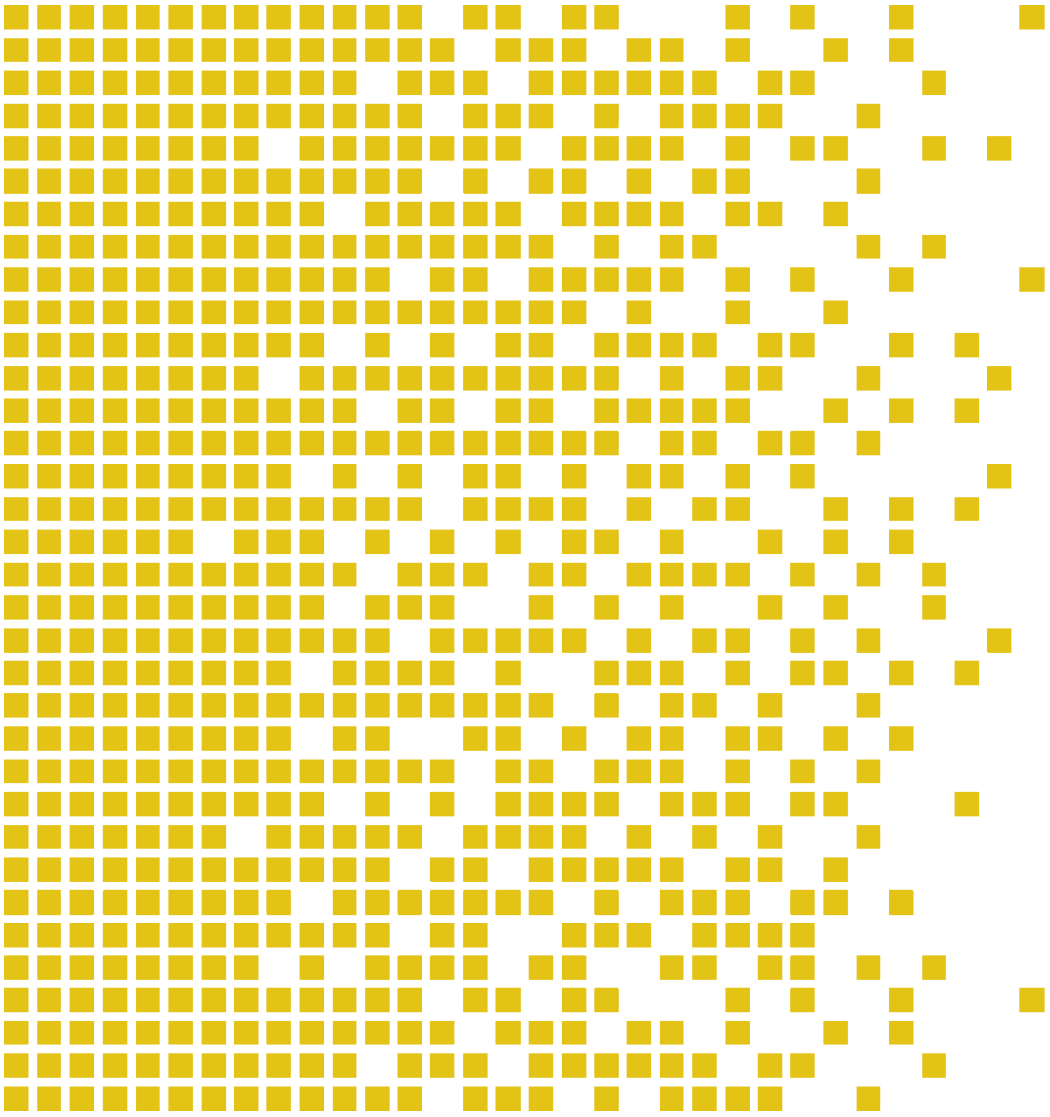
SERTIT-113 CR Certification Report

Issue 1.0 28 September 2018

Expiry date 28 September 2023

X-Ware IoT Platform SC v5.11



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Express Logic X-Ware IoT Platform SC is a
"RTOS for IoT applications, including TCP/IP, TLS and MQTT" .

X-Ware IoT Platform SC version 5.11 has been evaluated under the terms of the Norwegian Certification Authority for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) augmented components of Evaluation Assurance Level EAL 4+ augmented with ALC_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Certification team	Kjartan Jæger Kvassnes, SERTIT Arne Høye Rage, SERTIT
Date approved	28 September 2018
Expiry date	28 September 2023

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
MQTT	Message Queuing Telemetry Transport
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

[2] CCRA (2017), *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[5] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[6] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[7] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[8] Express Logic (2018),
"X-Ware IoT Platform SC Security Target v2.0 2018-08-22" .

[9] Brightsight (2018) Evaluation Technical Report. Common Criteria EAL4 augmented with ALC_FLR.1 Evaluation of «X-Ware IoT Platform SC», v4.0, 2018.08.24.

[10] *Express Logic (2018) Supporting TOE guidance documents*

a. NetX Duo MQTT (NetX Duo MQTT) for clients User Guide Revision 5.11

b. NetX Duo the high-performance real-time implementation of TCP/IP standards User Guide Revision 5.11

c. NetX Secure User Guide Revision 5.11SP1

d. ThreadX the high-performance embedded kernel User Guide Revision 5.8

e. X-Ware IoT Platform SC Security Guidance 2018-08-22

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of X-Ware IoT Platform SC version 5.11 to the Sponsor, Express Logic, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the ST[8] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The version of the product evaluated was X-Ware IoT Platform SC and version 5.11.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Express Logic .

The TOE consists of an embedded RTOS, an IPv4/IPv6 network stack, a TLS implementation and a MQTT implementation.

The TOE format is a collection of source code files written in standard C, organized in four groups:

- netx_duo (IP stack)
- netx_mqtt (Message Queuing Telemetry Transport)
- netx_secure (TLS implementation)
- threadx (underlying RTOS)

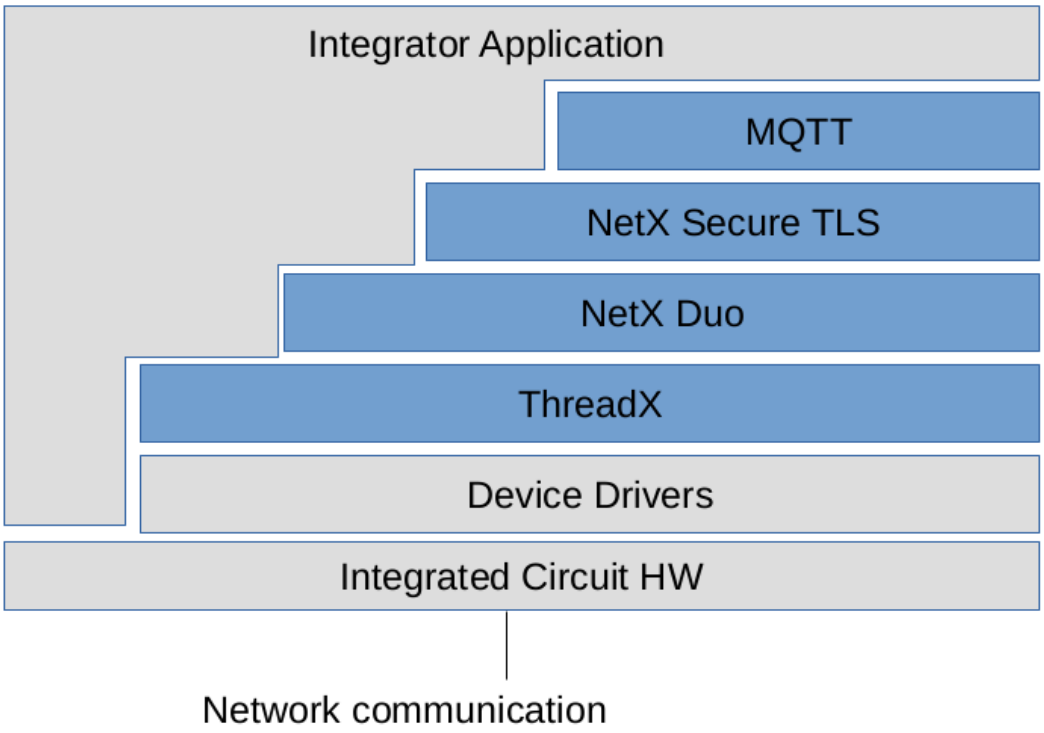
intended to be compiled jointly with the user application to produce an executable binary. Furthermore, the TOE requires a non-TOE software including the device drivers for the hardware abstraction, memory management, cryptographic libraries, RNG and timer tick, and a non-TOE hardware platform with at least one network interface.

The ST[8] sections 1.3 and 1.4 provide a full description.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The figure below depicts the TOE structure with the TOE parts in scope of the evaluation highlighted in blue.



4.4 Protection Profile Conformance

The ST[8] did not claim conformance to any protection profile/cPP.

4.5 Assurance Level

The ST[8] specified the assurance components for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4+, augmented by ALC_FLR.1. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in ST[8] section 3.2.

4.7 Security Claims

The ST[8] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.MITM: An attacker might eavesdrop or tamper with the security sensitive network communication between the TOE and another trusted IT product.

4.9 Threats Countered by the TOE's environment

No threats or attacks that are countered by TOE's environment are described.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- A.TRUSTED_INTEGRATOR: The integrator is assumed to be competent and will use the security functionalities needed by the complete IoT solution following the TOE guidance documentation, including the usage of secure cipher suites. The integrator will not attempt to thwart the TOE security functionalities nor bypass them.

4.12 Security Function Policy

- P.TRUSTED_PLATFORM: The underlying platform will run in a trusted environment, out of an attacker's physical reach or will be tamper and side channel resistant in a way that is capable of sustaining the TOE's functionality in its operating environment.
- P.MQTTTLS: The TOE must provide a secure MQTT implementation that is available over TLS.
- P.UNDERLYING_CRYPTO: The integrator will use cryptographic services provided by means of the underlying Device Drivers' layer that fulfill [RFC3447][FIPS197][SP80067][FIPS1804][FIPS1981]. The underlying cryptography will be resistant to timing attacks when operating with secret or private keys.
- P.INTEGRATOR_SECRETS: The integrator secrets confidentiality and integrity, including keys, will be preserved by the integrator's application while on integration application's memory space. The keys and temporary secrets that are allocated in memory by the TOE during a secure session with another trusted IT product must be cleared from the TOE's memory space when the session is terminated.

4.13 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[1]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of both the Arrangement on the

Recognition of Common Criteria Certificates in the Field of Information Technology Security, CCRA[7], and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOGIS MRA[6] and the evaluation was conducted in accordance with the terms of these Arrangements.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[8], which prospective consumers are advised to read. To ensure that the ST[8] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[5].

SERTIT monitored the evaluation in accordance with SD001E[1] which was carried out by the Brightsight Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final ETR[9] to SERTIT in 2018.08.24. SERTIT then produced this Certification Report.

4.14 General Points

The evaluation addressed the security functionality claimed in the ST[8] with reference to the assumed operating environment specified by the ST[8]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 4 assurance package augmented with ALC_FLR.1.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.1	Basic flaw remediation
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the ST[8]. The results of this work were reported in the ETR[9] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance documents[10] provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluators considered three categories of vulnerabilities:

- Vulnerabilities resulting from a search through the developer's documentation.
- Vulnerabilities resulting from the source code analysis
- Vulnerabilities stemming from the implementation of the TLS secure layer, TLS certificates management and known TLS vulnerabilities.

The source code analysis and the evaluator's tests showed that the possible vulnerabilities resulting from the vulnerability analysis could not be exploited.

5.6 Developer's Tests

The Developer Testing consists of an automated testing application that automatically run multiple test and categorize them by the TOE subsystems:

- NetX Duo: 388 tests.
- NetX Secure TLS: 44 tests.
- MQTT: 23 tests
- ThreadX: implicitly tested in all other tests.

The developer provided the source code of the testing application, the necessary support and tools to compile it and a hardware platform to run the test in the form of a developing board, in order to allow repetition of the developer's testing. The developer also provided an automated tool (LCOV) which reports the coverage of the tests in terms of lines of source code, branches and functions.

5.7 Evaluators' Tests

For independent testing, evaluators decided to repeat the complete test suite because it was more efficient than performing a sampling of the developer testing, using the test application and hardware platform provided by the developer.

The evaluator also analyzed the ST and TOE design in order to devise a test plan covering the TOE SFRs implementation. The evaluator independent test plan is summarized below:

TEST	SHORT DESCRIPTION
IND.SELF-TEST	To verify that self-test is functionality is implemented and available for the integrator.
IND.SESSION-TERMINATION	To verify that a fatal error destroys the TLS session including the session's secrets.
IND.TLS.CONFIG.PROTOCOLS	To verify that weak protocols are not supported
IND.TLS.CONFIG.CERT-CHAIN	Verify that a TOE TLS client sends an unknown CA alert when receiving a complete certificate chain where the root certificate is unknown to the TOE.
IND.TLS.CONFIG.CIPHERSUITES	Test cipher suites are supported by a TOE
IND.TLS.CONFIG.COMPRESSION	Test compression methods a TOE TLS client supports
IND.TLS.CONFIG.RENEGOTIATION	Test that TOE does not support insecure renegotiation
IND.TLS.CONFIG.EXTENSIONS	Verify the extensions supported by the TOE according to [RFC5246 ch.7.4.1.4]
IND.TLS.IMP.VERSIONS	Verify secure protocol negotiation
IND.TLS.IMP.RNG	Verify quality of random numbers in TLS session establishment
IND.TLS.IMP.CIPHER-SUITES	Verify the TOE rejects weak cipher suites
IND.TLS.IMP.EXTENSIONS	Verify TOE does not accept MD5
IND.TLS.IMP.CERT-VERIFY	Verify certificates management
IND.TLS.INTEGRITY	Verify the TLS integrity checks
IND.TLS.RECORD	Verify correct management of TLS records
IND.TLS.KEY-CALCULATION	Verify key management implementation
IND.TLS.LENGTH-CHECKS	Verify correct management of TLS record length
IND.TLS.CHANGE-CIPHER	Verify TOE rejects insecure change of cipher suites
IND.TLS.ALERT	Verify that the TOE raises an alert on insecure events

Additionally, evaluators conducted the following penetration test:

TEST	SHORT DESCRIPTION
PEN.TLS.CERT_FUZZING	Try to send malformed certificates to bypass the certificate validation.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that X-Ware IoT Platform SC version 5.11 meets the specified Common Criteria Part 3 augmented components of Evaluation Assurance Level EAL 4+ augmented with ALC_FLR.1 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Security Target

The developer did not provide a Security Target Lite and accepted to publish the complete Security Target [8] used for the evaluation.

6.3 Recommendations

Prospective consumers of X-Ware IoT Platform SC version 5.11 should understand the specific scope of the certification by reading this report in conjunction with the ST[8]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST[8].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance[10] documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

- TOE name: X-Ware IoT Platform SC
- TOE version: 5.11

X-Ware IoT Platform SC consists of the following items:

- ThreadX version 5.8sp2: industrial grade IoT RTOS
- NetX Duo version 5.11: advanced dual IPv4 & IPv6 TCP/IP network stack
- NetX Secure TLS version 5.11sp1: TLS cryptographic protocol on top of the NetX Duo network stack
- MQTT version 5.11: Message Queuing Telemetry Transport messaging protocol on top of the NetX Secure TLS TLS implementation

The TOE components and documentation is delivered to the customer via the developer sharefile web site.

TOE Documentation

The supporting guidance documents evaluated were:

a. NetX Duo MQTT (NetX Duo MQTT) for clients User Guide Revision 5.11

b. NetX Duo the high-performance real-time implementation of TCP/IP standards User Guide Revision 5.11

c. NetX Secure User Guide Revision 5.11SP1

d. ThreadX the high-performance embedded kernel User Guide Revision 5.8

e. X-Ware IoT Platform SC Security Guidance 2018-08-22

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

TOE Configuration

The following configuration was used for testing:

```
TOE reference:
TOE name: X-Ware IoT Platform SC
TOE version: 5.11
X-Ware IoT Platform SC consists of the following items:
ThreadX version 5.8 with Service Pack 2 (SP2)
NetX Duo version 5.11
NetX Secure TLS version 5.11 with Service Pack 1(SP1)
MQTT version 5.11
```

Environmental Configuration

The following network diagram describes the scenario used to perform testing: