

Zertifikat

Die Zertifizierungsstelle der TÜV NORD CERT GmbH
bescheinigt hiermit dem Unternehmen

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

für das IT-Produkt

RedteaSIM OS - nuSIM_App_nRF9120, V1.0.9.0

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)
Version 10.0
Security Assurance Level SEAL-4

der TÜV NORD CERT GmbH. Die Anforderungen sind in der Anlage zum Zertifikat
zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats mit der ID 6150.25 und besteht aus 4 Seiten.

Essen, 10.01.2025

Zertifizierungsstelle der TÜV NORD CERT GmbH



Zertifikatsgültigkeit:
10.01.2025 – 10.01.2027



Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV NORD CERT GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „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

Evaluierungsbericht

- „Evaluierungsbericht – Sicherheitstechnische Qualifizierung, RedteaSIM OS - nuSIM_App_nRF9120, V1.0.9.0“, 2.0 vom 06.01.2025, TÜV Informationstechnik GmbH

Evaluierungsanforderungen

- „Trusted Site Security / Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ) Anforderungskatalog der Version 10.0“, Dokumentationsversion 2.9 vom 11.11.2022, TÜV Informationstechnik GmbH
- Produktspezifische Sicherheitsanforderungen (siehe unten)

Die Evaluierungsanforderungen sind am Ende zusammenfassend aufgeführt.

Zertifizierungsgegenstand

Zertifizierungsgegenstand ist „RedteaSIM OS - nuSIM_App_nRF9120, V1.0.9.0“ der RedTea Mobile Pte. Ltd.. Dieser wird im Evaluierungsbericht detailliert beschrieben.

Evaluierungsergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-4 sind erfüllt.
- Die produktspezifischen Sicherheitsanforderungen sind erfüllt.
- Alle im Betriebshandbuch beschriebenen Anforderungen müssen vollständig und korrekt umgesetzt werden.

Die im Evaluierungsbericht genannten Empfehlungen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

Die folgenden produktspezifischen Sicherheitsanforderungen lagen der Zertifizierung zugrunde und wurden überprüft:

1. Zeitlich begrenzte Evaluation

Die Evaluation ist zeitlich begrenzt und umfasst eine achtwöchige Testphase.

2. Sichere Speicherung von AKA-Schlüsseln und OPC-Werten

Die nuSIM stellt die Integrität und Vertraulichkeit von Schlüsseln zur Authentifizierung und zum Schlüsselaustausch (AKA-Schlüssel) sowie von OPC-Werten (Operator Variant Algorithm Configuration) sicher. AKA-Schlüssel und OPC-Werte sind gegen logische, physikalische und Seitenkanalangriffe geschützt.

3. Integrität von Netzwerkkonfigurationseinstellungen und ausführbarem Code

Die nuSIM schützt die Integrität von Netzwerkkonfigurations-einstellungen sowie die Integrität von ausführbarem Code.

4. ~~Sichere erneute Profilbereitstellung (optional)~~

~~Die nuSIM implementiert Maßnahmen zur erneuten Profilbereitstellung (Re-Provisioning). Die erneute Profilbereitstellung stellt die Integrität und Vertraulichkeit von AKA-Schlüsseln und OPC-Werten als auch die Integrität von Netzwerkkonfigurationsdaten sicher.~~

5. ~~Sichere Firmwareaktualisierung (optional)~~

~~Die nuSIM ermöglicht eine Aktualisierung der Firmware. Hierbei wird die Integrität und Vertraulichkeit von ausführbarem Code und Daten sichergestellt. Der Firmwareupdateprozess kann nur vom nuSIM-Hersteller ausgeführt werden. Rückspielen von älteren Firmwareständen wird verhindert.~~

6. Monotones Verhalten von Sequenznummern (SQN)

Die nuSIM implementiert Maßnahmen, um ein monoton steigendes Verhalten von Sequenznummern (SQNs) sicherzustellen, die für die Authentisierung und den Schlüsselaustausch verwendet werden.

Zusammenfassung der Evaluierungsanforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 10.0

1 Technische Sicherheitsanforderungen (ab SEAL-1)

Die technischen Sicherheitsanforderungen müssen dokumentiert, widerspruchsfrei und überprüfbar sein. Die Spezifikation muss in Anlehnung an ISO/IEC 17007 erfolgen. Des Weiteren müssen die technischen Sicherheitsanforderungen im Rahmen einer individuellen Bedrohungs- und Risikoanalyse hergeleitet sein, sie müssen aus bereits definierten Schutzprofilen hergeleitet sein, oder sie müssen konform zu veröffentlichten Sicherheitsanforderungen anerkannter Autoritäten oder Gremien der IT-Sicherheit sein. Weiterhin müssen sie für den Einsatzzweck des IT-Produkts angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Architektur und Design (ab SEAL-3)

Das IT-Produkt muss sinnvoll und verständlich strukturiert sein. Seine Komplexität darf keinen Einfluss auf die Sicherheit haben. Es darf keine konzeptionellen Schwachstellen enthalten, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können. Die Härtungs- und Schutzmaßnahmen müssen angemessen und wirkungsvoll sein.

3 Entwicklungsprozess (ab SEAL-3)

Die Entwicklung des IT-Produkts muss im Rahmen eines definierten Development Life Cycle erfolgen, der mindestens die Phasen Planung, Analyse, Design, Implementierung, Test, Deployment und Maintenance berücksichtigt. Die Maintenance Phase des Development Life Cycle muss Schwachstellen berücksichtigen und beseitigen, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können. Im Rahmen der Test Phase des Development Life Cycles müssen Tests bezogen auf die Sicherheitsfunktionalität des IT-Produkts berücksichtigt werden.

4 Betriebsvorgaben (ab SEAL-4)

Die Dokumentation bestehend aus den sicherheitsrelevanten Vorgaben an die Betriebsumgebung des IT-Produkts, den Handbüchern zur Installation und Administration sowie den Handbüchern für die Endbenutzer muss gut verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

5 Schwachstellenanalyse und Penetrationstests (ab SEAL-2)

Die Sicherheitsmaßnahmen des IT-Produkts müssen einer Überprüfung durch Penetrationstests standhalten. Es darf nicht möglich sein, Sicherheitsmaßnahmen zu brechen oder zu umgehen. Das IT-Produkt muss sicher konfiguriert sein, muss alle definierten technischen Sicherheitsanforderungen erfüllen und darf keine ausnutzbaren Schwachstellen haben.

6 Sourcecode-Analyse (ab SEAL-4)

Der Sourcecode darf keine Verwundbarkeiten, Fehler oder Inkonsistenzen enthalten, wie beispielsweise undokumentierte Befehle, Parameter oder Testfunktionen.

7 Änderungsmanagement (ab SEAL-5)

Das Patch-Management muss lückenlos dokumentiert und für das IT-Produkt geeignet sein. Das Vorgehen bei Änderungen am IT-Produkt muss klar definiert und geeignet sein. Die beteiligten Personen müssen damit vertraut und Verantwortlichkeiten müssen eindeutig geregelt sein. Änderungen an dem IT-Produkt dürfen nicht zu einer Reduzierung des erreichten Sicherheitsniveaus führen.

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Evaluierungskriterien. Ein Zertifikat kann erteilt werden, wenn ein IT-Produkt die Evaluierung erfolgreich durchlaufen und mindestens den Level SEAL-3 erreicht hat.

		Security Assurance Level				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluierungskriterien	Technische Sicherheitsanforderungen	X	X	X	X	X
	Architektur und Design			X	X	X
	Entwicklungsprozess			X	X	X
	Betriebsvorgaben				X	X
	Schwachstellenanalyse und Penetrationstests		X	X	X	X
	Sourcecode-Analyse				X	X
	Änderungsmanagement					X

Tabelle: Evaluierungskriterien und Security Assurance Level für IT-Produkte