Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

CoCoNet Computer-Communication Networks GmbH
Parsevalstraße 9 b
40468 Düsseldorf

für das Softwareprodukt

MULTIVERSA Token für Smartphones, Version 2.0.4

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ), Version 10.0
Security Assurance Level SEAL-3

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.
Die Anlage ist Bestandteil des Zertifikats und besteht aus 7 Seiten.
Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Security TÜViT® 2021 Trusted Product

Certificate ID: 6142.21

Zertifikatsgültigkeit:
26.07.2021 – 26.07.2023

Essen, 26.07.2021

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

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

- „Prüfbericht Sicherheitstechnische Qualifizierung, MULTIVERSA Token für Smartphones, Version 2.0.4“, Berichtsversion 1.4 vom 23.07.2021, 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)

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist das Softwareprodukt „MULTIVERSA Token für Smartphones“, Version 2.0.4 der CoCoNet Computer-Communication Networks GmbH. Dieser ist im Prüfbericht detailliert beschrieben.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheits-technische Qualifizierung nach Security Assurance Level SEAL-3 sind erfüllt.
- Die produktspezifischen Sicherheitsanforderungen sind erfüllt.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

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

1 Datenspeicherung

Die schützenswerten Daten (kryptographisches Schlüssel-material, Passwörter, Konfigurationsdaten) werden nach Best-Practices der iOS/Android-Plattformen verwaltet. Die schützenswerten Daten werden mittels iOS-Keychain bzw. Android-Keystore verschlüsselt und lokal gespeichert.

2 Kryptographie

Die Verschlüsselung schützenswerter Daten basiert auf symmetrischer sowie asymmetrischer Kryptographie mit dynamisch ausgehandelten Schlüsseln. Die kryptographi-schen Verfahren verwenden aktuelle Algorithmen und Vorgehensweisen, die der EBICS-Spezifikation v2.5 ent-sprechen.

3 Authentifizierung

Der Prüfgegenstand dient als besitzbasiertes 2-Faktor-Authentifizierungsmerkmal. Vor jeder Nutzung muss sich der Nutzer erfolgreich authentifizieren.

Bei Inaktivität des Nutzers über einen festgelegten Zeitraum wird eine erneute erfolgreiche Authentifizierung durch den Nutzer erzwungen. Es ist ein Schutz vor exzessiven Authentifizierungsversuchen implementiert. Akzeptierte Passworte müssen in ihrer Komplexität der Richtlinie SP 800-63B (Appendix A) der NIST genügen.

4 Transportverschlüsselung

Die Transportverschlüsselung für die Kommunikation zum Backend genügt der EBICS-Spezifikation v2.5. Schützenswerte Daten (kryptographisches Schlüsselmaterial, Nutzerkennungen) werden nicht im Klartext übermittelt. Im Rahmen der TLS-Verbindung werden nur Serverzertifikate von vertrauenswürdigen Zertifizierungsstellen akzeptiert, die im Zertifikatsspeicher der zugrundeliegenden iOS/Android-Plattform als vertrauenswürdig hinterlegt sind. Die Serverzertifikate des Backends werden zusätzlich geprüft (Certificate Pinning oder Certificate Transparency), um den Server zu authentifizieren.

5 Verwendung von plattformspezifischen Schnittstellen

Gemäß Best-Practices der verwendeten iOS/Android-Plattformen werden alle eingehenden Daten validiert. Es werden nur Berechtigungen auf der iOS/Android-Plattform angefordert, die für die Ausführung von Funktionen zwingend erforderlich sind. Angebotene Funktionen werden durch das Berechtigungskonzept der iOS/Android-Plattformen vor unbefugten Zugriffen durch andere Prozesse geschützt.

6 Code Qualität und Build-Einstellungen

Die im öffentlichen App-Store der iOS/Android-Plattform provisionierten App ist mit einem gültigen Entwicklerzertifikat

signiert. Während des Kompilierungsvorgangs wird der Code obfuskiert. Im Binärcode sind keine Debugging Symbole enthalten. Treten in Sicherheitsfunktionen Fehler auf, werden diese nach Best-Practices der iOS/Android-Plattform behandelt. Es werden nach Best-Practices der iOS/Android-Plattform Sicherheitsfunktionen des Compilers und ein automatisches Speichermanagement genutzt.

7 Manipulationssicherheit

Es wird eine Gerätebindung mit dem Smartphone hergestellt. Es ist eine grundlegende Erkennung von nicht vertrauenswürdigen Umgebungen (Jailbreak/Root) vergleichbar zu den empfohlenen Best Practice Gegenmaßnahmen aus dem OWASP Mobile Security Testing Guide (MSTG-RESILIENCE-1) umgesetzt. Zudem werden grundlegende Gegenmaßnahmen implementiert, die die Verwendung eines Debuggers, vergleichbarer Werkzeuge und/oder eines Emulators verhindern (MSTG-RESILIENCE-2).

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