TÜVNORD

Certificate

The certification body of TÜV NORD CERT GmbH
hereby awards this certificate to the company

Certificate validity:
2025-01-10 – 2027-01-10

RedTea Mobile Pte. Ltd.
29 Media Circle, #02-14/1
Singapore (138565), Singapore

to confirm that its IT product

RedteaSIM OS – nuSIM_App_nRF9120, V1.0.9.0

fulfils all requirements of the criteria

Security Qualification (SQ)
Version 10.0
Security Assurance Level SEAL-4

of TÜV NORD CERT GmbH. The requirements are summarized in the appendix to the
certificate.

The appendix is part of the certificate with the ID 6150.25 and consists of 4 pages.

Essen, 2025-01-10

Zertifizierungsstelle der TÜV NORD CERT GmbH

To Certificate

TÜV ®

Appendix to the certificate
with the ID: 6150.25
page 1 of 5

Certification scheme

The certification body of TÜV NORD CERT GmbH performs its certifications based on the following certification scheme:

- German document: „Zertifizierungssystem für IT-Zertifikate (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV NORD CERT GmbH", D503-CP-001, Rev. 00/09.24, TÜV NORD CERT GmbH

Evaluation report

- German document: "Evaluierungsbericht – Sicherheitstechnische Qualifizierung, RedteaSIM OS - nuSIM_App_nRF9120, V1.0.9.0", 2.0 as of 2025-01-06, TÜV Informationstechnik GmbH

Evaluation requirements

- "Trusted Site Security / Trusted Product Security, Security Qualification (SQ) Requirements Catalog for version 10.0", documentation version 2.9 as of 2022-11-11, TÜV Informationstechnik GmbH

- Product-specific security requirements (see below)

The evaluation requirements are summarized at the end.

Evaluation target

Evaluation target is the "RedteaSIM OS - nuSIM_App_nRF9120, V1.0.9.0" of RedTea Mobile Pte. Ltd.. It is detailed in the evaluation report.

Evaluation result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-4 are fulfilled.

- The product-specific security requirements are fulfilled.

- All requirements described in the operating manual have to be fully and correctly implemented.

The recommendations of the evaluation report have to be regarded.

Appendix to the certificate
with the ID: 6150.25
page 2 of 5

Product-specific security requirements

The following product-specific security requirements are the basis of the certification and have been checked:

1. **Time Boxed Evaluation**

The evaluation follows a time-boxed approach comprising a eight (8) week testing phase.

2. **Secure Storage of AKA-Keys and OPC Values**

The nuSIM maintains the integrity and confidentiality of keys for authentication and key agreement (AKA-keys) and Operator Variant Algorithm Configuration (OPC) values. AKA-keys and OPCs are protected against attacks such as logical, physical and side-channel attacks.

3. **Integrity of Network Configuration Settings and Code**

The nuSIM protects the integrity of network configuration settings. Any executable nuSIM code is integrity protected, too.

4. ~~Secure Profile Re-Provisioning (optional)~~

~~The nuSIM provides means for profile re-provisioning. The re-provisioning maintains the integrity and confidentiality of AKA-Keys and OPCs as well as the integrity of network configuration settings.~~

5. ~~Secure Firmware Update (optional)~~

~~The nuSIM provides means to update the firmware, maintaining integrity and confidentiality of all code and data. The firmware update process can only be completed by the nuSIM vendor and provides rollback protection.~~

6. **Monotonic Behaviour of Sequence Numbers (SQN)**

The nuSIM provides means to ensure monotonic increasing behaviour of SQNs that are used during authentication and key agreement.

Appendix to the certificate
with the ID: 6150.25
page 3 of 5

Summary of the evaluation requirements for the Security Qualification (SQ), version 10.0

1   Technical Security Requirements (as of SEAL-1)

The technical security requirements must be documented, consistent and verifiable. The specification must be made in accordance with ISO / IEC 17007. In addition, technical security requirements must be derived in the framework of an individual threat and risk analysis, they must be derived from previously defined protection profiles, or they must conform to published security requirements of recognized authorities or bodies of IT security. Furthermore, they must be appropriate to the intended use of the IT product and meet applicable security demands.

2   Architecture and Design (as of SEAL-3)

The IT product must be structured reasonably and understandable. Its complexity must not have any impact on security. It must not contain any conceptual vulnerability that allows bypassing or disabling security-relevant components. The hardening and protection measures must be adequate and effective.

3   Development Process (as of SEAL-3)

Development of the IT product must follow a defined development life cycle taking into account at least the phases of planning, analysis, design, implementation, testing, deployment and maintenance. The maintenance phase of the development life cycle must consider and eliminate vulnerabilities that allow bypassing or disabling security-relevant components. As part of the testing phase of the development life cycle tests with respect to security functionality of the IT product must be considered.

4   Operating Instructions (as of SEAL-4)

The documentation consisting of security requirements for the operating environment of the product, manuals for installation and administration as well as manuals for the end user must be clearly understandable and comprehensible. The documentation must be known to authorized person and always be readily accessible.

5   Vulnerability Assessment and Penetration Testing (as of SEAL-2)

The security measures of the IT product must withstand penetration testing. It must not be possible to break or circumvent security measures. The IT product must be configured securely, must meet all of the defined technical security requirements and must not have any exploitable vulnerability.

Appendix to the certificate
with the ID: 6150.25
page 4 of 5

6 Source Code Analysis (as of SEAL-4)

The source code must not contain vulnerabilities, errors or inconsistencies, such as e. g. undocumented commands, parameters and test functions.

7 Change Management (as of SEAL-5)

Patch management must be completely documented and suitable for the IT product. The procedure for amendments of the IT product must be clearly defined and appropriate for the IT product. Persons involved must be familiar with it and responsibilities must be clearly defined. Amendments of the IT product must not lead to a reduction of the security level achieved.

Appendix to the certificate
with the ID: 6150.25
page 5 of 5

Security Assurance Level

The following table shows the applicable evaluation criteria for the security assurance level. A certificate can be issued for IT products having successfully passed the evaluation and reaching an overall level of at least SEAL-3.

		Security Assurance Level				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluation criteria	Technical Security Requirements	X	X	X	X	X
	Architecture and Design			X	X	X
	Development Process			X	X	X
	Operating Instructions				X	X
	Vulnerability Assessment and Penetration Testing		X	X	X	X
	Source Code Analyse				X	X
	Change Management					X

Table: Evaluation criteria and Security Assurance Level of IT product