ETSI TR 103 118 V1.1.1 (2015-08)

Machine-to-Machine communications (M2M);
Smart Energy Infrastructures security;
Review of existing security measures and convergence investigations

Reference
DTR/SmartM2M-021

Keywords
privacy, security, smart grid, smart meter

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document reviews security methods provided by deployed standards used in the Smart Energy industry (e.g. IEC 62351 [i.7], IEC 62443 [i.8]) or mandated by regulation (e.g. Requirements from the German BSI for Smart Meter Gateways and Secure Element) as well as gaps identified by the Smart Grid Information Security group for the M/490 mandate, in order to identify areas where ETSI may bring additional value, e.g. by extending or harmonising security solutions where possible.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Department of Energy & Climate Change: "The Smart Metering System" (leaflet).

NOTE: Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/336057/smart_metering_leaflet.pdf.

[i.2] Federal Office for Information Security: "Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)", Version 1.3, March 2014 and "Protection Profile for the Security Module of a Smart Meter Gateway (SecMod-PP)", Version 1.03 December 2014.

NOTE: Available at https://www.bsi.bund.de/SharedDocs/Zertifikate/PP/aktuell/PP_0073.html and https://www.bsi.bund.de/SharedDocs/Zertifikate/PP/aktuell/PP_0077+V2.html, respectively.

[i.3] Federal Office for Information Security: "Technische Richtlinie BSI TR-03109", Version 1.0, March 2013 (in German).

NOTE: Available at https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html.

[i.4] Association of Energy Network Operators in the Netherlands: "P1 Companion Standard - Dutch Smart Meter Requirements", Version 5.0, May 2014.

NOTE: Available at http://www.netbeheernederland.nl/publicaties/publicatie/?documentregistrationid=272367618.

[i.5] CEN/CENELEC/ETSI Smart Grid Coordination Group: "SG-CG/M490/H-Smart Grid Information Security", annex 4 to BT149/DG9624/DV, December 2014.

NOTE: Available at ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf.

[i.6] IEC 62056-1-0: "Electricity Metering Data Exchange - The DLMS/COSEM Suite", parts 1 to 9.

[i.7] IEC 62351: "Power Systems Management and Associated Information Exchange - Data and Communications Security", parts 1 to 11.

[i.8] IEC 62443: "Industrial Communication Networks - Network and System Security", parts 1 to 3.

[i.9] OMS® group: "Open Metering System Specification" V4.0.2.

NOTE: Available at http://oms-group.org/en_downloads.html.

[i.10] Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids: "Cyber Security of the Smart Grids - Summary Report".

NOTE: Available at http://www.google.fr/url?url=http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm%3Fdoc_id%3D1761&rct=j&frm=1&q=&esrc=s&sa=U&ei=-8E0VZHOIdDnaOPygagD&ved=0CBsQFjAA&usg=AFQjCNHB4SJKYalZyCqgACofDTaLHXGHxQ.

[i.11] European Union Agency for Network and Information Security: "Smart Grid Security Recommendations for Europe and Member States", July 2012.

NOTE: Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations.

[i.12] Smart Grid Task Force, Expert Group 2: "Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment - Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems", March 2014.

NOTE: Available at https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

[i.13] House of Commons - Committee of Public Accounts: "Update on Preparations for Smart Metering", 12th Report of Session 2014-15.

NOTE: Available at http://www.publications.parliament.uk/pa/cm201415/cmselect/cmpubacc/103/103.pdf.

[i.14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.16] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services.

[i.17] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[i.18] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.19] Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[i.20] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

NOTE: Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910.

[i.21] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.22] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.23] IETF RFC 7027: "Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)".

[i.24] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

[i.25] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.26] IEC TR 62210:2003: "Power system control and associated communications - Data and communication security".

[i.27] IEEE 1686-2013: "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities".

[i.28] CEN EN 13757-2:2004: "Communication systems for and remote reading of meters - Part 2: Physical and link layer".

[i.29] CEN EN 13757-3:2013: "Communication systems for and remote reading of meters - Part 3: Dedicated application layer".

[i.30] CEN EN 13757-4:2013: "Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)".

[i.31] IETF RFC 4493: "The AES-CMAC Algorithm".

[i.32] CENELEC EN 62056-61:2007: "Electricity metering - Data exchange for meter reading, tariff and load control - Part 61: Object identification system (OBIS)".

[i.33] OMS® group: "Open Metering System - Technical Report 01 - Security", Issued 1.1.0-2012-12-20. Superseded by [i.9].

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
ANSSI	French Network and Information Security Agency (Agence Nationale de la Sécurité des Systèmes d'Information)
BSI	German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CBC	Cipher Block Chaining
CCA	Climate Change Agreements
CEN	European committee for standardization (Comité Européen de Normalisation)
CGI	Consultants in management and information technology (company name) (Conseillers en Gestion et Informatique)
CMAC	Cipher-based Message Authentication Code
CMS	Cryptographic Message Syntax
CNIL	French National Commission on Information Technology and Liberties (Commission Nationale de l'Informatique et des Libertés)
DCC	Data and Communication Company
DECC	Department of Energy & Climate Change
Defra	Department for environment food & rural affairs

DG	Director General
DKE	German Commission for Electrical, Electronic & Information Technologies (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik)
DLMS	Device Language Message Specification (Distribution Line Message Specification)
DPIA	Data Protection Impact Assessment
DSMR	Dutch Smart Metering Requirements
DSO	Distribution System Operator
EAN	European Article Number
EC	European Commission
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EG2	Expert Group 2
EN	European Norm
ENISA	European Network and Information Security Agency
EnWG	Energy Industry Act (Energiewirtschaftsgesetz)
ESMIG	European Smart Metering Industry Group
ETSI	European Telecommunication Standards Institute
EU	European Union
FIOM	Foundation Interim Operating Model
FOI	Freedom Of Information
FSG	Foundation Strategy Group
FTTS	Foundation Testing and Trialling Strategy
GB	Great Britain
HHT	Hand Held Terminal
HMAC	Hash-based Message Authentication Code
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standardization Organization
ISP	Independent Service Provider
IT	Information Technology
LMN	Local Metrological Network
M/441	Mandate 441
M/490	Mandate 490
M2M	Machine-to-Machine
MAC	Message Authentication Code
M-Bus	Meter Bus
NTA	Netherlands Technical Agreement
OBIS	OBject Identification System
Ofgem	Office of gas and electricity markets
OMS®	Open Metering System
oneM2M	Partnership Project
PHY	Physical
PIN	Prior Information Notice
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PLC	Public Limited Company
RF	Radio Frequency
SCADA	Supervisory Control And Data Acquisition
SDAG	Solution Design Advisory Group
SEC	Smart Energy Code
SG-CG	Smart Grid Coordination Group
SGIS	Smart Grid Information Security
SM-CG	Smart Meter Coordination Group
SMGW	Smart Meter Gateway
SMIP	Smart Meter Implementation Programme
SMRG	Smart Meter Regulation Group
SQW	Segal Quince Wicksteed (company name)
TLS	Transport Layer Security
UK	United Kingdom
VIF/DIF	Value Information Field / Data Information Field
WAN	Wide Area Network

Wbp	Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens)
WG	Working Group
Wi-Fi®	Wireless Fidelity
wM-Bus	wireless Meter Bus

4 Privacy and Security Regulations

4.1 EU Level Regulation

The 2014 M/490 SGIS Report assesses the impact in the different member states of the foreseen migration from a privacy directive (translated into legislation at the level of the member states) to a privacy regulation, i.e. a common EU level legislation applicable in all member states:

- EU Directive 95/46/EC [i.14] on processing of personal data; and
- EU Directive 2002/58/EC [i.15] on processing of personal data and the protection of privacy in the electronic communications sector.

According to the commission recommendation of 9th March 2012 on preparation for the roll-out of smart metering systems, these two directives are "fully applicable to smart metering which processes personal data, in particular in the use of publicly available electronic communications services for contractual and commercial relations with customers". This recommendation provides further guidance on how the directives should apply to the smart metering systems.

Other directives that impact security and privacy are the following:

- Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services [i.16]
- Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [i.17]
- Directive 1999/93/EC on a Community framework for electronic signatures [i.18]
- Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [i.19]
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [i.20]

4.2 France

4.2.1 Data Security Rules

The Data security offered by products or information systems may be certified as provided in the Decree #2002-535 of 18th April 2002.

ANSSI (French Network and Information Security Agency) is responsible for approving assessment centers and give an opinion on the certification of systems. Certification is given by the Prime Minister following their assessment by approved centers.

Concerning the electricity metering, the order of 4th January 2012 requires system operators to have their metering system certified under Decree #2002-535 of 18th April 2002.

This certification implies compliance with a security referential specified by ANSSI.

4.2.2 Privacy Protection Rules

The *Commission nationale de l'informatique et des libertés* (CNIL) is responsible for ensuring that information technology remains at the service of citizens, and does not jeopardize human identity or breach human rights, privacy or individual or public liberties.

The automated processing of personal data is subject to a prior declaration to CNIL.

Specifically regarding Smart Metring Systems, Decree #2001-630 of 16th July 2001 (Decree #2004-183 of 18th February 2004 for gas) requires system operators to keep confidential commercially sensitive data (information whose disclosure could undermine the rules of free and fair competition and non-discrimination). Metering data are commercially sensitive.

In its resolution #2012-404 of 15th November 2012, CNIL issued recommendations primarily on data collected (consent and limiting load curve sampling period), the duration of data retention (no conservation beyond the time required) the recipients of the data (habilitation) and security measures (assessment and regular updating).

4.3 Germany

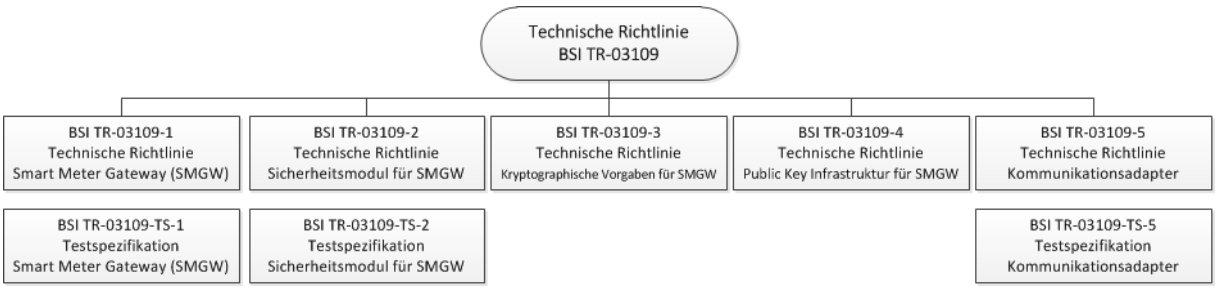
In Germany, legal and regulatory requirements are already in force for energy- and telecommunication enterprises. New legal requirements are in preparation for other critical infrastructures like finance, transport, food industry and health services. The new laws explicitly define critical infrastructures and the obligation to prove that these infrastructures are operated securely. This has to be done by certified procedures and properly documented, i.e.by an Information Security management system like the ISO/IEC 27000 series [i.21]. Notification of security incidents to the authorities will be mandatory.

In the legal framework of energy regulations, the metering service is a market driven business like the energy supply. Actually, the metering services are still done by the DSOs (Distribution System Operators). There are about 900 DSOs for electricity and about 700 DSOs for gas. But, besides of pilot projects, the roll-out of smart meters has not started yet. According to the Energy Industry Act (EnWG) the installation of smart meters and smart meter gateways is mandatory for consumers with an annual consumption of more than 6 000 kWh. The Ministry of Economics and Energy mandated the Federal Office for Information Security (BSI) to issue specifications for a smart meter gateway in order to meet concerns about privacy raised by the Federal Commissioner for Data Protection and Freedom of Information**.** These smart meters and gateways have to fulfil security requirements like Common Criteria Protection Profile and a Technical Specification to ensure interoperability between different metering Service Providers.

These specifications are:

- Protection Profile for the Gateway of a Smart Metering System (BSI-CC-PP-0073) [i.2]
- Protection Profile for the Security Module of a Smart Meter Gateway (BSI-CC-PP-0077) [i.2]
- Technische Richtlinie / Technical Guideline (BSI TR-03109) [i.3]

where the BSI TR-03109 is a collection of documents (only in German) specifying data formats, protocol stacks for WAN and metering communication, administration requirements and Public Key Infrastructure.



The German DKE group AK461.0.143 has specified the protection at the interface between the Smart Meter Gateway (SMGW) and the WAN or external entity. The specification is part of BSI TR-03109-1 [i.3].

Only outgoing connections from the SMGW to the external entity are allowed. The SMGW is the TLS client, whereas the external entity is TLS server. Initiation with ECDSA signed wakeup from Administrator is optional. http(s) and additional content protection with CMS (based on PKCS#7) are used: first encrypted and authenticated, than signed. The external entity can replace the signature for pseudonymization reasons. Mutual X.509 PKI authentication is required, no http authentication. The certificate types are:

- TLS (SMGW, administrator, other external entities);
- SubCA (e.g. administrator);
- RootCA+LinkCertificate;
- Content signature (SMGW, Admin);
- Content encryption (SMGW, Admin, external entities);
- etc.

The exposed resources according to a RESTful access concept are based on certificate authentication.

Current TLS parameters for WAN:

- TLS1.2 (IETF RFC 5246 [i.22]);
- Cyphersuites min ECDHE_AES128_CBC_SHA256 and ECDHE_AES128_GCM_SHA256 transition to AES256 and SHA384 later;
- Using X.509 PKI certificates. ECDSABrainpoolP256r1 Signed, SHA256;
- ECC Curves, BrainpoolP256, NISTP384, BrainpoolP384, BrainpoolP512. Only with NamedCurveIDs (IETF RFC 7027 [i.23]);
- No session resumption, but session resume (max. session lifetime 2 days);
- Preference for Encrypt-than-MAC indicated, no Truncated HMAC (to be updated in 2015).

In 2013, a metering system ordinance (Messsystemverordnung), which refers to the BSI specifications was drafted by the German government and notified according to the "Directive 98/34/EC of the EUROPEAN PARLIAMENT and of the COUNCIL" [i.24], which is laying down a procedure for the provision of information in the field of technical standards and regulations.

Up to now, smart meters and gateways, which are compliant with the German legal and regulatory requirements are not available for a roll-out. The stakeholders are still waiting for additional ordinances. The missing ordinances for the energy sector to clarify the obligations and scale of roll-out and the allocation of the costs are expected for mid-2015.

4.4 Netherlands

An initial project law to impose mandatory roll-out of smart meters in the Netherlands was turned down in the Dutch Parliament in 2009 due to consumer concerns, which triggered serious actions from the Dutch DSOs to enhance consumers trust. Their association, Netbeheer Netherlands, enforces a code of conduct for the processing of personal data by Grid Operators and made a study on the Security and Privacy of Smart Metering that served as a basis to develop the security aspects of the Dutch Smart Metering Requirements (DSMR) specification [i.4], which have already been iterated several times.

The most important rules in the Netherlands for recording and using personal data have been set forth in the Wet bescherming persoonsgegevens (Wbp; Dutch Personal Data Protection Act). This act was unanimously adopted by the Dutch Senate on 23 November 1999 and accepted by the Dutch Congress on 3 July 2000. The act came into force on 1 September 2001.

The Wbp relates to every use - 'processing' - of personal data, from the collection of these data up to and including the destruction of personal data.

Smart meters in the Netherlands are the property of Grid operator. Almost 1 million smart meters have been installed during the first phase of roll-out until 2014. In 2015, the Grid operators start with the large-scale roll-out. 12 million gas and electrical smart meters are expected to be installed by 2020.

On the smart meter a "P-1 port" exists which is intended for display purposes in home. The P-1 port can also be used for connection to an external facility (e.g. external provider/web interface) to show the metering values.

In the Netherlands the data owner is the owner of the (personal) data. This means in the context of smart energy and smart meter data, the grid operator is collecting the information and is also the owner of the information. In the Netherlands every household, every building has a unique European Article Number (EAN-code) for its water, gas and electricity meter. In principle the DSO knows the address and the EAN-code. The smart meter ID is connected to the EAN-code. The smart meter data is send to the DSO.

The customer has a contract with a service provider. The DSO sends the meter data to the service provider.

Customers have a right for access to "their" metering data, which may be granted via local or web-based interfaces. Suppliers have to provide customers with monthly usage and billing information.

The customer:

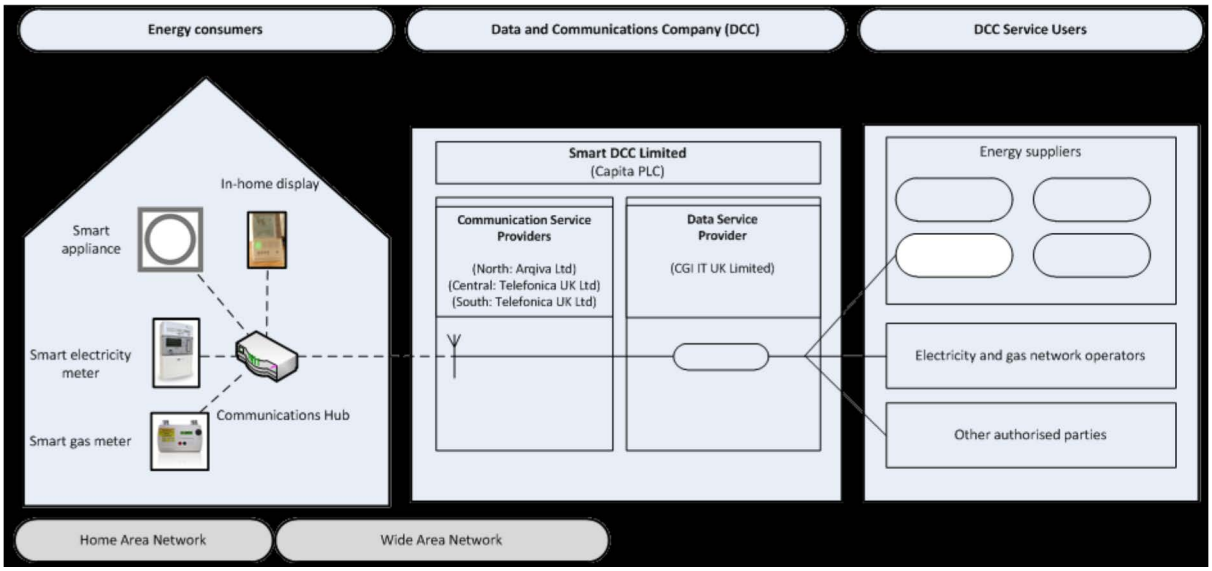
- Gets the smart meter in his or her home, which the grid operator can read remotely.
- Can (whether or not the meter allows remotely readings) readout the meter to get insight in detailed information, which gives a reflection of energy consumption and energy production.
- Can resist the smart meter (opt-out).
- May refuse initial placement.
- Or may (if the meter is already installed) make the smart meter witless (when no measurement data can be readout remotely).
- Gives permission for the smart meter (opt-in).
- Gives permission to the energy supplier or Independent Service Provider (ISP), and then the energy supplier or ISP is authorized to retrieve the measurement data.
- Can ask for priority placement of the smart meter.
- Can use smart meter information for an understanding of the energy consumption and energy production, for instance for energy saving purposes.

4.5 United Kingdom

4.5.1 Department of Energy & Climate Change - Shared Smart Metering National Infrastructure

NOTE: This clause is copied from [i.1].

"The diagram illustrates the main parts of the smart metering systems showing the equipment and communications within energy consumers' homes. It shows the organizations that will use the information provided by smart meters (DCC Service Users), and the system provided by the Data and Communication Company (DCC) which will link these organizations with the smart meters.



The Smart Metering System

Equipment and communications within energy consumers' homes

The smart metering equipment installed by energy suppliers will normally consist of a smart electricity meter, a smart gas meter, and a communications hub. Energy suppliers will offer all domestic customers an In Home Display at no cost as part of the installation process. These devices are explained below.

Smart electricity and gas meters

Existing electricity and gas meters in consumers' homes will be replaced with smart versions. Unlike traditional meters, they automatically pass accurate meter readings to energy suppliers, and support new functions including enabling smart appliances and time of use tariffs.

In-Home Display

The in-home display will allow consumers to see what energy they are using and how much it is costing in near real time. The display can also show information about the amount of energy used in the past day, week, month and year. This will help people to understand and control their energy consumption.

Communications hub

The communications hub has two functions. Firstly it allows the smart meters and In-Home Display to communicate with each other over a Home Area Network, in a similar way to wireless computer networks (Wi-Fi®). Secondly it provides a link to the Wide Area Network which allows information to be sent to and from meters by energy suppliers, energy network operators and energy service companies.

Organizations that will use the information provided by smart meters (DCC Service Users)

A number of organizations will communicate with smart meters. Consumers will have a choice about how their energy consumption data is used, apart from where it is required for billing and other activities that energy companies are legally required to undertake.

Energy Suppliers: *A consumers' energy supplier will communicate remotely with smart metering equipment to take meter readings, to update pricing information on the In-Home Display and to take readings on change of supplier or change of tenancy.*

Energy Networks: *The organizations that operate the energy network infrastructure will be able to access data, to help them understand the loads on their network at the local level and to respond to loss of supply issues. Energy networks will have better information upon which to manage and plan current activities and move towards smart grids which support sustainable energy supply.*

Organizations offering services: *Consumers can choose to allow other organizations to have access to the data from their smart meter. For example, switching sites could use accurate information on the amount of energy used to advise consumers on the best tariff and energy supplier. As the roll-out proceeds, an increasing range of devices should become available to help consumers manage their energy usage, including smart appliances which can operate automatically when electricity is cheaper.*

Smart meter communications outside the home: the Data Communications Company and the Wide Area Network

The Data and Communications Company will put in place communications across Great Britain to send and receive information from smart meters to energy suppliers, energy network operators and energy service companies. The Data and Communications Company will be operated by Capita PLC under a licence regulated by Ofgem.

The Data and Communications Company will manage three main subcontractors. CGI IT UK Limited is the Data Services Provider which controls the movement of messages to and from smart meters. Arqiva Limited and Telefonica UK Limited are the Communications Service Providers and will put in place the Wide Area Network. Arqiva will do this for Scotland and the north of England. Telefónica will cover Wales and the rest of England.

Further information

Further information about smart meters can be found on the Government's website at https://www.gov.uk/smart-meters-how-they-work

Smart Metering Implementation Programme: information leaflet: https://www.gov.uk/government/publications/smart-metering-implementation-programme-information-leaflet

Smart Metering Implementation Programme non-domestic leaflet: https://www.gov.uk/government/publications/smart-metering-non-domestic-leaflet".

4.5.2 Smart Metering Equipment Technical Specifications

Equipment technical specifications can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/39368/2393-smart-metering-industrys-draft-tech.pdf

https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version

Other Security related information can be found at:

Smart meter data access and privacy

The Smart Metering System Leaflet

Call for evidence on smart meter data access and privacy

Smart metering implementation programme: draft technical specifications

Smart metering security risk assessments

Smart Metering Implementation Programme: Draft licence conditions and technical specifications for the roll-out of gas and electricity smart metering equipment

5 Standardized Security Methods

5.1 Relevant ISO/IEC Specifications

As IEC is the traditional standardization body for the electricity sector, security and privacy issues related to smart energy are already covered to a certain extend by IEC specifications. Most security standards in major M2M verticals assume PKI deployments.

Furthermore general purpose security specifications from ISO such as the ISO/IEC 27000 [i.21] series for IT security recommendations or ISO/IEC 15408 [i.25] for Common Criteria Security Assurance remain applicable references in the domain.

The most important standards considered today in the domain are listed below. They generally assume the deployment of a Public Key Infrastructure to manage security credentials, though some challenges are acknowledged, e.g. the difficulty to manage key revocation when entities may not enjoy permanent or high bandwidth connectivity. The M/490 Smart Grid Information Security WG report [i.5] is a good source for further precisions.

- In the Smart Metering domain, IEC 62056-1-0 (DLMS) [i.6] is being enhanced to cover secure communication services between the metering infrastructure and third parties.
- In power distribution systems, the IEC 62351 series [i.7] is the reference for Data and Communication Security.
- SCADA and Industrial Control System standards such as the IEC 62443 series [i.8] are used as a reference for some smart grid assets.
- Other security related standards:
  - IEC TR 62210 [i.26]: Power system control and associated communications - Data and communication security.
  - IEEE 1686-2013 [i.27]: Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.

5.2 ETSI M2M and oneM2M

ETSI and the partnership project oneM2M developed standards of a horizontal M2M service platform. These standards also include security solutions.

Though some energy industry groups consider the concept of a horizontal M2M service platform with interest, migration from currently applied vertical standards to such new standards does not appear feasible in the short term. To be adopted by the energy market, it appears that security services provided through an M2M service platform need to be provided by an entity trusted by energy domain stakeholders, in confidentiality from other involved parties such as transport network providers.

5.3 OMS®

5.3.1 Introduction

The OMS® (Open Metering System) Group is a forum of technical associations in Germany related to electricity, water and gas, as well as utilities and internationally operating meter manufacturers. The group has developed the OMS® specification, which enables interoperability between meters by standardized communication interfaces and systems. OMS® is the only system specification, which integrates all the media like electricity, gas, water and heat into one system. The specification is based on the European M-Bus standard (CEN EN 13757) as well as the Dutch NTA 8130 and is applied to the **(Wireless-)M-Bus interface between Smart Meter and Smart Meter Gateway**.

The OMS® Group develops specifications for users/implementers of the CEN EN 13757 standards family (CEN TC294 WG4) to clarify ambiguities, select profiles, give examples for implementation, define conformance/interoperability tests and define the certification of OMS® devices. The OMS® specifications cover:

- CEN EN 13757-3 [i.29] (M-Bus Application Layer)
- CEN EN 13757-2 [i.28] (Wired M-Bus PHY and Link-Layer)
- CEN EN 13757-4 [i.30] (Wireless M-Bus PHY and Link-Layer)

The OMS® specification also describes a mapping for interoperability between OBIS (CENELEC EN 62056-61 [i.32]) and M-Bus Application Layer VIF/DIF.

In October 2011, the OMS® Security Task Force was established to develop the Technical Report OMS® TR-01 [i.33], which fulfills the requirements of the German Federal Office for Information Security (BSI) for a "Local Metrological Network" (LMN) interface between a Smart Meter and a Smart Meter Gateway (SMGW). These requirements are described in the Technical Report BSI TR-03116-3. These requirements had been derived from the national data protection requirements for personal consumption data. Private data and data, from which persons can be identified have to be protected at high level.

OMS® TR-01 [i.33] describes where existing CEN EN 13757 protocols are extended by a secure Transport Layer for bi-directional or uni-directional communication. OMS® TR-01 was published as an annex to BSI TR-03109-1 in 2013, which passed the EU notification procedure. In 2014, the OMS® TR-01 became part of the OMS® Specification 4.0.2 [i.9] describing the Authentication Fragmentation Layer with Key Derivation for encryption and MAC.

5.3.2 Uni-directional wM-Bus Communication

The use of uni-directional wireless M-Bus communication is mainly required for, e.g. heat cost allocators, gas meters, and water meters. The following security features are defined:

- Symmetrical Preshared-Key ("Master-Key") installed inside the device by the manufacturer and transmitted out-of-band to the SMGW Administrator. Master Key can only be changed with physical device access.
- Key Derivation Function based on AES128-CMAC with monotonously increasing non-resettable counter used to derive Message Keys for MAC and Encryption.
- Message-MAC (AES128-CMAC IETF RFC 4493 [i.31]) and/or Message-Encryption with AES128-CBC with IV=0.

5.3.3 Bi-directional (w)M-Bus Communication

Bi-directional wireless M-Bus communication has to be used if it is possible:

- Uses TLS1.2 with X.509 self-signed certificates for direct trust.
- Private/Public ECC-Keypair generated by SMGW for meter shall be changed every 6/7 years initiated by SMGW Administrator.
- Initial Communication based on Symmetrical Preshared-Key ("Master-Key") installed inside the device by the manufacturer, transmitted out-of-band to SMGW Administrator. Master Key shall be changed every two years within TLS secured channel (SMGW generated, initiated by Administrator). New Master Key delivery on secure channel to Administrator.
- Key Derivation Function based on AES128-CMAC with monotonously increasing non-resettable counter used to derive Message Keys for MAC.
- Additional Message-MAC (AES128-CMAC IETF RFC 4493 [i.31]) to protect against DoS attacks using initial TLS Handshake.
- Meter is TLS-Client and SMGW is TLS-Server, because the SMGW is more DoS-resistant "by design".

5.3.4 TLS Parameters for Local Metrological Network

The following TLS parameters are defined:

- TLS1.2 (IETF RFC 5246 [i.22]).
- Cyphersuites min ECDHE_AES128_CBC_SHA256 and ECDHE_AES128_GCM_SHA256.
- Using small (< 255 Bytes) self-signed X.509 certificates (no subject, no issuer required but possible); ECDSA-NISTP256 signed, SHA256.
- HMAC truncation, Max_Fragmentsize_Extension required by server (SMGW) for low-bandwidth RF channels.
- ECC Curves NISTP256 (min), BrainpoolP256, NISTP384, BrainpoolP384; only with NamedCurveIDs (IETF RFC 7027 [i.23]).
- No session resumption, but session resume (max. session lifetime 1 month or 5 MByte cumulated record data volume).

NOTE: OMS® is an example of a suitable products available commercially. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of these products.

5.4 ESMIG Initiatives on Privacy and Security

In an effort to accompany the European Commission actions around the M/441 and M/490 mandates, the European Smart Metering Industry Group set up a Task Force on Privacy and Security, to harmonise the vision from the industry and promote EU level harmonisation of foreseen national regulations in the Energy Domain, which at this stage remain very specific to each national context. In particular the enforcement in Germany of specifications from the BSI requiring security certification of Smart Metering Gateway relying on hardware security module and Common Criteria Protection Profile triggered an effort to compare national security certification schemes in the major European countries (Germany, UK and France), and investigations are under way to determine to which extend a security certification obtained in one country could be automatically validated in other countries, if EU countries could come up with a sufficiently harmonised approach to allow this. Such EU level harmonisation, which is further supported by efforts from a DG CONNECT Expert Group [i.10] and initiatives from ENISA [i.11], is essential to enable economy of scale on security assessment costs and favour deployment of proven security implementation at affordable price.

6 Gaps, Alignments and New Developments

6.1 SM-CG M/441 Security and Privacy Report

The SM-CG Ad-Hoc Workgroup on data security and privacy has so far developed three reports. The most recent report "Privacy and Security approach - Part III" comprises an overview of the smart metering threat landscape as well as the set of mitigating measures and the link between threats and security requirements from its first report. Final comments on Part III are now being incorporated.

As regards further work, the workgroup is continuing to work on completion of the SM-CG security package (Use Cases, Threats, Requirements, Techniques) and on security certification approaches. In addition the workgroup is linked with EG2 (on Best Available Techniques for security and privacy) and the DPIA test phase, and is participating in both these initiatives, which run until June and October 2016 respectively (see clause 6.2).

6.2 Standardization Gaps Identified by the M/490 SGIS WG

The M/490 SGIS report of 2014 [i.5] identified a number of gaps in security standardization addressing security certification and tests aspects which may be critical to ensure alignment of security levels on the European energy infrastructure despite local national influences. It is important to understand that the SGIS work focuses primarily on security requirements standards rather than specific implementations. The SGIS methodology includes a risk assessment step to derive the relevant security requirement standards to apply based on a specific use case, and also integrates Privacy Impact Assessment based on the DPIA template [i.12] developed by EG2 of the Smart Grid Task Force and approved by the Article 29 Working Party at the European level. This DPIA template describes a process that should be undertaken by the stakeholders involved in a metering infrastructure deployment, according to their responsibilities, to demonstrate due diligence for complying with applicable EU Data Protection legislation. In addition to this, EG2 has been enlarged into a Stakeholders Forum in charge of selecting the "Best Available Techniques" for preserving security and privacy in smart metering systems, with the purpose of recommending promising implementations.

The main security recommendations are contained in the ENISA "Smart Grid security recommendations for Europe and Member States" [i.11], which also identifies further actions being pursued to enhance security and harmonisation of deployments across Europe.

7 Recommendations

7.1 Privacy

Despite different national and cultural approaches across Europe, the advent of EU wide privacy regulation, supported by the Smart Metering Data Protection Impact Assessment Template [i.12] and ongoing selection of "Best Available Techniques" to preserve privacy in smart energy infrastructures, together provide a solid basis to address consumer's privacy concerns in a consistent way across the Member States.

The biggest challenge may lie in the need to influence existing utilities culture to evolve from centralized information model, where raw metering data are blindly collected to a central database or cloud without any filtering or prior processing, toward the distributed information concept that stems from the Data Minimization principle inherent to Privacy-by-Design: Ideally each energy system stakeholder should be able to extract at the point of collection (i.e. the Smart Meter) only those data that are required for their legitimate purpose or granted access by the data subject.

Though even with restricted computing resources, with sufficient standardization, even the simplest IT systems can be made to support the remote application management feature implied by the above requirement, digital meters are still perceived (and often conceived!) as a mere dumb evolution of mechanical meters integrating a remote communication means, rather than as a "smart" component integrated within the energy information system. It takes time and efforts to change people's mentality!

However, in the UK for example, there are questions being raised on whether savings could be achieved by not providing an in-home display to households who wanted to use other devices such as smart phones or tablets to receive data. The security and privacy issues of moving away from a dedicated locked down device using say ZigBee® to a fully open device using alternative protocols such as Wi-Fi® or Bluetooth® would need to be very carefully considered [i.13].

Another aspect that would determine the security and privacy of the entire system are the procedures for use of the Hand Held Terminal (HHT) or equivalent that provides the local commissioning and maintenance capability for smart meters and communications hubs.

7.2 Security

Despite the efforts undertaken by ENISA to ensure a minimum security level that could apply to a European energy grid, the security of critical infrastructures such as smart energy grids remain a national prerogative of each European member state. Additionally, national regulations in the domain related to e.g. meter ownership or market structure, are heavily influenced by each country's history and differ widely. Such factors influence the economic and technical aspects of smart grid deployments, which in turn have impact on the relevant security measures derived from risk assessment.

These constitute major obstacles preventing integration of member state's energy networks into a pan-European energy grid. Furthermore, in several countries, enforcement of proper security measures applying to critical infrastructures such as energy grids is either disconnected from similar measures applying in neighbouring countries, or non-existent.

It has been recognized that the enforcement of proper security levels at an affordable cost would require the definition of a common security protection profile as well as an equivalence or unification between certification schemes applied across member states. While efforts to develop equivalence between national schemes are progressing, divergence between national security regulations may increase to the point where the definition of a common protection profile becomes unfeasible.

Without successful efforts to harmonise the national security regulations applying to critical infrastructures in the different member states, not only the advent of a secure pan-European energy grid will be compromised, but the security of each national infrastructure may suffer from weaknesses arising from the boundaries with neighbouring states.

A common protection profile cannot be standardized by ETSI. The definition of a common protection profile should be addressed at EU level.

Annex A:
Further Information

Smart Meter deployments in UK are the most mature in terms of security in Europe. More information about the security deployment framework in UK is provided in this annex.

- Smart meters

  Part of Housing, Safety environment

  Smart meters keep track of your energy consumption through a digital display in your home - installation dates, meter readings, cost.

- Smart Meters statistics

  - Published on: 26 September 2013
  - Collection
  - Departments: DECC

  This series brings together all documents relating to smart meter statistics.

- Smart meters code of practice

  - Published on: 18 August 2011
  - Consultation outcome
  - Departments: DECC

  Smart meters code of practice.

- Southern Water universal metering

  - Published on: 11 July 2013
  - FOI release
  - Departments: Defra

  Compulsory fitting of water meters by Southern Water.

- Smart meter data access and privacy

  - Published on: 5 April 2012
  - Consultation outcome
  - Departments: DECC

  Smart meter data access and privacy.

- Smart meters hothouse

  - Published on: 26 July 2011
  - Guidance
  - Departments: DECC

  "Smart Meters Hothouse diagram - the Hothouse concentrates the Design Working Groups to complete the final assembly and assurance of the Smart…"

- Smart meter consumer engagement strategy
  - Published on: 5 April 2012
  - Consultation outcome
  - Departments: DECC

  Smart meter consumer engagement strategy.

- Smart Meters Programme
  - Published on: 10 May 2013
  - Policy paper
  - Departments: DECC

  Smart Meters Programme Delivery Plan.

- Smart Meter Regulation Groups

  The Smart Meter Regulation Groups (SMRG) provide information and opinions of stakeholders to the Smart Meter Implementation Programme (SMIP).

- The Smart Metering System Leaflet
  - Published on: 8 October 2013
  - Guidance
  - Departments: DECC

  This leaflet explains how the smart metering system will work from late 2015, when a new shared smart metering national infrastructure is in place.

- Smart Meters: programme plan
  - Published on: 20 December 2012
  - Policy paper
  - Departments: DECC

  "Updated delivery plan representing the Government's current view of the approach and timescales for delivery of the GB Smart Metering Programme…"

- Smart Metering: implementation programme
  - Published on: 13 December 2012
  - Policy paper
  - Departments: DECC

  "Smart Meters Tranche 2 Licence conditions. The licence condition modifications governing the consumer engagement strategy, data access and privacy…"

- Justification of Practice: application for a lattice smart gas meter
  - Published on: 12 October 2012
  - Policy paper
  - Departments: DECC

  Application for Justification of Practice: LATTICE Smart Gas Meter.

- Smart Metering non domestic leaflet
  - Published on: 2 September 2013
  - Guidance
  - Departments: DECC

  Frequently asked questions about non-domestic smart metering.

- The prohibition order for smart metering communication activities
  - Published on: 10 February 2012
  - Consultation outcome
  - Departments: DECC

  The prohibition order for smart metering communication activities.

- Speech to the Smart Metering Forum
  - Published on: 21 November 2013
  - Speech
  - Departments: DECC

  Baroness Verma addressed the Smart Metering Forum.

- Call for evidence on smart meter data access and privacy
  - Published on: 18 August 2011
  - Consultation outcome
  - Departments: DECC

  Call for evidence on smart meter data access and privacy.

- Smart meters statistics: methodology note
  - Published on: 26 September 2013
  - Statistics
  - Departments: DECC

  Methodology note accompanying quarterly statistical releases on the number of smart meters in domestic properties and smaller non-domestic sites.

- Smart metering implementation programme: draft technical specifications
  - Published on: 4 August 2011
  - Policy paper
  - Departments: DECC

  "The smart metering industry's recommended technical specifications for smart metering equipment. An industry produced suite of documents providing…"

- Smart Metering Implementation Programme - Licence Conditions for Operational Requirements and Accession to, and Compliance with, the Smart Energy Code

  - Published on: 10 May 2013
  - Guidance
  - Departments: DECC

  Smart Meters licence condition modifications.

- Delivering smart meters to homes and businesses

  - Published on: 27 July 2010
  - Consultation outcome
  - Departments: DECC

  "On 27 July 2010, the Government with Ofgem published a prospectus containing proposals for the delivery of electricity and gas smart metering…"

- Smart Meters: Consumer Advisory Group

  Responsible for making sure consumer interests remain central to the Smart Metering Implementation Programme.

- Smart Meters: Modifications to the standard conditions of electricity and gas supply licences

  - Published on: 30 November 2012
  - Policy paper
  - Departments: DECC

  "Licence conditions for the roll-out of gas and electricity smart metering systems and a code of practice for the installation of smart metering…"

- Smart metering system and equipment testing

  - Published on: 27 August 2013
  - Closed consultation
  - Departments: DECC

  Consultation on the testing of smart metering systems and equipment under the Smart Energy Code (SEC).

- Smart Metering Implementation Programme: technical specifications

  - Published on: 18 December 2012
  - Policy paper
  - Departments: DECC

  The requirement to install metering equipment in Great Britain which complies with these Smart Metering Equipment Technical Specifications.

- Smart metering security risk assessments

  - Published on: 31 May 2012
  - Consultation outcome
  - Departments: DECC

  "The Government's smart metering policy will require changes to the existing regulatory and commercial framework governing the electricity and…"

- Smart meter statistics data: quarter 2 2013

  - Published on: 26 September 2013
  - Statistics
  - Departments: DECC

  Quarterly statistics on the roll-out of smart meters in Great Britain.

- Smart metering implementation programme: information leaflet

  - Published on: 2 September 2013
  - Guidance
  - Departments: DECC

  An information leaflet giving an overview of the smart metering implementation programme for the domestic sector.

- Smart Metering Implementation Programme: First Annual Progress Report on the Roll-out of Smart Meters

  - Published on: 19 December 2012
  - Policy paper
  - Departments: DECC

  This is the first annual report on progress with the roll-out of smart meters. It provides an introduction to smart metering and the benefits to consumers.

- Smart meters

  "Smart meters are the next generation of gas and electricity meters. They are part of our plan for upgrading the UK's energy system. We aim for all homes and small businesses to have smart meters by 2020. Energy..."

- Smart Meters: Foundation Strategy Group

  The Foundation Strategy Group (FSG) oversees the Foundation Interim Operating Model (FIOM) and the Foundation Testing and Trialling Strategy (FTTS) group - all part of the Smart Metering Implementation Programme.

- Smart Meters Implementation Programme: delivery plan

  - Published on: 23 December 2011
  - Corporate report
  - Departments: DECC

  "Revised delivery plan representing the Government's current view of the approach and timescales for delivery of the GB Smart Metering Programme…"

- Contract notice for Smart Metering Implementation Programme services

  - Published on: 30 August 2011
  - Policy paper
  - Departments: DECC

  "The contract notice for IT data services with regards to the Smart Metering Implementation Programme, for consulting, software development, …"

- Licence conditions for non-domestic smart metering issues

  - Published on: 22 October 2013
  - Open consultation
  - Departments: DECC

  Seeking views on draft licence conditions for non-domestic smart metering issues.

- Smart Metering Implementation Programme: Draft licence conditions and technical specifications for the roll-out of gas and electricity smart metering equipment

  - Published on: 18 August 2011
  - Consultation outcome
  - Departments: DECC

  "Smart Metering Implementation Programme: Draft licence conditions and technical specifications for the roll-out of gas and electricity smart…"

- Smart Meters: Foundation Testing and Trialling Strategy Group

  The Foundation Testing and Trialling Strategy (FTTS) Group helps with the planning of the end-to-end delivery cycle of the smart meters programme.

- Smart Meters: Stage 1 of the Smart Energy Code

  - Published on: 17 July 2013
  - Consultation outcome
  - Departments: DECC

  Smart Metering Implementation Programme: Supplementary consultation on draft legal text to support transitional arrangements.

- Study on Access to Smart Meter Benefits for Blind and Partially Sighted Consumers

  - Published on: 25 March 2013
  - Policy paper
  - Departments: DECC

  The Smart Meters Programme commissioned SQW to look at options for ensuring that blind and partially sighted consumers can access the benefits for smart meters.

- Information requirements for monitoring and evaluation of smart meters

  - Published on: 31 May 2012
  - Consultation outcome
  - Departments: DECC

  "The Government's smart metering policy will require changes to the existing regulatory and commercial framework governing the electricity and…"

- Smart Meters: Consumer Engagement and Roll-out Group

  A forum to discuss all consumer-facing issues relating to the smart meter programme, including benefits realization.

- Smart metering implementation programme: Foundation Smart Market

  - Published on: 5 August 2013
  - Consultation outcome
  - Departments: DECC

  Seeking views on how meters installed in the foundation stage will be adopted into the enduring arrangements; and whether regulation is required to support smart change of supplier.

- Smart Meters: Solution Design Advisory Group

  The Solution Design Advisory Group (SDAG) will enable the Smart Metering Implementation Programme to continue to draw upon the experience of industry participants and other stakeholders.

- Smart for all: understanding consumer vulnerability during the experience of smart meter installation

  - Published on: 29 January 2013
  - Research and analysis
  - Departments: DECC

  Research to inform stakeholders of good practice for the roll-out of smart meters.

- Statistical release: Smart meters, Great Britain, quarter 2 2013

  - Published on: 26 September 2013
  - Statistics
  - Departments: DECC

  This quarterly release presents statistics on the roll-out of smart meters in Great Britain.

- Smart meters data and communications company: implementation programme prior information notice

  - Published on: 28 July 2011
  - Policy paper
  - Departments: DECC

  "The prior information notice (PIN) 148947-2011 for the Service Provider Procurement Project of the Smart Meters Data and Communications Company…"

- Role of Community Groups in Smart Metering-Related Energy Efficiency Activities
  - Published on: 25 March 2013
  - Policy paper
  - Departments: DECC

  A research report to help build an understanding of how community groups might best be involved in consumer engagement for the smart meter roll-out.

- The Green Deal and Prepayment Meters
  - Published on: 6 March 2013
  - Guidance
  - Departments: DECC

  How the Green Deal works for pre-payment customers.

- Smart Meters RF Survey
  - Published on: 8 June 2012
  - Policy paper
  - Departments: DECC

  Final report for DECC by Red-M.

- Climate Change Agreements: deadline for data submission and sub-metering requirements
  - Published on: 6 May 2013
  - Policy paper
  - Departments: DECC

  Guidance to clarify the deadline for submitting data and installing sub-metering to comply with the CCA regulations.

- Policy design of the regulatory and commercial framework for DCC
  - Published on: 29 September 2011
  - Consultation outcome
  - Departments: DECC

  Smart Metering Implementation Programme consultations.

Annex B: Bibliography

ISO 15118: "Road Vehicles -- Vehicle to Grid Communication Interface".

Department of Energy & Climate Change: "Smart Metering Implementation Programme - Great Britain Companion Specification (GBCS)", Version 0.8.1, November 2014.

NOTE: Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/380611/GBCS_v0.8.1.docx.

European Commission DG CONNECT Expert Group: "Security & Resilience of Telecom Networks for Smart Grids".

NOTE: Documents available at https://ec.europa.eu/digital-agenda/en/news/cybersecurity-smart-grids.

CEN/CENELEC/ETSI: "Security & Privacy Ad-Hoc Group Report".

Smart Grids Task Force: several reports, e.g. "Regulatory recommendations for data handling, data safety and data protection" and "Commission recommendations on preparation for the roll-out of smart metering systems".

NOTE: Available at http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters.

History

Document history		
V1.1.1	August 2015	Publication