Certificate

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

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

to confirm that its nuSIM Product

## RedteaSIM OS v1.2.8 - nuSIM v1.1.2.8

fulfils all requirements of the criteria

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

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

The appendix is part of the certificate and consists of 6 pages.

The certificate is valid only in conjunction with the evaluation report.

Security TÜViT® 2022 Trusted Product

Certificate ID: 6143.22

© TÜViT – TÜV NORD GROUP – www.tuvit.de

24

Certificate validity:
2022-09-12 – 2024-09-12

Essen, 2022-09-12

Dr. Christoph Sutter
Head of Certification Body

**TÜV Informationstechnik GmbH**
TÜV NORD GROUP
Am TÜV 1
45307 Essen, Germany
www.tuvit.de

TO CERTIFICATE

## Certification Scheme

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following certification scheme:

- German document: “Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

## Evaluation Report

- “Evaluation Report Security Qualification Trusted Product Security Evaluation Scheme RedteaSIM OS v1.2.8 - nuSIM v1.1.2.8”, report version 2 as of 2022-09-12, TÜV Informationstechnik GmbH

## Evaluation Requirements

- “Trusted Site Security / Trusted Product Security, Security Qualification (SQ), Requirements Catalog for version 10.0”, documentation version 2.8 as of 2020-03-16, TÜV Informationstechnik GmbH
- product-specific security requirements (see below); optional requirements that are printed in grey are not part of the certification

The evaluation requirements are summarized at the end.

## Evaluation Target

The target of evaluation is the nuSIM product “RedteaSIM OS v1.2.8 - nuSIM v1.1.2.8” 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 including optional requirements 4 and 6 are fulfilled.

The recommendations of the evaluation report have to be regarded.

## Product-specific security requirements

The following product-specific security requirements are based on the document “nuSIM SECURITY EVALUATION CONCEPT, version 6 as of 2021-01-25.

### 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) (optional)

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

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

### 1 Technical Security Requirements

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

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

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

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.

## 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.

## Security Assurance Level

The following table shows the applicable 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<br>Evaluation Criteria | SEAL-1 | SEAL-2 | SEAL-3 | SEAL-4 | SEAL-5 |
|---|---|---|---|---|---|
| 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 products