Certification Report

Version 2.0

1 February 2019

CSA_CC_17001

for

NetCrypt Family Series S20/R100/U1000/U2000 Version 2.6.4

From

ST Electronics (Info-Security) Pte Ltd

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorising Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	29 June 2018	Released
2.0	1 February 2019	Covered under CCRA

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the NetCrypt Family Series S20/R100/U1000/U2000, Version 2.6.4. It is a hardware IP Encryptor and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

- NetCrypt S20
- NetCrypt R100
- NetCrypt U1000
- NetCrypt U2000
- TOE preparative and operative guidance (NETCRYPT FAMILY SERIES S20/R100/U1000/U2000 Administrator's Guide, Version 1.0.0 are provided in PDF format in CD delivered with TOE)

The Family of TOE consists of portable (NetCrypt S20) and rack mounted (NetCrypt R100/U1000/U2000) hardware IP Encryptor that enables the user to leverage on public Ethernet/IP infrastructure to form a secure VPN between itself and a peer TOE. It employs AES algorithm for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as Internet Key Exchange (IKE) protocols for keys derivations and authentications. All models provide the same security functionalities. The evaluated configuration is a gateway-to-gateway configuration with only local management.

The evaluation of the TOE has been carried out by An Security Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL2 and completed on 25 June 2018. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The Security Target [1] is the basis for this certification. It is not based on a certified Protection Profile.

The Security Assurance Requirements (SARs) are based entirely on the assurance components defined in Part 3 of the Common Criteria [2]. The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2.

The Security Functional Requirements (SFRs) relevant for the TOE are outlined in chapter 6.2 of the Security Target [1]. The Security Target claims conformance to CC Part 2 extended [3].

The SFRs are implemented by the following TOE Security Functionality:

TOE Security Functionality	
Security Audit	The TOE is able to generate audit records of security-relevant events occurring on the TOE. Generated audit records include date and time stamp, event message. The TOE

	provides administrators with the ability to retrieve and view audit records stored within the TOE, where they are protected from unauthorised modification and deletion. The TOE has limited audit records storage capacity and it can only store up to a maximum of 10,000 audit records, where the oldest audit records are then overwritten by new audit records.
Cryptographic Support	The TOE implements cryptographic algorithms that provide key management, data encryption and decryption, RSA signature generation and verification, secure hashing and key-hashing features in support of higher level cryptographic protocols, including IKEv2 for keys derivations and authentications, and IPSec (ESP only) to provide confidentiality and integrity protections to data traffic.
Identification and Authentication	The TOE requires administrators to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers a locally connected management interface (network port) for interactive administrative sessions. The TOE supports the local administration with 2-factor authentication (2FA) using an external cryptographic token (KeyCrypt).
Security Management	TOE's security management functions are accessed using the TOE management application (NetCrypt Administrative Management software) via the Management port. An administrator may connect a workstation to the management port of the TOE and authenticate to it. Closing of the management software will terminate the interactive session. Access control of TOE's security management functions relies on assigned role for each user account. The TOE has a built-in RS232 console port which provides limited management functions.

Protection of TOE	The TOE implements self-test (Cryptographic) is performed during initial startup to ensure its cryptographic functions are operating properly. The self-test may also be triggered by an authorised Administrator manually.
Protection of User Data	User data sent from the trusted network segment within one TOE to the other TOE's trusted network segments is protected with confidentiality and integrity protections. The protection of user data is in accordance to the security policy defined within the TOE.
Trusted Channels	The TOE provides secure IPSec communication channel between TOE and another peer TOE after successful device-to-device authentication through IKEv2 protocol.

Table 1: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1].

This Certification covers the configurations of the TOE as outlined in chapter 5.3 of the report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [4] [3] [2];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (http://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **28 June 2023**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is:

NetCrypt Family Series S20/R100/U1000/U2000 Version 2.6.4.

The following table identifies the TOE deliverables:

Type	Name	Version	Form of Delivery
HW	NetCrypt S20 pre-installed with firmware version 2.6.4	HW Model 9910-8000-0723	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
HW	NetCrypt R100 pre-installed with firmware version 2.6.4	HW Model 9910-8000-1190	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
HW	NetCrypt U1000 pre-installed with firmware version 2.6.4	HW Model 9910-8000-0733	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
HW	NetCrypt U2000 pre-installed with firmware version 2.6.4	HW Model 9910-8000-1281	In-house courier for local delivery within Singapore. Trusted courier delivery for overseas delivery
SW	NETCRYPT FAMILY SERIES S20/R100/U1000/U2000 Administrator's Guide	Version 1.0.0	PDF format stored within CD to be delivered together with TOE

Table 2: Deliverables of the TOE

The guide for receipt and acceptance of the above mentioned TOE are described in chapter 2 of the Administrative Guidance [9].

Additional identification information relevant to this Certification procedure as follows:

TOE	NetCrypt Family Series S20/R100/U1000/U2000 Version 2.6.4
Security Target	NetCrypt Family Series S20/R100/U1000/U2000 Security Target V1.0 Issue A, 19 June 2018
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Assurance Level/cPP	EAL 2
Developer	ST Electronics (Info-Security) Pte. Ltd
Sponsor	ST Electronics (Info-Security) Pte. Ltd
Evaluation Facility	An Security Pte. Ltd
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA_CC_17001
Certificate Validity	**29 June 2018** till **28 June 2023**

Table 3: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the selected set of SFRs and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- User Data Protection
- Protection of the TSF
- Trusted Channels

Specific details concerning the above mentioned security policies can be found in chapter 6 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Usage Assumptions	Description
OE.TRUSTED_ADMIN	The administrators are trusted, well trained and follow all administrator guidance.

Table 4: Usage Assumptions

Environmental Assumptions	Description
OE.KEYCRYPT	The administrator uses a cryptographic token conforming to: • JavaCard System Standard 2.2 Configuration Protection Profile, Version 1.0b EAL4+ • Secure Signature Creation Device Protection Profile Type 2 v1.04 EAL4+ • Secure Signature Creation Device Protection Profile Type 3 v1.05 EAL4+
OE.TIME_STAMP	The environment shall provide a reliable time stamp to the TOE.
OE.PHYSICAL_ENV	The physical environment of the provisioning and deployment site shall prevent unauthorised physical and logical access to the TOE.
OE.PEER_TOE	The administrator shall only configure the TOE to communicate with another peer TOE.

Table 5: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to those claims made in the Security Target [1].

5.3 Evaluated Configuration

The evaluated configuration is a gateway-to-gateway configuration with only local management and an external cryptographic token (KeyCrypt) used for 2-factor authentication.

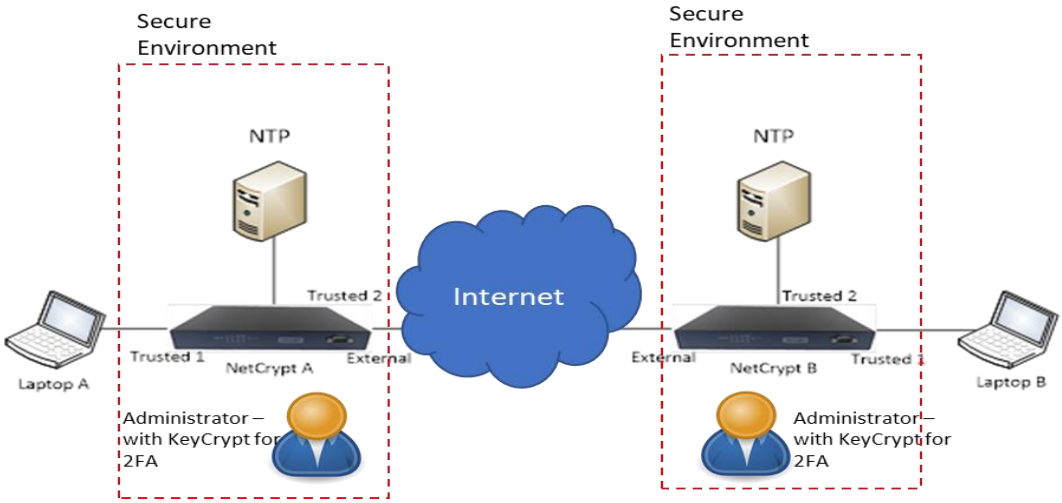

Figure 1: Evaluated configuration

5.4 Non-Evaluated Functionalities

Potential users of the TOE are advised that some functional and services have not been evaluated as part of the evaluation. Potential users of the TOE shall carefully consider their requirements for using functions and services outside of the evaluated configuration.

These non-evaluated functionalities include:

- Random number generation. While testing and assessment were done on the entropy, no assurance claims were made.
- Secure channel between NetCrypt administrative software and the TOE. The potential user shall ensure the provisioning and deployment of the TOE is done in a physically secure premise. More information is available in section 4.2 of the Security Target [1].
- Remote management of the TOE over public network (i.e. via the black segment). The potential users are to adhere to the administrative guidance to manage the TOE via the management port and within the trusted network.
- Anti-physical tampering mechanism.

5.5 Non-TOE components

The TOE requires additional components (i.e. hardware/software/firmware) for its operation. These non-TOE components include:

- NetCrypt Administrative Management software
- PKCS#11 Compliant USB Cryptographic token.

More information is available in section 1.3.1 of the Security Target [1].

6 Architecture Design Information

The general architecture consists of 8 subsystems.

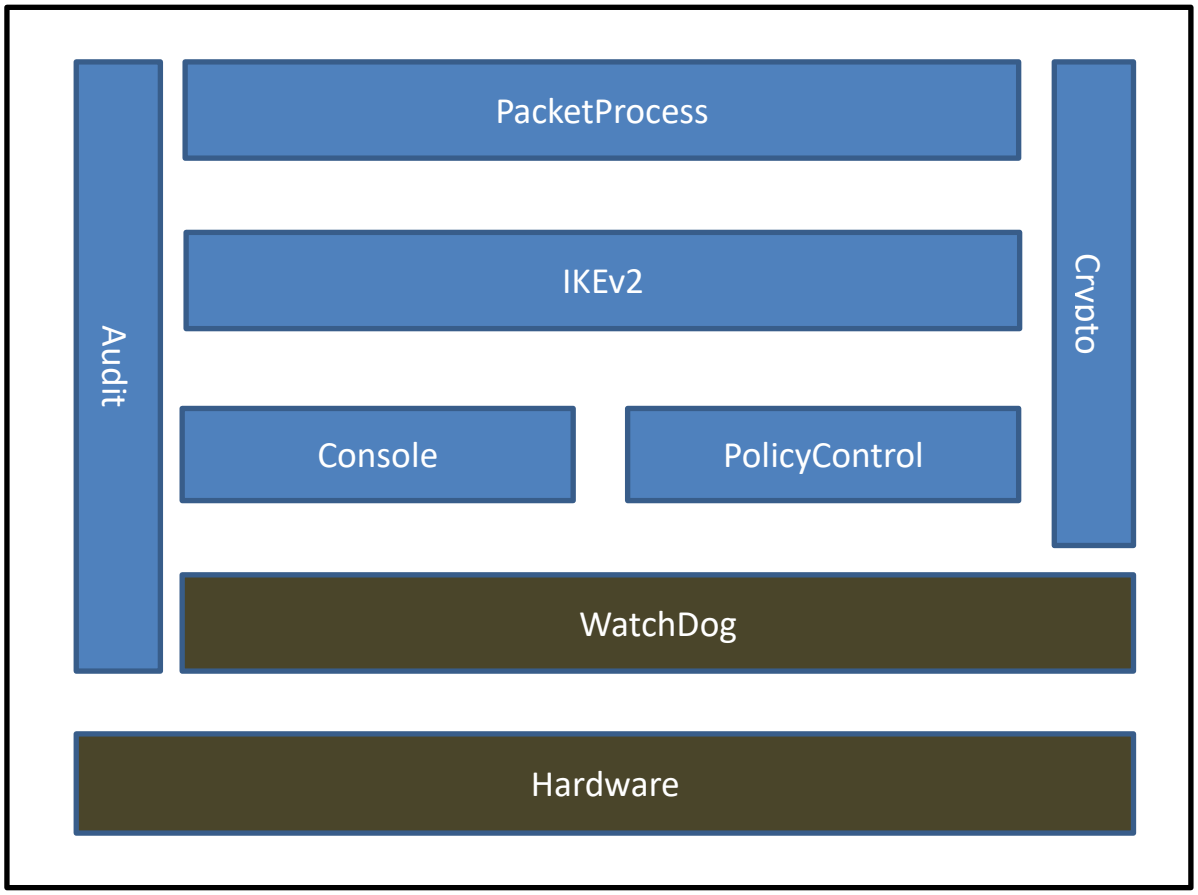

Figure 2: Subsystems of TOE

Subsystem	Description
Watchdog	Performs loading of kernel modules, retrieval of encryption key, perform self-test and launches other processes such as PacketProcess, PolicyControl and Console. (SFR-supporting)
Hardware	Provides the memory and flash storage operations, LEDs indication, rebooting of TOE and reading of network information. (SFR-supporting)
PacketProcess	Controls all packets flow between the trusted and untrusted network segment and performing both

	confidentiality and integrity protection in term of IPSec. It also enforces a set of firewall rule on the untrusted network segment. (SFR-Enforcing)
PolicyControl	Performs security configurations and settings. It compiles the security policies and stores them securely. (SFR-Enforcing subsystem)
IKEv2	Performs the Internet Key Exchange (IKE) protocol to negotiate for a known IPSec session key between 2 TOE devices in a secure manner, using algorithms and key sizes specified in the security policy. (SFR-Enforcing)
Console	The Console subsystem provides limited functions such as factory reset, network interface information through the RS232 interface. (SFR-Enforcing)
Crypto	Provides cryptographic functions specified in the security policy. (SFR-Enforcing)
Audit	The Audit subsystem provides the means for events to be logged. Events such as for the followings are logged: Key Exchanges messages System messages Error messages Audit subsystem will be getting time from either backend or frontend if NTP is used. Backend is through the secure gateway, while front end from its internal trusted network segment. (SFR-Enforcing)

Table 6: Subsystems of TOE

7 Documentation

The evaluated documentation is listed in Table 2: Deliverables of the TOE and is being provided with the product to the customer. These documentation contains the required information for secure usage of the TOE in accordance with the Security Target. The documentation is shipped securely together with the TOE.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer performed testing only with the S20 model as the differences between the hardware platforms are only related to the provided hardware environment that has no impact on the security of the TOE.

8.1.2 Test Configuration

The network diagram describes the base setup used for both developer's and evaluator's testing. Some tests required additional network components (e.g. sniffers etc).

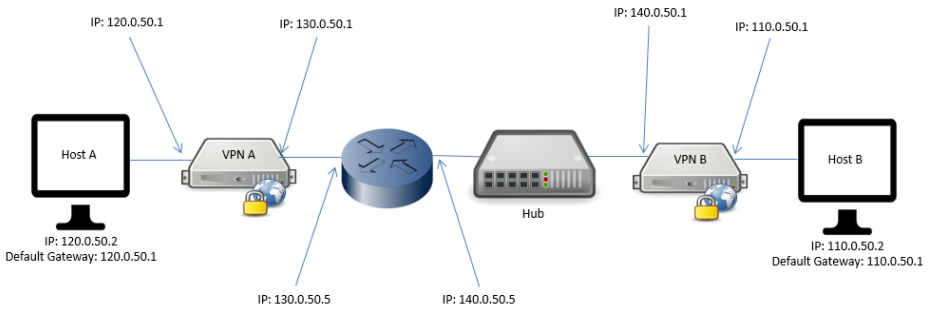

Figure 3: Developer's test DEV1 setup

The TOE used for testing is configured according the chapter 5, 6 and 7 of NetCrypt Series Administrator's Guide [9] for gateway-to-gateway setup.

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluator analysed the developer's test coverage, test plans and procedures, expected and actual test results.

The evaluator repeated all of the developer tests at the CCTL premise and verified the accuracy of the developer's test results.

With input from the Certification Body, the evaluator further devised additional tests cases for the TOE:

- Verification of the correct implementation of AES-256-CBC
- Verification of the correct implementation of SHA-256

- Verification of the correct implementation of HMAC-SHA256
- Verification of the correct implementation of RSA signature generation
- Verification of the secure values for p, q and d of RSA algorithm modulus 2048
- Verification of the quality of random number generated by TOE
- Verification of the TOE's External Port to only accept IKEv2 packets
- Verification of TOE's console port ability to handle erroneous input while maintaining secure state

8.2.2 Test Configuration

The same test configuration as described in section 8.1.2.

8.2.3 Test Results

All of the developer's test were verified by the evaluator to conform to the expected results from the test plan.

The evaluator's additional test cases identified that the RSA algorithm was not implemented based on standard implementation. The values of p, q and d of the RSA algorithm were not chosen securely. Consequently, the firmware was re-engineered. The revised firmware (i.e. v2.6.4) was re-tested and produced satisfactory results.

8.3 Penetration Testing (AVA_VAN)

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the TOE and to demonstrate that the vulnerabilities were not exploitable in the intended environment of the TOE.

The general approach for the vulnerability analysis is based on the following:

- Public domain vulnerability analysis of the TOE specific vulnerability (both hardware and software);
- Public domain vulnerability analysis of the TOE-type vulnerabilities (i.e. vulnerabilities that are generic for VPN gateway) and a scanning tool was used to identify generic potential vulnerabilities.
- Analysis of the TOE deliverables (ARC, TDS, FSP, AGD etc).

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.2) treating the resistance of the TOE to an attack with the Basic attack potential.

The evaluator then devised attack scenarios where potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. Thereafter the evaluator analysed the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential Basic was actually successful.

The evaluator found no exploitable vulnerability in the TOE when operated in

the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available, the user of the TOE should request the sponsor to provide a re-certification. In the meantime, a risk assessment should be conducted to

1) determine the suitability of deploying uncertified updates and patches; or
2) to retain usage of the existing certified version and take additional measures in order to maintain system security.

In addition, the potential user should note the functionalities listed in section 5.4 that are not evaluated and determine that these exclusions are acceptable for his/her usage.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Testing Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IKE	Internet Key Exchange
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] ST Electronics (Info-Security), "NetCrypt Family Series S20/R100/U1000/U2000 Security Target, Version 1.0," ST Electronics (Info-Security), Singapore, 2018.

[2] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2017-04-003], Version 3.1 Revision 5," 2017.

[3] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Numnber CCMB-2017-04-002], Version 3.1 Revision 5," 2017.

[4] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model [Document Number CCMB-2017-04-001], Version 3.1 Revision 5," 2017.

[5] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5," 2017.

[6] Cyber Security Agency of Singapore (CSA), "SCCS Publication 1 - Overview of SCCS, Version 5.0," 2018.

[7] Cyber Security Agency of Singapore (CSA), "SCCS Publication 2 - Requirements for CCTL, Version 5.0," 2018.

[8] Cyber Security Agency of Singapore (CSA), "SCCS Publication 3 - Evaluation and Certification, Version 5.0," 2018.

[9] ST Electronics (Info-Security), "NetCrypt series (S20/U1000/U2000/R100) Administrator's Guide, Version 1.0.0," 2018.

[10] Common Criteria Recognition Arrangement Management Committee, "Operating Procedures - Conducting Shadow Certifications [Document number 2004-07-01]," 2017.

----------End of Report ----------