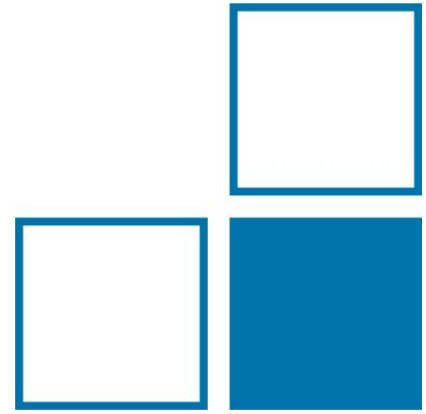
Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
National Metrology Institute

ENG63 GridSens

Sensor network metrology for the detemination of electrical grid characteristics

WP4 Security and Standardisation

Yiyang Su, Joerg Neumann



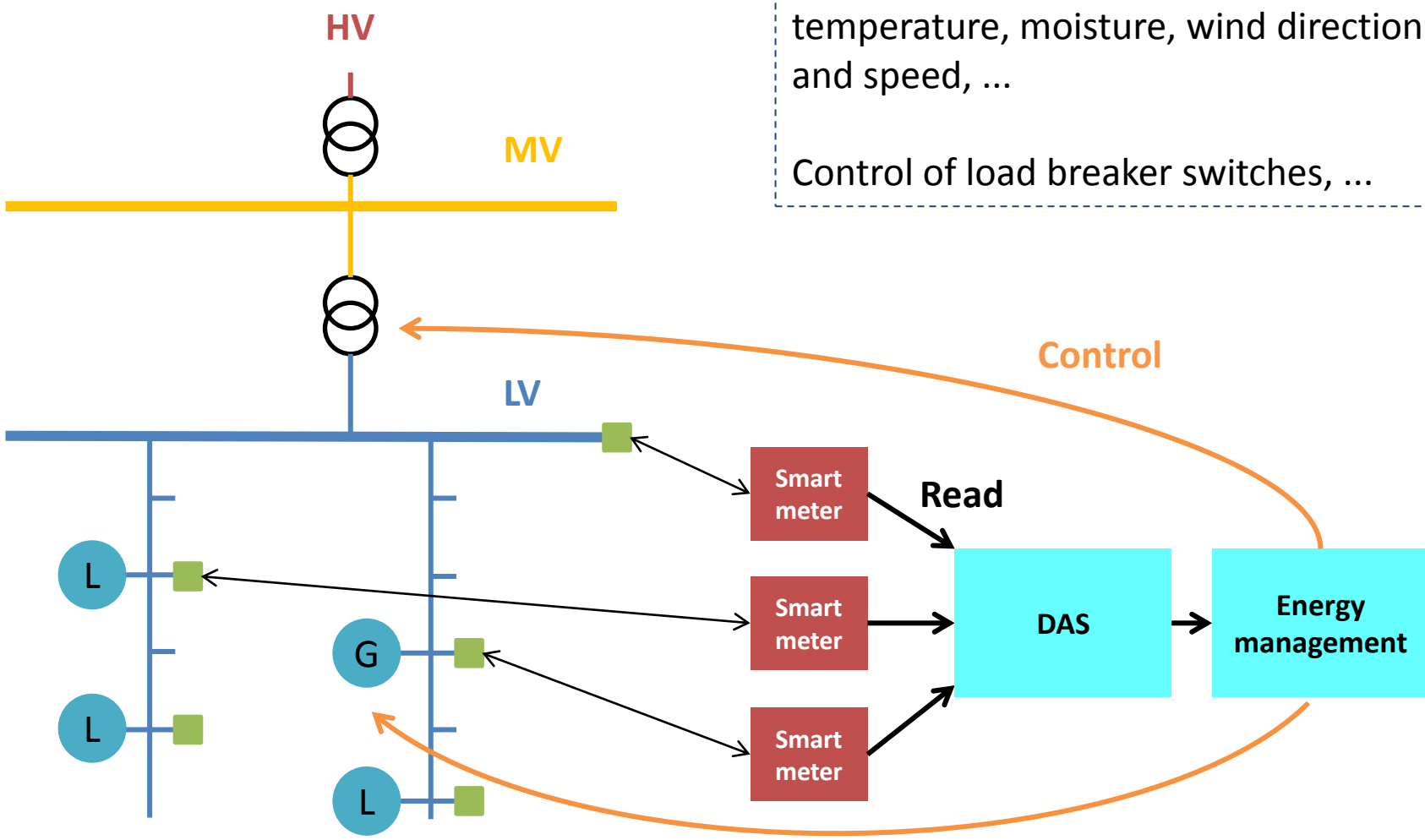
Overview

- Motivation
- Security concept
- Progress

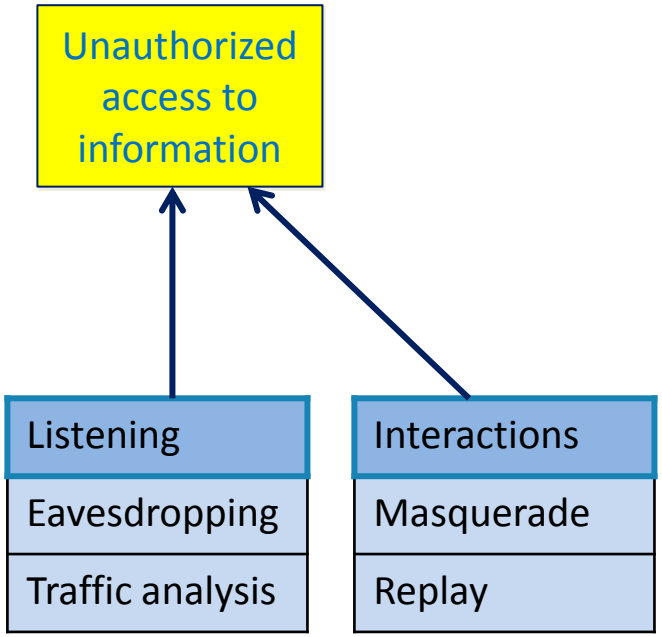
Motivation

Measurements of voltage, current, temperature, moisture, wind direction and speed, ...

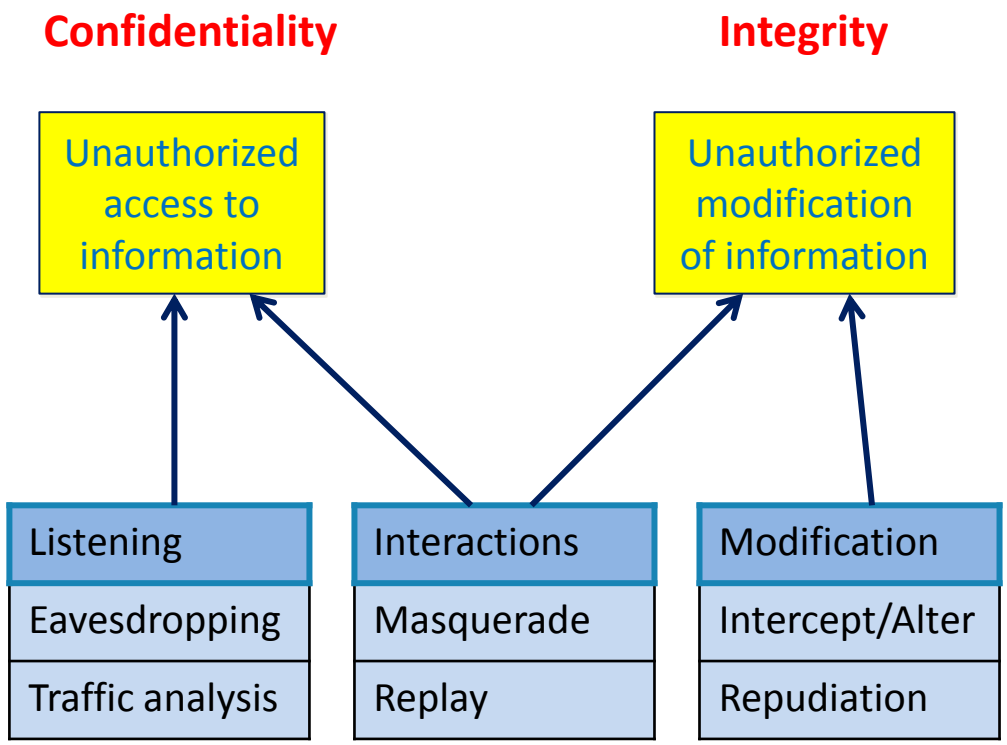
Control of load breaker switches, ...



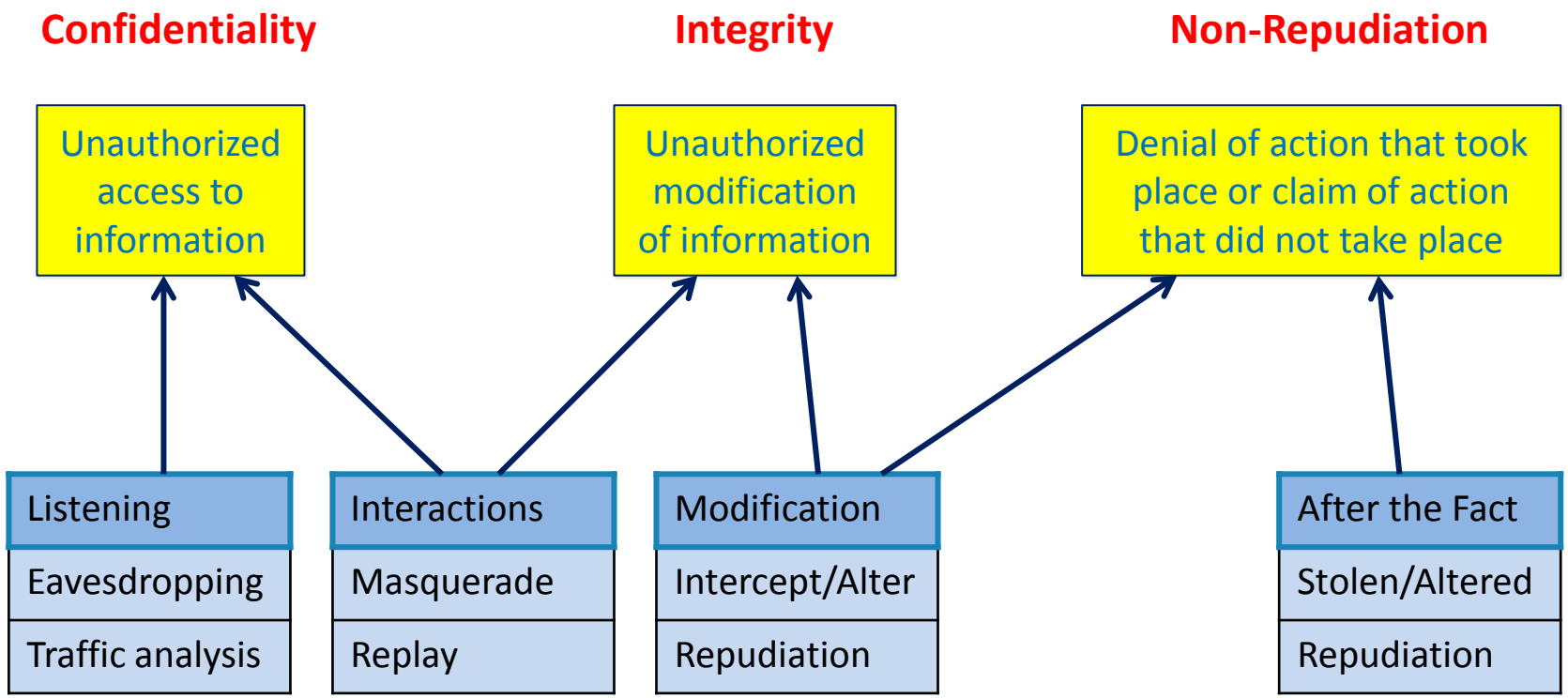
Confidentiality



Security requirements, threats and attacks

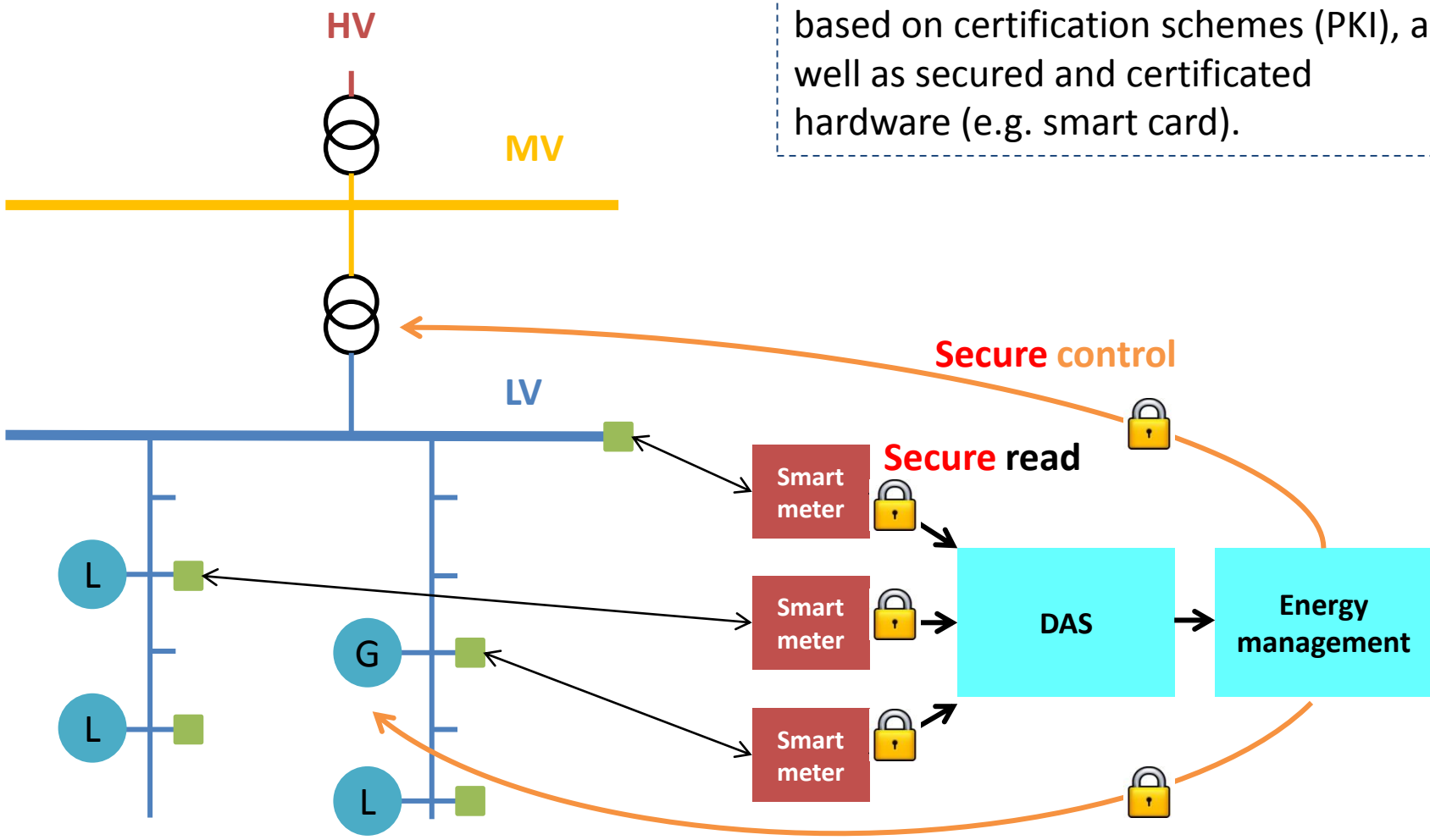


Security requirements, threats and attacks



Security concept

Bidirectional end-to-end authetication based on certification schemes (PKI), as well as secured and certificated hardware (e.g. smart card).



Bidirectional end-to-end authetication

Signature generation and verification

Public key algorithm:

Rivest-Shmair-Adleman (RSA),

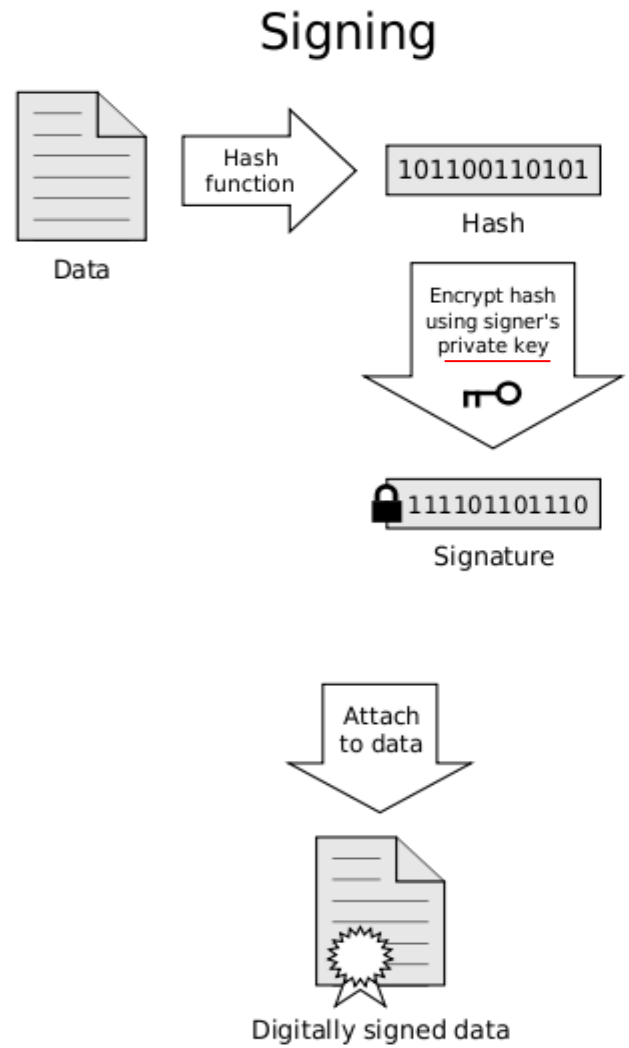
Elliptic Curve Digital Signature Algorithm (ECDSA)

Each entity has one pair of cryptographic keys:

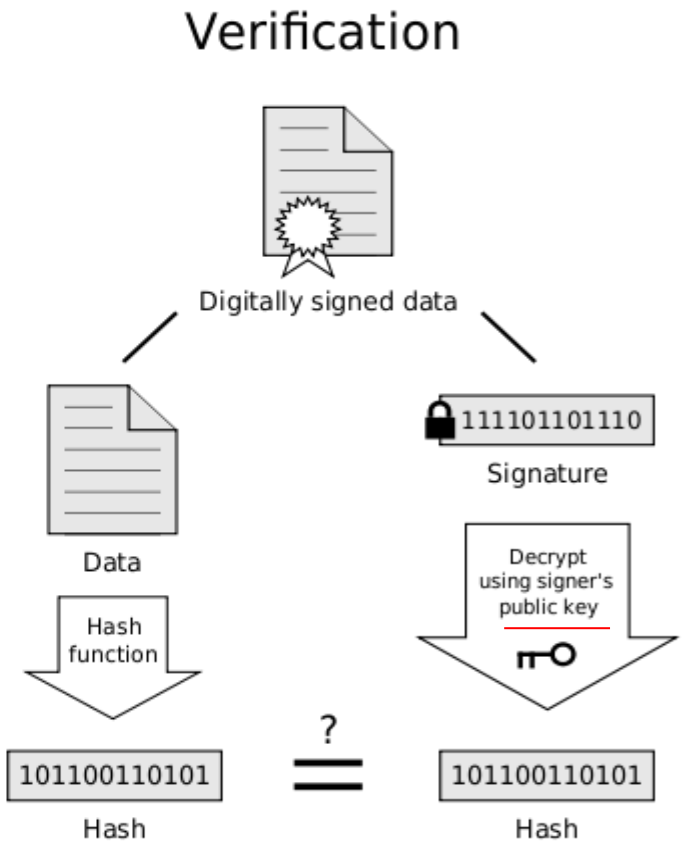
private cryptographic key is used to generate a signature,

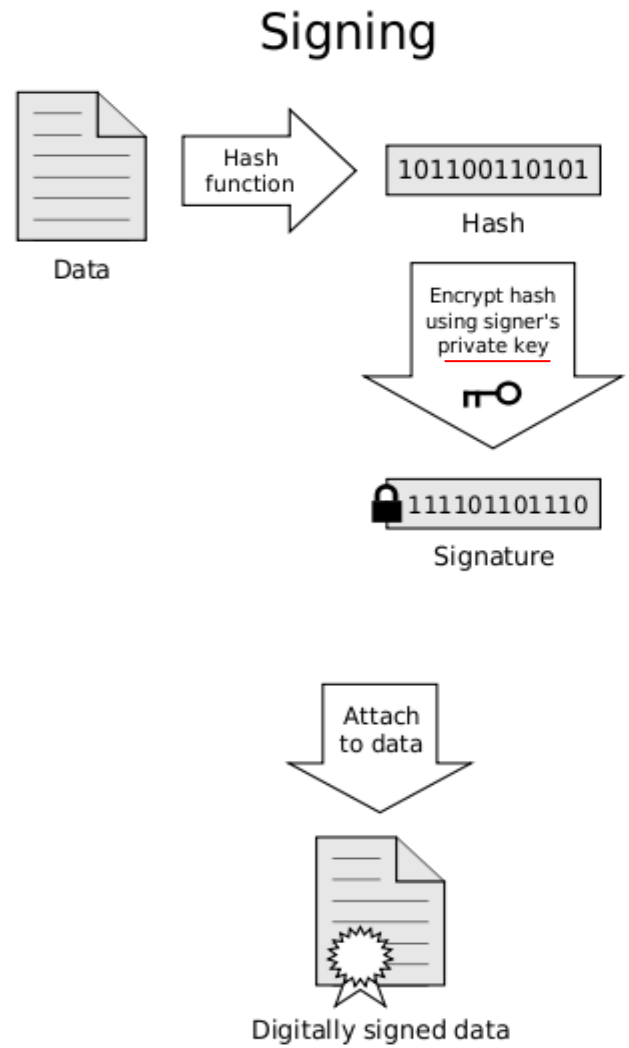
public cryptographic key is used to verify the signautre

Signature generation and verification



Signature generation and verification





Public key infrastructure

By only using public key algorithms we are facing following problems:

- Who can generate the cryptographic key pair?
- Who can guarantee the cryptographic key pair can be trusted?
- How can different entities exchange thier public cryptographic key?

Public key infrastructure

By only using public key algorithms we are facing following problems:

- Who can generate the cryptographic key pair?
- Who can guarantee the cryptographic key pair can be trusted?
- How can different entities exchange thier public cryptographic key?

A suitable key managemet is required:

Public Key Infrastructure (PKI)

Public key infrastructure

Certificate Authority (CA):

- generates key pair
- offers public key certificate certifying that the private key associated with the public key in the certificate belongs to that user

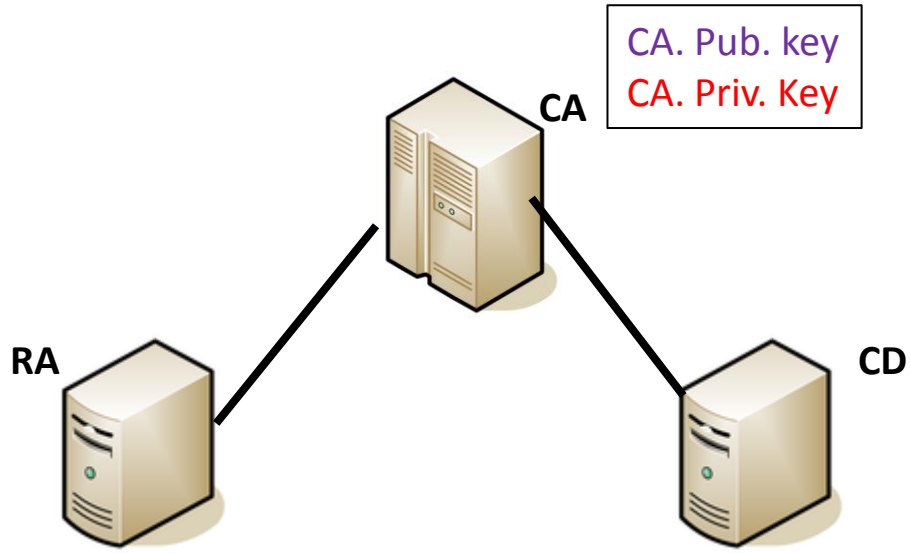
Registration Authority (RA):

- verifies the identity of users requesting key pairs from CA
- delivers key pair to verified users

Central Directory (CD):

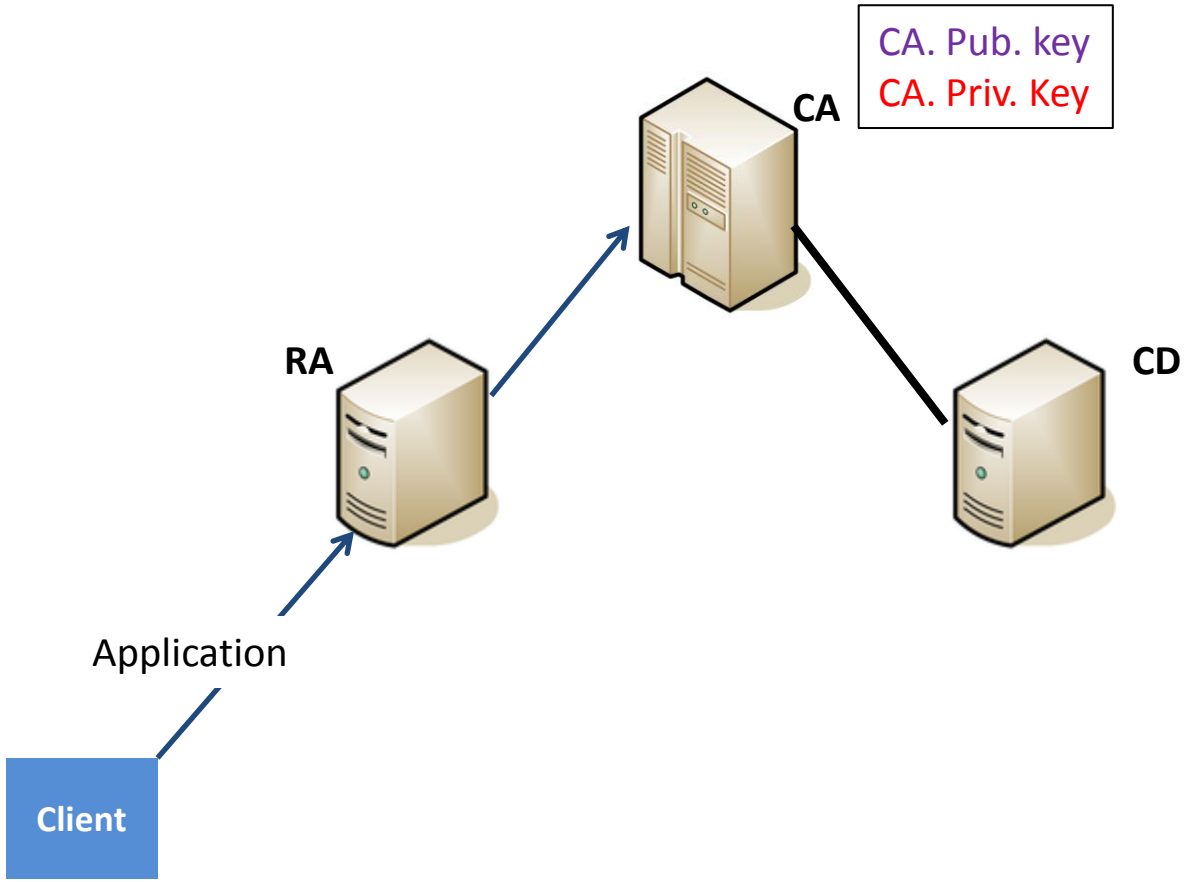
- a secure location in which to store and index public key certificate

Public key infrastructure

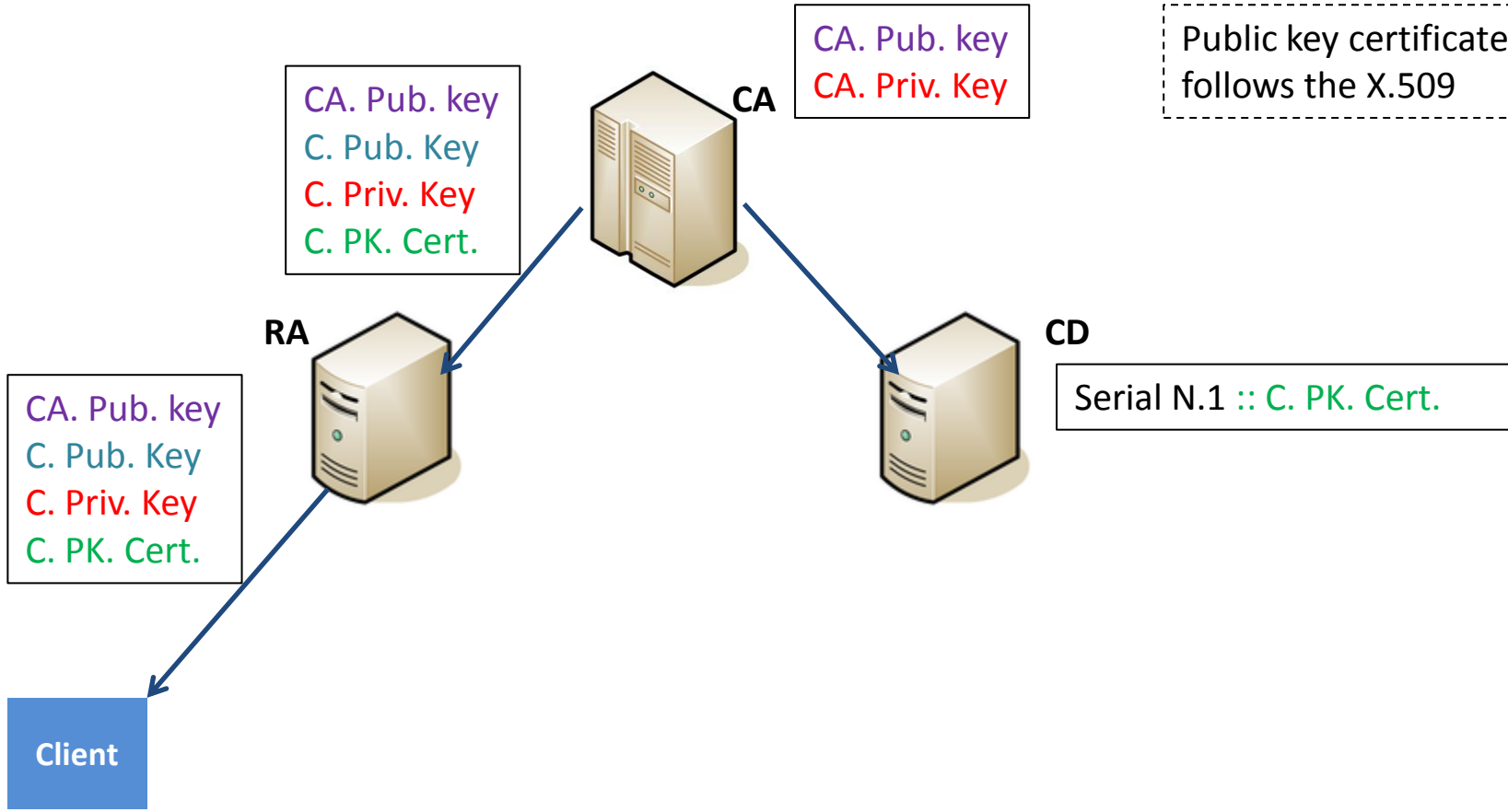


Client

Public key infrastructure



Public key infrastructure

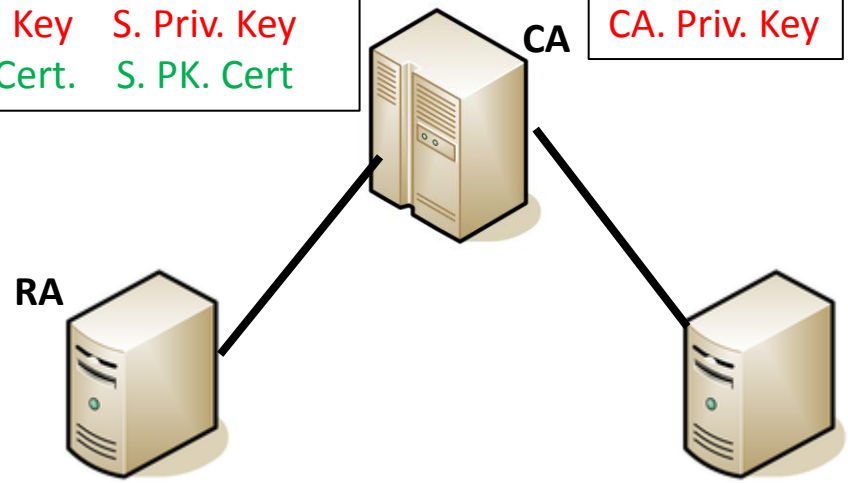


Public key infrastructure

C. Pub. Key S. Pub. Key
C. Priv. Key S. Priv. Key
C. PK. Cert. S. PK. Cert

CA. Pub. key
CA. Priv. Key

Public key certificate follows the X.509



Serial N.1 :: C. PK. Cert.
Serial N.2 :: S. PK. Cert.

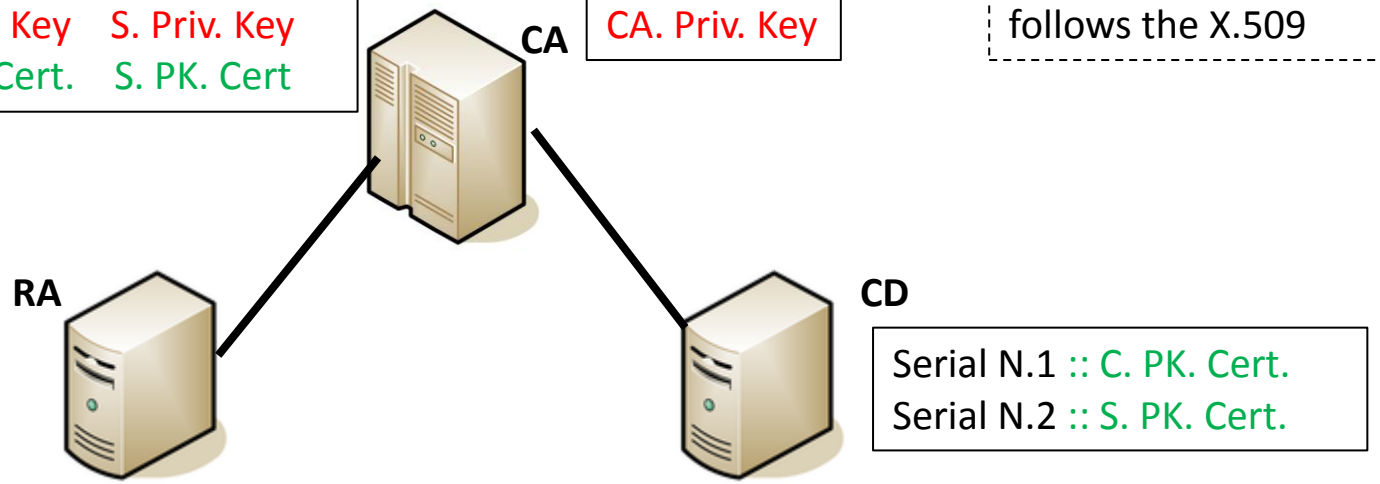
Client

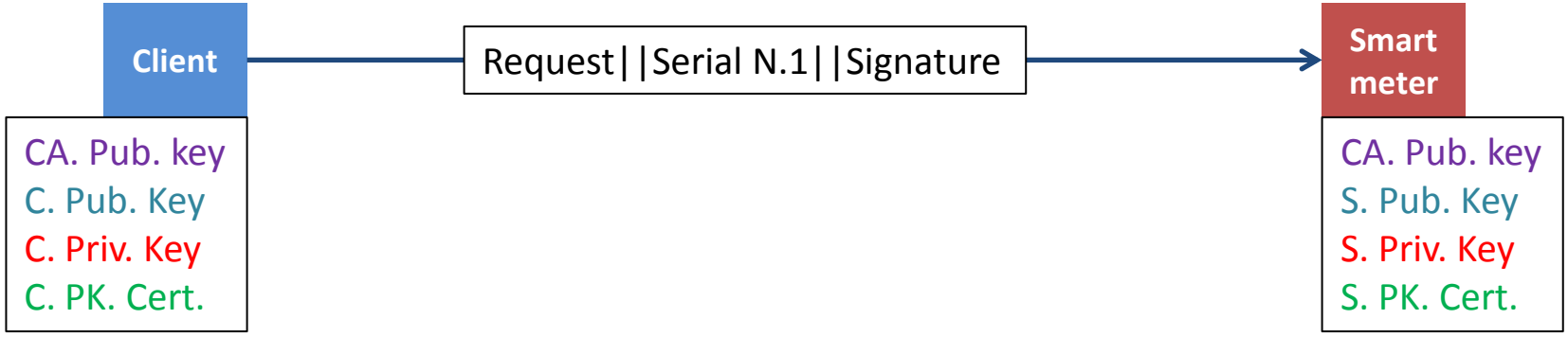
CA. Pub. key
C. Pub. Key
C. Priv. Key
C. PK. Cert.

Smart meter

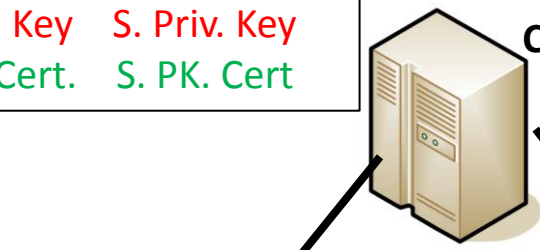
CA. Pub. key
S. Pub. Key
S. Priv. Key
S. PK. Cert.

Public key infrastructure





Public key infrastructure



C. Pub. Key S. Pub. Key
C. Priv. Key S. Priv. Key
C. PK. Cert. S. PK. Cert

CA

CA. Pub. key
CA. Priv. Key

Public key certificate follows the X.509

RA

CD

Serial N.1 :: C. PK. Cert.
Serial N.2 :: S. PK. Cert.

Request||Serial N.1

Client

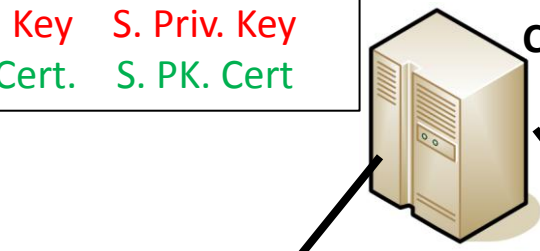
CA. Pub. key
C. Pub. Key
C. Priv. Key
C. PK. Cert.

Request||Serial N.1||Signature

Smart meter

CA. Pub. key
S. Pub. Key
S. Priv. Key
S. PK. Cert.

Public key infrastructure



C. Pub. Key S. Pub. Key
C. Priv. Key S. Priv. Key
C. PK. Cert. S. PK. Cert

CA

CA. Pub. key
CA. Priv. Key

Public key certificate follows the X.509

RA

CD

Serial N.1 :: C. PK. Cert.
Serial N.2 :: S. PK. Cert.

Serial N.1 :: C. PK. Cert.

Client

CA. Pub. key
C. Pub. Key
C. Priv. Key
C. PK. Cert.

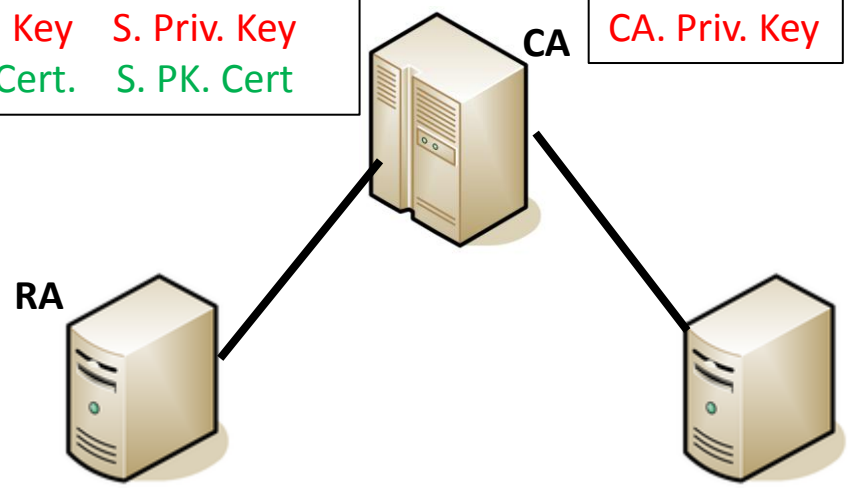
Request||Serial N.1||Signature

Smart meter

CA. Pub. key
S. Pub. Key
S. Priv. Key
S. PK. Cert.

Public key infrastructure

C. Pub. Key S. Pub. Key
C. Priv. Key S. Priv. Key
C. PK. Cert. S. PK. Cert



CA. Pub. key
CA. Priv. Key

Public key certificate follows the X.509

Serial N.1 :: C. PK. Cert.
Serial N.2 :: S. PK. Cert.

Verification

Client

CA. Pub. key
C. Pub. Key
C. Priv. Key
C. PK. Cert.

Smart meter

Request||Serial N.1||Signature

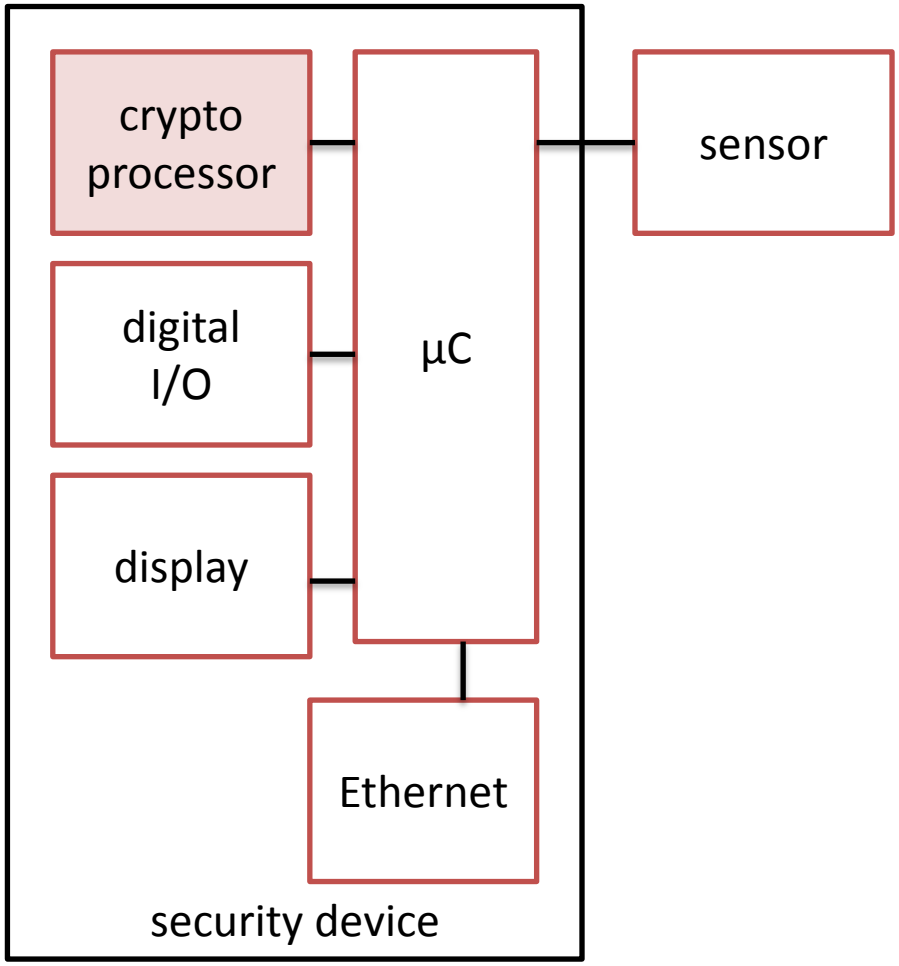
Serial N.1 :: C. PK. Cert.

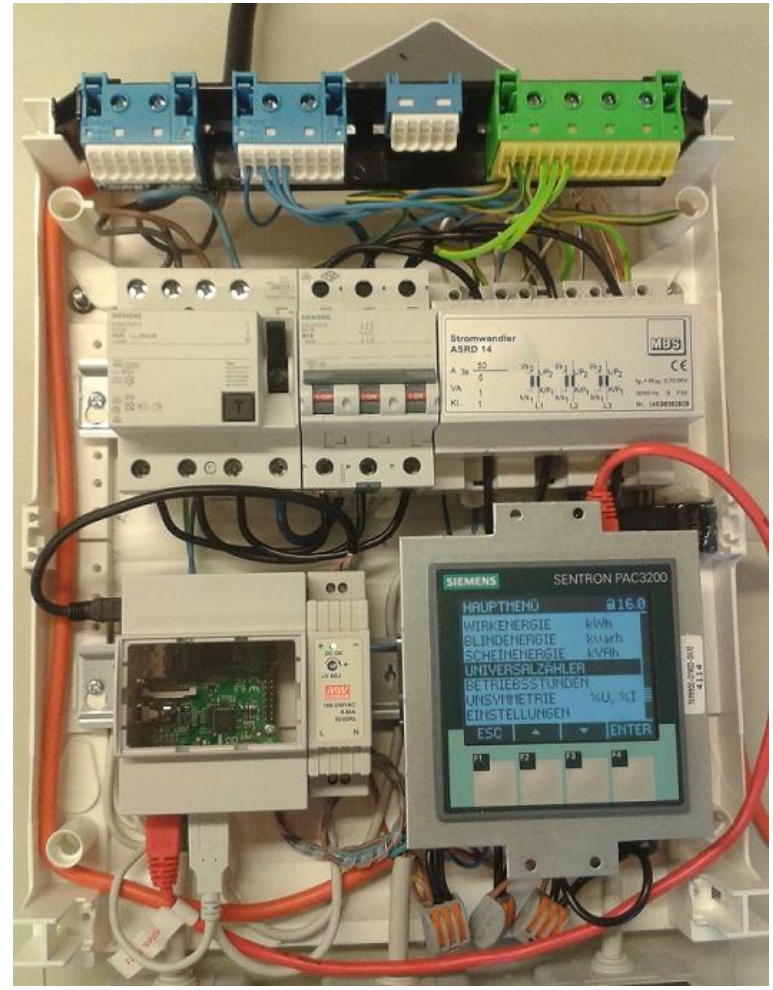
CA. Pub. key
S. Pub. Key
S. Priv. Key
S. PK. Cert.

Progress

- Retrofitting of a meter with security device.

Retrofitting of a meter with security device.

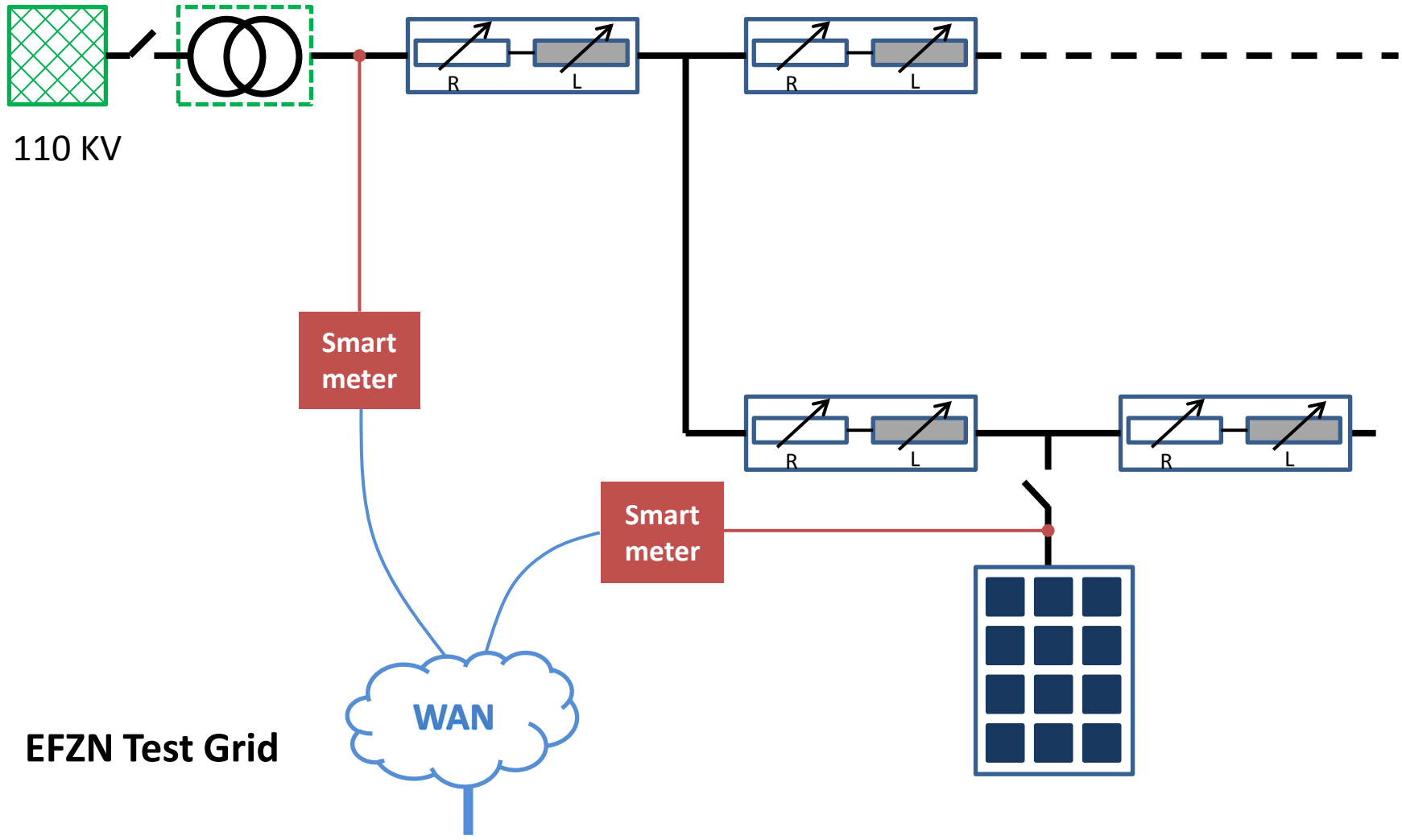




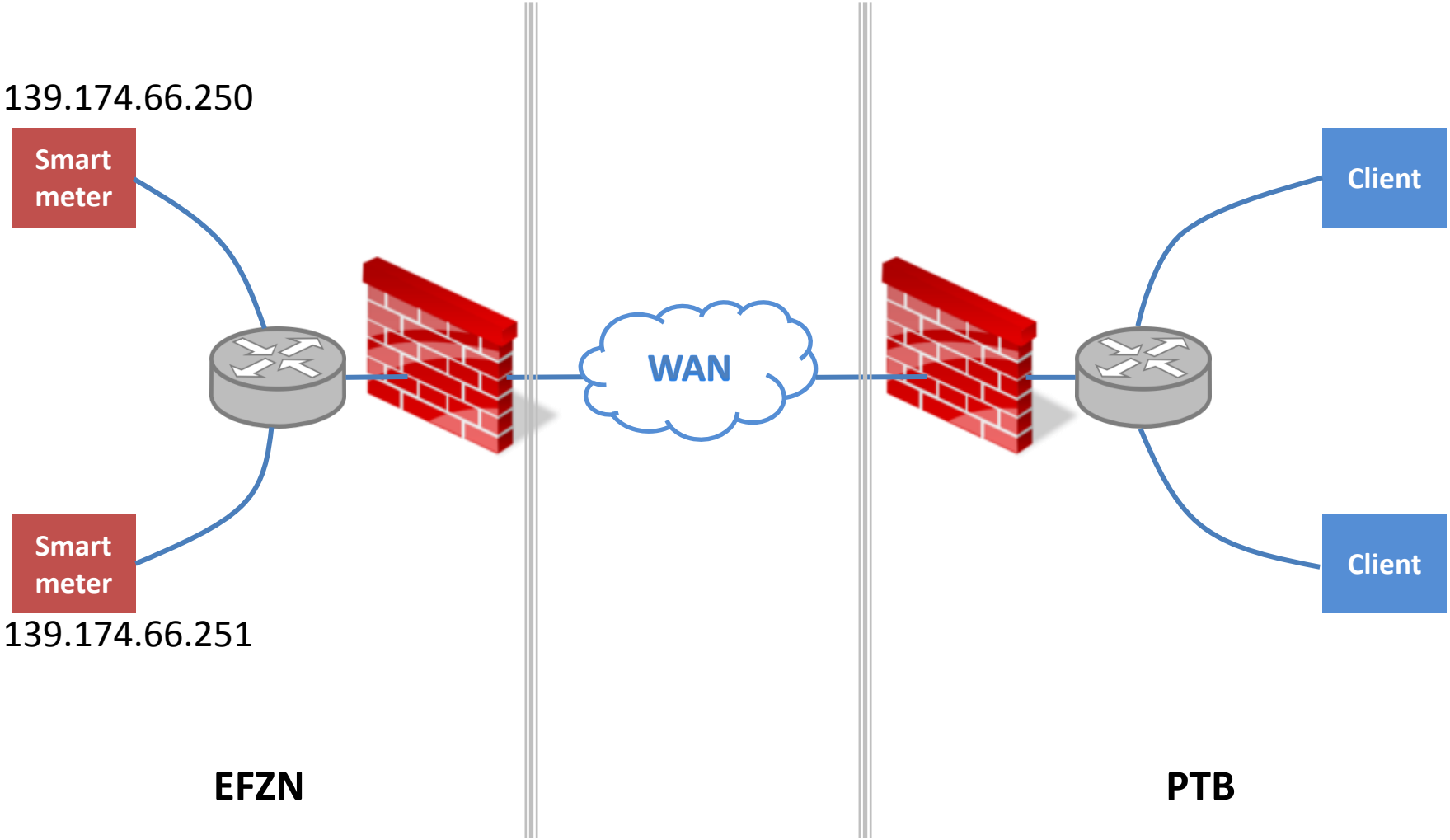
Progress

- Retrofitting of a meter with security device
- Install retrofitted meter in test grid

Sensor set up in the test grid



Communication between EFZN and PTB



Progress

- Retrofitting of a meter with security device
- Install retrofitted meter in test grid
- Define suitable data set for secure communication

Data set

```
signed_measurement_data_type ::= SEQUENCE {
        measurement_data        measurement_data_type
        measurement_data_sig    autehntication_param_type
}

measurement_data_type ::= SEQUENCE {
        measurement_time        date_time
        sequence_nr             Long usigned16
        meter_ident             OCTET STRING      /* printable string */
        meter_number            OCTET STRING      /* printable string */
        location_ident          OCTET STRING      /* printable string */
        counter_values          SEQUENCE OF value_type
        error_code              Unsigned16
        state                   BIT STRING
}

autehntication_param_type ::= SEQUENCE {
        signature               sig_type
        certificate_info        certificate_info_type
}
```

Progress

- Retrofitting of a meter with security device
- Install retrofitted meter in test grid
- Define suitable data set for secure communication
- Set up PKI system

Besides the security requirment, the smart meter must also appropriate to the metrological requirements of Smart Grids:

Response time of a measurement must be as soon as requiered

Besides the security requirment, the smart meter must also appropriate to the metrological requirements of Smart Grids:

Response time of a measurement must be as soon as requiered

Because of additional security device the reaction time of the smart meter is increased

Dynamic behaviour of the smart meter

1. Modularization of the smart meter.

2. Analyse the dynamic behaviour of the communications between different modules and of program functions:

   - communication between µC and crypto processor
   - communication between µC and sensor
   - program execution time of signing and verification, if crypto libraries are applied
   - program execution time of other functions, e.g. mapping; encodeing/ decoding

3. Possibility of optimization.

Many Thanks

Scope of WP4 Security and standardisation

4.1: Validation of secured distributed measurement systems

4.2: Definition of generic data model

4.3: Investigation of the dynamic behavior of secured measurement systems

4.4: Testing security of non-device measurement functions

4.5: Investigation of measurement strategies for sensors with cryptography

Progress

Retrofitting of a sensor with secured communication hardware

Chosen sensor

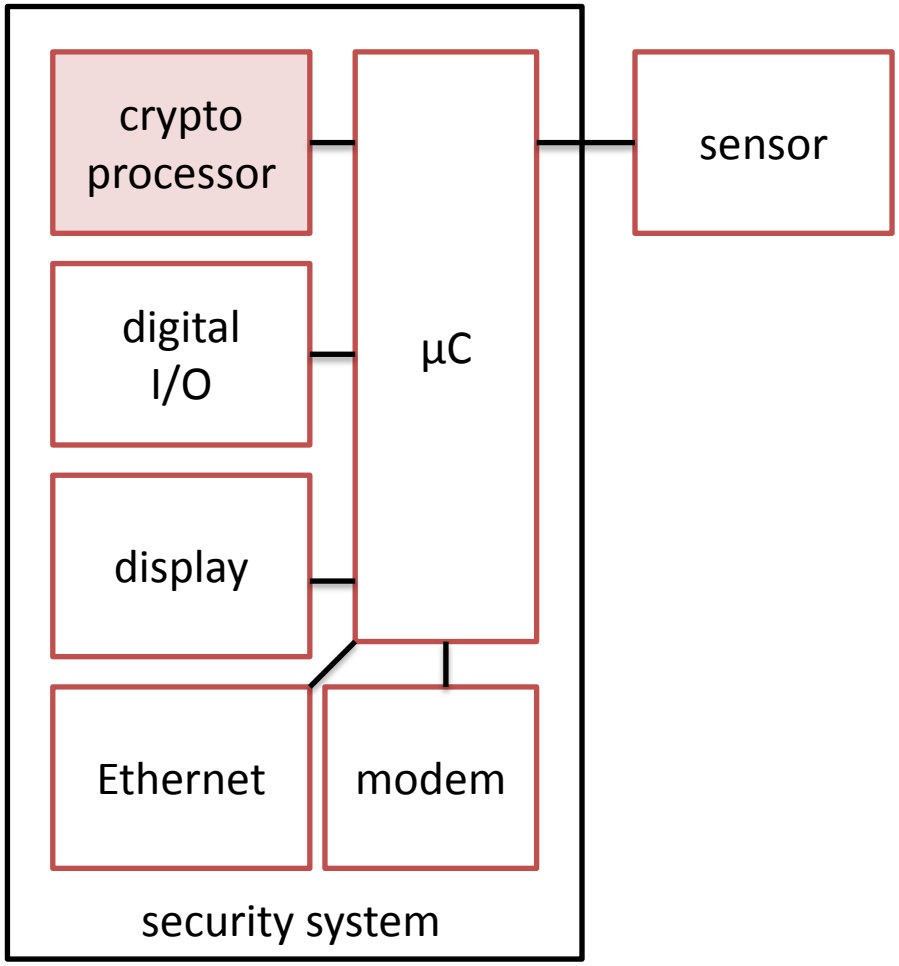
Meter 7KM PAC3200 (D4.1.4)

Communication interface with Modbus TCP

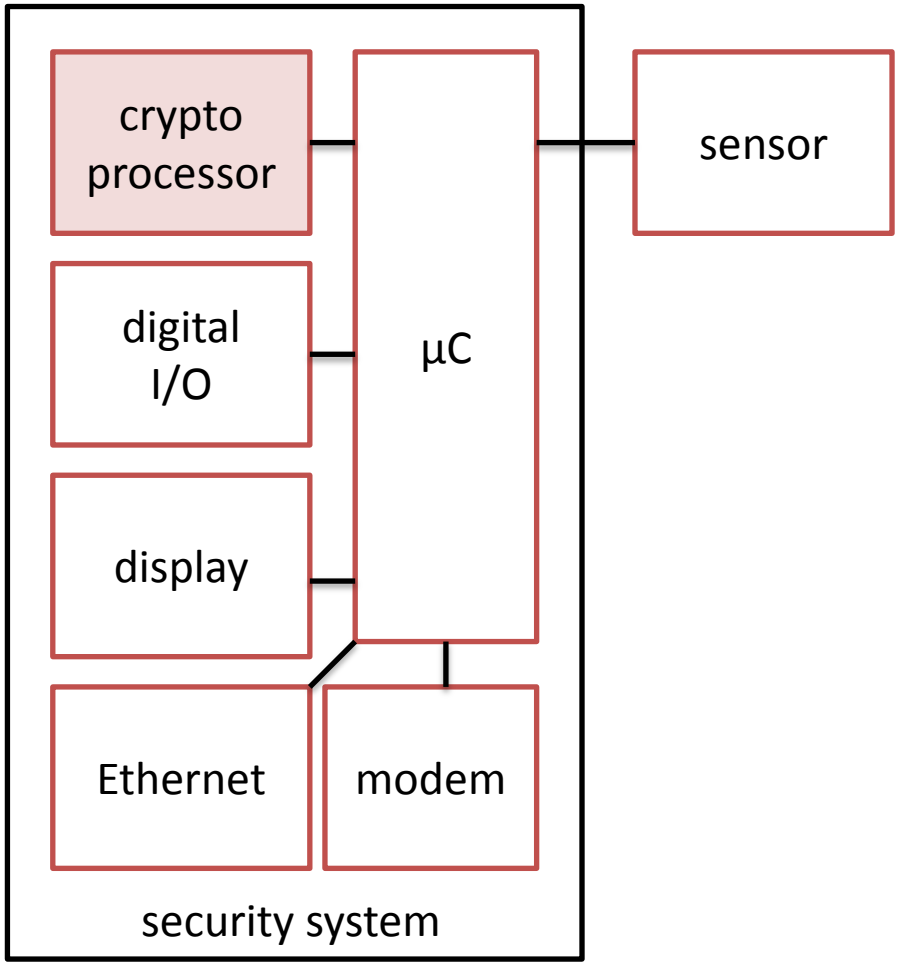
Table 3-3 Measured variables

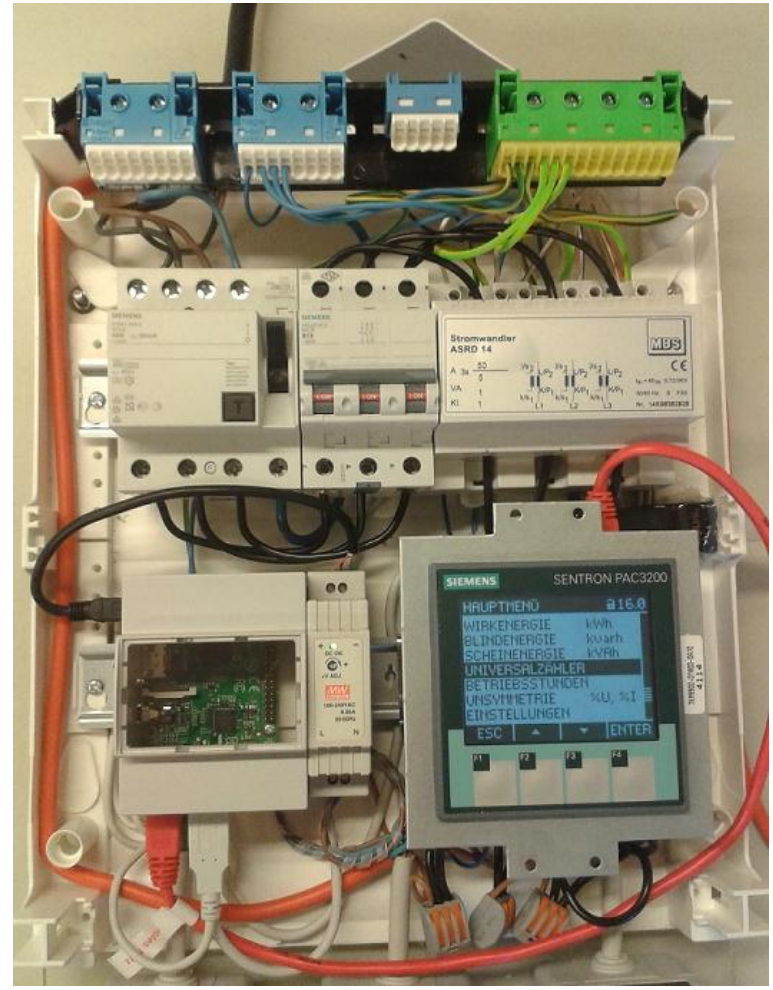
Root-mean-square values	Designation	Instantaneous value	Min.	Max.	Mean value over all phases	Mean value over demand period
Phase-to-neutral voltage	V_{a-n} / V_{b-n} / V_{c-n}	✓	✓	✓	✓[1)]	
Phase-to-phase voltage	V_{a-b} / V_{b-c} / V_{c-a}	✓	✓	✓	✓[1)]	
Current	I_a / I_b / I_c	✓	✓	✓	✓[1)]	
Apparent power per phase	VA_a / VA_b / VA_c	✓	✓	✓		
Active power per phase import/export	$\pm W_a$ / $\pm W_b$ / $\pm W_c$	✓	✓	✓		
Reactive power per phase positive/negative	$\pm VAR_a$ / $\pm VAR_b$ / VAR_c	✓	✓	✓		
Total apparent power	VA_{total}	✓	✓	✓		
Total active power import/export	$\pm W_{total}$	✓	✓	✓		✓[2)]
Total reactive power positive/negative	$\pm VAR_{total}$	✓	✓	✓		✓[2)]

Retrofitting of sensor with secure hardware

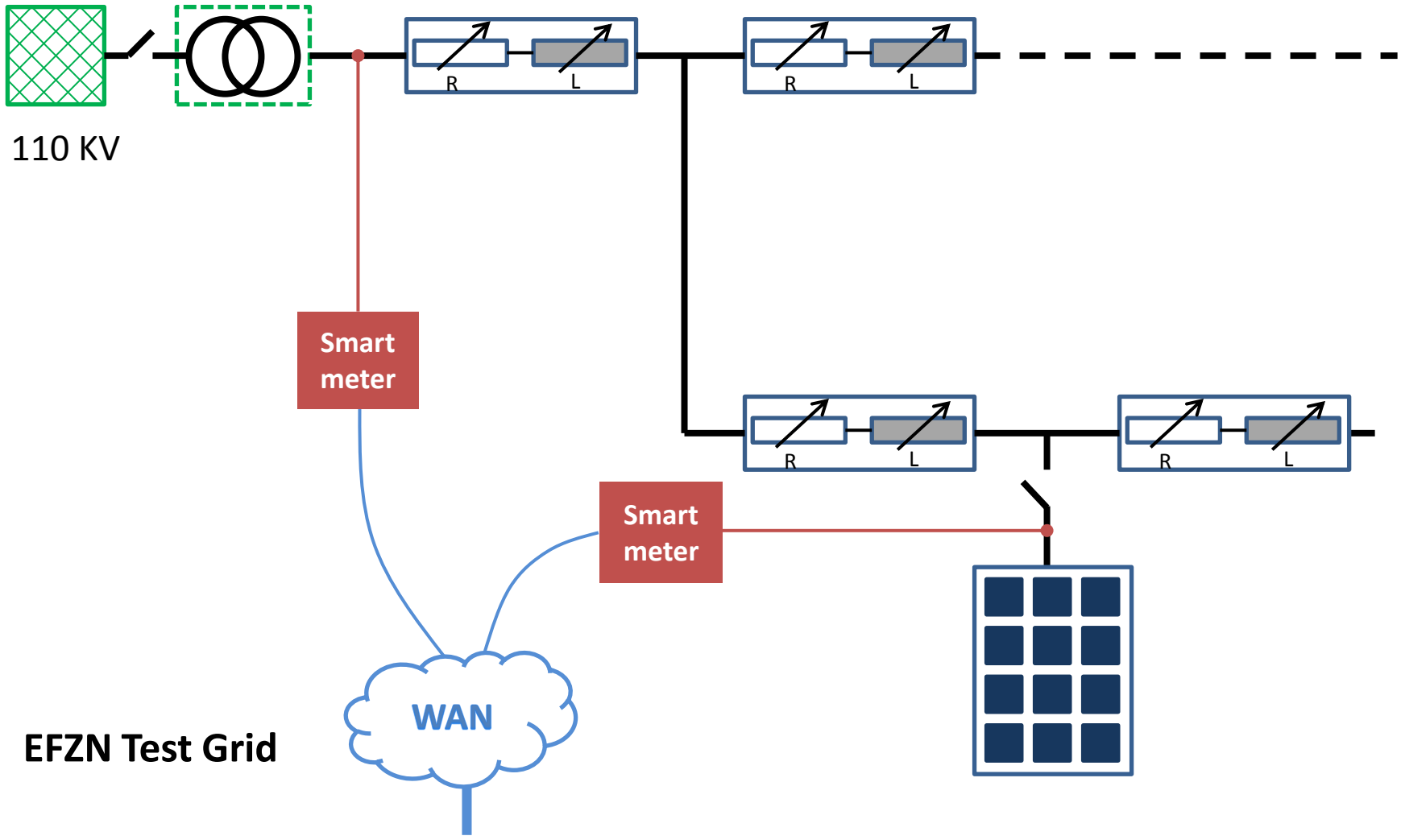


Retrofitting of sensor with secure hardware

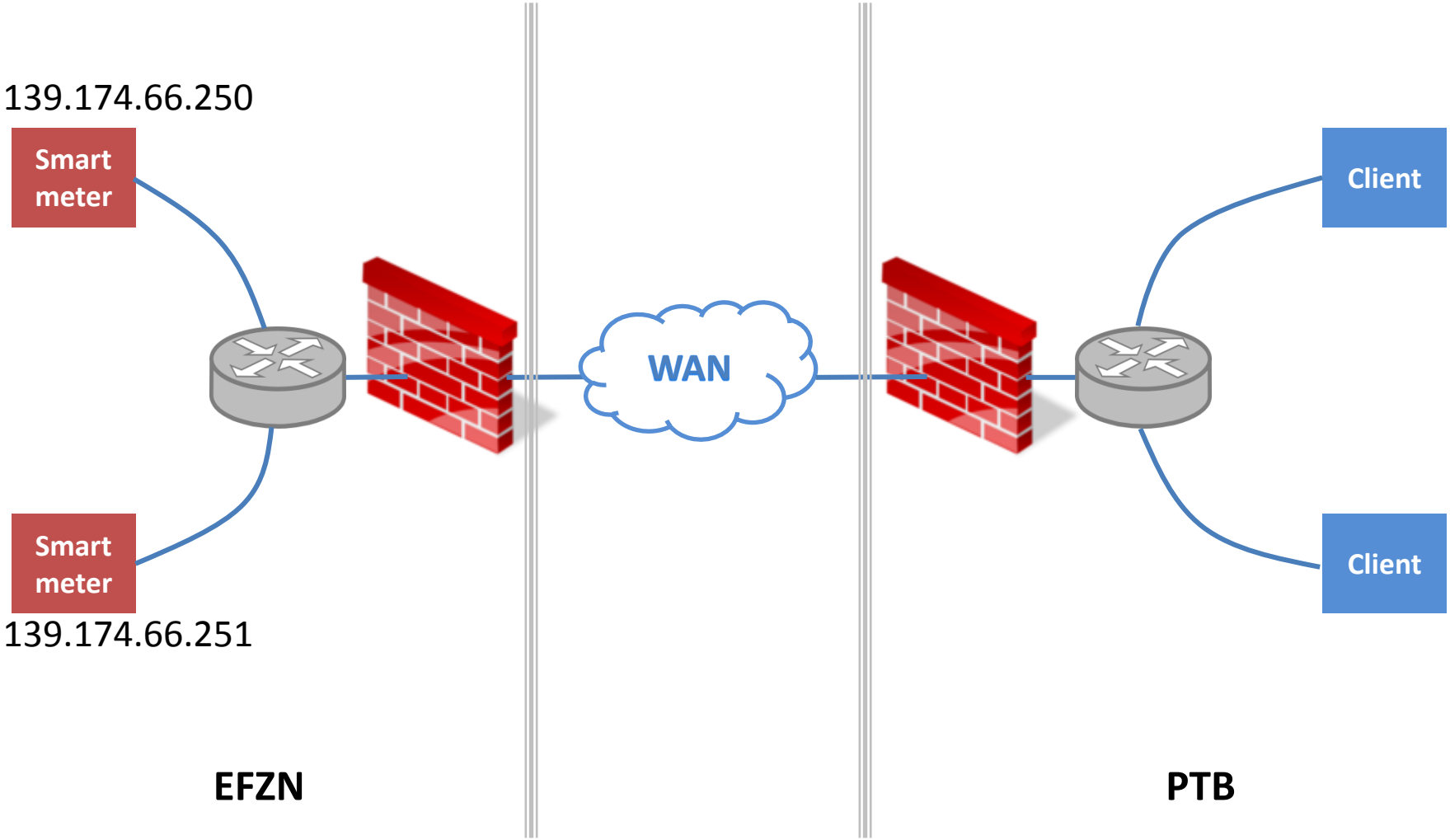




Sensor set up in the test grid



Communication between EFZN and PTB



Standards review

Standard for communication and information:

IEC 61968-100, IEC 61850-90-2, IEC 61850-8-2, IEC 61400-25-4, IEC 60870-5-101, IEC 60870-5-104, IEC 61850-8-1, IEC 61158, IEC 61784-1, etc.

Standard for cyber security:

IEC 27001, IEC 27002, IEC 62351, IEC 62056-5-3, NISTIR 7628

Standards review

Standard for communication and information:

IEC 61968-100, IEC 61850-90-2, IEC 61850-8-2, IEC 61400-25-4, IEC 60870-5-101, IEC 60870-5-104, IEC 61850-8-1, IEC 61158, IEC 61784-1, etc.

Standard for cyber security:

IEC 27001, IEC 27002, IEC 62351, IEC 62056-5-3, NISTIR 7628

Actual implementation:

DLMS/COSEM with additional authentication parameters (asymmetric key algorithm)

DLMS & additional authentication parameters


```
measurement data :: = SEQUENCE
{
   measurement_time
   sequence_number
   meter_identifier
   meter_number
   location_identifier
   counter_values
   error_code
}
```

C4

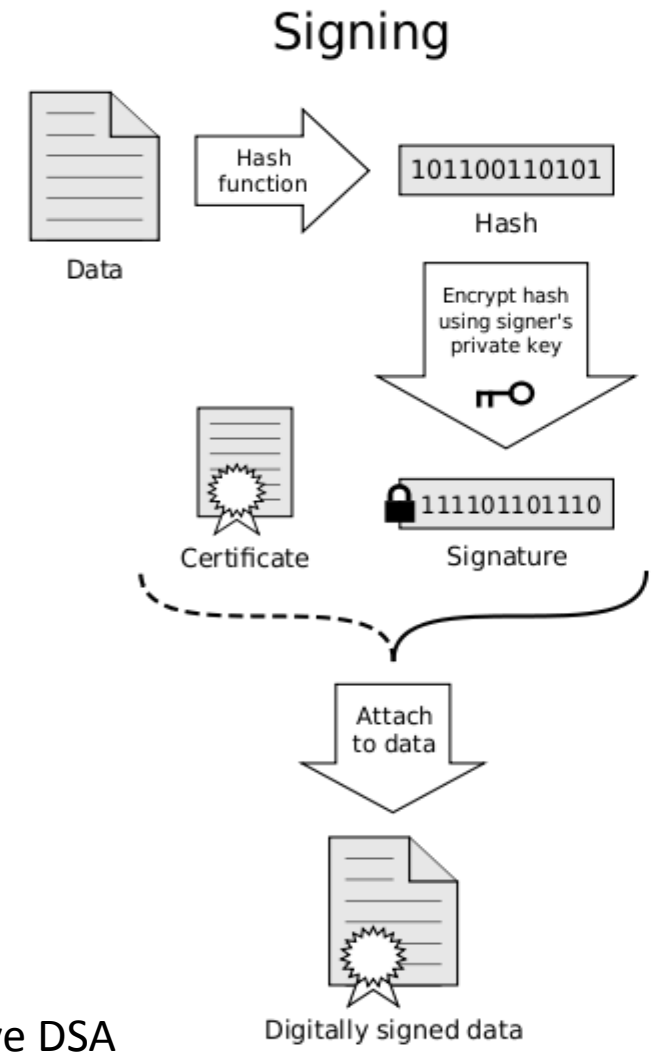
01

80

00 09 30

14 10 01 15 02 23 54 89
AE 23 51 62 79 32 36 21
BC 25 9A 12 E2 3C B2 10
87 82 65 27 39 02 87 C1

DLMS & additional authentication parameters



Elliptic Curve DSA

DLMS & additional authentication parameters

C4

01

80

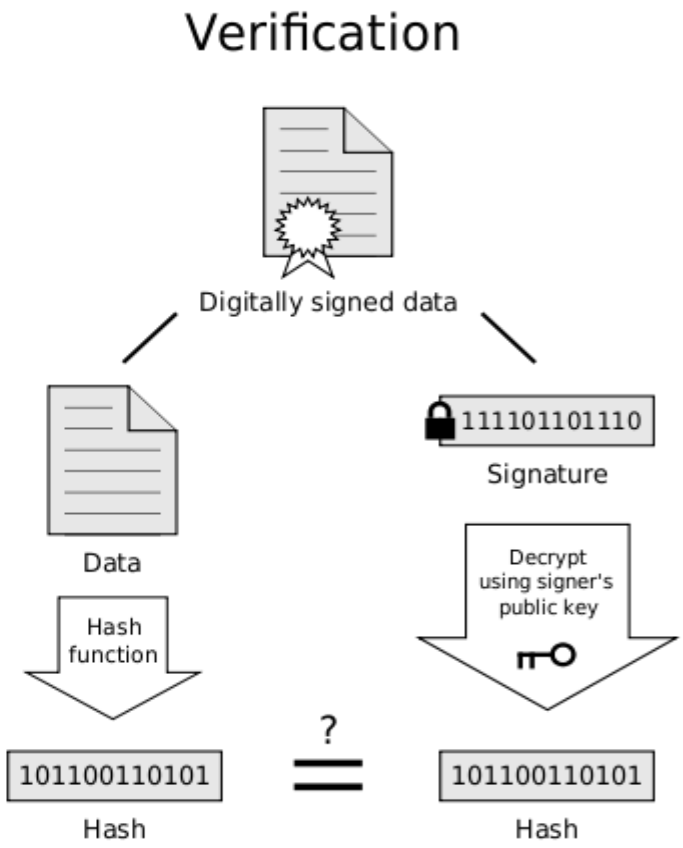
00 09 30

14 10 01 15 02 23 54 89
AE 23 51 62 79 32 36 21
BC 25 9A 12 E2 3C B2 10
87 82 65 27 39 02 87 C1

AB 56 43 2D 89 9E 00 F1
72 68 23 8B B7 23 67 CA

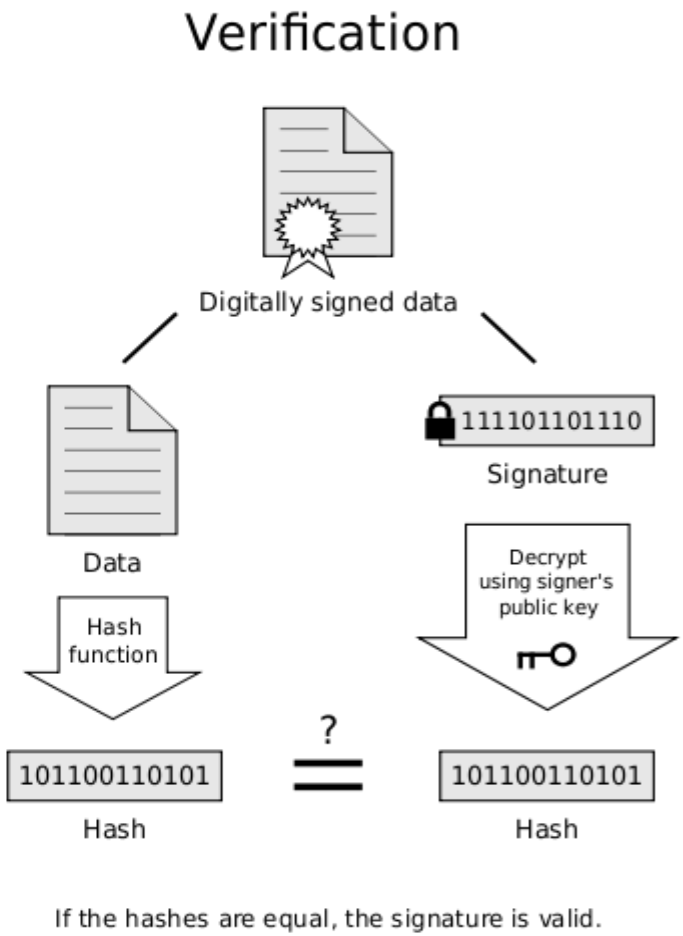
authentication parameters :: =
signature

DLMS & additional authentication parameters



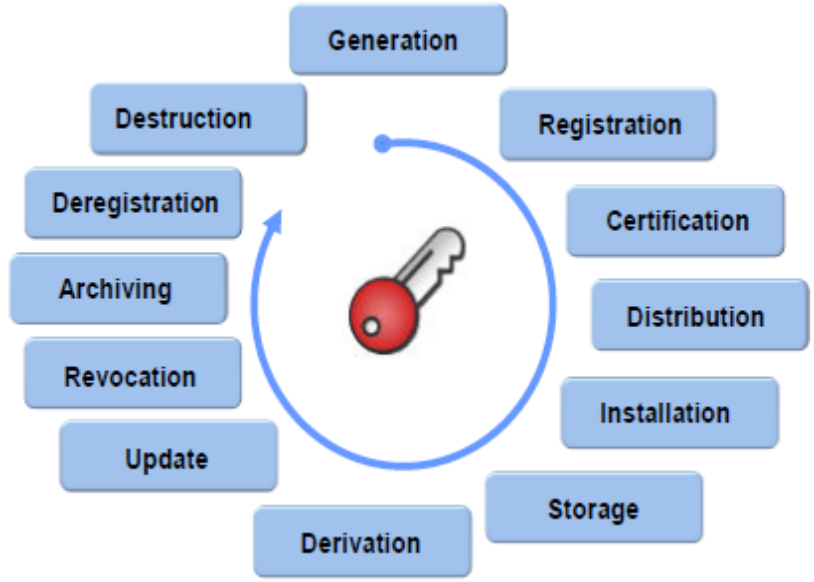
If the hashes are equal, the signature is valid.

DLMS & additional authentication parameters



Can this concept offer a secure communication?

Specification of generation, distribution, revocation, and handling of digital certificates and cryptographic keys to protect digital data and its communication.



- Asymmetric keys algorithm: public key infrastructure (PKI)

Reference: IEC 62351-11

Dynamic behaviour of the smart meter

Besides the security requirment, the smart meter must also appropriate to the metrological requirements of Smart Grids:

Response time of a measurement must be as soon as requiered

Besides the security requirment, the smart meter must also appropriate to the metrological requirements of Smart Grids:

Response time of a measurement must be as soon as requiered

Because of additional security device the reaction time of the smart meter is increased

Dynamic behaviour of the smart meter

1. Modularization of the smart meter.

2. Analyse the dynamic behaviour of the communications between different modules and of program functions:

   - communication between µC and crypto processor
   - communication between µC and sensor
   - program execution time of signing and verification, if crypto libraries are applied
   - program execution time of other functions, e.g. mapping; encodeing/ decoding

3. Possibility of optimization.

Many Thanks

Many Thanks