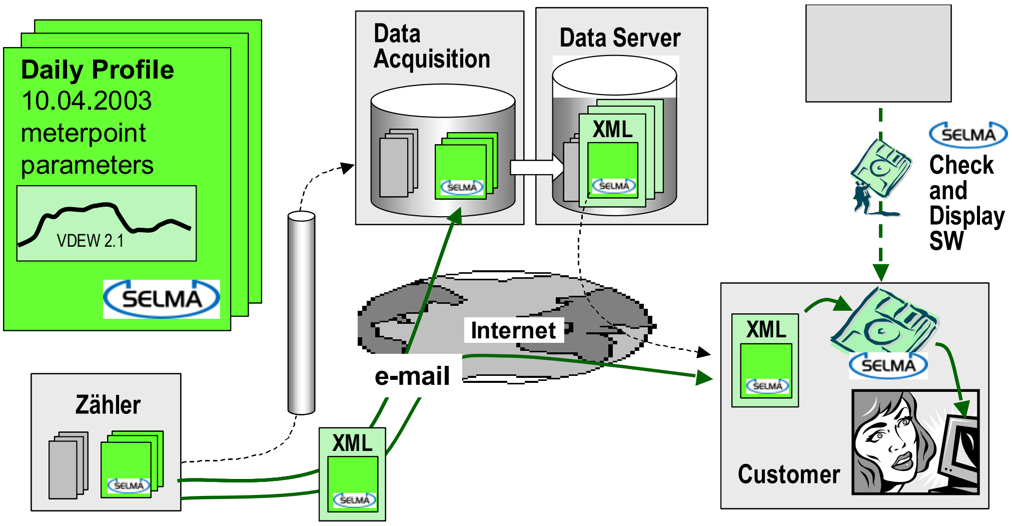

Figure 3: Authenticated measuring data for the validation of the customer bill

4.2 Software Certification

The architecture of the measuring device must be adapted to the new possibilities offered by electronic certification of software and parameters. In figure 4 it is shown how – according to the established approval practice – the software must be partitioned into „certified SW (signed by the certification body) and “approved SW” (signed by the approval body). The download handler classified the SW and intitiates the corresponding signature verification. During the initial approval process it is made sure that the download handler correctly performs the classification of the SW and that the signature verification is correctly done.

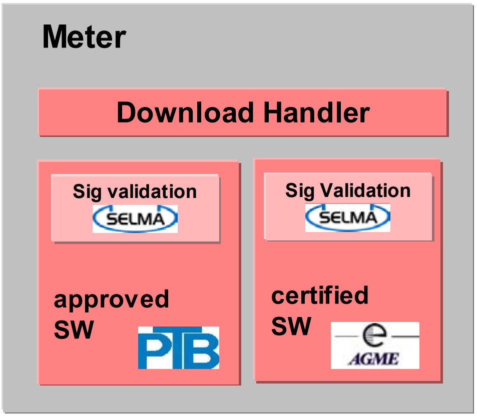

Figure 4: Certified software/parameter handling

5 The signature unit as standard component

The signature method described in section 3 is based on standard algorithms according to [4] and [5]. By using these standards an internationally accepted security level is reached. In addition, standards guarantee independence of the manufacturers.

Selma goes one step further in standardisation. In order to ease the approval process for the introduction of the novel technology in the metering environment, Selma uses a pre-certified signature module. The module comes in form of a chip-card as shown in figure 5 in the lower left corner. The chip-card is placed under the certification seal of the meter. Manufacturers using the pre-certified chip-card are relieved from additional approval tests for the signature unit.

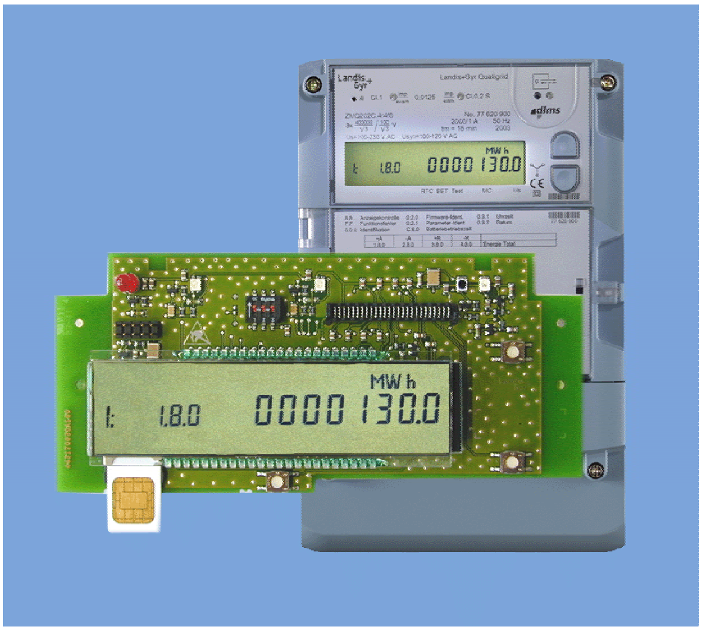

Figure 5: Cryptochip as standard solution

6 Outook

Selma offers a security concept matched to the business processes around energy consumption metering. The signature of the measurement data greatly simplifies the validation of the consumption data at any point of the process chain (from the meter to the bill). With Selma, customer call-backs and re-readings of meters can be avoided. In addition, Selma enables downloading of certified software/parameter packages. With Selma meter maintenance can be automated and the maintenance costs can be substantially reduced. Selma is based on established international standards and can therefore be easily integrated into existing IT infrastructures. The Selma security architecture is scalable and can be introduced step by step; i.e. the investment risk can be kept low.

7 References

[1] Lastenheft Elektronische Elektrizitätszähler, Erweiterte Version 2.1, VDN, Okt. 2002.

[2] IEC62056-62 Electricity metering – Data exchange for meter reading, Part 62: Interface Classes.

[3] SELMA, 1.7 Datenmodelle, V1.7, 19.11.03

[4] National Institute of Standards and Technology, .NIST: FIPS Publication 180-1: Secure Hash Standard (SHS-1),. May 1995.

[5] American National Standards Institute, .Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),. ANSI X9.62-1998, 1998.