Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

HID Global Corporation
611 Center Ridge Drive
Austin TX 78753, USA

für das IT-Produkt

Physical Access Control Credential, Seos, FW-Stände 1.1.27 & 1.1.28

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ), Version 10.0
Security Assurance Level SEAL-5

der TÜV Informationstechnik GmbH. Die Prüfanforderungen 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® 2020 Trusted Product

Certificate ID: 6139.20

Zertifikatsgültigkeit:
17.07.2020 – 17.07.2022

Essen, 17.07.2020

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

- Englisches Dokument: „Evaluation Report Security Qualification Trusted Product Security Evaluation Scheme, Physical Access Control Credential, Seos, FW-Stände 1.1.27 & 1.1.28“, Version 1, Revision B vom 13.07.2020, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Anforderungskatalog: Trusted Site Security / Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ) der 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 IT-Produkt „Physical Access Control Creditial, Seos, FW-Stände 1.1.27 & 1.1.28“ der HID Global Corporation. Dieses IT-Produkt ist ein Zugangskontrollausweis mit einem Sicherheitsbaustein (Secure Element) mit Seos Core Betriebssystem. Das Seos Core Betriebssystem erlaubt Lese-

und Schreibzugriffe auf Daten basierend auf starken Authentifizierungsalgorithmen. Das IT-Produkt ist für den Einbau in Zutrittskontrollsystemen bestimmt und im Prüfbericht detailliert beschrieben.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheits-technische Qualifizierung nach Security Assurance Level SEAL-5 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 Identifizierung & Authentifizierung

Das IT-Produkt muss den Benutzer eindeutig identifizieren und authentifizieren. Ferner muss sich das IT-Produkt gegenüber einem Benutzer eindeutig identifizieren und authentifizieren.

2 Vertrauenswürdiger Pfad

Zum Schutz der Integrität und der Vertraulichkeit von übertragenen Daten muss die Kommunikation zwischen dem authentifizierten IT-Produkt und dem authentifizierten Benutzer über einen vertrauenswürdigen Pfad hergestellt werden.

3 Zugriffskontrolle

Das IT-Produkt muss sicherstellen, die nur authentifizierte Benutzer, Daten in ihren Speicherbereichen lesen, verändern, hinzufügen oder entfernen können.

4 Generierung von Zufallszahlen

Das IT-Produkt muss die Generierung von Zufallszahlen unterstützen, die für die Verwendung in kryptographischen Algorithmen geeignet sind.

5 Resistenz gegen Angriffe

Das IT-Produkt muss resistent gegen bekannte Angriffe auf Smartcards sein. Hierzu zählt die Verwendung kryptographisch starker Algorithmen sowie Maßnahmen gegen physikalische und logische Angriffe.

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