Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin

www.selma-project.de

Secure Transfer of Measurement Data

Norbert Zisky
Physikalisch-Technische Bundesanstalt

Market needs

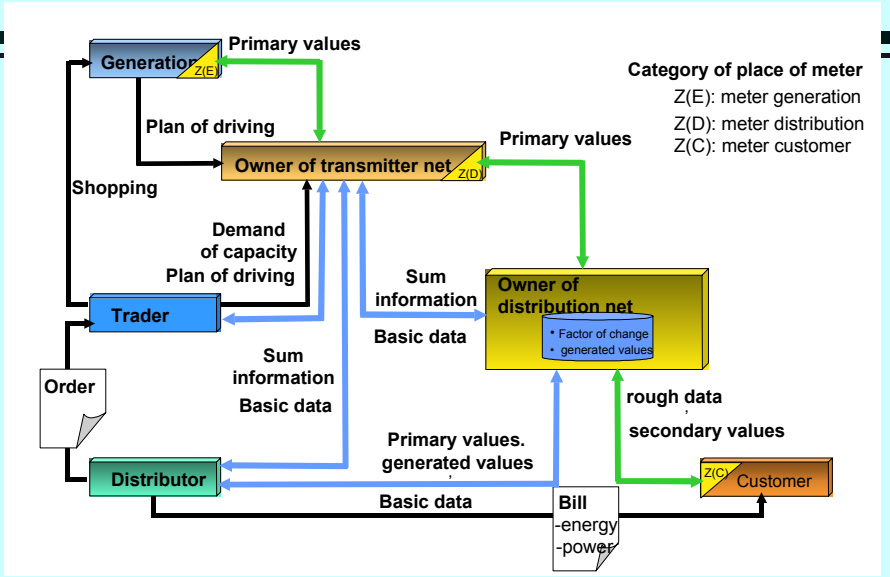
- Liberalized markets require secure and traceable data exchange processes from the meter to the bill via open systems
- Threats, attacks
- Quality assurance
- Consumer protection
  - integrity
  - authenticity
  - confidentiality
  - availabilty

meter

data transfer
data storing

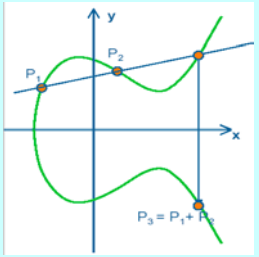
Invoice
Meter-id: ABC453
location: XWZ773
.....
amount1: 233.2 €
amount2: 1567.4 €
total sum: 1800.6 €

Liberalised energy market

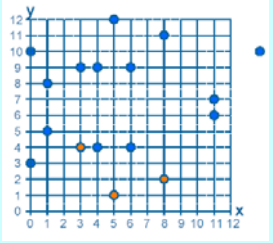


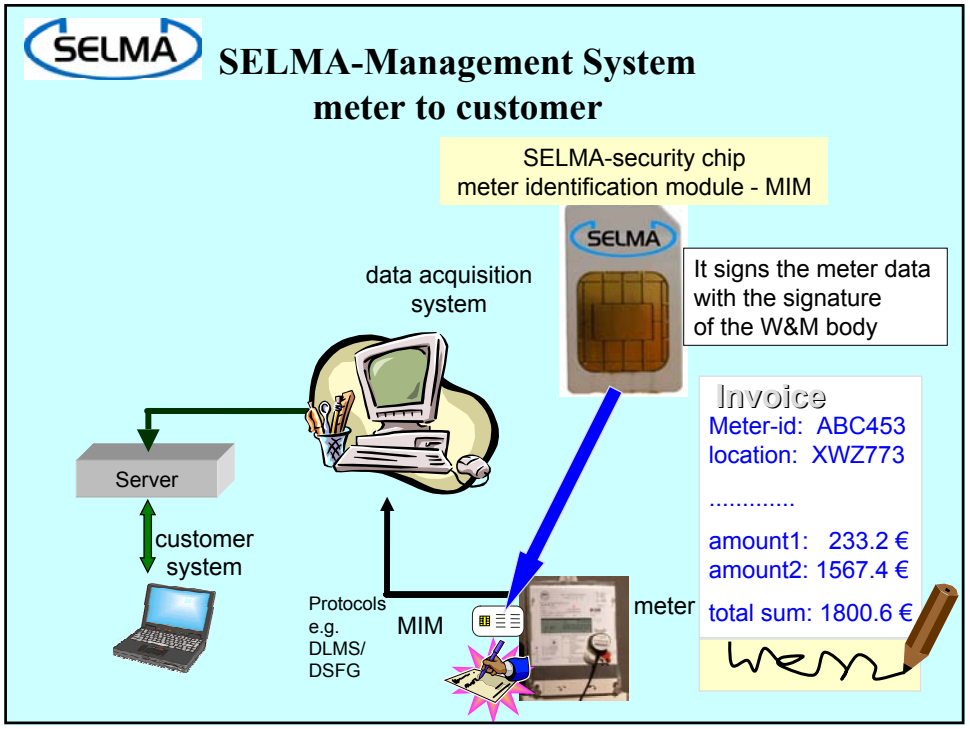
Security concept

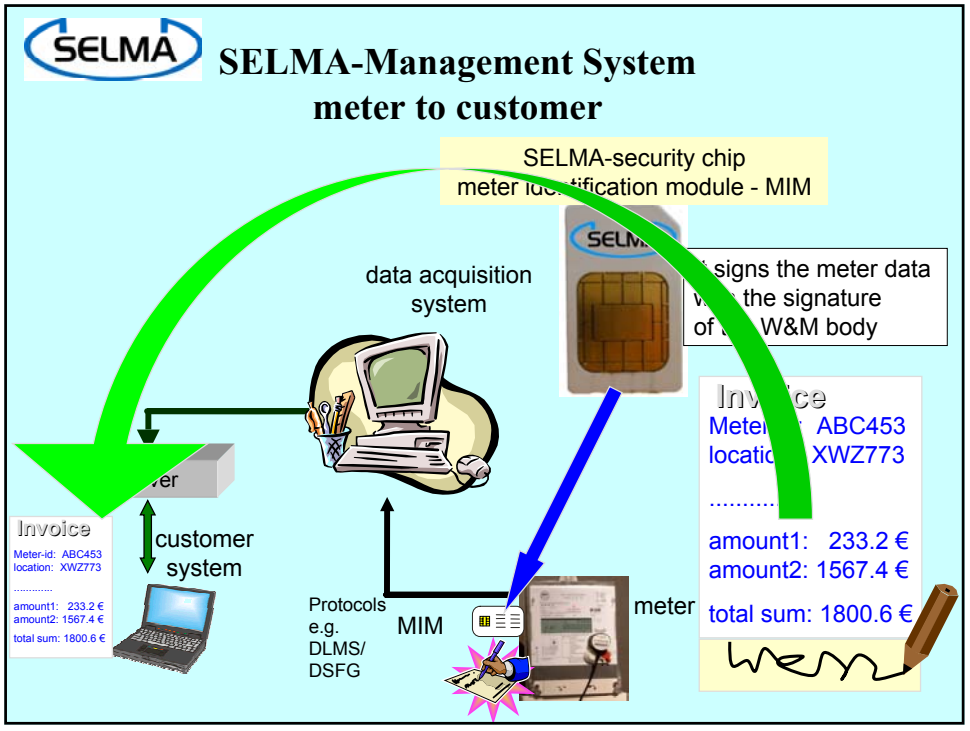
- General: Use of cryptographic methods
- Use of Hash functions to make sure the **integrity** of data, use for SELMA: **SHA-1**
- Use of asymmetric signature procedures for **authenticity** of data, use for SELMA: ECC technique, (Elliptic Curve Cryptography) - **ECDSA**

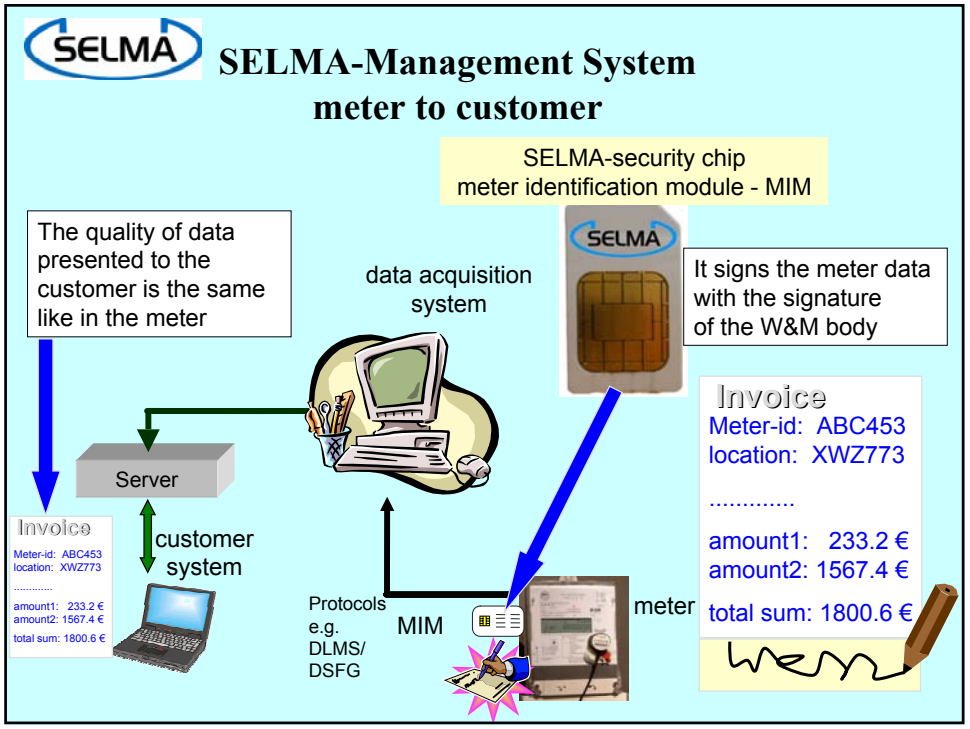


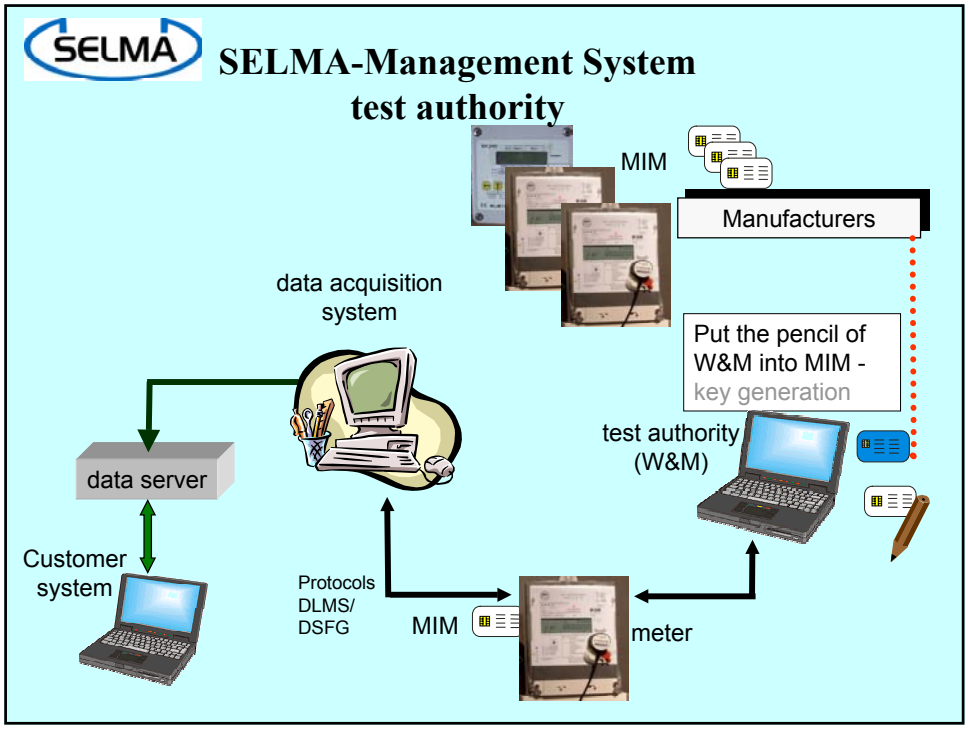
Quelle: Siemens AG, Dr. Erwin Heß



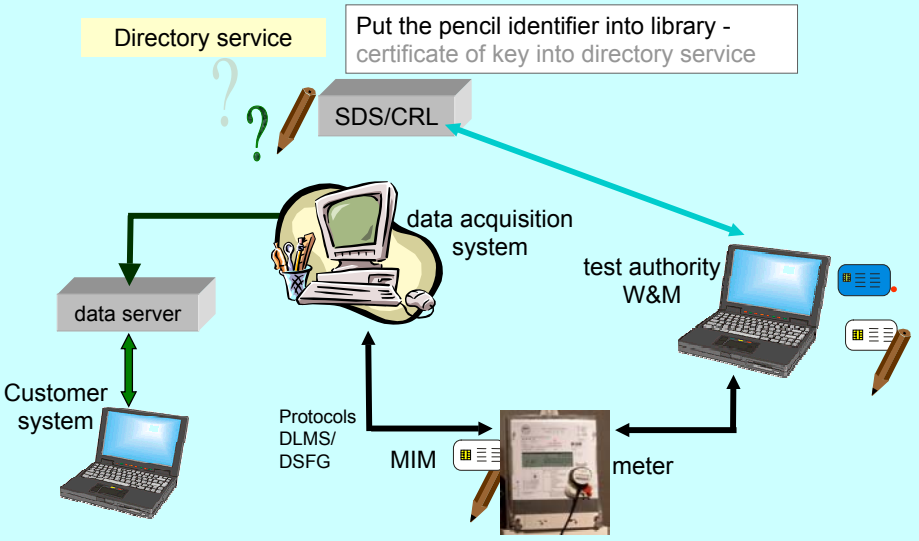

SELMA-Management System
meter to customer
SELMA-security chip
meter identification module - MIM
data acquisition
system
It signs the meter data
with the signature
of the W&M body
Invoice
Meter-id: ABC453
location: XWZ773
.....
amount1: 233.2 €
amount2: 1567.4 €
total sum: 1800.6 €
Server
customer
system
Protocols
e.g.
DLMS/
DSFG
MIM
meter


SELMA-Management System
meter to customer
SELMA-security chip
data acquisition
system
customer
system
Protocols
e.g.
DLMS/
DSFG
MIM
meter

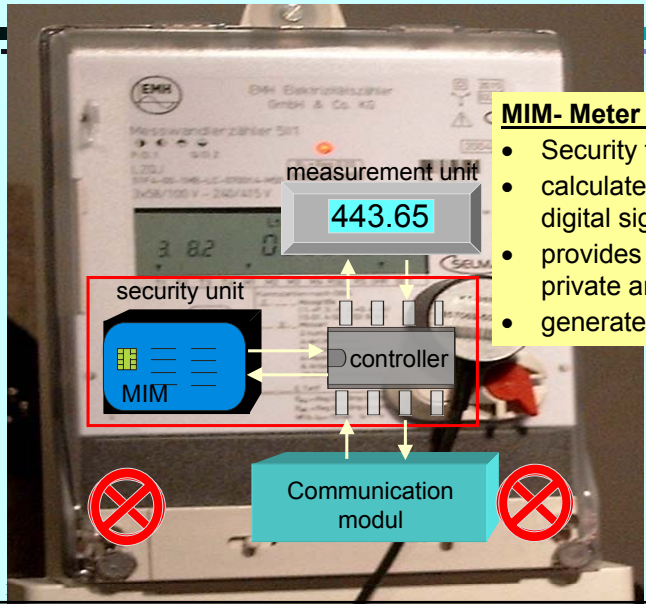

SELMA-Management System
meter to customer
SELMA-security chip
meter identification module - MIM
The quality of data presented to the customer is the same like in the meter
data acquisition system
It signs the meter data with the signature of the W&M body
Invoice
Meter-id: ABC453
location: XWZ773
.....
amount1: 233.2 €
amount2: 1567.4 €
total sum: 1800.6 €
Server
customer system
Protocols e.g. DLMS/ DSFG
MIM
meter


SELMA-Management System
test authority
MIM
Manufacturers
data acquisition system
Put the pencil of W&M into MIM - key generation
test authority (W&M)
data server
Customer system
Protocols DLMS/ DSFG
MIM
meter

SELMA-Management System directory service



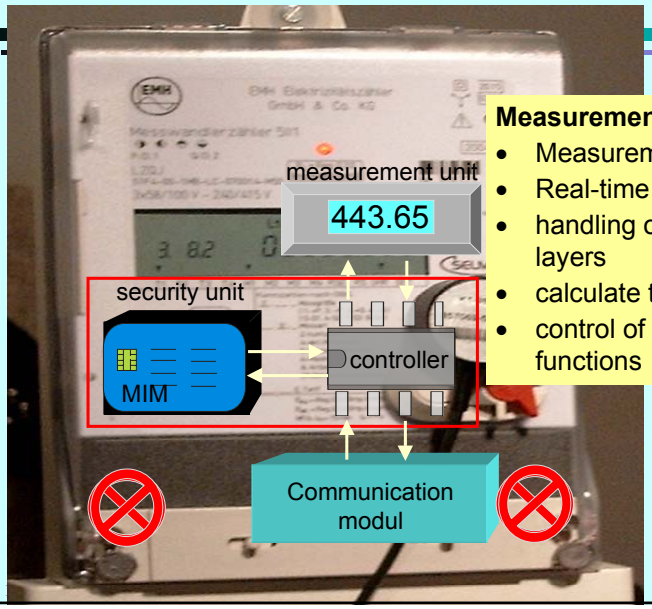
SELMA measurement device



MIM- Meter Identification Module

- Security functions
- calculates and verifies the digital signatures
- provides secure memory for private and public keys, etc.
- generates the pair of keys

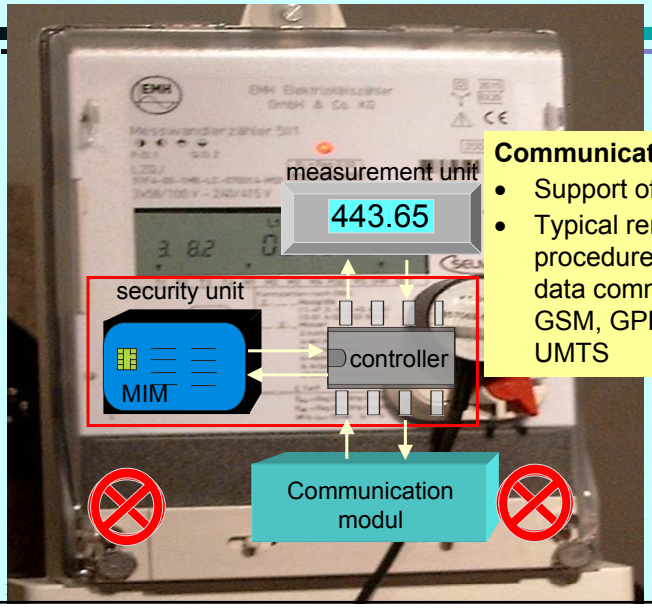
SELMA measurement device



Measurement unit and controller

- Measurement
- Real-time clock
- handling of higher protocol layers
- calculate the hash value
- control of management functions

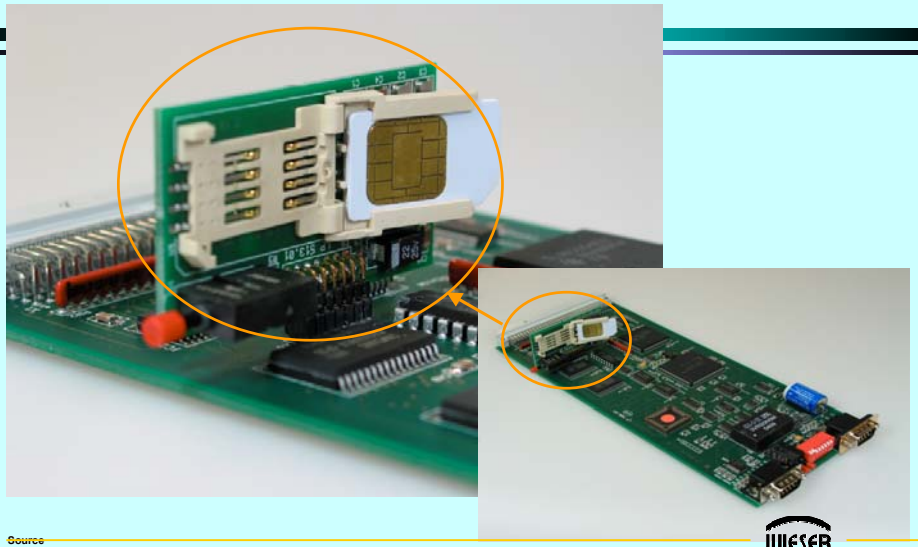
SELMA measurement device



Communication modul

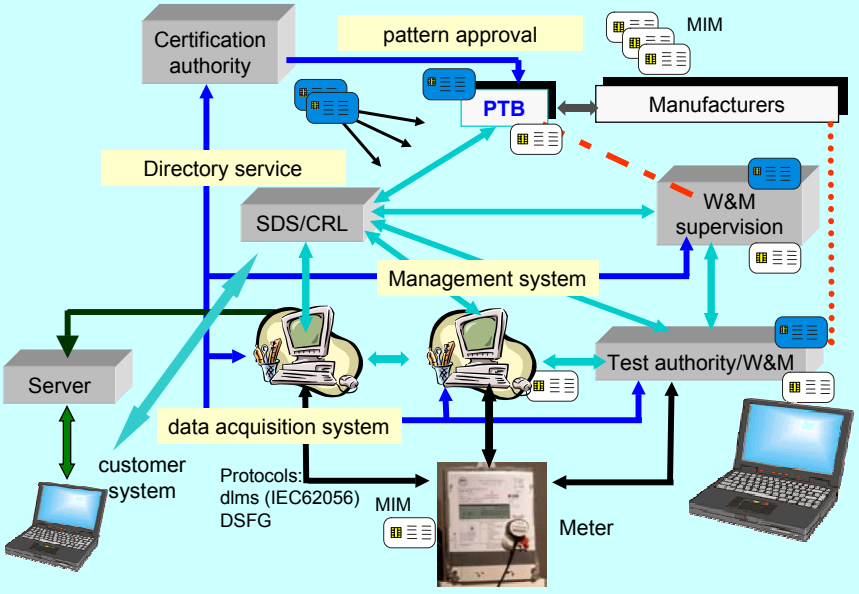
- Support of protocol layer 1 to 3
- Typical remote reading procedures in measurement data communication PSN, GSM, GPRS (strong growing), UMTS

Typical SELMA - board

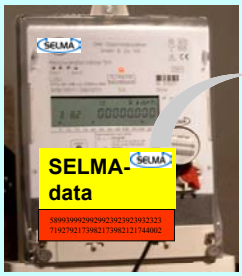


Source
Karl Wieser GmbH, Anzingerstr. 14, 85560 Ebersberg, Tel: 08092/2097-0, Fax: 08092/2097-10, http://www.karlwieser.de

SELMA system environment



Energy data Verification - Overview



SELMA-meter

Data acquistion system

Data base

EDM-
data

customer
SERVER

Costume
/EDM-da

SELMA-Data exchange XML

SELMA-
data

SELMA-
data

Customer
system
CLIENT

verify of signature

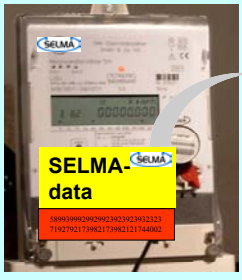
Presentation of
SELMA-data

SELMA-
data

Download of Data

Presentation of
customer-data

Energy data Verification - Overview



SELMA-meter

Data acquistion system

Data base

EDM-
data

customer
SERVER

Costume
/EDM-da

SELMA-Data exchange XML

SELMA-
data

SELMA-
data

Customer
system
CLIENT

verify of signature

Presentation of
SELMA-data

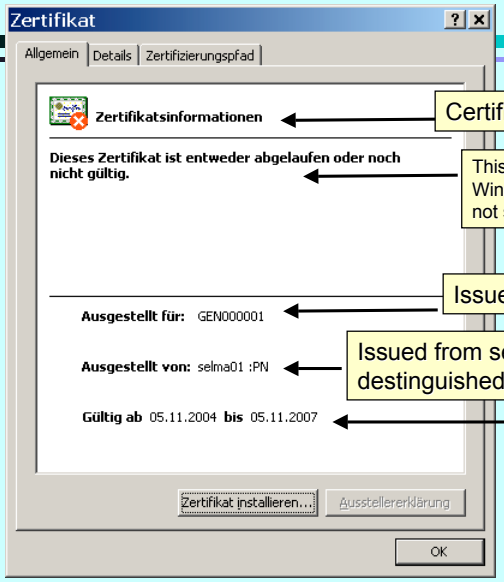
SELMA-
data

Download of data

Presentation of
customer-data

Check of certificate!!

Verification of a meter certificate (1)



Certificate information

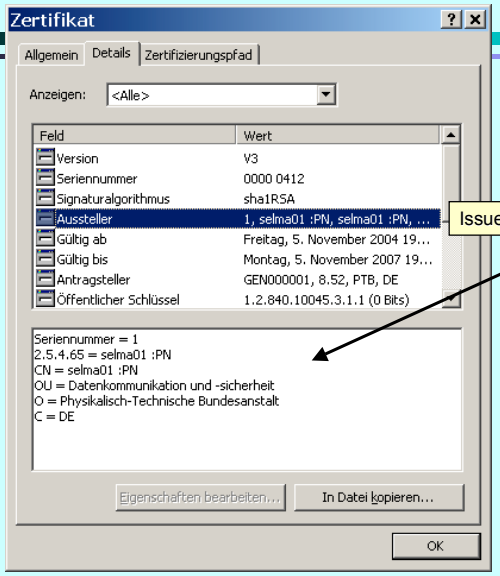
This message is generated because the Windows OS certificate verification model do not support the chain model

Issued for meter : GEN000001

Issued from selma01:PN (common name of destinguished name of test authority)

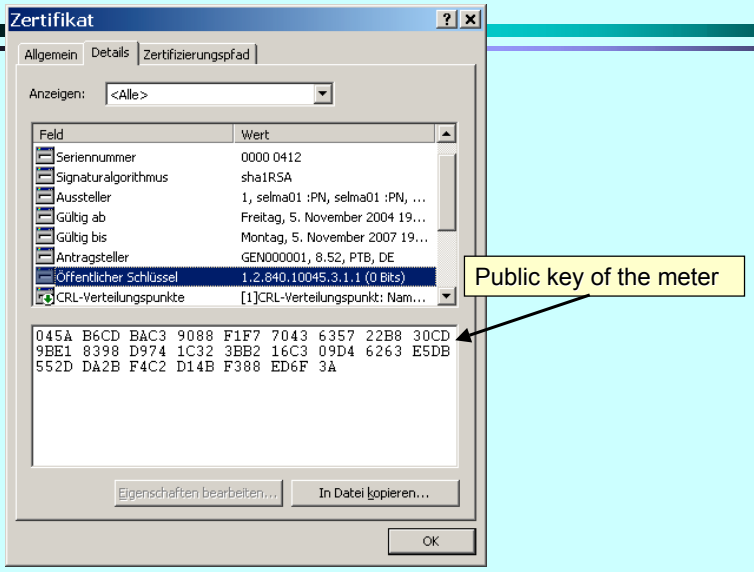
Certificate valid period

Verification of a meter certificate (2)

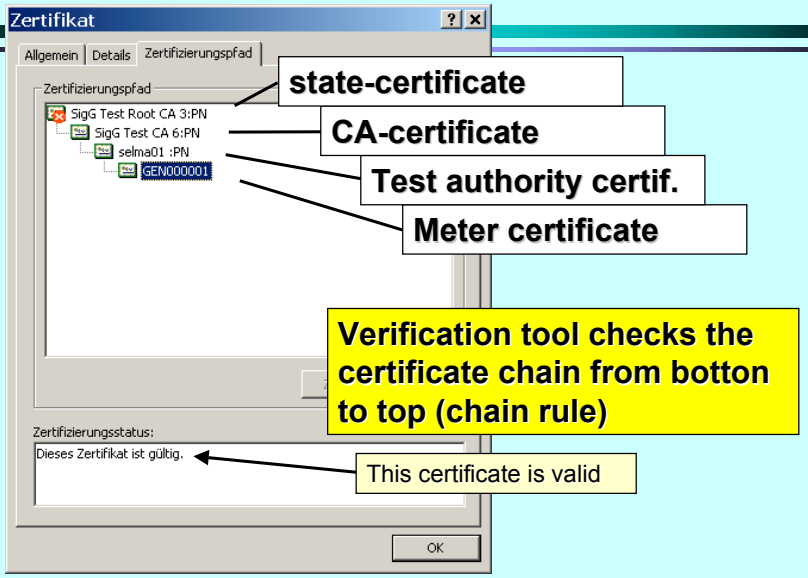


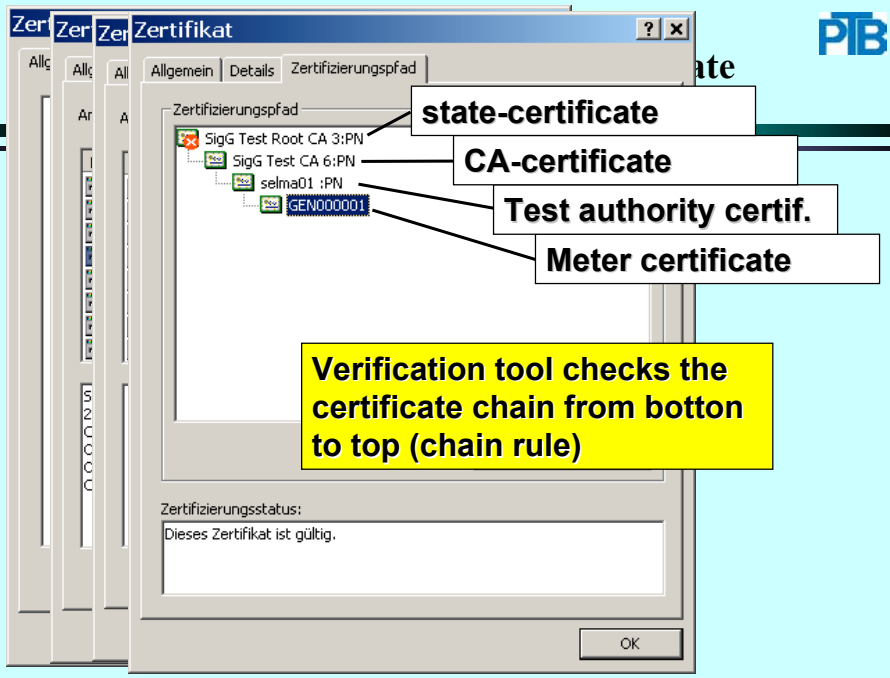
Issuer of certificat: - the full destiguished name

Verification of a meter certificate (3)



Verification of a meter certificate (4)





Energy data verification - Overview

9 month - SELMA field trial

90	electricity meters	EMH; L+G; Görlitz
60	gas meters	Wieser; Elster
3	data acquisition systems	Görlitz; ITF-EDV-Fröschl
4	testing authorities	AGME; EAM; EnBW; RWE
7	device management systems	all testing authorities
1	SELMA-Directory-Service (SDS)	University of Siegen
customer systems (EVM)		all project members

Aims of the field trail

- Verification of SELMA technique under real conditions
- Proof of accepance of all SELMA functions

Summary: SELMA.....

- offers a secure and traceable data exchange concept from the meter to the bill.
- provides a security architecture supporting the authentication of measuring data and the secure data access
- represents a comprehensive security concept adapted to the needs of liberalized energy (electricity, gas, water, heat) markets.
- considers the complete metering process chain – from calibration and installation to measurement and billing.

Advantages of SELMA

- All parties get the correct measurement data
- All signed data are testable over the whole live cycle
- High quality of data
- Open and scalable security
- Secure data transfer via open channels
- Consideration of existing international standards
- Taking into account the economic and regulatory conditions in the metering environment

SELMA represents a best practice cryptographic solution for metrology purposes

Outlook

- Improvement of SELMA - test procedures
- Testing of hard and software for SELMA-meters and system technique
- Evaluation of the SELMA - field trial
- Fixing of the next steps

From 2005 Use of SELMA-technique

Verified and prooved procedures for the exchange of measurement data subject to legal verification

Many thanks for your attention