Landis+Gyr

manage energy better

Creating a platform of trust

Meter data transmission the secure way

Philip Mason

Topics

Introduction

The EU regulatory environment for smart meter security and privacy

Achieving interoperability in smart meter communications security

How using encrypted and authenticated messaging builds trust

The Gridstream® secure communications implementation

Introduction

Drivers for secure smart metering systems

Suppliers want to …

Ensure the availability of energy supply

Comply with regulations

Reduce business risk

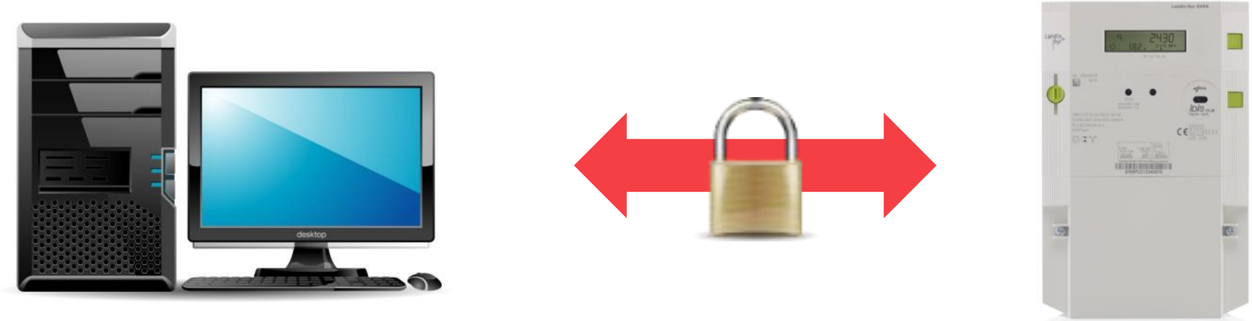
Consumers want …

Their personal information to be protected

Focus of this webinar

The information flow between smart meters and head end systems

Secure communication technology



Head End System

Smart Meter

The EU regulatory environment for smart meter security and privacy

Philip Mason | © Landis+Gyr | 03 April 2014

EU publications influencing smart metering

EU Recommendation 2012/148/EU

Preparations for the roll-out of smart metering systems

Directive 95/46/EU

The protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2002/58/EC

The processing of personal data and the protection of privacy in the electronic communications sector

Directive 95/46/EU

The protection of individuals with regard to the processing of personal data and on the free movement of such data

- ***Personal data*** **shall mean any information relating to an identified or identifiable natural person** Article 2a
- ***Processing of personal data*** **means** <u>**any**</u> **operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, storage, … disclosure by transmission, …** Article 2b

Directive 2002/58/EC

The processing of personal data and the protection of privacy in the electronic communications sector

- **Service providers should take appropriate measures to safeguard the security of their services..** Paragraph (20)
- **Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications..** Paragraph (21)

EU Recommendation 2012/148/EU

Preparations for the roll-out of smart metering systems

- **Directives 95/46/EC and 2002/58/EC are fully applicable to smart metering which processes personal data, in particular in the use of publicly available electronic communications services** Article (7)
- **Data protection and information security features should be built into smart metering systems before they are rolled out** Article (10)
- **The use of encrypted channels is recommended** Paragraph 1.24

Barriers to a single approach on smart metering security

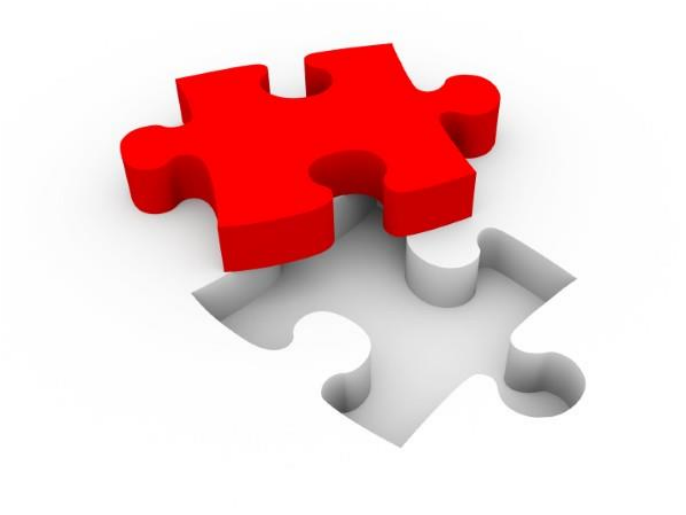
Different security architectures have been proposed by France, Germany, Netherlands, Spain and the UK

Broad European landscape of national and industry security guidelines

Slow and loosely coordinated path to European standardization and regulation

Security may be considered by governments to be a national interest

Security may be used to protect markets



Comparison with the situation in the USA

Centralized approach driven by the US American federal government

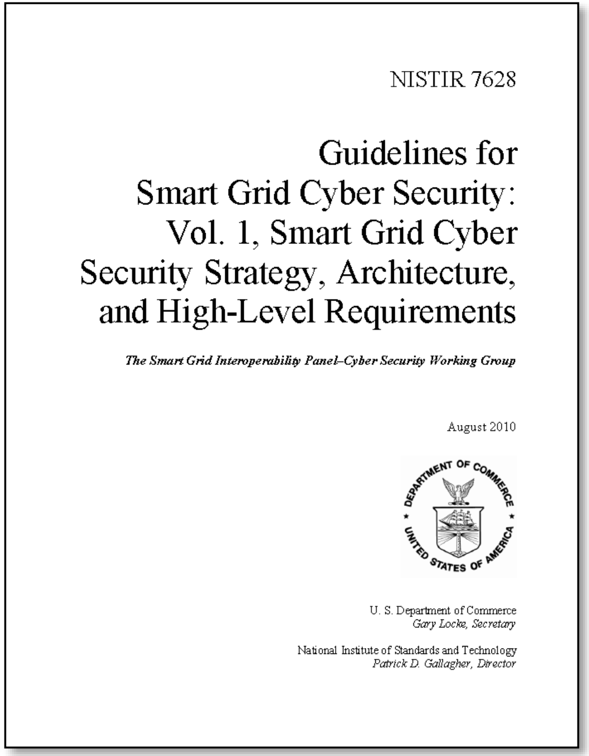
NISTIR 7628

National Institute of Standards and Technology Interagency Report

A very relevant set of documents laying out the benchmark for activity in the area of smart grid cyber security

Wide ranging and influential also in Europe

Next step may be to introduce compliance testing and certification



NISTIR 7628

Guidelines for
Smart Grid Cyber Security:
Vol. 1, Smart Grid Cyber
Security Strategy, Architecture,
and High-Level Requirements

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 2010

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Achieving interoperability in smart meter communications security

Philip Mason | © Landis+Gyr | 03 April 2014

What is interoperability and why is it important?

Interoperability means ..

Systems can be built up with components from different suppliers

Devices from different suppliers can be interchanged with no change in functionality

It is important because ..

It gives a utility the ability to be flexible in the way it purchases system components

A utility can install meters from several suppliers and be sure that they will work side-by-side in the smart metering system

Associations driving smart meter interoperability

DLMS-COSEM

Device Language Message Specification

COmpanion Specification for Energy Metering

IEC 62056

IDIS

Interoperable Device Interface Specifications

Interoperable secure communications verified by IDIS

Who takes the responsibility ?

Available Standards

Companion Specification

4: Semantic Interoperability — Understanding of concepts contained in the data st ures

3: Syntactic Interoperab — g of data es in the essages

2: Netwo ability — Exchange of messages via different networks

1: Basic Connectivity — Physical and logical connection

1. Select Standards

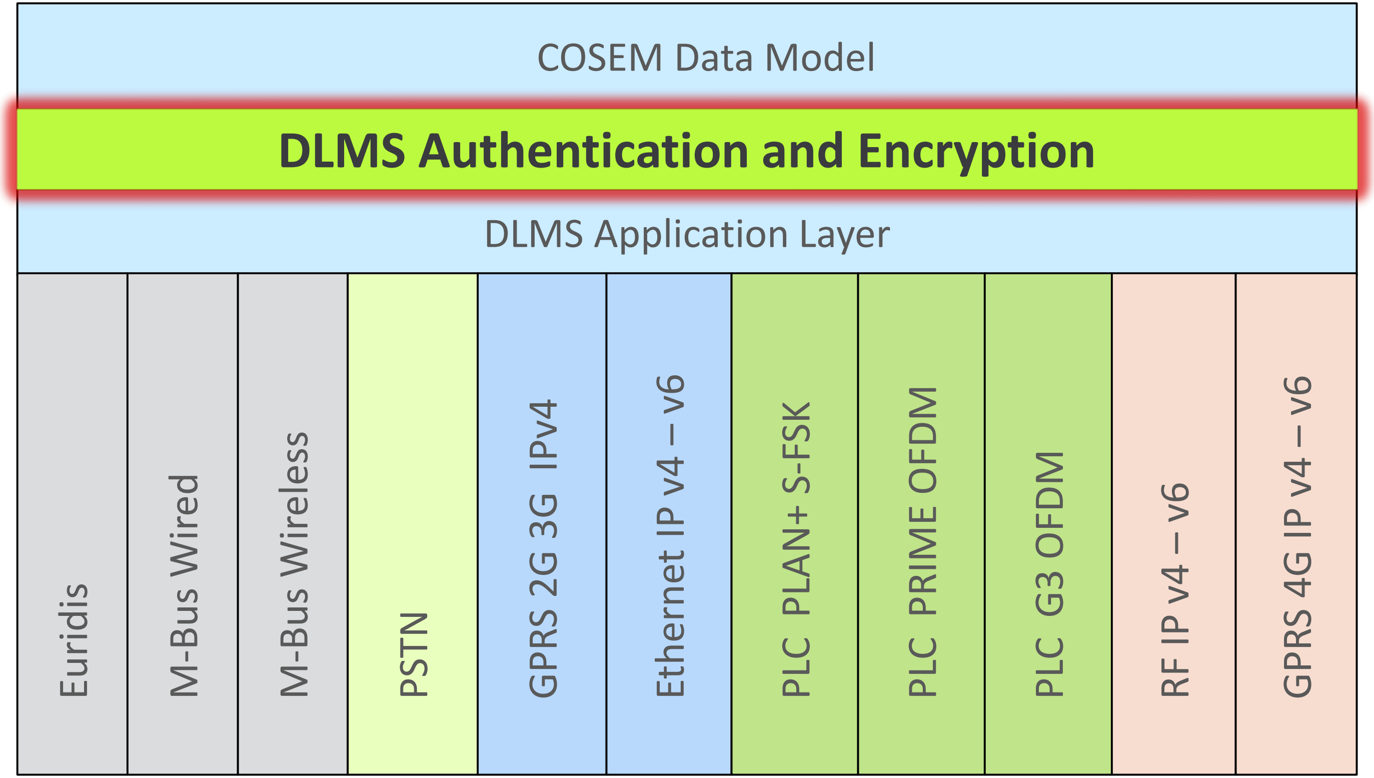
IDIS

1	logical_name			octet_string[6
2	buffer			array
3	capture_objects			array[2]
4	capture_period			double
5	sort_method			
6	sort_object			
7	entries_in_use			
8	profile_entries			
1	reset			
	Event Object – Fraud Detectio			
1	logical_name			
2	value			
		M	M	
				octet_string[6
				array
				array[2]
				double_long_u
	od			enum
	_object			capture_objec
	entries_in_use			double_long_u
8	profile_entries			double_long_u
1	reset			integer
	Abstract objects – User interface			
	Consumer Message Text	M	M	

2. Select Options

3. Test for conformance

IDIS security supports multiple transport layers



COSEM Data Model

DLMS Authentication and Encryption

DLMS Application Layer

Euridis

M-Bus Wired

M-Bus Wireless

PSTN

GPRS 2G 3G IPv4

Ethernet IP v4 – v6

PLC PLAN+ S-FSK

PLC PRIME OFDM

PLC G3 OFDM

RF IP v4 – v6

GPRS 4G IP v4 – v6

How using encrypted and authenticated messaging builds trust

How can we build trust?

Ensure message confidentiality

Disclose information only to authorized entities

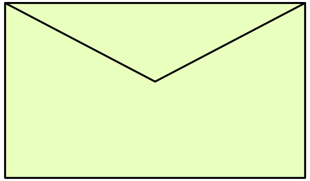
Ensure message integrity

Do not allow information to be changed

Ensure message authenticity

Show information only to entities whose right of access has been verified

DLMS cryptography is trustworthy

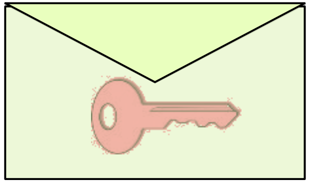


Confidentiality & Integrity

Header	Frame Counter	Ciphered message

Authenticity

Header	Frame Counter	Ciphered message	Authentication Tag



Secure Key Distribution

Header	Frame Counter	Key wrapped with Master Key

DLMS message cryptography

DLMS uses AES-GCM-128

<u>A</u>dvanced <u>E</u>ncryption <u>S</u>tandard

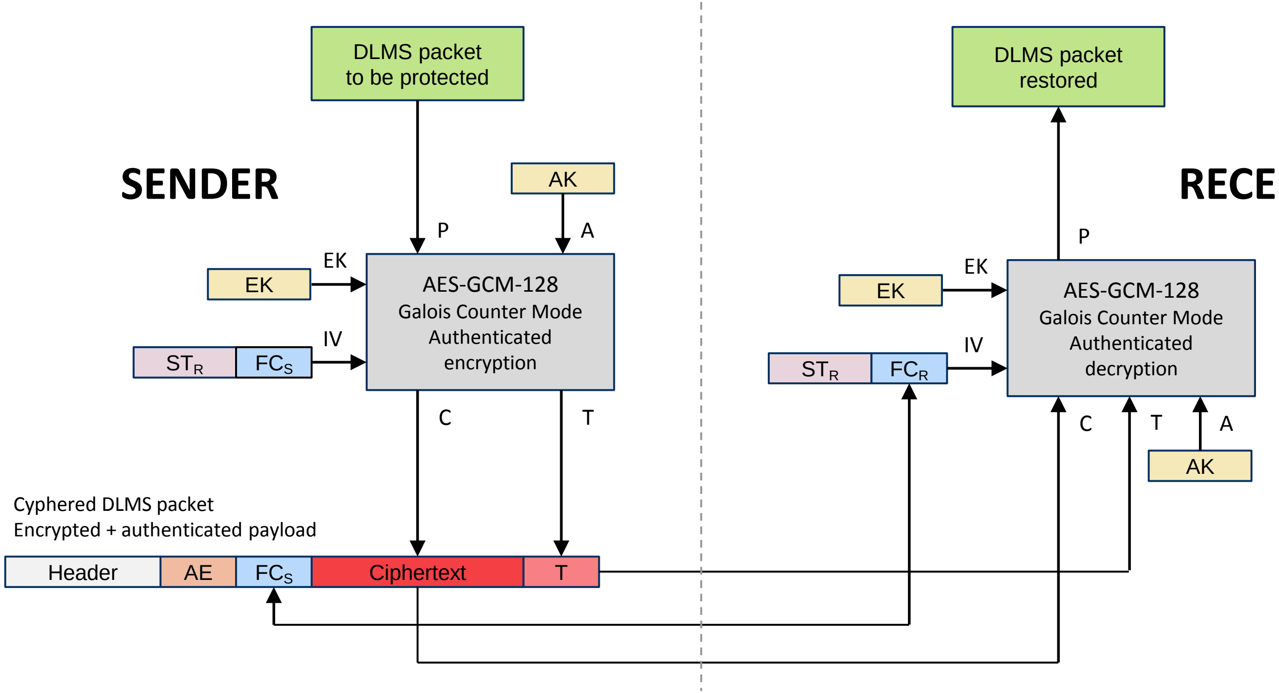
<u>G</u>alois <u>C</u>ounter <u>M</u>ode

<u>128</u>-bit key lengths

With multiple symmetric keys

- Authentication Key
- Unicast Encryption Key
- Broadcast Encryption Key
- Key Encryption Key

DLMS message cryptography



DLMS packet to be protected
SENDER
AK
P
A
EK
EK
AES-GCM-128 Galois Counter Mode Authenticated encryption
IV
ST_R
FC_S
C
T
Cyphered DLMS packet
Encrypted + authenticated payload
Header
AE
FC_S
Ciphertext
T
DLMS packet restored
RECEIVER
P
EK
EK
AES-GCM-128 Galois Counter Mode Authenticated decryption
IV
ST_R
FC_R
C
T
A
AK

AE = Authenticated encryption
AK = Authentication key
C = Cyphertext
EK = Encryption key
FC = Frame counter

IV = Initialization vector
P = Plaintext
ST = System title
T = Authentication tag

The Gridstream® secure communications implementation

Europe, Middle East and Africa

Philip Mason | © Landis+Gyr | 03 April 2014

Gridstream®

Gridstream® is Landis+Gyr's integrated smart metering platform

It combines energy measurement devices, communications, software applications and professional services

Gridstream® secure communications

DLMS applied to power line and mobile communications

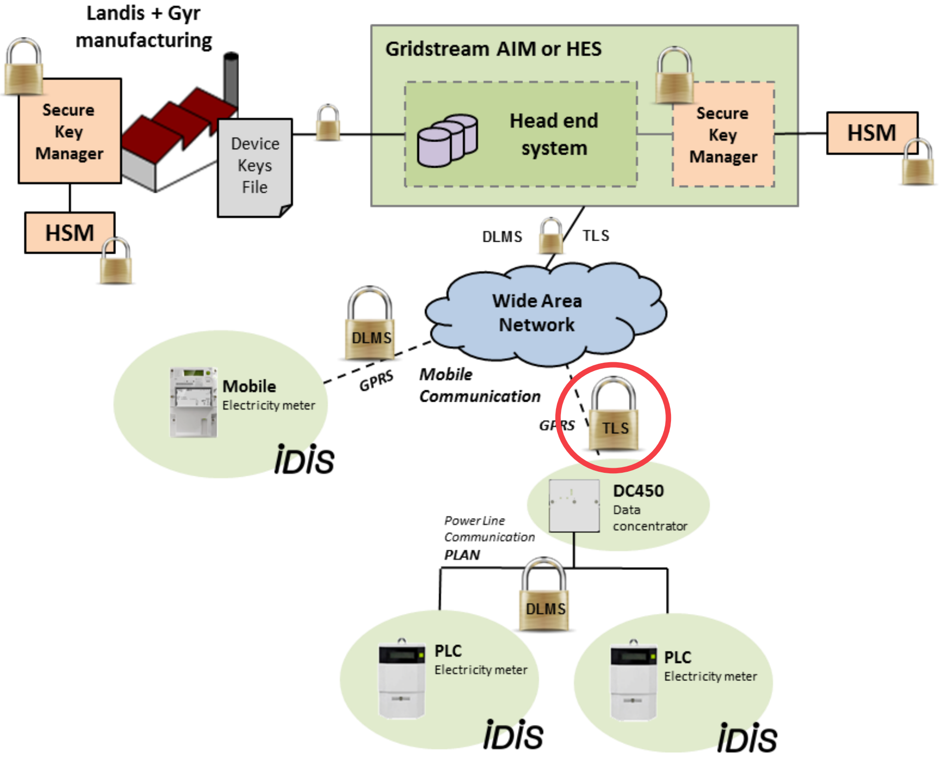
Driven by IDIS[1] industry association

DLMS[2] symmetric keys

TLS[3] tunnel to data concentrator

SKM[4]/HSM[5] for crypto-management

Initial key generation



[1] Interoperable Device Interface Specifications
[2] Device Language Message Specification
[3] Transport Layer Security
[4] Secure Key Manager
[5] Hardware Security Module

Smart metering context

The communications bandwidth used over power line channels is low (of the order of a few kbit/s)

Meters have limited processing capacity, they are not smart phones

The number of meters in customer roll outs varies widely (over a range of approximately 10k – 10M devices)

Technology suited to smart metering

DLMS cryptography is appropriate for securing communication with smart meters

- Application layer cryptography works with many transport layers
- The processing capacity necessary for GCM-AES-128 symmetric key algorithms is low, particularly compared to asymmetric key algorithms
- Adds only a small protocol overhead for encryption/authentication
  < 10% compared to no encryption/authentication
- Unique set of keys per meter protects against system wide attacks
- Excellent scalability: The amount of computing resources necessary for operational key management in the head end system is independent of the number of meters, a single HSM can serve millions of meters

Why use a Hardware Security Module?

Highest level of protection for root cryptographic assets

True random number generation for initializing key creation algorithms

Highest level of tamper resistance and physical security

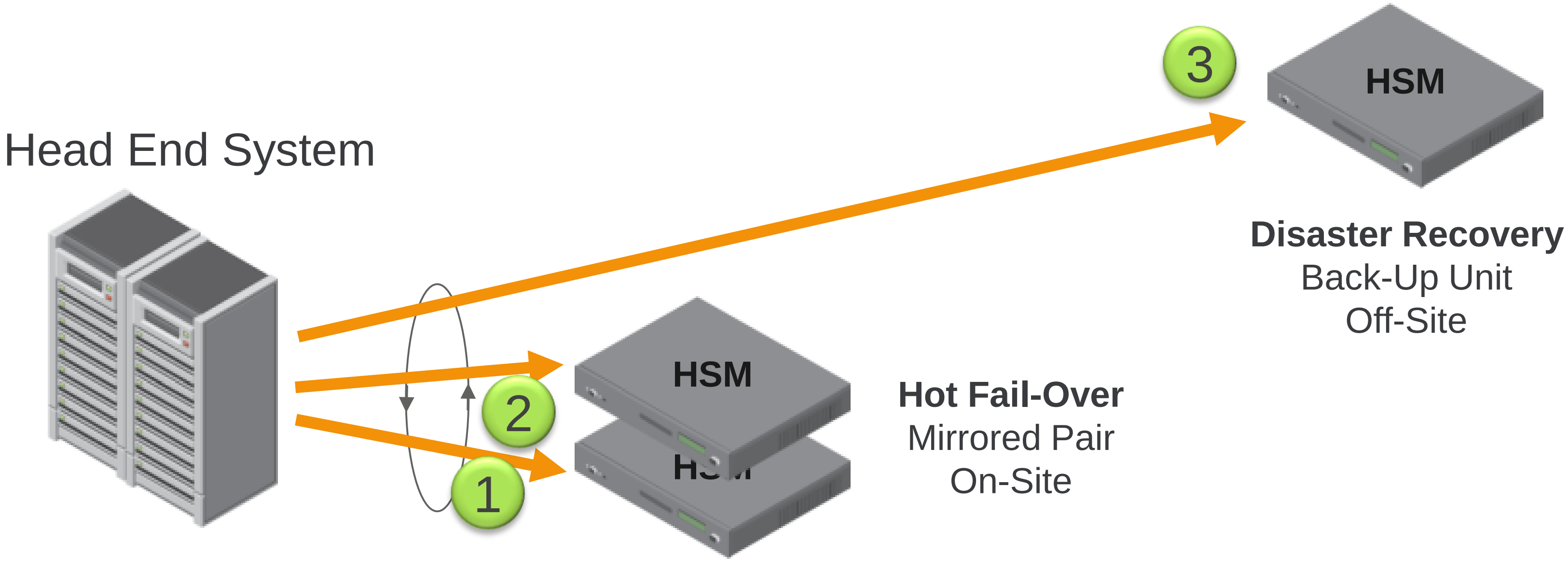
Most reliable storage, fail-over and disaster recovery

SafeNet®

THE DATA PROTECTION COMPANY

System resilience

The availability of keys can be guaranteed with a resilient infrastructure



Gridstream® symmetric key cryptography

Used between DLMS server and client

- Meter to data concentrator (Power line)
- Meter to head end system (Mobile)

Each meter uses a unique set of keys

The meter, the data concentrator and the head end system share the same keys

Replacement keys are distributed securely

Keys are stored securely

Gridstream® asymmetric key cryptography

Data concentrator to head end system

Access to data concentrator web management tool

Access to meter field installation tool

Distribution of initial keys from meter manufacturing facility to operative head end system

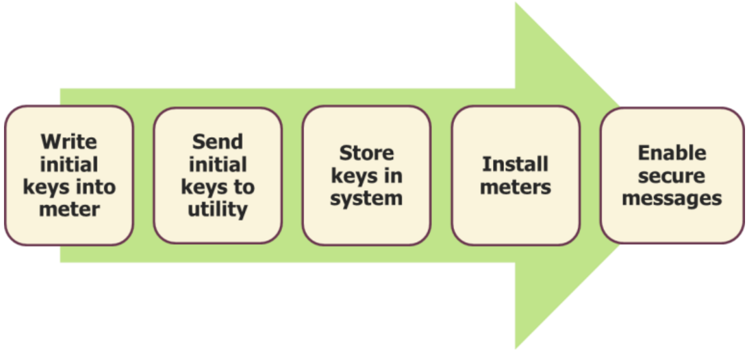
Gridstream® key distribution

Symmetric key cryptography for meter data

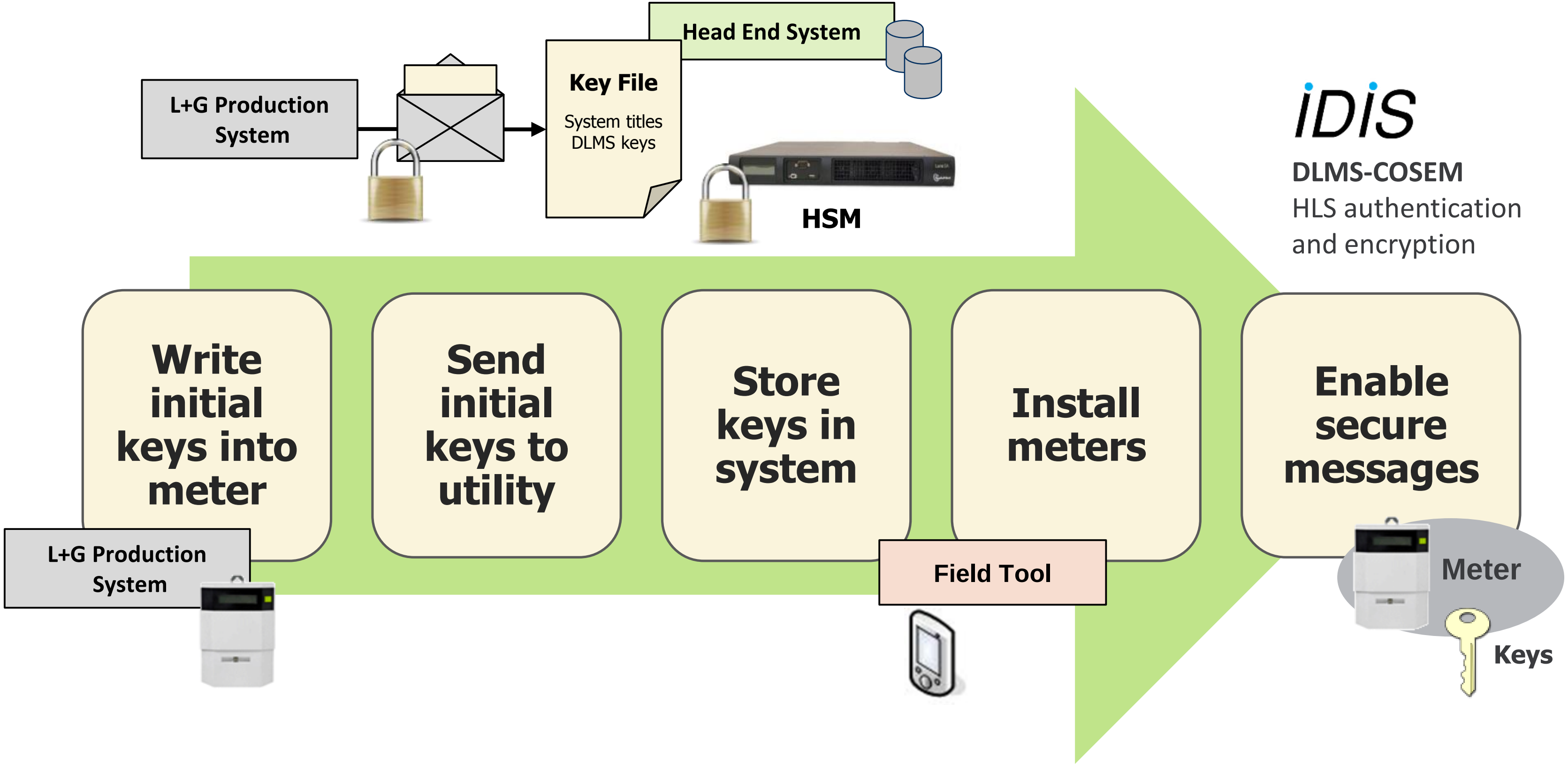
The meter and the head end system need to use identical keys

A set of initial keys are written into the meter at production

A set of identical keys are sent securely from the production facility to the customer’s head end system where they are stored securely



Gridstream® secure deployment



iDIS

DLMS-COSEM

HLS authentication and encryption

The benefits of secure communications

Reduce the risk of supply disruption caused by malicious attack over smart meter communication channels

Ensure Availability

Protect Assets

Prevent malicious damage to smart meter infrastructure caused by unauthorized devices

Ensure the confidentiality of consumer energy measurement data between head end system and meter

Comply with Privacy Regulations

Reduce Risk

Reduce exposure to business risk due to compromised privacy, network cyber attack, and energy theft

Presentation summary

Drivers for secure smart metering

Network protection, regulation and consumer privacy

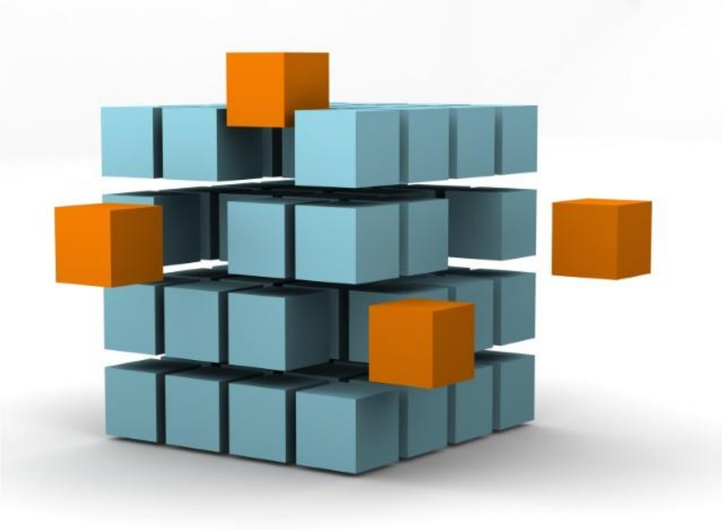
What it takes to create trust

Confidentiality, integrity and authenticity

The European Union environment

Need to comply with the privacy directives and the smart meter recommendation

Some barriers to the adoption of a common EU approach to smart grid security



Presentation summary

Interoperable security with IDIS

Application layer security supports many transport layers

IDIS verifies interoperability

Cryptography

Smart metering context

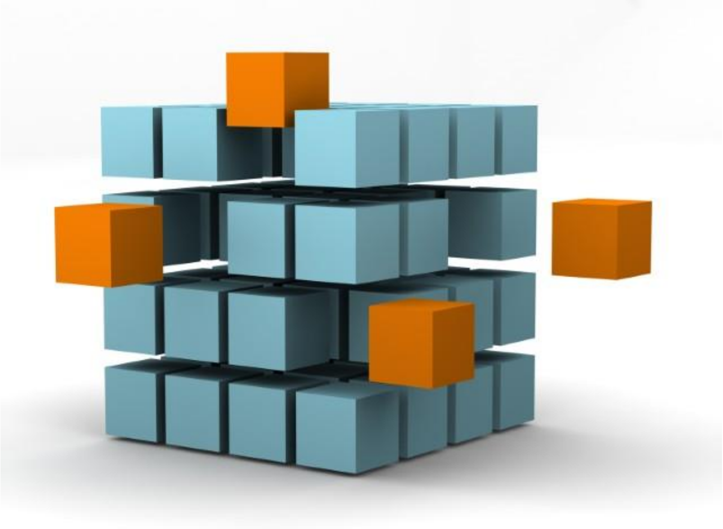
DLMS message authentication and encryption

The EMEA Gridstream® secure communications implementation

Key management

Hardware security modules

Benefits of secure communications



Landis+Gyr

manage energy better

Thank you for your attention