Certification Report

Edge Compute Note Protection Profile v1.0.7

Sponsor:	***Microsoft Corporation*** **200 150th Ave NE** **Receiving Bldg 123** **Redmond, WA** **98052-5302 US**
Developer:	***Prove & Run*** **77 av. Niel** **Paris** **75017 FR**
Evaluation facility:	***UL*** **Unit 2 Horizon, Wade Road, Kingsland Business Park** **Basingstoke, Hampshire** **RG24 8AH, UK**
Report number:	**NSCIB-PP-0112146-CR**
Report version:	**1**
Project number:	**0112146**
Author(s):	**Brian Smithson**
Date:	**8 October 2020**
Number of pages:	**9**
Number of appendices:	**0**

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

CONTENTS:

Foreword **3**

Recognition of the certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **6**

2.1 Protection Profile Identification 6
2.2 Security Policy defined by the Protection Profile 6
2.3 Re-used evaluation results **Fout! Bladwijzer niet gedefinieerd.**
2.4 Results of the PP Evaluation 8
2.5 Comments/Recommendations 8

3 Protection Profile **9**

4 Definitions **9**

5 Bibliography **9**

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.

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 Edge Compute Note Protection Profile v1.0.7 *[PP]*. The developer of the Edge Compute Note Protection Profile v1.0.7 is Prove & Run located in Paris, FR, and the sponsor of the evaluation and certification is Microsoft Corporation located in Redmond WA, US. A Certification Report is intended to assist prospective consumers 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 Edge Compute Node (ECN). A ECN is a piece of hardware and software located between a network of Internet of Things (IoT) leaf devices in an IoT network and an IoT Edge Cloud. It performs local processing of data from IoT leaf devices through a runtime environment offered to developers and of acting as a bridge between the IoT Edge Cloud and IoT leaf devices. The Edge Compute Node can be provisioned and administrated from the IoT Edge Cloud by a trusted administrator.

Within the Edge Compute Note protection profile, the Base-PP comprises an ECN Security Manager which provides the core security features needed for an Edge Compute Node.

To create a conforming Security Target for product evaluation, this Base-PP must be complemented with features defined in one of three PP-modules that are defined in appendices of the Edge Compute Note protection profile.

The PP-modules provide support for, respectively:

- Software-based secure boot and file system secure storage (provided by the TOE)
- HSM-based secure storage and cryptography (provided by the environment)
- Secure Enclave-based secure storage and cryptography (provided by the environment)

The protection profile has been evaluated by UL, located in Basingstoke, Hampshire, UK. The evaluation was completed on 8 October 2020 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 (standard) protection profile evaluations specified in the Common Criteria for Information Technology 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 Edge Compute Note Protection Profile v1.0.7 from Microsoft Corporation located in Redmond WA, US:

PP title	Edge Compute Node Protection Profile v1.0.7
PP version	Version 1.0.7, 4 September 2020
CC Version	3.1, revision 5
CC Conformance claim	Part 2 extended, Part 3 extended, EAL1 augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, and ALC_TSU_EXT.1
Required conformance	Conformance claims to this protection profile require **strict** conformance

2.2 Security Policy defined by the Protection Profile

The Protection Profile describes a set of security requirements for an Edge Compute Node (ECN), consisting of a piece of hardware and software located between a network of Internet of Things (IoT) leaf devices in an IoT network and an IoT Edge Cloud. It has the capability of performing local processing of data from IoT leaf devices through a runtime environment offered to developers and acts as a bridge between the IoT Edge Cloud and IoT leaf devices. The Edge Compute Node can be provisioned and administrated from the IoT Edge Cloud by a trusted administrator.

The security features of the ECN Security Manager (defined by the Base-PP) include the following:

- The Update function, which provides secure update.
- The Edge Runtime, which is the execution runtime for Edge modules.
- The Provisioning Library, which provides device identity lifecycle management.
- The Secure Communication Library, which provides support of TLS with X.509 certificates.
- The Cryptographic Library, which provides cryptographic services for the device, including cryptographic keys.
- The Monitoring Library, which generates and monitor security events for the TOE

In addition to the Base-PP, the Protection Profile defines three PP-modules. The TOE of the Base-PP is the ECN Security Manager which provides the core security features needed for an Edge Compute Node, but it must be complemented with features described in one of the three PP-modules that are defined in appendices the PP:

- **PP Configuration #1** extends the TOE's Base-PP with a software-based secure boot feature and secure storage for protected data (data-at-rest protection) on a persistent memory of the Edge Compute Node. The TOE is composed of the ECN Security Manager, as in the Base-PP, extended with the secure boot component and a secure storage component that includes cryptography required for secure storage.
- **PP Configuration #2** extends the TOE's Base-PP with a secure boot feature and a secure storage for protected data (data-at-rest protection) that is performed by in a HSM located in the operational environment of the TOE. The TOE is composed of the ECN Security Manager, as in the Base-PP, extended with support of the interaction with the HSM.
- **PP Configuration #3** extends the TOE's Base-PP with a secure boot feature and a secure storage for protected data (data-at-rest protection) that is performed by a Secure Enclave-located in the operational environment of the TOE. The TOE is composed of the ECN Security Manager, as in the Base-PP, extended with support of the interaction with the Secure Enclave.

To claim conformance to this Protection Profile, a Security Target **must** conform to the Base-PP and one of the PP-modules as described in the three PP configurations. **Strict** conformance is required.

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 for the Base-PP are:

- **Security Audit**: The TOE has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Authorized administrators can review audit logs and have the ability to search and sort audit records.
- **Cryptographic Support**: The TOE provides cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, and random number generation. The TOE additionally provides support for public keys, credential management and certificate validation functions. In addition to using cryptography for its own security functions, the TOE offers access to the cryptographic support functions for Edge modules.
- Identification and **Authentication**: The TOE provides the ability to use, store, and protect certificates that are used for authentication of the IoT Edge Cloud and to authenticate the TOE (static and dynamic attestation).
- **Protection of the TOE Security Functions**: The TOE provides a number of features to ensure the protection of TOE security functions. It protects against unauthorized data disclosure. The TOE ensures process isolation security for all Edge modules, with support from the Standard Execution Environment. The TOE includes self-testing features that ensure the integrity of executable program images and its cryptographic functions. Finally, The TOE provides a trusted update mechanism to update the TOE binaries itself.
- **Trusted Path for Communications**: The TOE provides protected communications with the IoT Edge Cloud.
- **Security Management**: The TOE provides several functions to manage security policies. This includes management of Edge Modules, cryptographic keys and certificates and auditable events.

The additional groups for PP-Configuration #1 (Secure Boot and File System Secure Storage PP-Module) are:

- **Secure storage and related crypto**, which protects user data at rest and provides secure storage of cryptographic keys and certificates.
- **Secure boot and hardware-protected keys**, which authenticates executable code loaded from boot prior to its execution based on a hardware-protected certificate and provides hardware protection for the cryptographic keys used for secure storage. This low-level firmware and possibly related support from the Standard Execution Environment is outside of the ECN Security Manager and may be device-specific.

The additional group for PP-Configuration #2 (HSM-Based Secure Storage and Cryptography PP-Module) is:

- **Secure communication** with trusted IT product (HSM).

The additional group for PP-Configuration #3 (Secure Enclave Secure Storage and Cryptography PP-Module) ais:

- **Secure communication** with trusted IT product (Secure Enclave)

2.4 Security Assurance Requirements

The TOE security assurance requirements claimed in the Protection Profile are based on the assurance components defined in part 3 of the Common Criteria for the Evaluation Assurance Level 1 package augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, and extended with ALC_TSU_EXT.1. Thus, the SAR claim is called: **Common Criteria Part 3 extended, EAL1 augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, and ALC_TSU_EXT.1**.

2.5 Results of the PP Evaluation

This evaluation was conducted using the methodology described in the *[CEM]* for each configuration defined in the Edge Compute Node Protection Profile by flattening all the components of the Base-PP with each of the PP-Modules to create three PP-Configurations, and to evaluate the resulting PP-Configurations as a separated standard PPs using the APE class.

The evaluation results from the Base-PP Intermediate Report were reused by the ITSEF for each one of the evaluated PP-configurations.

The evaluation lab documented their evaluation results in the *[ETR]* and determined that the claims as made in the *[PP]* are in conformance with the requirements for (standard) 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]* and approved the *[ETR]* on 8 October 2020.

2.6 Comments/Recommendations

To create a conforming Security Target for product evaluation, strict conformance to the Base-PP **must** be complemented by strict conformance to one of three PP-modules that are defined in appendices of the Edge Compute Note protection profile:

1. Software-based secure boot and file system secure storage.
2. HSM-based secure storage and cryptography
3. Secure Enclave-based secure storage and cryptography

Note that HSM (referenced in Support for HSM-Based Secure Storage and Cryptography Module) and Secure Enclave (referenced in Support for Secure Enclave-Based Secure Storage and Cryptography Module) are in the operation environment. Their respective PP-modules only provide interfaces and support functions).

3 Protection Profile

The Edge Compute Note Protection Profile, v1.0.7, 4 September 2020 *[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:

ECN	Edge Compute Node
HSM	Hardware Security Module
IoT	Internet of THings
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]	Edge Compute Note Protection Profile v1.0.7 Evaluation Technical Report, UL13306316, Version 1.3, 4 September 2020.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Edge Compute Note Protection Profile, v1.0.7, 4 September 2020.

(This is the end of this report).