PowerTech Belgrade 2023

LEADING INNOVATIONS FOR RESILIENT & CARBON-NEUTRAL POWER SYSTEMS

25-29 JUNE, 2023, BELGRADE, SERBIA

Integration of Remote Attestation into IEC 61850

Bastian Fraune[1], Torben Woltjen[1], B. Siemers[2], Prof. Dr. Sethmann[1]

1) RG Computer Networks and Information Security, Bremen

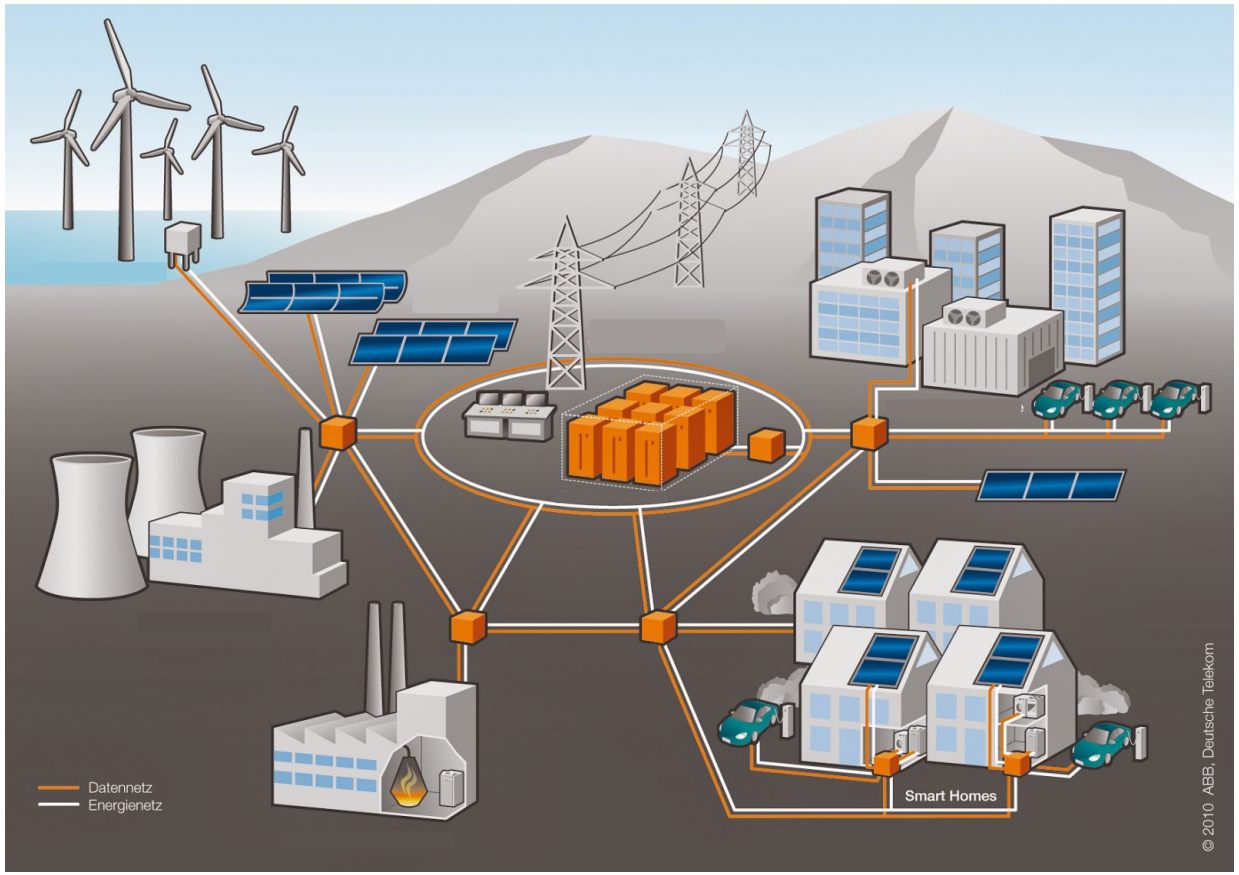
2) R&D Division Energy, OFFIS Oldenburg

City University of Applied Sciences Bremen, Germany

Outline

- Motivation
- Remote Attestation
- IEC 61850
- Concept + Results
- Conclusion

Motivation



- Distributed energy production
- Information technology is backbone of power grid
- Attacker
  - Use vulnerabilities (in IEDs)
  - Change software / configurations
  - Copy credentials
- IED ownership?

- → Secure IEDs hardware layer as basis
- → Query integrity data remote

Remote Attestation

Requirements

- Trusted Platform Module 2.0 (TPM2)
  - Secure crypto-processor
  - Platform integrity
  - Platform configuration register
    - Cryptographic records
  - Root of trust
  - Measured boot

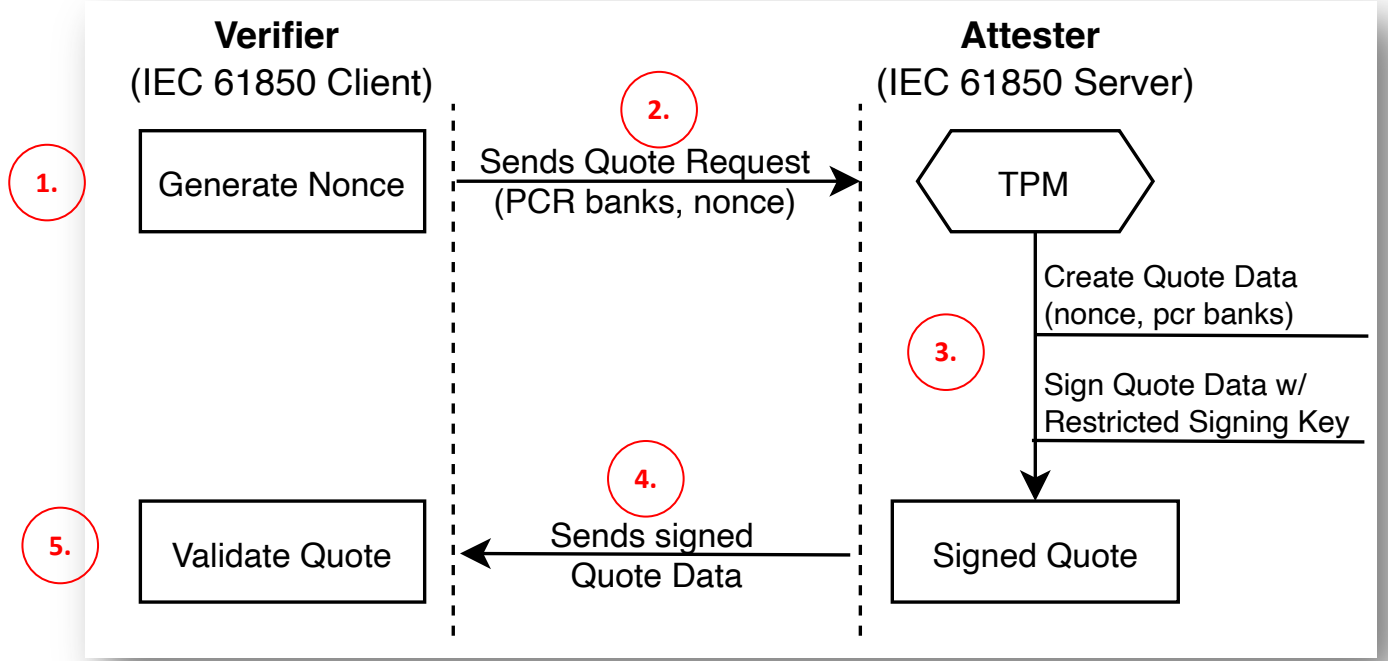
Remote Attestation

- Procedure
- Attest integrity of software / components
- Between two parties
  - Attester (IED) & Verifier (control centre)

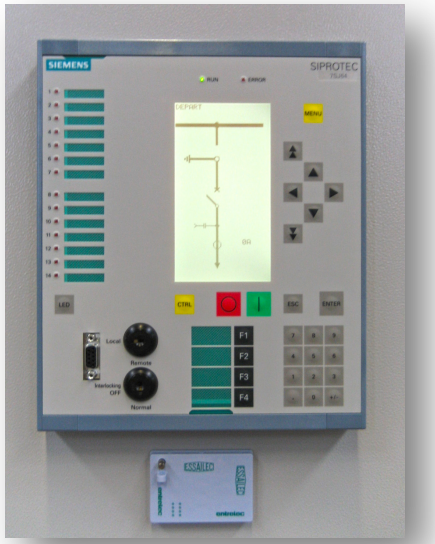
Remote Attestation

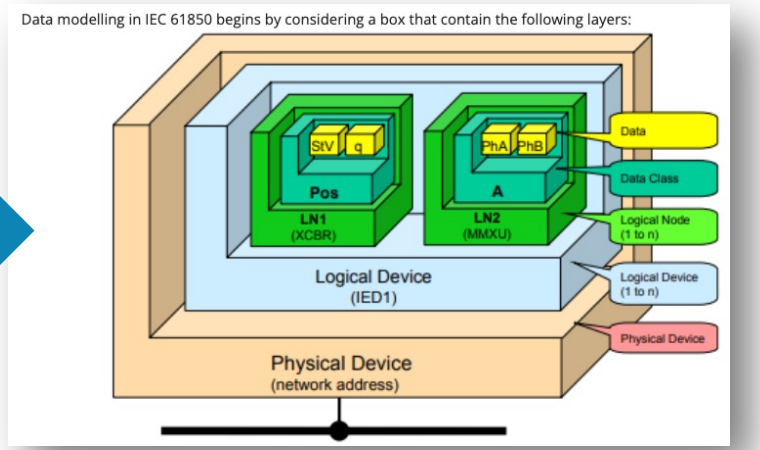
Process of Remote Attestation

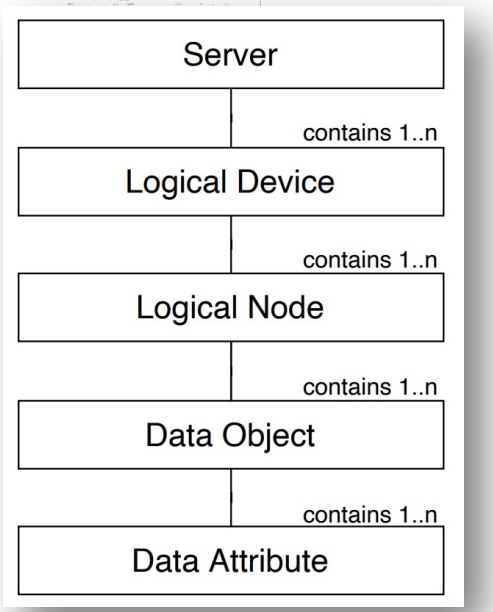
- 1. Generate Nonce (~random number)
- 2. Request information
- 3. TPM create quote & sign it
- 4. Send quote to verifier
- 5. Validate quoted data



IEC 61850 Information Model



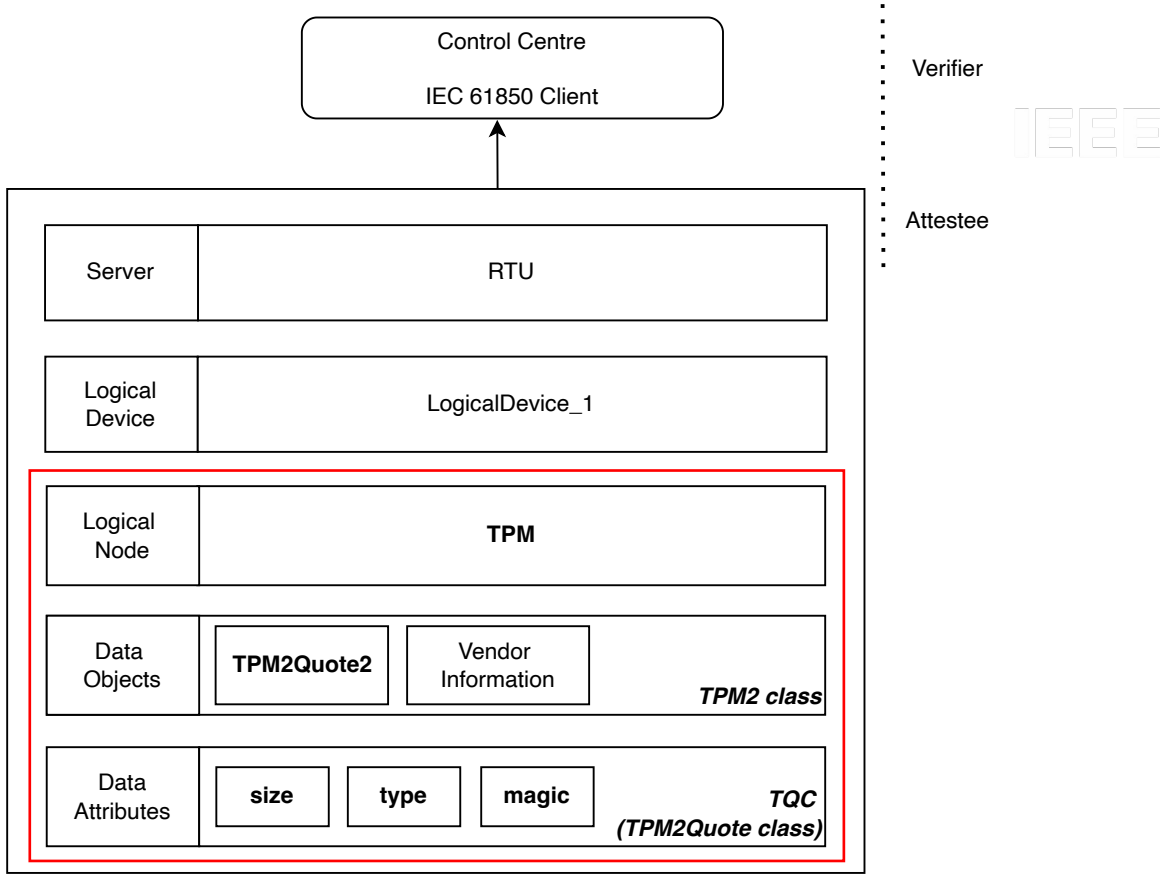




Result

New information entities

- Logical Node
- Data Objects
- Data Attributes



Results

New data attribute classes for IEC 61850

- TPM2 (data object)
- TPM2-QUOTE (attributes)

TPM2-QUOTE class

Attribute Name	Attribute Type	FC	Value / Range / Description	M/O/C
Data Attribute				
status				
size	BdaInt16U	OR	Size of the attestation data structure	M
TPMS_ATTEST				
magic	BdaVisibleString	OR	The indication that this structure was created by a TPM (always TPM_GENERATED_VALUE)	M
type	BdaVisibleString	OR	Type of the attestation structure. In this case "TPM_ST_ATTEST_QUOTE"	M
qualifiedSigner	BdaInt16U[]	OR	Qualified Name of the signing key	M
extraData	byte[] / TPM2B_DATA	OR	External information supplied by caller	M
TPMS_CLOCK_INFO				
clock	BdaInt64	OR	Clock, resetCount, restartCount and safe	M
firmwareVersion	BdaInt64	OR	TPM vendor specific value identifying the version number of the firmware.	M
resetCount	BdaInt32	OR	Number of occurrences of TPM Reset since the last TPM2_Clear()	M
restartCount	BdaInt32	OR	Number of times that TPM2_Shutdown() or _TPM_Hash_Start have occurred since the last TPM Reset or TPM2_Clear().	M
safe	BOOLEAN	OR	No value of clock greater than the current value of clock has been previously reported by the TPM. Set to YES on TPM2_Clear().	M
TPMS_PCR_SELECTION				
pcrSelecrAlgHash	BdaVisibleString	OR	The hash algorithm associated with the selection.	M
sizeofSelect	BdaInt8	OR	The size in octets of the pcrSelect array	M
pcrSelect	BdaInt8U (rep. byte)	OR	The bitmap of selected PCR.	M
pcrDigest	BdaInt8U (rep. byte)	OR	Digest of the selected PCR using the hash of the signing key.	M
pcrUdpateCounter	BdaInt32	OR	Number of selection structures. A value of zero is allowed.	M
pcrs	BdaInt8U[] (rep. byte)	OR		M

Conclusion

Summary

- Increasing attacks on power grid
  - IEDs can be tampered
  - Manipulations on hard- and software
- TPM2 chip provides cryptographic recordings
- Remote Attestation
  - Process to query integrity state information
  - Securely transmit TPM2's recordings
- IEC 61850 information model has been used

Conclusion

- Integration into IEC 61850
  - Logical node for TPM2-module
  - Data object to provide TPM2 functions
  - Data attributes

THANK YOU FOR YOUR ATTENTION!

PowerTech Belgrade 2023

LEADING INNOVATIONS FOR RESILIENT & CARBON-NEUTRAL POWER SYSTEMS

25-29 JUNE, 2023, BELGRADE, SERBIA

Contact Information:

Bastian Fraune
City University of Applied Sciences Bremen
Bastian.Fraune@hs-bremen.de

PowerTech Belgrade 2023
LEADING INNOVATIONS FOR RESILIENT & CARBON-NEUTRAL POWER SYSTEMS
25-29 JUNE, 2023, BELGRADE, SERBIA

BACKUP: Platform Configuration Register (PCR)