Kurzgutachten

Zeitpunkt der Prüfung

01.08.2012 bis 28.02.2013

Adresse des Antragstellers

DIGITTRADE GmbH
Ernst-Thälmann-Str. 39
06179 Teutschenthal

Adresse der Sachverständigen

Rechtsanwalt Stephan Hansen-Oest
Neustadt 56
24939 Flensburg
E-Mail sh@hansen-oest.com

Dipl. Inf. (FH) Andreas Bethke
Papenbergallee 34
25548 Kellinghusen
E-Mail bethke@datenschutz-guetesiegel.sh

Kurzbezeichnung

DIGITTRADE – High Security HDD HS256S

Detaillierte Bezeichnung

Bei dem Produkt "High Security HDD HS256S" der Firma DIGITTRADE GmbH handelt es sich um eine externe Festplattenlösung mit 256-Bit Full Disk AES Hardwareverschlüsselung im CBC-Modus und Authentifizierung über eine Smartcard (nachfolgend „Karte“) und PIN.

Die auf der Festplatte gespeicherten Daten sind im Hinblick auf die Vertraulichkeit der Daten vor unbefugtem Zugriff geschützt, etwa wenn diese Festplatte gestohlen, verloren oder verlegt wird. Der Schutz erstreckt sich auch auf logische oder physikalische Angriffe. Hierfür sind folgende Sicherheitsmechanismen implementiert:

1. Eine Full-Disk-Hardwareverschlüsselung mittels 256-Bit AES im CBC-Modus,
2. eine 2-Faktor-Authentifizierung mittels Smartcard und PIN nach dem Prinzip „Besitzen und Wissen“,
3. die Verwaltung des Verschlüsselungsschlüssels (Erstellen, Ändern, Kopieren und Zerstören)

sowie eine externe Speicherung des Verschlüsselungsschlüssels. Bei diesen Schlüsseln handelt es sich um Zufallsschlüssel, die von den Karten selbst erzeugt werden.

Dieser Schlüssel liegt permanent auf der Karte. Von dort wird er nach dem Einlegen der Karte und der Verifizierung, ob die Karte für das Gerät zugelassen ist (Prüfung einer sog. „Match-ID“), und Eingabe der PIN temporär in den Festplattencontroller gelesen.

Wird die Karte aus dem Gerät entfernt, wird der temporäre Schlüssel im Controller automatisch gelöscht, es sei denn, dass dieser sog. Lock-Out-Modus deaktiviert wird.

Ein Schlüssel kann auf eine andere Karte kopiert werden und ein Schlüssel auf einer Karte kann mutwillig zerstört werden (womit diese Karte unbrauchbar ist, andere Karten mit demselben Schlüssel jedoch weiter verwendet werden können).

Es ist jedoch auch möglich den Schlüssel auf allen Karten „ungültig“ werden zu lassen, in dem für ein Gerät ein neuer Schlüssel erzeugt wird. Damit gehen sämtliche Daten auf der Festplatte verloren, da keine „Umschlüsselung“ stattfindet, sondern die Festplatte für den Gebrauch mit dem neuen Schlüssel initialisiert werden muss. Dies bedeutet, dass ein Schlüssel an ein Gerät gebunden wird. Die Funktion hierfür ist im Gerät implementiert und wird durch eine Tastenfolge gestartet. Nach einer Initialisierung wird die Festplatte als „neu“ erkannt und muss vom Betriebssystem formatiert werden.

Alle Sicherheitsfunktionen sind vollständig innerhalb der HS256S implementiert.

Im Detail bedeutet dies, dass alle Daten während der Übertragung von der bzw. auf die Festplatte in Echtzeit ver- und entschlüsselt werden.

Die Aufgabe der Verschlüsselung übernimmt dabei ein nach FIPS 197 zertifiziertes Kryptomodul, das zwischen der Schnittstelle zum PC und der Festplatte selbst sitzt. Festplatte und das Kryptomodul sind dabei in einem Gehäuse untergebracht. Die Schnittstelle zum PC ist über USB und FireWire realisiert.

Der benötigte Schlüssel wird auf einer Chipkarte erzeugt und dort verschlüsselt gespeichert. Der Chipkartenleser ist ebenfalls in das Gehäuse integriert.

Der Zugriff auf die Chipkarte oder auch Smartcard ist durch einen 8-stelligen numerischen Code (PIN) gesichert, der über eine integrierte Tastatur eingegeben wird. Die PIN ist dabei an die jeweilige Smartcard gekoppelt. Die HS256S erkennt durch die Match ID der Smartcard, ob sich auf der Smartcard ein für die Festplatte gültiger Schlüssel befindet. Der Hersteller unterscheidet zwischen zwei PINs: Der Smartcard-PIN und der Geräte-PIN.

Die **Smartcard-PIN** ist ein Authentifizierungsmerkmal, das der Benutzer benötigt, um zusammen mit der passenden Smartcard auf die Daten zugreifen zu können.

Mittels der Smartcard-PIN ist es möglich, den kryptografischen Schlüssel auf der Smartcard zu erstellen, zu ändern, zu kopieren und unauffällig in Gefahrensituationen zu zerstören.

Die **Geräte-PIN** ist ein Administrationsmerkmal, das keinen Zugriff auf die Daten erlaubt. Sie ermöglicht jedoch

- eine neue Smartcard auf der HS256S zu initialisieren und
- den Lock-Out Modus zu aktivieren / deaktivieren.

In Kombination mit der Smartcard-PIN ermöglicht sie den kryptografischen Schlüssel auf eine andere Smartcard zu kopieren

Das Gehäuse ist mittels DIGITTRADE-eigenem Aufkleber (Hologramm) versiegelt, so dass ein gewaltsames Öffnen und somit ein möglicher Manipulationsversuch leicht erkannt wird.

DIGITTRADE bietet seinen Kunden zwei mögliche Chipkarten an:
Zum einen die Smartcard „Oberthur Cosmo 64 v5.4 FIPS-140-2 Level 3” der französischen Firma Oberthur und zum anderen die Smartcard „NXP J3A081 Secure Smart Card Controller Rev. 3 (kurz JCOP v.2.4.1 R3)” der niederländischen Firma NXP Semiconductors mit DIGITTRADE HS256S Java Card Applet version 1.3 (vorinstalliert auf der Smartcard).

Standardmäßig wird die Oberthur Cosmo-Smartcard mit dem Produkt ausgeliefert. Diese ist 2007 durch das amerikanische NIST zertifiziert worden. Es kann aber auch ein Satz der NXP-Smartcard angefordert werden. Diese sind vom BSI unter der Nummer (BSI-DSZ-CC-0675-2011) nach EAL5 zertifiziert.

Der Unterschied für den Hersteller zwischen den Karten besteht in der Ansprache. Während die Karte von Oberthur bereits mit einem „fertigen“ Applet ausgeliefert wird, das der Hersteller unverändert nutzt, wird für die Karten von NXP ein eigenes Applet geschrieben, in dem die Funktionen zur Generierung der zufälligen Schlüssel (für die spätere AES-Verschlüsselung),

sowie die Funktionen zum Schreiben/Speichern und Lesen/Laden des Schlüssels auf und von der Karte angesprochen werden.

Das Produkt stellt dem Benutzer folgende Funktionen zur Verfügung:

- Anmelden an einer HS256S
- Verwaltung des kryptografischen Schlüssels mithilfe der Smartcard
  - Erstellen und Ändern eines kryptografischen Schlüssels
  - Zerstören eines kryptografischen Schlüssels
  - Ändern der Smartcard-PIN
- Geräte-PIN-Funktionen
  - Ändern der Geräte-PIN
  - Aktivieren/Deaktivieren des Lock-Out Modus
  - Kopieren von kryptografischen Schlüssels zwischen zwei Karten (nur zusammen mit der Smarcard-PIN)
  - Initialisieren einer neuen Smartcard

Der Prüfgegenstand umfasst folgende Komponenten:

- das Digittrade HS256S Java Card Applet Version 1.3 in Verbindung mit der Smartcard „NXP P5CD081 J3A081 JCOP v2.4.1 R3, BSI-DSZ-CC-0675-2011“ der Firma NXP Semiconductors,
- das ID-One Applet in Verbindung mit der Smartcard “Oberthur Cosmo 64 v5.4 FIPS-140-2 Level 3”,
- der integrierte Kartenleser,
- das Tastenfeld,
- der Controller,
- das Verschlüsselungsmodul,
- die Kommunikation zwischen Smartcard und Controller,
- das Host Interface (USB & Firewire) sowie
- der Datenspeicher (Protected Storage)

Da das Produkt mit unterschiedlichen Festplatten (SSD, HDD) in unterschiedlichen Größen angeboten wird, wurde die Funktionalität der oben genannten Komponenten exemplarisch mit einer Festplatte evaluiert.

Gleiches gilt für die Smartcards der Firmen Oberthur und NXP Semiconductor, die zur Evaluierungsumgebung gehören, aber nicht eigenständig zertifiziert wurden.

Die Kaufabwicklung auf der eigenen Webseite ist nicht Bestandteil des Prüfgegenstands.

Tools, die zur Herstellung des IT-Produktes verwendet wurden

Eclipse

JCOP tools von NXP (beinhaltet alle Entwicklungswerkzeuge für die Java Card™ Platform)

uberSVN (Versionsverwaltung)

Toshiba IDE

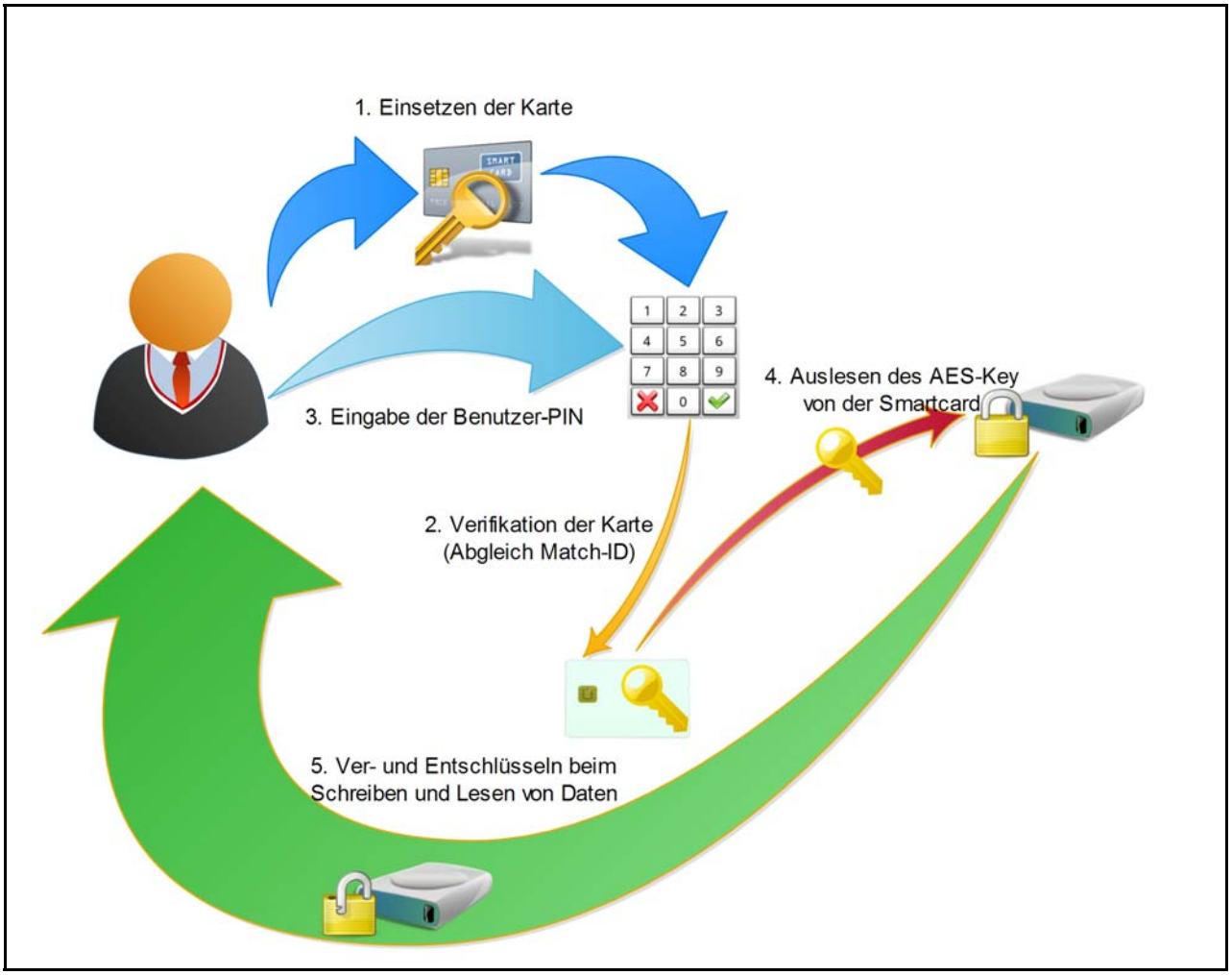
Zweck und Einsatzbereich

Zweck des Verfahrens ist die automatische Verschlüsselung von Daten (aller Art) zur Speicherung auf einer externen Festplatte. Der Hersteller hat keinen Einfluss auf die Art der Daten.

Da alle Daten, die auf der Festplatte gespeichert werden verschlüsselt werden, können auch Daten mit Personenbezug oder besonders schutzbedürftige Daten mit dem Produkt verarbeitet werden.

Das Verfahren ist damit grundsätzlich auch für den Einsatz bei öffentlichen Stellen des Landes Schleswig-Holstein geeignet.

Modellierung des Datenflusses



Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog Version 1.2

Zusammenfassung der Prüfungsergebnisse

Das Produkt ist für die Datenspeicherung und Datenverwaltung jeglicher Daten gedacht. Im Umgang mit dem Produkt ist die datenverarbeitende Stelle selbst verantwortlich für die Verarbeitung von persönlichen Daten und dem Zweck der Verarbeitung von Daten.

Jedoch werden Benutzer der DIGITTRADE High Security HS256S über relevante Fragen des Datenschutzes durch spezifische Hinweise zum Datenschutz in der Bedienungsanleitung informiert.

Der Hersteller hat auf dem Controller ein sog. zertifiziertes "Krypto-Modul" verbaut, das für die eigentliche Ver- und Entschlüsselung der Daten sorgt.

Die zum Einsatz kommenden Verschlüsselungsverfahren dienen dazu, den Schutz der auf dem Datenträger gespeicherten Daten vor der unbefugten Kenntnisnahme durch Dritte zu gewährleisten. Dabei kommen neben der reinen Verschlüsselung der Daten auf der Festplatte vor allem zusätzliche Komponenten, wie eine Smartcard mit PIN-Verfahren, zum Einsatz. Die Daten werden mittels AES-CBC Algorithmus mit einer Schlüssellänge von 256 Bit verschlüsselt. Um Zugriff auf die Daten zu bekommen, muss der Benutzer sowohl im Besitz der Festplatte, als

auch der Smartcard, als auch des 8-stelligen PINs sein, um Zugriff auf den AES-Schlüssel zu erhalten, der sich auf der Smartcard befindet.

Zwar können Daten mit Personenbezug auf der (mobilen) Festplatte gespeichert werden, jedoch sind diese verschlüsselt, so dass ein Zugriff auf die Daten selbst nur in Kombination mit dem Schlüssel und der PIN möglich ist. Spezielle Rechte/Rollen beim Zugriff auf die Daten gibt es durch das Produkt selbst nicht. Das Produkt ist jedoch mit Betriebssystemen nutzbar, die Rollen und Rechte vergeben.

Aus Sicht der Gutachter wurden durch die Kopplung einer bestimmten Smartcard an ein Gerät und die Eingabe des 8-stelligen PIN in Verbindung mit der endgültigen Vernichtung der Karte (und somit einer Sperrung des Zugriffs auf die Daten) bei mehrmaliger Falscheingabe angemessene Maßnahmen zur Identifizierung und Authentifizierung getroffen. Eine echte Passwortverwaltung ist jedoch nicht vorhanden.

Der Hersteller hat Funktionen in sein Produkt implementiert, die das sichere Löschen von Daten garantieren. Zum einen kann man auf Daten durch Zerstörung aller Smartcards nicht mehr auf die mit diesen Karten verschlüsselten Daten zugreifen. Eine Rekonstruktion ist (nach derzeitigem Stand der Technik) nicht durchführbar. Zum anderen können kryptografische Schlüssel geändert werden, die eine Löschung der Daten durch eine Initialisierung der Festplatte bedingt, falls man die der Smartcard zugeordnete Festplatte weiterhin benutzen möchte.

Nach Änderung des Schlüssels können alte Daten nicht wieder hergestellt werden. Dies kann auch dann nicht geschehen, wenn noch eine Smartcard mit einem alten Schlüssel existiert und die Festplatte für diesen Schlüssel wieder "benutzbar" gemacht wird, da dies immer mit eine Initialisierung der Festplatte einher geht.

Der Hersteller empfiehlt in seiner Anwenderdokumentation nach der Zerstörung der Schlüssel immer eine anschließende Formatierung der Festplatte mittels Betriebssystem, so dass auch weiterhin keine Daten rekonstruiert werden können.

Die Festplatte kann für jegliche IT-Anwendung verwendet werden, und somit können im Betrieb auch einzelne Datensätze, aber auch einzelne Daten gelöscht werden. Eine gesonderte Dokumentation durch das Produkt ist hierbei nicht vorgesehen.

Insgesamt entspricht das Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit in adäquater Art und Weise.

Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das Produkt verwendet Technologien zur Hardware-Verschlüsselung (AES 256 Bit, CBC-Modus) sowie eine Zwei-Faktor-Authentifizierung (Schlüssel auf der Smartcard und die Kenntnis der Smartcard-PIN). Dadurch wird sichergestellt, dass der Zugriff auf Daten durch unbefugte Personen auch bei Verlust oder Diebstahl des Gerätes nicht möglich ist.

Darüber hinaus gibt der Hersteller in seinem Handbuch umfangreiche Hinweise zum datenschutzkonformen Umgang mit dem Produkt.

Hiermit bestätige ich, dass das oben genannte IT-Verfahren den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Die ausführliche Analyse liegt bei.

Ort, Datum

Unterschriften der Sachverständigen