


Trusted Key Manager for Smart Utilities

RE.Learn

What the Internet of Energy (IoE) means to power generation, transmission and distribution



Francis D'Souza – VP IoT Services

17 October 2018



Gemalto enables our clients to deliver trusted digital services



CAPTURING BIOMETRIC
DATA & VERIFYING
IDENTITIES



PROTECTING
MOBILE BANKING
& FUND TRANSFERS



PROVIDING LICENSING
SOLUTIONS TO PROTECT
AND MONETIZE SOFTWARE



DELIVERING HARDWARE
AND SOFTWARE TO
CONNECT CARS
AND OTHER DEVICES



ENCRYPTING DATA
SO THAT IT'S UNUSABLE
IN A BREACH



POWERING CONTACTLESS
PAYMENT FROM CARDS,
MOBILES AND WEARABLES



Quietly, utilities are becoming massive IoT networks

Utilities need to become connected networks

- ▶ To reduce opex (field intervention)
- ▶ To get real-time consumption alignment with new distributed energy resources (DER)
 - solar and wind farms, private solar panel....
- ▶ To enable new services: Smart Home, Facility management, P2P



Energy distribution system operators (DSO) need to trust the data that is coming from the meters in order to:



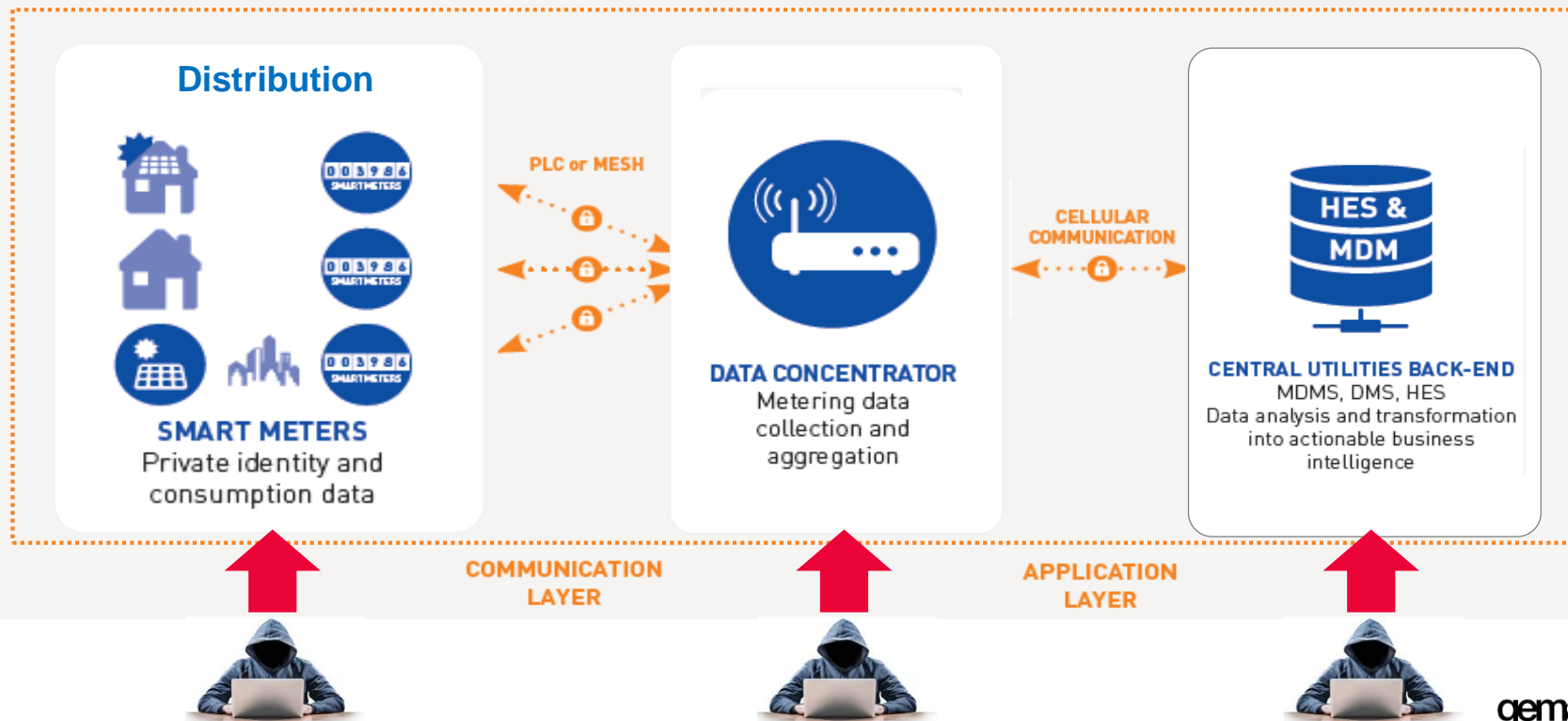
Monetize customer data



Adapt the production supply in real time

The Advanced Metering Infrastructure is becoming a critical IoT network that opens new doors for attackers

Advanced metering Infrastructure (AMI)



Real life story #1

Tampering with the Smart meter data

In the Caribbean, former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash. The altered meter typically reduces a customer's bill by 50% to 75%

Many smart meter devices deployed do little to obfuscate the credentials needed to change their settings or to authenticate 3rd parties (same Admin password Hardcoded in the meter)

Cost of Fraud on smart meters



>5%

of annual turnover was at risk

Real life story #2

Spying on the data concentration points through gateways

South American hackers tapped into Data Concentrators data to draw accurate picture of the personal schedule any expensive electronics of the occupants and to plan burglaries

Issues come from data sent in clear or with poor encryption



Real life story #3

Attack the grid from the back-end to inflicts extensive damages



In Europe, hackers sent false commands to meters to turn them off (or to turn on some connected pieces of equipment), resulting in potential national-scale disruptions: hours-long blackout affecting about 80,000 people

Little is been implemented at the meter level to define which commands received can be trusted

3 reasons for Utilities to mandate security in their networks



Security : It is all about 4 KEY principles

Principle #1

Trust the source
sending the data

Manage Strong
identity through well
diversified
private keys
managed from the
factory
(never passwords)



Principle #2

Ensure that the
exchange of data is
**among trusted
entities**

Mutual authentication
between meters,
gateways and back-
end through PKI



Principle #3

Make sure **only the
authorized servers**
can read the data

Encrypt the data
In all data exchanges
to ensure privacy and
integrity



Principle #4

Enable **security
updatability** on the
meters to cope with
evolving threats

Sign all software
updates and
renew device keys



With such growing connected end-points, **regulation** is been defined in many countries

► Regulations enforcement



Bundesamt
für Sicherheit in der
Informationstechnik

ANSSI



Agence nationale
de la sécurité
des systèmes d'information



(UK)

Department
of Energy &
Climate Change



► Implementing security best practices

NIST : National Institute for standards & technology

- Keys update every 1 to 5 years

EU cybersecurity rules on data protection (GDPR)
and security of critical infrastructure (EPCIP)

- End-to-end data encryption & access management

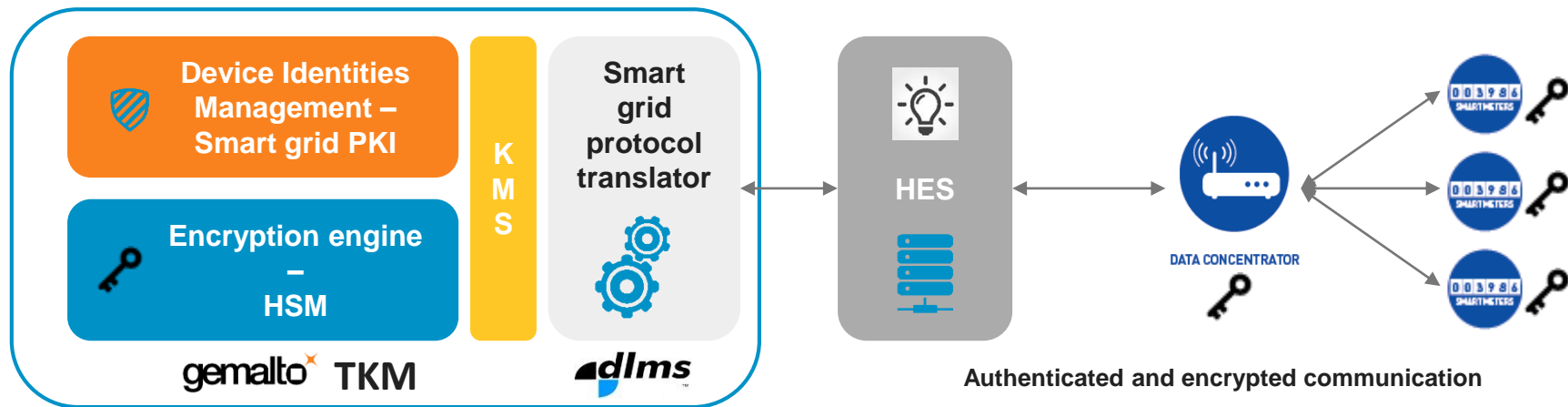


Gemalto

Trusted Key Manager

Solution overview

Gemalto TKM brings trust to the smart grid operational processes



Key generation



In factory
Key injection

Key life cycle



On the field device **identity**
provisioning



Data **encryption**
& **integrity**
validation



Secure device
update

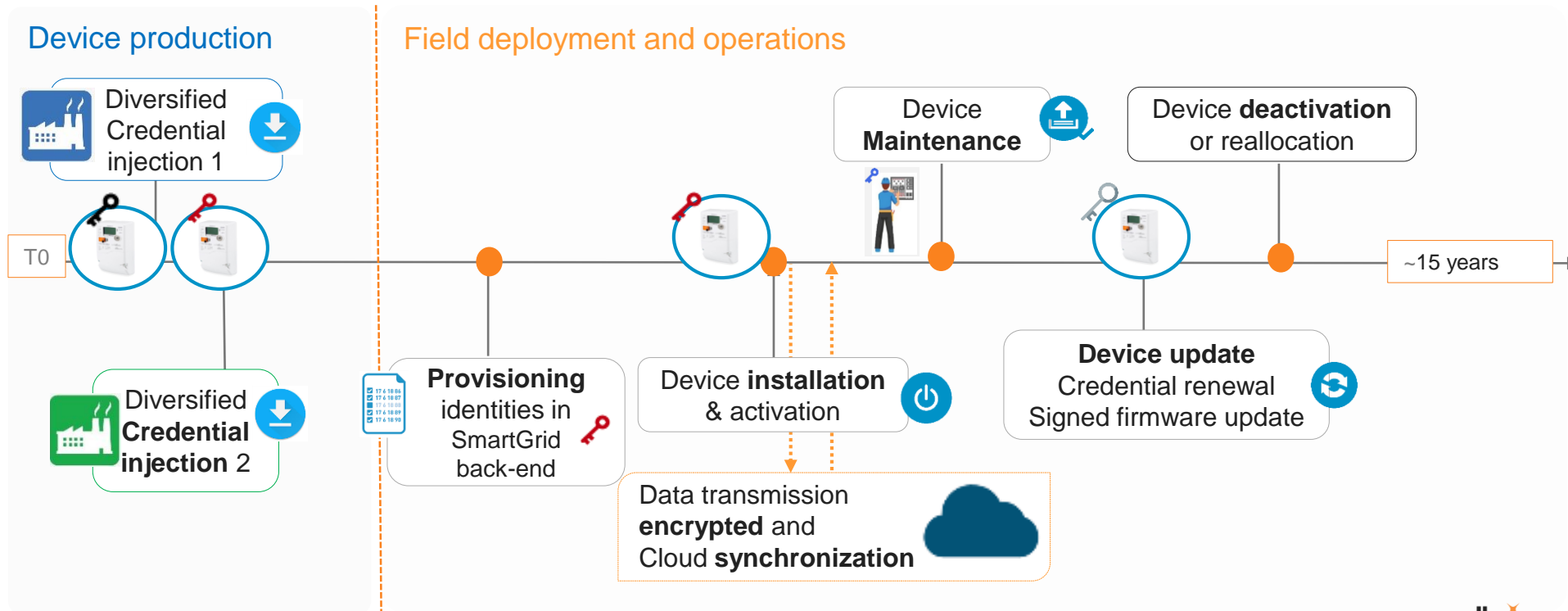


Keys/certificates lifecycle
management



User accounts
management

Gemalto TKM enables automatic **device life cycle management** all along the smart meter processes



Industry recognition

IoT Global Awards 2018 winners named at Smart IoT London



Posted by IOT NOW MAGAZINE
MARCH 21, 2018

London, UK,

Wednesday, March 21st, 2018:



gemalto
security to be free

IoT NOW
HOW TO RUN AN IOT ENABLED BUSINESS

Category :

SMART CITIES, GOVERNMENT & UTILITIES

Best Service:

Gemalto, End-to-end Cybersecurity solution for smart Utilities

[Link IoT Now PR](#)



Home

PREVIOUS

BACK TO SUMMARY

NEXT

BUSINESS WIRE



Gemalto Strengthens Trust in Smart Energy with Its New End-to-End Security Solution

14
MAY
2018


AMSTERDAM

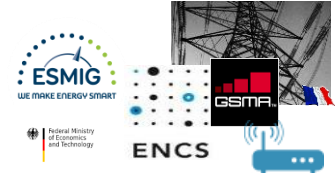
Gemalto (Euronext NL0000400653 GTO), the world leader in digital security, is strengthening trust in the smart energy sector with an end-to-end security solution which protects the entire ecosystem. Deployed by smart meter makers and distribution systems operators, the offer provides seamless connectivity solutions, secure digital identities and

<https://www.gemalto.com/press/pages/gemalto-strengthens-trust-in-smart-energy-with-its-new-end-to-end-security-solution.aspx>

Gemalto footprint in metering business



- Security Design Services
 - Security Evaluation
 - Certification
-  **Trusted Labs**
Creating trust in a connected world



- HES Provider
- System Integrator
- Metering Factory



- HES Provider
- System Integrator
- DSO



- Data Concentrator Provider



- MNO
- Metering provider



- Metering provider



Gemalto TKM Key solution benefits



Comprehensive and Tailor made for Smart metering (DMLS support, PKI preconfigured)



Ready to use, allows faster time to market



Operational Simplicity to control OPEX



Future proof for growing security requirements

THANK

YOU