

DLMS/COSEM over PLC – security of meter data exchange over open networks

Győző Kmethy
President – DLMS User Association

Contents

- Changes in the metering landscape
- DLMS/COSEM and smart metering
- Information security controls in DLMS/COSEM

Changes in the metering landscape

- Meter data exchange developments
 - local reading
 - remote one-way control
 - HHU reading
 - remote two-way data exchange
 - from private to public and exposed networks
 - from proprietary protocols to public protocols
 - functional enrichment
 - variety of communication media
 - from dumb meters to smart meters
- Market developments
 - from monopolistic to regulated markets
 - from stable bi-lateral relationship to dynamic multi-lateral relationships

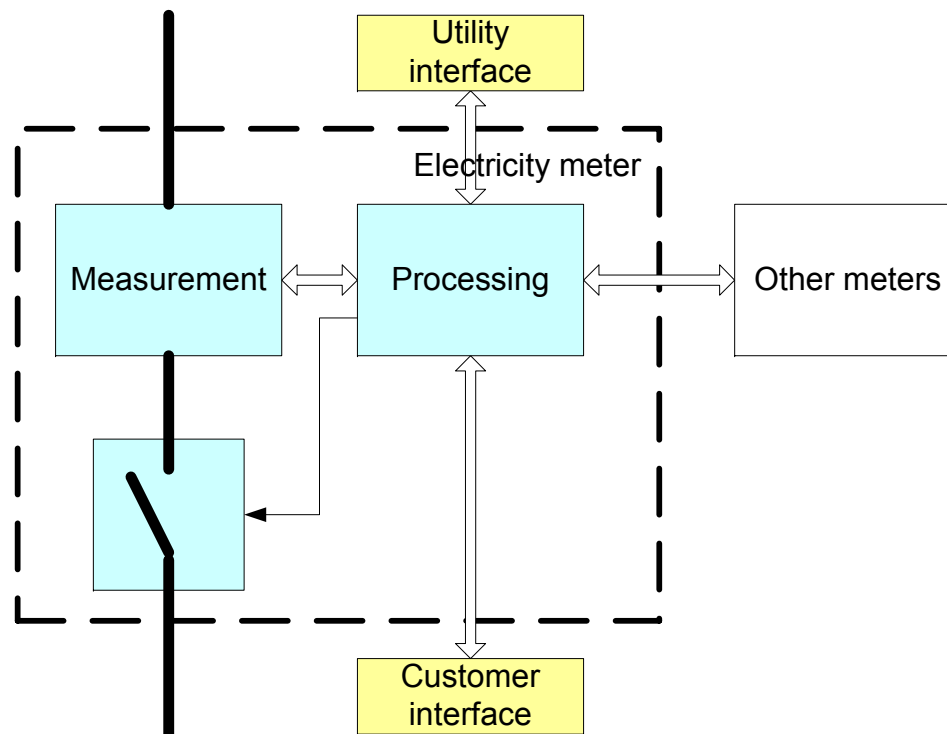
The smart grid vision



- “Critical infrastructure”
- Smart grids need smart meters

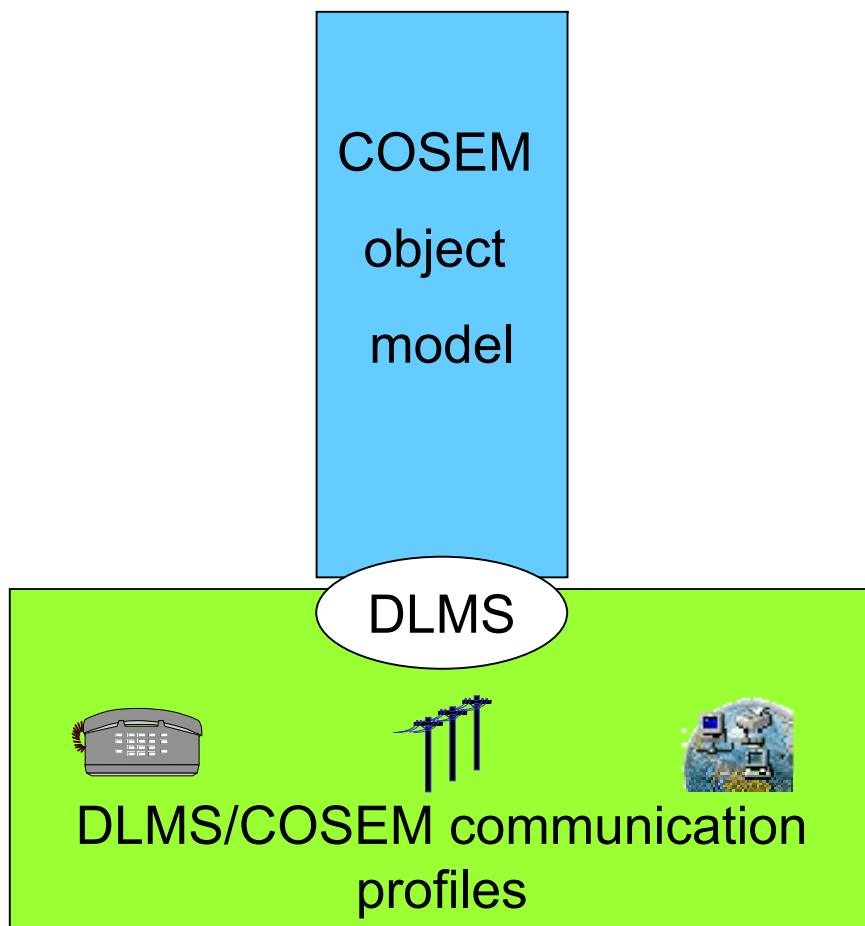
What is a smart meter?

- Multiple tariffs
- Load profiles
- Bi-directional flow
- Voltage quality
- Anti-tamper
- Utility interface
 - Data exchange
 - Remote parametrization
 - Load control
 - Contract management
 - Payment management
- Customer interface
- Interface for other meters



All data must be integrated into business processes

DLMS/COSEM and smart metering



- Modelling smart meter functionality
- Adding new data security elements
- Adding new communication profiles

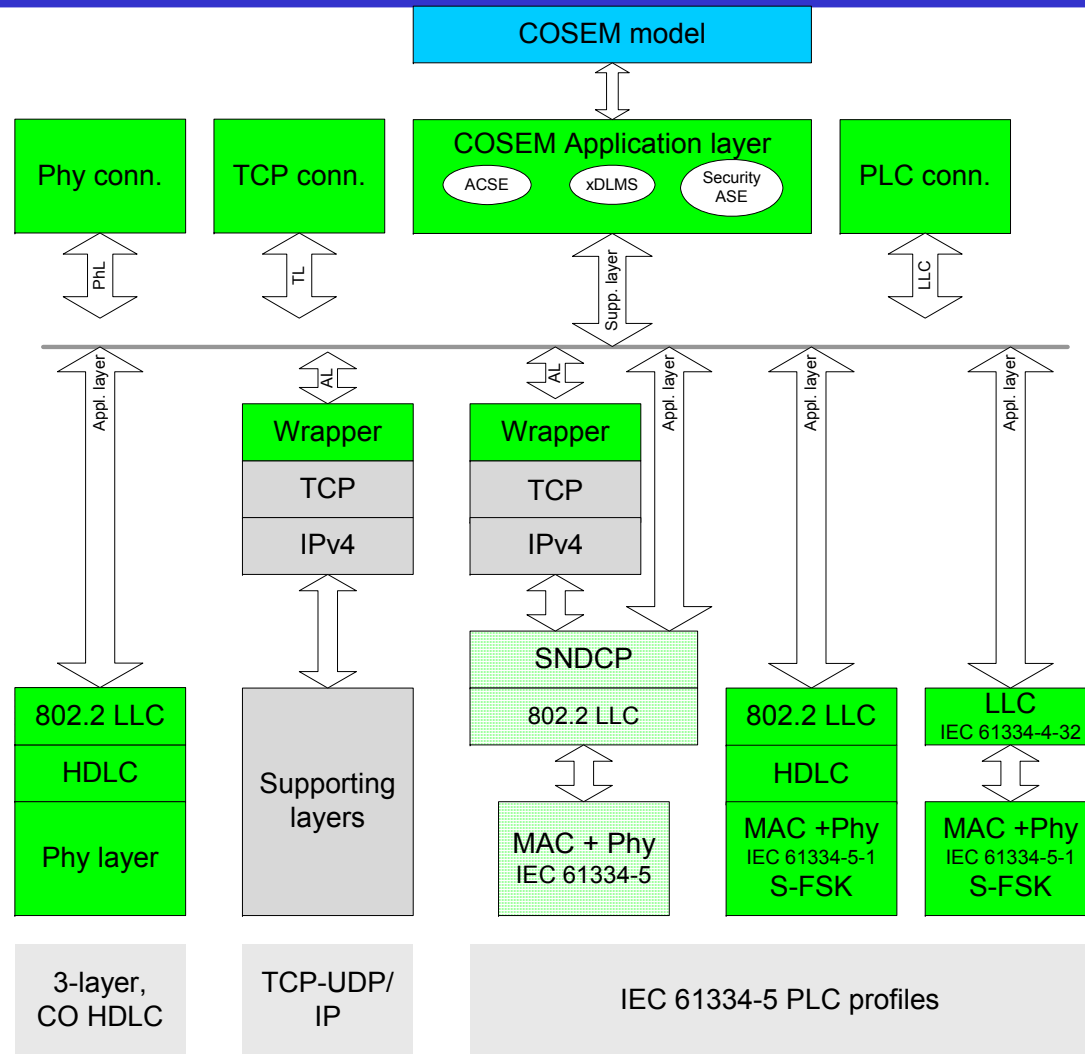
Due to the orthogonality of DLMS/COSEM, the object model and the communication profiles can be developed independently

What kind of data for smart metering

- Measurement data
- Configuration data
- Contract data
- Customer information
- Load control commands

Authentication and confidentiality may become important

DLMS/COSEM communication profiles

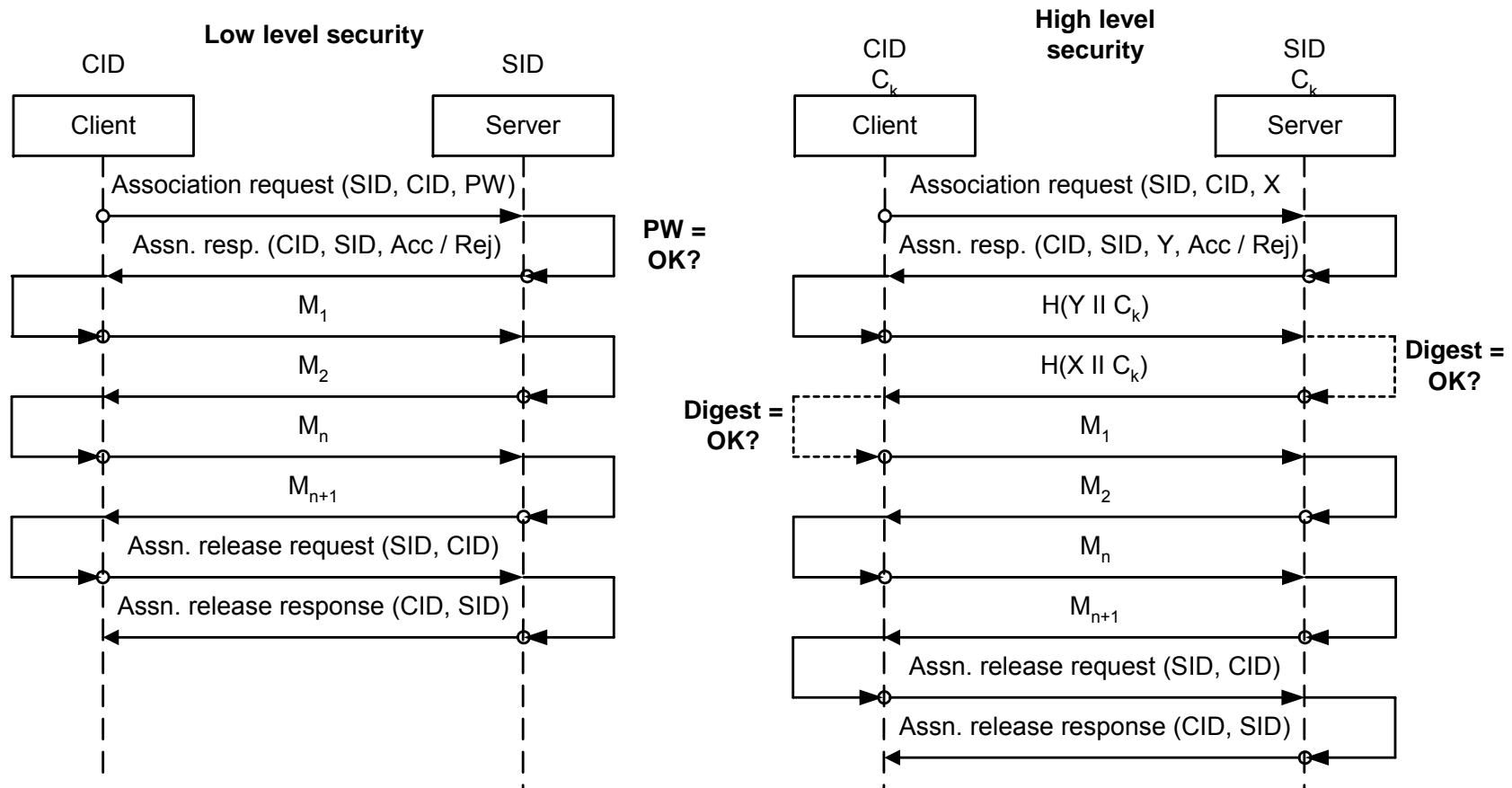


DLMS/COSEM security toolbox

- Access security
 - peer authentication: client only (LLS) or client / server (HLS)
 - association specific view of objects: list, access rights
- Security event logs
- Message security
 - authentication to ensure integrity and authenticity (legitimate source)
 - encryption to prevent an illegitimate user to obtain unauthorised information
 - encrypted authentication



Peer authentication



CID: Client address, SID: Server address, C_k : shared secret, X: client challenge to server, Y: server challenge to client, H: Hash function, producing the message digest, ||: concatenation operation

Security event logs

- Log each application association establishment (successful and failed)
 - date_time
 - event code
 - event data
- Log changes of security management information

Message security tools

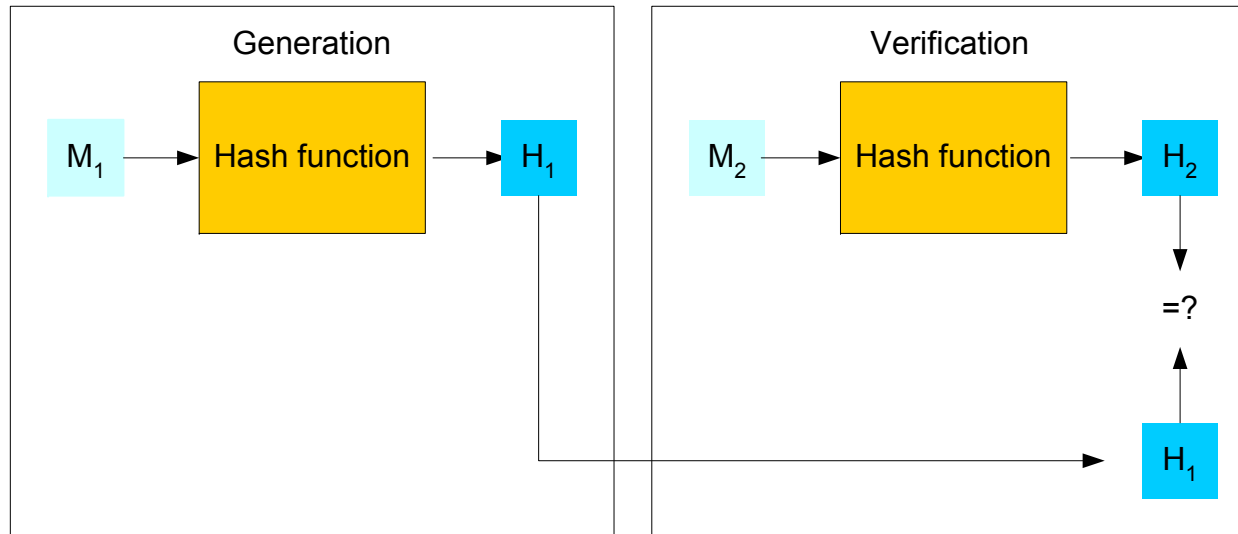
Non-cryptographic:
Protection against
unintentional changes

- Parity bits
- Cyclic Redundancy
Check (CRC)
 - suitable for larger
streams of data

Cryptographic: Protection
against attacks

- Hash functions (digest)
 - integrity
- Symmetric key cryptography
 - confidentiality
 - authentication
 - encrypted authentication
- Asymmetric (public) key
cryptography
 - (encryption)
 - digital signature
 - non-repudiation (with TTP)

Hash functions



- Short representation of a longer message: digest
- Suitable to verify that the message has not changed
- Used also in keyed message authentication (HMAC) and digital signature algorithms
- Selected algorithms: MD-5 (RFC 1321), SHA-1 (FIPS 180)

Symmetric / asymmetric key cryptography

Symmetric keys

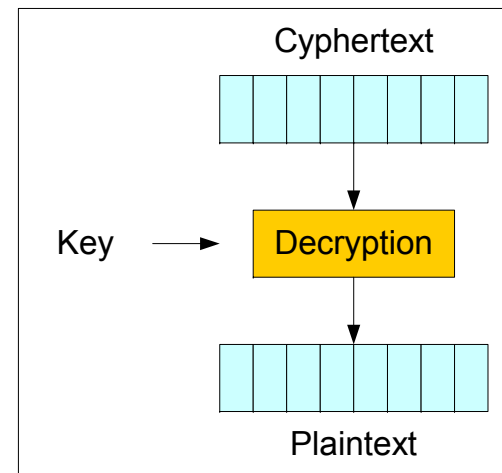
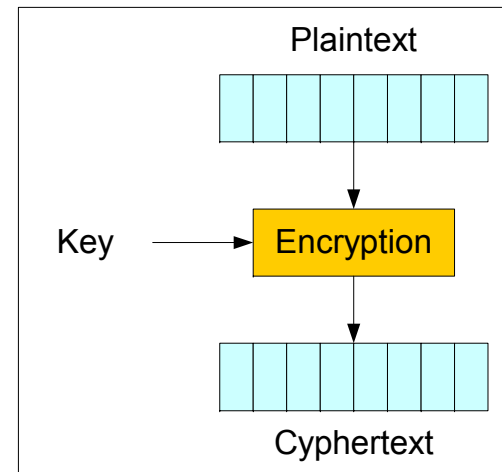
- same key to apply and remove protection
- keys must be kept secret
- unique key for each relationship and for each purpose
 - encryption
 - authentication
 - key wrapping
- not computation intensive
- suitable for single-authority single-user environments

Asymmetric (public) keys

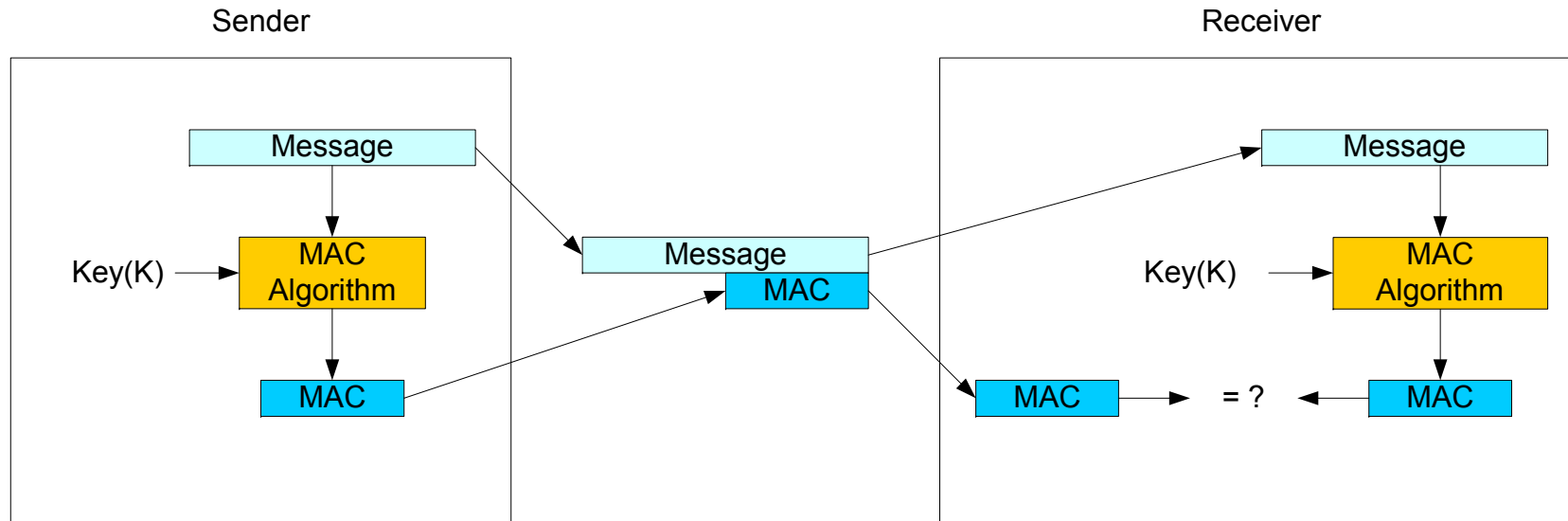
- private / public key pair
 - to sign data
 - for each type of key agreement process
 - to receive transported key
- no unique key needed for each relationship
- computation intensive
- best suited for open multi-user environment

Message encryption

- two identical secret keys
- selected encryption algorithms: TDES, AES
- stream or block cipher
- modes of operation for block cipher:
 - Cipher Block Chaining Mode
 - Counter Mode
- selected algorithms: TDES-CBC, AES-CBC-128



Message authentication



Protects message integrity and authenticity

- Selected algorithms:
 - HMAC-MD5, HMAC-SHA-1-96 (FIPS 198)
 - AES-X-CBC-MAC-96, RFC 3566 (variable length plaintext)

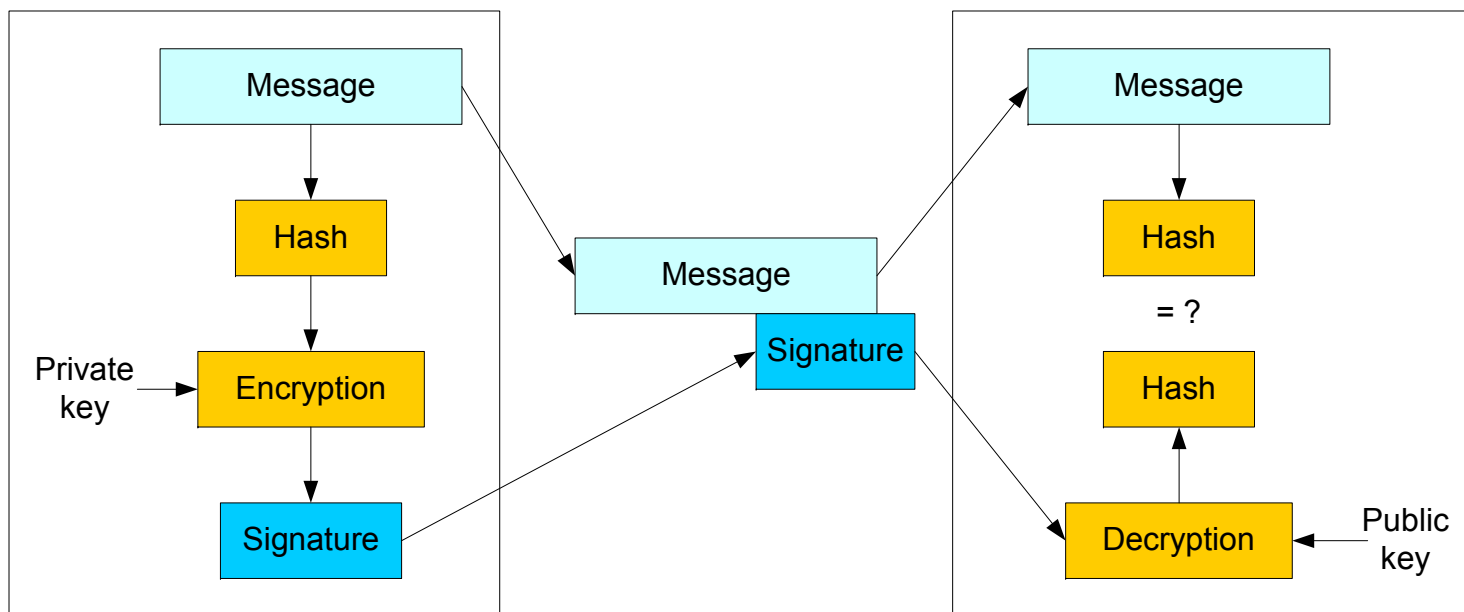
Authenticated encryption

- Provides authenticity and confidentiality of the payload
- Provides authenticity of additional information
- Selected algorithms:
 - CCM: Counter with Block Chaining Message Authentication code (NIST 800-38C)
 - Galois-Counter mode (NIST 800-38D)

Key wrapping

- Encryption algorithm to encapsulate cryptographic keys
 - protecting keys while in untrusted storage
 - transmitting key over untrusted networks
 - session keys can be transported by encrypting them under a long-term encryption key
- Selected algorithms:
 - TDES-WRAP,
 - AES-WRAP

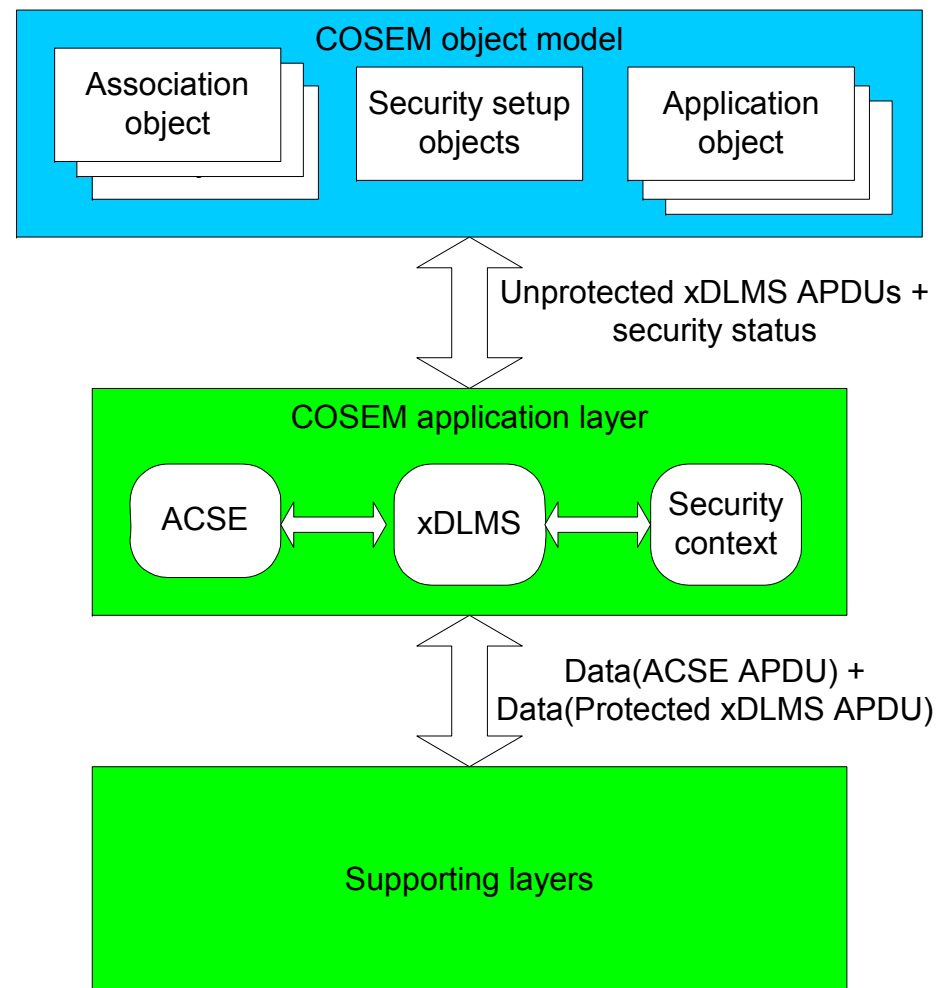
Digital signature



- Uses a pair of Private key / Public key
- Links a message with a particular person (application process)
- Can provide non-repudiation in co-operation with a TTP
- Provides the basis of SELMA

Security implementation in DLMS/COSEM

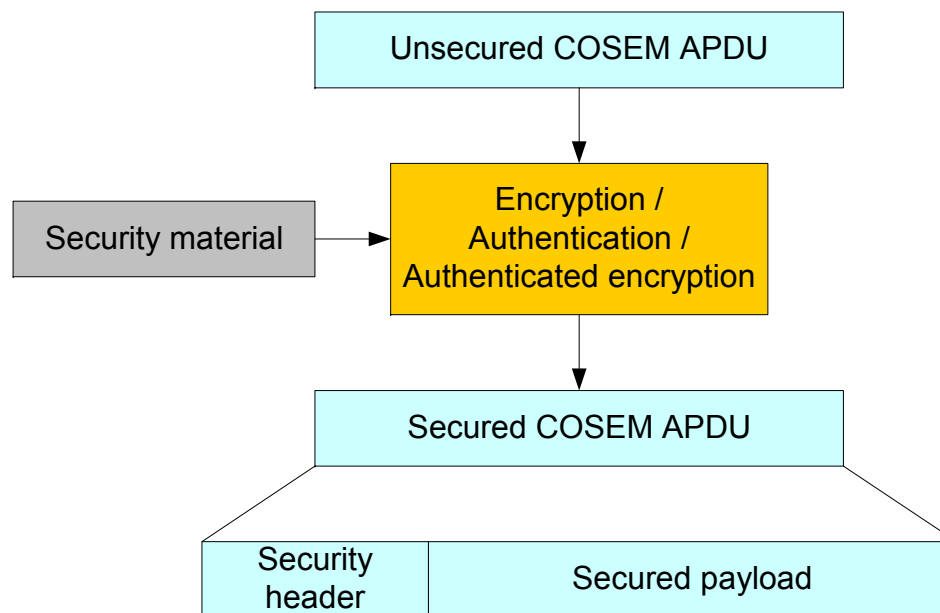
- Association objects control application associations
- Security setup objects allow to manage security features
- ACSE negotiates application context and authentication mechanism
- Lower layers provide CRC



Managing security

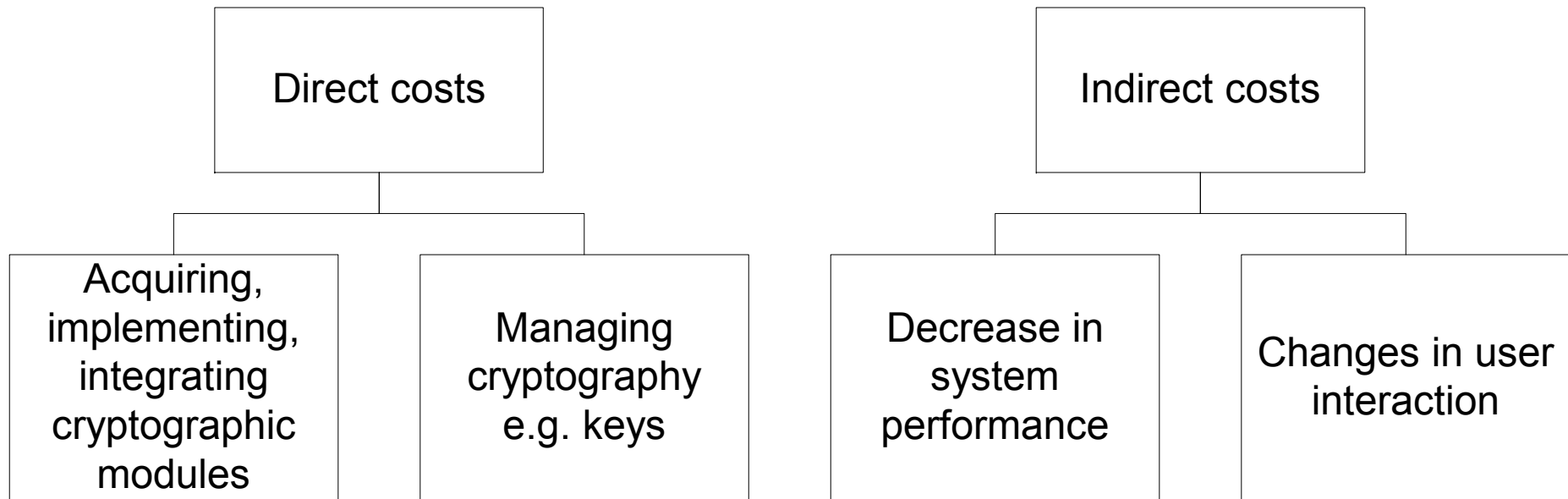
- Application-context allows to negotiate if ciphered APDUs are used or not
- Mechanism-name allows to negotiate the authentication and encryption algorithm to be used
- A new security setup object manages the security policy and key update
- New version of Association LN / Association SN class specifies new access rights to attributes and methods: authenticated R / W / R-W

Secured COSEM APDUs



- Security header:
 - Security control: Security_suite_id + A + E
 - Security suite dependent parameters

Costs of cryptography



Security controls must be cost-effective

Summary

- DLMS/COSEM is being extended for smart metering applications
 - object model
 - security elements
 - communication profiles

Thank you for your attention!