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

TECHNICAL REPORT

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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

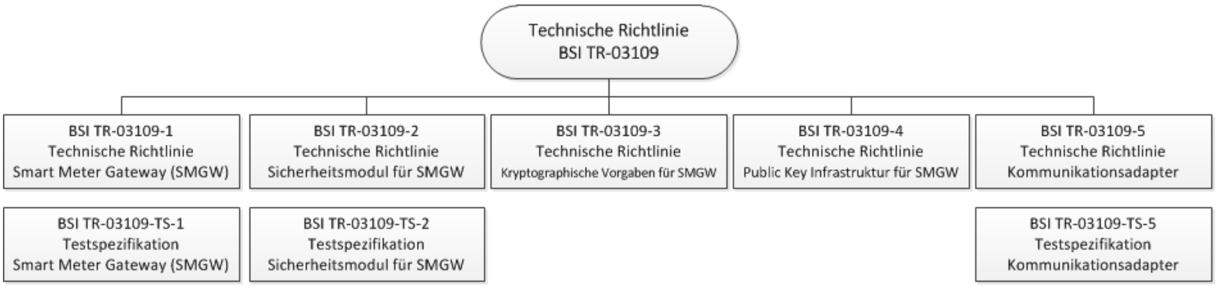
In Germany, legal and regulatory requirements are already in force for energy- and telecommunication enterprises. New legal requirements are in preparation for other critical infrastructures like finance, transport, food industry and health services. The new laws explicitly define critical infrastructures 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].