Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Vodafone GmbH
Ferdinand-Braun-Platz 1
40549 Düsseldorf

für das Produkt

Vodafone Secure SIM (VSS) – Secure Login, V1.0

die Erfüllung aller Anforderungen der Kriterien

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

der TÜV Informationstechnik GmbH. Die Prüfanforderungen 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 zugehörigen Prüfbericht bis zum 30.09.2015.

Security PQ6122.13 TÜViT® 2013 Trusted Product

Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-PQ6122.13

Essen, 09.09.2013

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

Zertifizierungssystem

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

- „Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜV Informationstechnik GmbH

Prüfbericht

- „Vodafone Secure SIM (VSS) – Secure Login“, V1.0, Berichtsversion 1.3 vom 02.09.2013, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, Version 10.0 vom 21.03.2011, TÜV Informationstechnik GmbH
- Produktspezifische Sicherheitsanforderungen (siehe unten)

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Der Prüfgegenstand „Vodafone Secure SIM (VSS) – Secure Login“, V1.0 der Vodafone GmbH besteht aus folgenden Komponenten:

- VSS Infrastrukturkomponenten, Release 1.0, welche als Kernsysteme im Rechenzentrum der Vodafone GmbH betrieben werden.

- Customer Administration Portal, Release 1.0, welches als WebAccess Portal auf Seiten eines Dienstleisters der Vodafone GmbH betrieben wird.
- SIM-Applet, Release 1.0, welches auf der SIM-Karte des Mobiltelefons des Kunden integriert ist.

Die VSS Infrastrukturkomponenten werden zentral im Rechenzentrum der Vodafone GmbH aufgestellt und betrieben. Das Customer Administration Portal wird in Abhängigkeit des Anwendungsszenarios zentral durch einen Dienstleister der Vodafone GmbH betrieben und durch den Kunden genutzt. Das SIM-Applet auf der SIM-Karte des Mobiletelefons wird durch Kunden der Vodafone GmbH genutzt.

Der Prüfgegenstand erlaubt den Kunden der Vodafone GmbH die Durchführung einer 2-Faktor-Authentisierung basierend auf Wissen (SIM-Applet PIN) und Besitz (SIM). Er umfasst die folgenden beiden Anwendungsszenarien:

- VPN-Gateway, 2-Faktor-Authentisierung mittels RADIUS am VPN-Authentisierungsserver des Kunden oder des Dienstleisters und
- Webportal, 2-Faktor-Authentisierung mittels SAML am WebAccess Portal des Kunden oder des Dienstleisters.

Die Komponenten VPN-Gateway und Webportal der Anwendungsszenarien unterliegen dem Verantwortungsbereichs des Kunden und sind nicht Teil des Prüfgegenstandes. Eine detaillierte Beschreibung des Prüfgegenstands ist im Prüfbericht enthalten.

Prüfergebnis

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

Die im Prüfbericht genannten Anmerkungen und Auflagen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

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

1 Identifizierung & Authentifizierung

Das IT-Produkt muss den Benutzer unter Berücksichtigung des SIM-Applets auf der SIM-Karte als Security Token eindeutig identifizieren und authentifizieren. Die Authentisierungsdaten der 2-Faktor-Authentisierung müssen hinreichend stark sein, um gängigen Angriffen ausreichend lange standzuhalten.

2 Zugriffskontrolle

Das IT-Produkt muss Funktionen bereitstellen, die es ermöglichen, Zugriffsrechte der Benutzer einzuschränken. Dies gilt insbesondere für die Mandantenfähigkeit des Customer Administration Portals im Rahmen der Anwendungsfälle: VPN-Authentisierungsserver / WebAccess Portal. Ein Kunde darf nicht auf Daten anderer Kunden zugreifen.

Einem Angreifer darf es mit vertretbarem Aufwand nicht möglich sein, sich unbefugt Rechte auf den zentralen VSS-

Serverkomponenten des IT-Produkts zu verschaffen. Die VSS-Serverkomponenten im dedizierten VSS-Netz im Rechenzentrum der Vodafone GmbH und der Dienstleister weisen keine bekannten ausnutzbaren Schwachstellen auf.

3 Transportverschlüsselung

Die Kommunikation über unsichere Netze (wie z. B. das Internet) muss über einen vertrauenswürdigen Kanal erfolgen, der die Vertraulichkeit der übertragenen Daten sicherstellt.

4 Datenflusskontrolle

Das IT-Produkt muss sicherstellen, dass extern nur betrieblich notwendige Verbindungen möglich sind. Dies gilt insbesondere für die Verbindungen zwischen

- den zentralen VSS-Serverkomponenten und den kundenseitigen VPN-Gateway/WebAccess-Portal,
- den zentralen VSS-Serverkomponenten und dem Customer Administration Portal,
- den zentralen VSS-Serverkomponenten und der IT-Infrastruktur als VSS-Umgebung und
- den zentralen VSS-Serverkomponenten und den Administratoren.

5 Logging

Sicherheitsrelevante Ereignisse werden durch Sicherheits-komponenten der IT-Infrastruktur protokolliert und fließen in ein Melde- und Alarmierungswesen ein.

TÜV®

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

1 Technische Sicherheitsanforderungen

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

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

Die Entwicklung des IT-Produkts muss im Rahmen eines definierten Development Life Cycles erfolgen, der mindestens die Phasen Planung, Analyse, Design, Implementierung, Test, Deployment und Maintenance berücksichtigt. Die Maintenance Phase des Development Life Cycles muss Schwachstellen berücksichtigen und beseitigen, mit deren

Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können. Im Rahmen der Testphase 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

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