



Certificate Report

Version 1.0

08 October 2026

CSA_CC_23005

For

NetCrypt Family Series S20/R100/U1000/U2000

From

ST Engineering Info-Security Pte Ltd

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing 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 information 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 for Certification Report

Version	Date	Changes
1.0	08 October 2026	Released

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, a hardware Internet Protocol (IP) encryptor, and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version			
Model Name	NetCrypt S20	NetCrypt R100	NetCrypt U1000	NetCrypt U2000
Part Number	9910-8000-0723	9910-8000-1190	9910-8000-0733	9910-8000-1281
PCBA Version	S20-110-A30	R100-320-B10	U1000-570-A30	U2000-570-A30
Firmware	2.7.2			

Table 1: TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

Name	Version	Method of Delivery
Netcrypt Series (S20/U1000/U2000/R100) Administrator's Guide,	2.0.3	Local delivery: ST Engineering delivery team Overseas delivery: Trusted courier

Table 2: List of guidance documents

The TOE is a hardware Internet Protocol (IP) encryptor. The TOE operates with a peer TOE to establish an IPsec tunnel. In turn, a trusted channel is established between the TOE and peer TOE.

The TOE consists of the following models shown below.

Model	Diagram
NetCrypt S20	
NetCrypt R100	
NetCrypt U1000	
NetCrypt U2000	

Table 3: NetCrypt Family Series S20/R100/U1000/U2000

The TOE consists of the following logical scope:

- Security Audit
- Cryptographic Support
- Protection of TSF
- Trusted Channel

The evaluation of the TOE has been carried out by Setsco-An Security Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL 2 and completed on 30 September 2026.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
<u>Security Audit</u> The TOE generates audit logs of security relevant events associated with the trusted channel.
<u>Cryptographic Support</u> The TOE implements cryptographic operations that supports the establishment of trusted channel.
<u>Protection of TSF</u> The TOE implements self-tests mechanism that preserves the TOE's secure state when a malfunction is detected.
<u>Trusted Channel</u> The TOE establishes trusted channel with a peer TOE to protect user data that is transported over the channel.

Table 4: 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 this 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.

Table of Contents

1	CERTIFICATION	9
1.1	PROCEDURE.....	9
1.2	RECOGNITION AGREEMENTS.....	9
2	VALIDITY OF THE CERTIFICATION RESULT	10
3	IDENTIFICATION	11
4	SECURITY POLICY	13
5	ASSUMPTIONS AND SCOPE OF EVALUATION.....	13
5.1	ASSUMPTIONS	13
5.2	CLARIFICATION OF SCOPE.....	14
5.3	EVALUATED CONFIGURATION.....	14
5.4	NON-EVALUATED FUNCTIONALITIES	14
5.5	NON-TOE COMPONENTS	15
6	ARCHITECTURE DESIGN INFORMATION.....	16
7	DOCUMENTATION	17
8	IT PRODUCT TESTING	17
8.1	DEVELOPER TESTING (ATE_FUN).....	17
8.1.1	<i>Test Approach and Depth.....</i>	<i>17</i>
8.1.2	<i>Test Configuration</i>	<i>17</i>
8.1.3	<i>Test Results</i>	<i>17</i>
8.2	EVALUATOR TESTING (ATE_IND).....	17
8.2.1	<i>Test Approach and Depth.....</i>	<i>17</i>
8.2.2	<i>Test Configuration</i>	<i>18</i>
8.2.3	<i>Test Results</i>	<i>18</i>
8.3	PENETRATION TESTING (AVA_VAN).....	18
8.3.1	<i>Test Approach and Depth.....</i>	<i>18</i>
9	RESULTS OF THE EVALUATION	20
10	OBLIGATIONS AND RECOMMENDATIONS FOR THE USAGE OF THE TOE	20
11	ACRONYMS.....	21
12	BIBLIOGRAPHY	22

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 [2] [3] [4];
- 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. Hence, the certification for this TOE is fully covered by the CCRA.

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 (<https://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 **07 October 2031**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 CCC SP-101-3 Publication 3 [8]. Potential users should check the SCCS website (<https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/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.

The following table identifies the TOE deliverables.

Identifier	Version			
Model Name	NetCrypt S20	NetCrypt R100	NetCrypt U1000	NetCrypt U2000
Part Number	9910-8000-0723	9910-8000-1190	9910-8000-0733	9910-8000-1281
PCBA Version	S20-110-A30	R100-320-B10	U1000-570-A30	U2000-570-A30
Firmware	2.7.2			

Table 5: TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE is described in the set of guidance documents.

Name	Version	Method of Delivery
Netcrypt Series (S20/U1000/U2000/R100) Administrator's Guide,	2.0.3	Local delivery: ST Engineering delivery team Overseas delivery: Trusted courier

Table 6: Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	NetCrypt Family Series S20/R100/U1000/U2000
Security Target	NetCrypt Family Series S20/R100/U1000/U2000 Security Target Version 2.0 Issue A
Developer	ST Engineering Info-Security Pte. Ltd.
Address of Developer	100 Jurong East Street 21 Singapore 609602
Sponsor	ST Engineering Info-Security Pte. Ltd.
Address of Sponsor	100 Jurong East Street 21 Singapore 609602
Evaluation Facility	Setsco-An Security Pte Ltd
Completion Date of Evaluation	30 September 2026
Evaluation Authority	Cyber Security Agency of Singapore (CSA)
Address of Evaluation Authority	Punggol Way Tower 92 #09-164 Singapore 829854
Certificate ID	CSA_CC_23005
Certificate Validity	5 years from date of issuance

Table 7: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

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

- Security Audit
- Cryptographic Support
- Protection of TSF
- Trusted Channel

Specific details concerning the above mentioned security policy can be found in Chapter 5 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:

Environmental Assumptions	Description
OE.TRUSTED_ADMIN	The TOE users are trusted and well-trained; this includes adhering to guidance documentations.
OE.PHYSICAL_ENV	The TOE user shall deploy the TOE in a physically secure environment.
OE.KEYCRYPT	The administrator shall ensure a cryptographic token will be used to store 2FA authentication keys.
OE.TIME_STAMP	The TOE user shall ensure that the operational environment provides a reliable time stamp to the TOE.
OE.IT_ENVIRONMENT	The TOE user shall ensure that the IT equipments supporting the operational of the TOE are always set up and used in a secure environment and kept up to date.

Table 8: 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 the claims made in the Security Target [1].

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

5.3 Evaluated Configuration

The TOE is a hardware Internet Protocol (IP) encryptor. The TOE operates with a peer TOE to establish an IPsec tunnel. In turn, a trusted channel is established between the TOE and peer TOE. Figure 1 below illustrates the evaluated configuration.

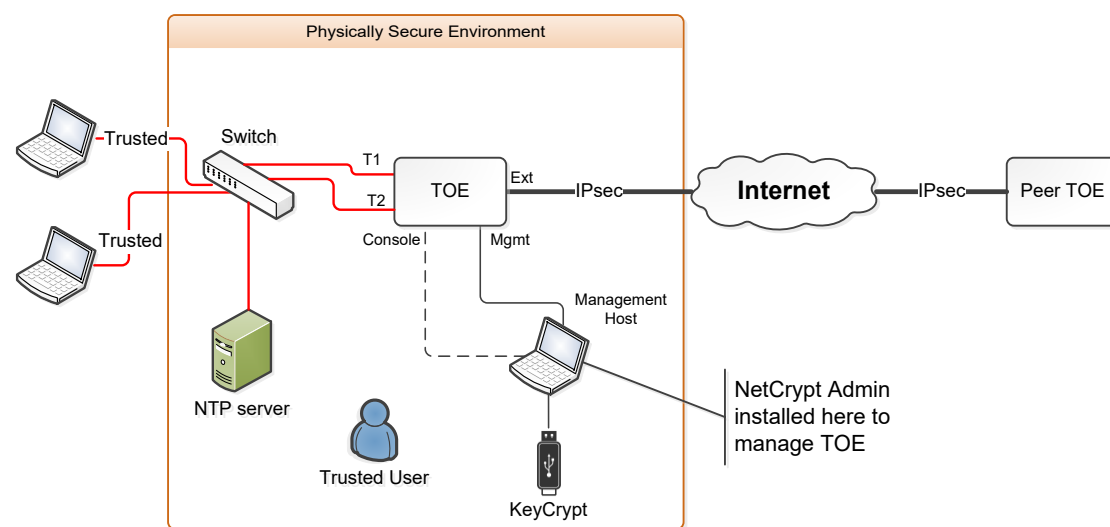


Figure 1: Evaluated Configuration

5.4 Non-Evaluated Functionalities

Users are advised that some functions and services have not been evaluated as part of the evaluation as clarified in section 5.2. Users should carefully consider their requirements for using functions and services outside of the evaluated configuration.

5.5 Non-TOE Components

The TOE is a hardware-based Internet Protocol (IP) encryptor whose operation depends on additional hardware and software components that are outside the scope of this evaluation:

Non-TOE Components	Purpose
NetCrypt Administrative Management software (NetCrypt Admin)	This is a software application that runs on a host machine. The host machine connects to the TOE via the TOE's Management Port. A TOE user uses this software application to access the TOE security management functions. For a TOE user to access the TOE security management functions, the TOE user must insert his/her KeyCrypt into the host machine. KeyCrypt shall then identify and authenticate the TOE user. Upon successful identification and authentication, the TOE user shall gain access to the TOE's security management functions. This is part of the TOE deliverables.
KeyCrypt	This is a USB token that a TOE user uses as part of a 2-Factor Authentication (2FA) process to access the TOE's security management functions. This is to be purchased separately by the user. This is part of the TOE deliverables.
Cryptographic Token Personalization tool	Software application to personalize KeyCrypt. This is part of KeyCrypt deliverables.
Peer TOE	The TOE communicates with a peer TOE to establish an IPsec tunnel, in turn, establishing a trusted channel.
NTP server	The NTP server provides reliable timestamp to the TOE for audit generation purpose.

Table 9: Non-TOE Components

6 Architecture Design Information

The following describes each subsystem:

Subsystem	Description
PacketProcess	- Enforces information flow between Trusted and Ext interfaces based on configured security policies. - Applies Red-Black tagging to Ethernet from coming from the Ext and Trusted interface. This ensures that packets that are encrypted through IPSEC or GTK are only allowed to go through the Ext to the untrusted network. - Forwards UDP 4500/500 packets only. Otherwise, the packets are dropped. - Rejects malformed packets.
IKEv2	- Identifies and authenticates peer TOE prior to establishing IPsec. - Perform key exchange with Peer TOE.
Watchdog	Enforces kernel security policies /dev/mem and /dev/kmem are read-only - disallow load or unload of kernel modules - disallow performing of raw I/O operations - disallow performing network administrative tasks - disallow setuid on files Reseeds PRNG (Crypto subsystem) - Every 10 minutes - When random data is retrieved from random pool.
PolicyControl	- The PolicyControl is designed as a server listening on the TCP port 50001 which is the default port for security configurations and settings through NetCrypt Admin. - Identify and authenticate administrators
Console	Provides limited functions such as factory reset, network interface information.
Crypto	The Crypto subsystem (consists of 2 parts in user and kernel space) provides cryptographic functions such as: - Asymmetric data encryption, decryption - RSA Digital Signature and verification - Symmetric data encryption, decryption - Message digest

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
Hardware	• Covers the memory and flash storage operations of Main Board, Daughter Board which performs HRNG and seedings to PRNG, LEDs indication, anti-tampering mechanism and TOE housing.

Table 10: Subsystem description

7 Documentation

The evaluated documentation as listed in

Name	Version	Method of Delivery
Netcrypt Series (S20/U1000/U2000/R100) Administrator's Guide,	2.0.3	Local delivery: ST Engineering delivery team Overseas delivery: Trusted courier

Table 6: Guidance Document (part of TOE deliverables)

is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer has performed extensive tests to validate the correctness of the TSF at both the TOE's TSFI-level and all SFRs claimed in the Security Target [1] are tested.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [10].

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

Based on Figure 1, the evaluator can identify 1 TSFIs i.e. Ext. This TSFI is exposed to threats from threat agents; other interfaces are made inaccessible by OE.TRUSTED_ADMIN and OE.PHYSICAL_ENV. To ensure the TSF adequately protects the user data, the TSFI implementation must achieve the following general objectives:

1. the implementation of IKEv2 and IPsec MUST be correct.
2. the implementation MUST be non-bypassable.

The evaluator strives to gain assurance in item 1 while item 2 shall be further analysed in AVA. Table 11 shows the analysis of devising a test subset.

Analysis	Test subset to be devised.
Based on analysis of ADV_FSP, the evaluator observed that the correct cryptographic implementation of IKEv2 and IPsec is crucial to protecting the confidentiality and integrity of user data transported between the TOE user and TOE.	The evaluator shall augment a test subset to verify the correctness of the implemented IKEv2 and IPsec cryptographic algorithms.

Table 11: Devising test subset

8.2.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [10].

8.2.3 Test Results

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

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN) treating the resistance of the TOE to an attack with the BASIC attack potential. i.e., amongst other that the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment.

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he first 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. He analysed then the results of these tests with the aim of determining whether at least one of the attack scenarios with the attack potential BASIC was successful.

The evaluator conducted a vulnerability search using public sources of information like the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD). The following keywords were used during the search:

- ST Engineering. This is the developer's name.
- NetCrypt. This is the TOE product name.
- IPsec and IKEv2. This is implemented in the TOE.
- VPN. This is the common term used for such TOE type.
- Internet Protocol (IP) encryptor. This is the TOE type.

However, these vulnerabilities are not applicable to the TOE.

As analysed in AVA, the evaluator identified the following as a potential vulnerability:

- VUL.1: Bypassing/tampering of PacketProcess and IKEv2 subsystem via Ext.

Based on the identified vulnerabilities, the evaluator reviewed the self-protection measures enforced by OE.TRUSTED_ADMIN and OE.PHYSICAL_ENV. Solely based on the ADV, the evaluator assessed that the risk of bypassing the TOE security functionality (TSF) is low.

The evaluator devised the following attack scenarios to validate the non-bypassability of PacketProcess Subsystem.

Penetration Test	Description
AS.1	Bypassing/tampering of PacketProcess and IKEv2 subsystem via Ext.
AS.2	Perform buffer overflow attack on Ext.

Table 12: Penetration Test Case

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: List of guidance documents 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 are 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.

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

The evaluators provided the additional recommendations and comments:

- The TOE can only work with another peer TOE and is not interoperable with other encryptors that employ IPSEC.
- Based on the evaluation configuration, remote management is not assessed.

No additional recommendation was provided by the Evaluation Authority.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test 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
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

- [1] ST Engineering, "NetCrypt Family Series S20/R100/U1000/U2000 Security Target version 2.0 Issue A", ST Engineering, Singapore, 2026.
- [2] 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.
- [3] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5," 2017.
- [4] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5," 2017.
- [5] Common Criteria Maintenance Board (CCMB), "Common Methodology 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 7.2," 2024.
- [7] Cyber Security Agency of Singapore (CSA), "SCCS Publication 2 - Requirements for CCTL, Version 7.2," 2024.
- [8] Cyber Security Agency of Singapore (CSA), "SCCS Publication 3 - Evaluation and Certification, Version 7.2," 2024.
- [9] ST Engineering, "NetCrypt Family Series S20/R100/U1000/U2000 Administrator's guidance version 2.0.3 Issue B", ST Engineering, Singapore, 2024.
- [10] ST Engineering Info-Security Pte. Ltd., " ETR CC EAL2 NetCrypt Family Series Version 2.0", 30 Sep 2026

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