Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

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

für das nuSIM Produkt

RedteaSIM OS v1.2.8 - nuSIM v1.1.2.8

die Erfüllung aller Anforderungen der Kriterien

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

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

Die Anlage ist Bestandteil des Zertifikats und besteht aus 6 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Security TÜViT® 2022 Trusted Product

Certificate ID: 6143.22

Zertifikatsgültigkeit:
12.09.2022 – 12.09.2024

Essen, 12.09.2022

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

ZUM ZERTIFIKAT

Zertifizierungsprogramm

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

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Prüfbericht

- Englisches Dokument: „Evaluation Report Security Qualification Trusted Product Security Evaluation Scheme, RedteaSIM OS v1.2.8 - nuSIM v1.1.2.8“, Berichtsversion 2 vom 12.09.2022, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Trusted Site Security / Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ)“, Anforderungskatalog für die Version 10.0, Dokumentationsversion 2.8 vom 16.03.2020, TÜV Informationstechnik GmbH
- Produktspezifische Sicherheitsanforderungen (siehe unten); ausgegraute, optionale Anforderungen sind nicht Bestandteil der Zertifizierung

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist das nuSIM Produkt „RedteaSIM OS v1.2.8 - nuSIM v1.1.2.8“ der RedTea Mobile Pte. Ltd. Dieser ist im Prüfbericht detailliert beschrieben.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-4 sind erfüllt.
- Die produktspezifischen Sicherheitsanforderungen einschließlich der optionalen Anforderungen 4 und 6 sind erfüllt.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

Die folgenden produktspezifischen Sicherheitsanforderungen basieren auf dem Dokument "nuSIM SECURITY EVALUATION CONCEPT“, Version 6 vom 25.01.2021.

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 Netzwerkkonfigurationseinstellungen 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. Rückeinspielen von älteren Firmwareständen wird verhindert.

6 Monotones Verhalten von Sequenznummern (SQN) (optional)

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

Zusammenfassung der Anforderungen 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 Prüfkriterien. Ein Zertifikat kann erteilt werden, wenn ein IT-Produkt die Prüfung erfolgreich durchlaufen und mindestens den Level SEAL-3 erreicht hat.

Security Assurance Level / Prüfkriterien	SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Technische Sicherheits-anforderungen	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: Prüfkriterien und Security Assurance Level für IT-Produkte