Certification Report

Protection Profile for Smart Meter Minimum Security requirements, Version 1.0

Sponsor and developer: ***European Smart Meter Industry Group***
Boulevard A. Reyers 80
1030 Brussel
Belgium

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-PP-0040161-CR**
Report version:	**1**
Project number:	**0040161**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**18 November 2019**
Number of pages:	**9**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number **PP-19-0040161**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

European Smart Meter Industry Group

Boulevard A. Reyers 80,1030 Brussels, Belgium

Product and assurance level

Protection Profile for Smart Meter Minimum Security requirements, Version 1.0

Assurance Package:

- EAL3 augmented with ALC_FLR.3

Project number **0040161**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity

Date of 1st issue : **19-11-2019**

Certificate expiry : **19-11-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.G.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Protection Profile for Smart Meter Minimum Security requirements, Version 1.0 *[PP]*. The developer of the PP is the European Smart Meter Industry Group located in Brussels, Belgium and they also act as the sponsor of the evaluation and certification. This Certification Report is intended to assist prospective users when judging the suitability of the protection profile for their particular requirements.

The PP is developed as a basis for the development of Security Targets in order to perform a certification of an IT-product (TOE. A smart supply meter is a device that monitors, and possibly limits, the consumption of electricity, gas, thermal energy or water provided by utilities supply markets and communicates with users via both local (“direct”) and network interfaces.

The protection profile has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 18 November 2019 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The results documented in the evaluation technical report *[ETR]*[1] for this protection profile provides sufficient evidence that the it meets the requirements for protection profile evaluations specified in de the Common Criteria for Information Security Evaluation. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the protection profile will be listed on the NSCIB Certified Protection Profile list. It should be noted that the certification results only apply to the specific version of the protection profile as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable for public review.

2 Certification Results

2.1 *Protection Profile Identification*

The Target of Evaluation (TOE) for this evaluation is the Protection Profile for Smart Meter Minimum Security requirements, Version 1.0 from European Smart Meter Industry Group located in Brussels, Belgium.

Title	Protection Profile for Smart Meter Minimum Security requirements
PP Version	Version 1.0, 30 October 2019
CC Version	3.1, revision 5
CC Conformance claim	Part 2 extended, Part 3 conformant, EAL3 augmented with ALC_FLR.3
Required conformance	Conformance claims to this protection profile require **strict** conformance

2.2 *Protection Profile Overview*

The Protection Profile describes a set of security requirements for smart meters, based on the 'minimum security requirements' for components of AMI infrastructures. The requirements are based on the concept that there are a common/generic set of underlying 'minimum' security requirements associated with smart metering requirement specifications in a number of EU Member States.

Members of the ad hoc SCG-SM1 Task Force on Privacy and Security have as a result developed a set of generic minimum requirements that are valid for most of the European Member States. From this set, the requirements applicable to smart meters (as opposed to other parts of the AMI) have then been used as the basis for this Protection Profile by translating them, with specification of additional detail where necessary, into Common Criteria Security Functional Requirements (SFRs) and refinements to the Security Assurance Requirements (SARs). The requirements defined in this Protection Profile can therefore serve as a basis for specific requirements of individual EU Member States, based on a risk analysis that has assessed the specific assets and actors applicable to their scheme.

2.3 *Security Functional Requirements*

Based on the Security Objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of Security Functional Requirements to be implemented by a TOE. The security functional requirements are divided in a number of functional groups. Every group contains one or more mutually coherent requirements. These groups are:

- Cryptographic Support: These describe the requirements for cryptographic key generation, key destruction and cryptographic operations.
- User Data Protection: These requirements define how user data shall be secured at rest and in transit.
- Identification and authentication: These requirements define user authentication for access to all types of data held on the TOE. Different types of data could have different authentication methods and re-authentication times
- Protection of the TSF: These requirements, together with some extended requirements, describe how the continuous secure operation and secure software updates are achieved during the TOE´s operational use.
- Security Management: These requirements specify the management the different management roles and their interaction, such as separation of capabilities.
- Security Audit: These requirements defined which system events are recorded and how these are protected.

The TOE Security Functional Requirements (SFR) are outlined in the *[PP]*, article 6. Some are selected directly from Common Criteria Part 2 and some are defined in the protection profile itself. Thus the SFR claim is called: **Common Criteria Part 2 extended**.

2.4 Security Assurance Requirements

The TOE security assurance requirements claimed in the Protection Profile are based entirely on the assurance components defined in part 3 of the Common Criteria for the Evaluation Assurance Level 3 package augmented with ALC_FLR.3. Thus, the SAR claim is called: **Common Criteria Part 3 conformant, EAL 3 augmented with ALC_FLR.3**.

(for the definition and scope of assurance packages according to CC see *[CC]*, part 3 for details).

2.5 Results of the PP evaluation

The evaluation lab determined that the claims as made in the Protection Profile for Smart Meter Minimum Security requirements, Version 1.0 *[PP]* are in conformance with the requirements for Protection Profiles as specified in class APE of the CC.

The certifier concluded that the evaluation lab has performed all APE work units in accordance with the APE section of the CEM. The findings are recorded in an Evaluation Technical Report *[ETR]*.

2.6 Comments/Recommendations

There are no specific Evaluator Comments or Recommendations.

3 Protection Profile

The Protection Profile for Smart Meter Minimum Security requirements, Version 1.0 *[PP]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AMI	Advanced Metering Infrasructure
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report Protection Profile for Smart Meter Minimum Security requirements, Version 1.0, Evaluation Technical Report Smart Meter PP – EAL3+, version 1.0, 06 November 2019.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[PP] Protection Profile for Smart Meter Minimum Security requirements, Version 1.0, 30 October 2019.

(This is the end of this report).