Version 1.8
08.10.2020

DIGITTRADE High Security

HS256 S3

external encrypted HDD/SSD

für Unternehmen und Behörden
for enterprise and government use

Benutzerhandbuch
User Manual

BITTE LESEN SIE DIE ANLEITUNG SORGFÄLTIG UND FOLGEN SIE DEN ANWEISUNGEN.

EINE FEHLERHAFTE BEDIENUNG KANN ZU SCHÄDEN AN DER DIGITTRADE HIGH SECURITY HS256 S3 (EXTERNE VERSCHLÜSSELTE HDD/SSD) SOWIE ZU DATENVERLUSTEN FÜHREN.

STELLEN SIE SICHER, DASS DIE VERSIEGELUNG UND DIE SICHERHEITSVERPACKUNG DES PRODUKTES NICHT BESCHÄDIGT WURDEN. ACHTEN SIE DABEI BESONDERS AUF DEN SICHERHEITSSCHRIFTZUG „DIGITTRADE SECURITY" AN DEN SEITEN DER SICHERHEITSVERPACKUNG (SIEHE KAPITEL 1.8).

Die digitale Fassung des Handbuchs kann auf www.digittrade.de im Download-Center heruntergeladen werden.

Produktversion:	DIGITTRADE High Security HS256 S3 (encrypted HDD/SSD) Version 1.0
Benutzerhandbuch Version:	1.8 (08.10.2020)

Inhaltsverzeichnis

1. Über die DIGITTRADE HS256 S3 **4**
1.1 Verschlüsselung 5
1.2 Zugriffskontrolle 5
1.3 Verwaltung der kryptografischen Schlüssel 6
1.4 Die Smartcard 6
1.5 Weitere Features 7
1.6 Die wichtigsten Eigenschaften im Überblick 7
1.7 Vorteile der DIGITTRADE HS256 S3 8
1.8 Sicherheitsverpackung und Versiegelungen 8

2. Eingabeoberfläche und USB-Anschluss **10**

3. Inbetriebnahme der HS256 S3 **11**
3.1 Einlegen der Smartcard 11
3.2 Eingabe der Smartcard-PIN 12
3.3 Ändern der Smartcard-PIN 13

4. Verwaltung der kryptografischen Schlüssel mit Hilfe der Smartcard-PIN **15**
4.1 Erstellen kryptografischer Schlüssel 15
4.2 Zerstören beider kryptografischer Schlüssel 16

5. Geräte-PIN-Funktionen **18**
5.1 Ändern der Geräte-PIN 18
5.2 Aktivieren/Deaktivieren des Lock-Out Modus (Geräte-PIN erforderlich) 19
5.3 Kopieren von kryptografischen Schlüsseln (Geräte-PIN erforderlich) 21
5.4 Initialisieren einer neuen Smartcard (Geräte-PIN erforderlich) 22

6. Initialisierung/Partitionierung und Formatierung unter Windows **23**

7. Initialisierung/Partitionierung und Formatierung unter MAC OS X **30**

8. Initialisierung/Partitionierung und Formatierung unter Linux **32**

9. Das richtige Dateisystem **35**

10. Anwendungsmöglichkeiten der HS256 S3 **36**

11. Technische Spezifikationen **41**

12. Fehlersuche **42**

13. Datensicherheit und Haftungsausschluss **44**

14. Datenschutzgerechter Umgang mit der HS256 S3 **44**

15. Sicheres Beenden nach Benutzung der HS256 S3 **46**

16. Aufbewahrung der Smartcard **47**

17. Lieferumfang **48**

18. Hinweis zum Schutz und Erhalt der Umwelt **48**

19. Schematische Funktionsübersicht **49**

1. Über die DIGITTRADE HS256 S3

Die externe Festplatte DIGITTRADE High Security HS256 S3 (externe verschlüsselte HDD/SSD) ermöglicht die datenschutzgerechte Speicherung und Aufbewahrung sowie den sicheren Transport der Geschäfts- und Privatdaten. Sie ist aufgrund ihrer Sicherheitsfunktionen eine der sichersten Möglichkeiten Daten mobil zu speichern.

Die auf der HS256 S3 gespeicherten Daten sind in Hinblick auf die Vertraulichkeit der Informationen vor unbefugten Zugriffen geschützt, etwa wenn die HS256 S3 verloren, verlegt oder entwendet wird sowie auch bei logischen oder physikalischen Angriffen auf diese.

Die DIGITTRADE HS256 S3 wird in einem komplett voreingestelltem Zustand geliefert und kann sofort verwendet werden. In der BSI-zertifizierten Konfiguration darf der Nutzer diese Festplatte jedoch erst in Betrieb nehmen, nachdem er zuvor die Smartcard PIN geändert, den Schlüssel auf der Smartcard selbst generiert und die Initialisierung der Smartcard durchgeführt hat.

Um die Sicherheitseigenschaften dieser Festplatte in vollem Umfang und innerhalb des Geltungsbereichs der BSI-Zertifizierung zu nutzen, sind zudem folgende Schritte erforderlich:

- Gewährleisten Sie, dass an Ihrem Host-System ein angemessener Schutz für alle aus dem geschützten Speicherbereich der DIGITTRADE HS256 S3 abgerufenen Daten besteht
- Sorgen Sie dafür, dass keine Malware auf die Festplatte übertragen werden kann
- Überprüfen Sie nach Erhalt der Festplatte die Sicherheitsverpackung (Kapitel 1.8)
- Überprüfen Sie den Umfang, die Vollständigkeit und die Richtigkeit der Lieferung (Kapitel 17)
- Überprüfen Sie nach der Erstanmeldung die Funktionen der Festplatte (Kapitel 3)
- Ändern Sie die Smartcard-PIN (Kapitel 3.3)
- Ändern Sie die Geräte-PIN (Kapitel 5.1)
- Erzeugen Sie zwei neue Kryptoschlüssel (Kapitel 4.1)
- Initialisieren Sie die Smartcard mit den neuen Kryptoschlüsseln auf die Festplatte und formatieren Sie diese anschließend im gewünschten Format (Kapitel 5.4, 6-9)
- Kopieren Sie die Kryptoschlüssel auf andere erhaltene Smartcards (Kapitel 5.3)
- Überprüfen Sie, ob die Anmeldung mit allen Smartcards möglich ist
- Vergewissern Sie sich fortlaufend, dass der Lock-Out Modus aktiviert ist (Kapitel 5.2)
- Für die wirksame Zerstörung eines Kryptoschlüssel ist das Löschen des Schlüssels auf allen Smartcards, die diesen speichern, notwendig. Alternativ dazu wird die Festplatte mit einem neuen Kryptoschlüssel vollständig überschrieben. (Kapitel 4.2)
- Behandeln Sie Ihre Authentifizierungsdaten vertraulich

- Der Verschlüsselungsschlüssel der Smartcard darf immer nur mit einer Festplatte verwendet werden

Eine ausführliche Beschreibung der oben genannten Schritte finden Sie in diesem Benutzerhandbuch in den entsprechenden Kapiteln.

Auf der Rückseite der Festplatte befinden sich der Typ, die Version sowie die Seriennummer der jeweiligen Festplatte. Da die Festplatte nicht updatefähig ist, sind diese Angaben für die Feststellung der Festplattenversion ausreichend.

Die DIGITTRADE HS256 S3 gewährleistet die Vertraulichkeit der Daten durch folgende Sicherheitsmechanismen:

- Verschlüsselung
- Zugriffskontrolle
- Verwaltung der kryptografischen Schlüssel

1.1 Verschlüsselung

- 256-Bit AES Full-Disk-Verschlüsselung im XTS-Modus

Das im Sicherheitsgehäuse integrierte Verschlüsselungsmodul führt eine komplette Verschlüsselung der Festplatte/SSD durch. Jedes gespeicherte Byte und jeder beschriebene Sektor auf der Festplatte/SSD werden nach 256-Bit AES (Advanced Encryption Standard) im XTS-Modus mittels zwei kryptografischer Schlüsseln mit jeweils 256-Bit verschlüsselt. Die DIGITTRADE HS256 S3 verschlüsselt außerdem temporäre Dateien und Bereiche, die von der Verschlüsselungssoftware oft unbeachtet bleiben.

1.2 Zugriffskontrolle

Die Zugriffskontrolle erfolgt nach dem Prinzip „Besitzen und Wissen":
Der Nutzer muss für den Zugriff auf die Daten eine passende Smartcard besitzen und die richtige 8-stellige Smartcard-PIN kennen.

Die Smartcard wird automatisch gesperrt und unbrauchbar, sobald die 8-stellige PIN acht Mal falsch eingegeben wurde. Die kryptografischen Schlüssel auf der Smartcard werden dabei unwiderruflich zerstört.

1.3 Verwaltung der kryptografischen Schlüssel

Mit Hilfe der Smartcard-PIN können die kryptografischen Schlüssel auf der Smartcard erstellt, geändert und zerstört werden (siehe Kapitel 4). Die Geräte-PIN ermöglicht die kryptografischen Schlüssel auf eine andere Smartcard zu kopieren, neue Smartcards auf der HS256 S3 zu initialisieren und den Lock-Out Modus zu verwalten. Hinweise dazu finden Sie in Kapitel 5.

Das Wissen über die Smartcard-PIN und die Geräte-PIN kann für bestimmte Anwendungsszenarien unter zwei Personen aufgeteilt werden, sodass eine Person nur die Smartcard-PIN und eine zweite Person nur die Geräte-PIN kennt. Besteht nur Kenntnis über die Geräte-PIN, ist kein Zugriff auf die Daten möglich.

Die beiden für die Ver- und Entschlüsselung notwenigen kryptografischen Schlüssel werden auf der Smartcard erstellt sowie verschlüsselt gespeichert. Damit besteht eine physische Trennung zwischen den verschlüsselten Daten und den kryptografischen Schlüsseln. Ein Auslesen dieser aus der DIGITTRADE HS256 S3 ist dadurch unmöglich.

Die kryptografischen Schlüssel werden nach korrekter Eingabe der Smartcard-PIN für die Ver- und Entschlüsselung der Daten an das Verschlüsselungsmodul der HS256 S3 übertragen. Es ergeben sich aus der externen Speicherung des Schlüsselpaares eine Vielzahl von Anwendungsmöglichkeiten, die in Kapitel 10 exemplarisch beschrieben werden.

1.4 Die Smartcard

Serienmäßig wird die Festplatte mit zwei Java-basierten und nach Common Criteria EAL5 zertifizierten Smartcards (NXP J2E081_M64 R3, CC EAL 5) ausgeliefert. Für die Benutzung gemäß BSI-Zertifizierung sind nur diese NXP Smartcards zugelassen. Sie werden in den folgenden Kapiteln als „die Smartcard“ bezeichnet.

Diese Smartcards ermöglichen das Erstellen, Kopieren, Ändern und Zerstören der kryptografischen Schlüssel. Die Schlüsselverwaltung erfolgt auf der Smartcard unabhängig von einem PC mit Unterstützung des DIGITTRADE HS256 S3 Applets.

Für die Anmeldung an der Festplatte verfügen beide Smartcards bei der Lieferung über die gleichen Krypto-Schlüssel. Die Smartcard-PIN kann für jede Smartcard unterschiedlich gewählt werden.

Auf der Vorderseite der Smartcard sind der Typ und die Seriennummer der jeweiligen Smartcard aufgetragen. Die Version der Festplatte HS256 S3 befindet sich auf der Rückseite.

Die zugelassenen Smartcards können bei DIGITTRADE zusätzlich bestellt werden. Diese werden ohne kryptografische Schlüssel ausgeliefert und besitzen die werkseitig voreingestellte PIN (siehe Kapitel 3.2). Zur Inbetriebnahme beachten Sie bitte die Kapitel 4.1, 5.3 und 5.4.

Warnung: *Wird eine ungültige oder defekte Smartcard in den zugehörigen Steckplatz eingesteckt, blinkt die „ERROR"-LED drei mal kurz und leuchtet dann dauerhaft rot. Sollte dieses Problem auftreten bzw. die Smartcard während der einzelnen Vorgänge sich ungewöhnlich verhalten oder Defekte aufzeigen, wenden Sie sich bitte an DIGITTRADE.*

1.5 Weitere Features

Dank des eingebauten Datenträgers im 2,5"-Format ist der mobile Datentresor klein und handlich. Die optionale Verwendung von SSD-Datenträgern bietet zusätzlichen Schutz vor Stößen und Erschütterungen. Die Datenübertragung und Stromversorgung erfolgt über den USB-Anschluss.

Die Hardwareverschlüsselung ermöglicht die Verwendung des Speichermediums unabhängig vom Anwenderbetriebssystem und geschieht transparent. Der Zugriff auf die Daten findet ohne Einschränkungen der Lese- und Schreibgeschwindigkeit statt.

1.6 Die wichtigsten Eigenschaften im Überblick

- 256-Bit AES-Full-Disk-Hardwareverschlüsselung im XTS-Modus mit zwei kryptografischen Schlüsseln
- 2-Faktor-Authentifizierung mittels Smartcard und 8-stelliger PIN
- externe Speicherung der kryptografischen Schlüssel
- Erstellen, Kopieren und Zerstören der kryptografischen Schlüssel durch den Nutzer
- hardwarebasiertes Verschlüsselungsmodul, Datenverschlüsselung aller gespeicherten Bytes und beschriebenen Sektoren
- bootfähig und unabhängig von Betriebssystemen (Unterstützung aller Betriebssysteme, Multimediageräte und Maschinen mit USB-Datenträger-Unterstützung)
- kompatibel mit USB 3.0 und USB 2.0
- keine Einschränkungen der Lese- und Schreibgeschwindigkeit
- handliches 2,5"- Format und robustes Metallgehäuse

1.7 Vorteile der DIGITTRADE HS256 S3

- Privat- und Geschäftsdaten sind sicher vor dem Zugriff Unbefugter geschützt
- einfache und sichere Handhabung durch Hardwareverschlüsselung: Anschließen, Anmelden, Verwenden
- alle Daten sind sofort verschlüsselt gespeichert
- keine Performanceverluste
- Integrationsmöglichkeit in bereits bestehende Smartcard-Infrastrukturen in Unternehmen

1.8 Sicherheitsverpackung und Versiegelungen

Um Manipulationen zu verhindern, wird für die Lieferung der Festplatte HS256 S3 und der Smartcards sowie für Nachlieferungen einzelner Smartcards eine spezielle Sicherheitsverpackung verwendet. Der Inhalt wird auf der Verpackung beschrieben.

Siegelverschluss

Bitte prüfen Sie nach Erhalt die Unversehrtheit des Sicherheitsschriftzugs „DIGITTRADE SECURITY" an den Seiten. Zusätzlich befindet sich am oberen Ende ein spezieller Siegelverschluss, der jegliche Manipulationsversuche anzeigt.

Mögliche Indikatoren sehen Sie in den folgenden Abbildungen:

So sieht der Siegelverschluss aus, wenn er korrekt verschlossen und nicht wieder geöffnet wurde. Der blaue Streifen unter dem oberen Bereich des Siegelverschluss und der blassgelbe Thermostreifen sind unbeschädigt.

Bei extremer Kälte (z.B. Einsatz von Kältespray) trennen sich Bereiche des blauen Verschlussbandes vom Trägermaterial. Die Warnung “STOP“ wird lesbar.

Durch starke Wärmeeinwirkung (z.B. durch Föhn) färbt sich der blassgelbe Thermostreifen rot.

Beim Einsatz von Lösungsmitteln löst sich die blaue Farbe des Siegelverschlusses auf. Die Manipulation ist sofort sichtbar.

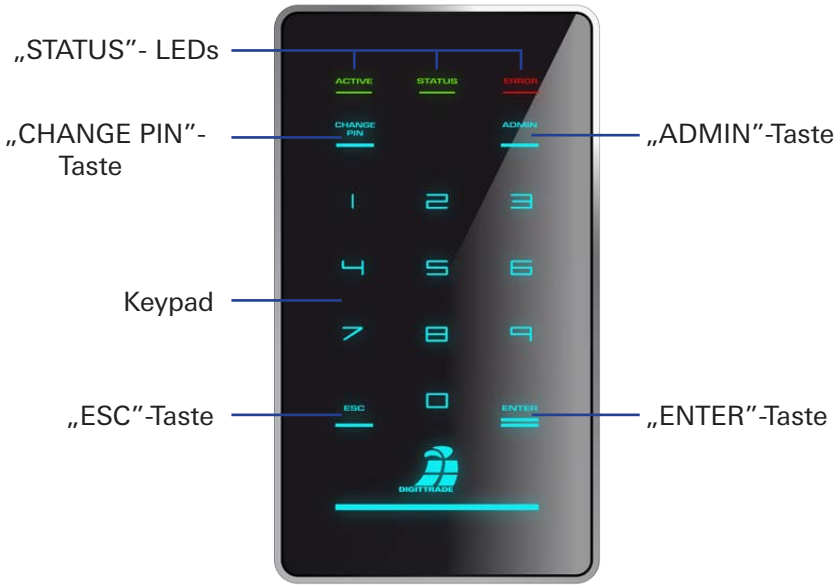
Stellen Sie nach Erhalt sicher, dass diese Idikatoren nicht ausgelöst wurden. Kontaktieren Sie Ihren Verkäufer, wenn Sie Manipulationen oder Beschädigungen an der Sicherheitsverpackung feststellen, da die Sicherheit der HS256 S3 in diesem Fall nicht gewährleistet werden kann.

Die Komponenten der HS256 S3 sind mit Epoxidharz versiegelt. Desweiteren ist an der Öffnungsstelle des Gehäuses der HS256 S3, wie unten abgebildet, ein Versiegelungsaufkleber angebracht. Diese Versiegelung wurde im Rahmen der BSI-Zertifizierung nicht bewertet.

Im Inneren der HS256 S3 befinden sich noch weitere Versiegelungsaufkleber.

2. Eingabeoberfläche und USB-Anschluss

Die DIGITTRADE HS256 S3 kann per USB-Schnittstelle mit dem Computer verbunden werden.



Die HS256 S3 hat drei Status-LEDs: „ACTIVE", „STATUS" und „ERROR".

Mögliche Farben:
„ACTIVE"-LED: leuchtet grün
„STATUS"-LED: leuchtet grün oder rot
„ERROR"-LED: leuchtet rot

Verbinden Sie die HS256 S3 mit Hilfe des mitgelieferten USB-Kabels mit Ihrem PC, Laptop oder einem anderen kompatiblen Gerät, das USB-Datenträger unterstützt.

Über den USB-Anschluss werden nicht nur die Daten übertragen, sondern auch die HS256 S3 mit Strom versorgt. Stellen Sie also sicher, dass die Festplatte immer direkt mit dem USB-Anschluss des PCs oder Laptops verbunden ist.

Hinweis: *Benutzen Sie die DIGITTRADE HS256 S3 nicht mit einem USB-Hub oder einem USB-Verlängerungskabel und gewährleisten Sie eine ausreichende Stromversorgung.*

3. Inbetriebnahme der HS256 S3

Die notwendige Stromversorgung der HS256 S3 erfolgt über den USB-Anschluss.

Nach dem korrekten Anschluss der DIGITTRADE HS256 S3 an den Computer leuchten zunächst die Status-LED „ACTIVE", „STATUS" und „ERROR" kurz gleichzeitig auf.

Danach ist Ihre DIGITTRADE HS256 S3 einsatzbereit, muss jedoch noch entsperrt werden. Halten Sie dazu eine der mitgelieferten Smartcards, sowie Ihre Smartcard-PIN bereit.

Hinweis: *Verwenden Sie aus Sicherheitsgründen nur Originalzubehör.*

3.1 Einlegen der Smartcard

Nachdem die DIGITTRADE HS256 S3 erfolgreich in Betrieb genommen wurde, muss sie noch für die Nutzung freigegeben werden.

Führen Sie dazu die Smartcard in den dafür vorgesehenen Smartcard-Steckplatz in Pfeilrichtung ein.

Wird eine ungültige oder defekte Smartcard in den zugehörigen Steckplatz eingesteckt, blinkt die „ERROR"-LED drei mal kurz und leuchtet dann dauerhaft rot. Wenden Sie sich in diesem Fall bitte an DIGITTRADE.

3.2 Eingabe der Smartcard-PIN

Nach der Inbetriebnahme und der erfolgreichen Erkennung einer gültigen Smartcard ist das Keypad der DIGITTRADE HS256 S3 beleuchtet und für die PIN-Eingabe bereit.

Jetzt kann die 8-stellige PIN eingegeben werden.

Die werkseitig voreingestellte PIN lautet: **1-2-3-4-5-6-7-8.**

Geben Sie diese über das Tastenfeld ein.

Bestätigen Sie die Eingabe mit „ENTER".

Hinweis: *Um die Sicherheit Ihrer Daten zu gewährleisten, ist es zwingend erforderlich, die voreingestellte Smartcard-PIN zu ändern (siehe Seite 14). Verändern Sie die Smartcard-PIN in regelmäßigen Abständen. Zusätzlich empfiehlt es sich, unterschiedliche PIN für die verschiedenen Smartcards zu verwenden. Die Smartcard-PIN muss vertraulich behandelt werden.*

Nach erfolgreicher Eingabe der Smartcard-PIN werden die kryptografischen Schlüssel von der Smartcard an das Verschlüsselungsmodul übertragen und die „STATUS"-LED leuchtet rot. Die DIGITTRADE HS256 S3 wird von Ihrem System als Wechseldatenträger erkannt und die Beleuchtung des Keypads erlischt. Während der Datenübertragung blinkt die „ACTIVE"-LED.

Der Zugriff auf den Datenträger ist somit freigegeben. Die Smartcard muss während des gesamten Betriebes in der DIGITTRADE HS256 S3 verbleiben. Beim Entfernen der Smartcard aus dem Gehäuse wird der Datenträger gesperrt (Lock-Out Modus). Bei Bedarf kann diese Funktion deaktiviert werden, sodass die Smartcard nach dem Freischalten der HS256 S3 entfernt werden kann und weiterhin ein Zugriff auf den Datenträger besteht. In diesem Fall leuchtet die „STATUS"-LED nach der Authentifizierung grün. Bei Entnahme der Smartcard erlischt die "STATUS"-LED und die "ACTIVE"-LED leuchtet grün. Nähere Informationen finden Sie im Kapitel 5.2.

Wurde eine falsche PIN eingegeben, blinkt die „ERROR"-LED auf und es ist ein akustisches Signal zu hören. Drücken Sie die „ESC"-Taste, um die PIN-Eingabe erneut zu starten.

Hinweis: *Die Smartcard wird automatisch gesperrt und unbrauchbar, sobald die 8-stellige PIN acht Mal falsch eingegeben wurde. Die kryptografischen Schlüssel der Smartcard werden dabei unwiderruflich zerstört.*

Hinweis: *Im freigeschalteten Zustand darf die HS256 S3 nicht unbeaufsichtigt verbleiben, um unbefugte Zugriffe zu vermeiden. Bitte beachten Sie, dass Sie beim Verlassen des Arbeitsplatzes oder bei der Nichtnutzung die DIGITTRADE HS256 S3 ordnungsgemäß abgemeldet sind. Dabei müssen jegliche Datenübertragungen abgeschlossen sein und die HS256 S3 vom USB-Anschluss getrennt werden. Bei aktiviertem Lock-Out Modus genügt es die Smartcard aus dem Festplattengehäuse zu entfernen.*

Aus Sicherheitsgründen wird empfohlen, sämtliche Eingabespuren zu verbergen, die Rückschlüsse auf die in der PIN verwendeten Ziffern ermöglichen können. Denkbare Maßnahmen sind:

1. Regelmäßiges Reinigen des Keypads, sodass keine Fingerabdrücke mehr erkennbar sind.

2. Regelmäßiges Tippen aller Tasten, sodass Fingerabdrücke gleichmäßig verteilt sind.

3. Verwendung spezieller Eingabestifte, die keine Spuren auf der Oberfläche des Keypads hinterlassen, wie z.B. den DIGITTRADE Stylus Pen.

3.3 Ändern der Smartcard-PIN

Um die PIN Ihrer Smartcard zu ändern, gehen Sie wie folgt vor:

1) Stecken Sie eine funktionierende Smartcard in den zugehörigen Steckplatz (siehe Kapitel 1.4 und 3.1) und stellen Sie sicher, dass das Keypad leuchtet.

Hinweis: *Leuchten die rote „ERROR" LED sowie das Keypad auf, initialisieren Sie zunächst diese Smartcard (siehe Kapitel 5.4).*

2) Drücken Sie die Taste „CHANGE PIN" und anschließend die „1".

3) Bestätigen Sie die Eingabe mit „ENTER". Die „STATUS"-LED blinkt mehrmals grün.

4) Geben Sie die aktuelle 8-stellige PIN ein und bestätigen Sie die Eingabe mit „ENTER".

5) Geben Sie die neue 8-stellige PIN ein und bestätigen Sie die Eingabe mit „ENTER".

6) Geben Sie die neue PIN nochmals ein und drücken Sie „ENTER".

Nach erfolgreichem PIN-Wechsel blinkt die „STATUS"-LED mehrmals grün und es sind drei Signaltöne zu hören. Die DIGITTRADE HS256 S3 wird anschließend von Ihrem System als Wechseldatenträger erkannt, die „STATUS"-LED leuchtet rot (bei aktiviertem Lock-Out Modus) und die Beleuchtung des Tastenfeldes erlischt.

Der Zugriff auf die Festplatte ist freigegeben.

War die PIN-Änderung nicht erfolgreich, blinkt die „ERROR"-LED rot auf. Drücken Sie die Taste „ESC" und beginnen Sie erneut mit dem 1. Schritt der PIN-Änderung.

Für die Änderung der Smartcard-PIN haben Sie acht Versuche. Danach wird die eingelegte Smartcard gesperrt und ist nicht mehr verwendbar.

Hinweis: *1. Die DIGITTRADE HS256 S3 akzeptiert nur 8-stellige PIN. Diese sollte zufällig gewählt werden. Verwenden Sie keine Trivial-PIN wie z.B. aufsteigende bzw. absteigende Ziffernreihen oder benutzerbezogene Zahlenfolgen wie Ihr Geburtsdatum oder Ihre Telefonnummer.*

2. Bitte wechseln Sie die Smartcard-PIN regelmäßig während der Benutzung der Festplatte sowie nach Erhalt der Smartcard und bei der Übergabe an andere Benutzer.

4. Verwaltung der kryptografischen Schlüssel mit Hilfe der Smartcard-PIN

Die kryptografischen Schlüssel werden auf einer zertifizierten Smartcard erzeugt und verschlüsselt gespeichert. Nach erfolgreicher PIN-Eingabe werden die kryptografischen Schlüssel an das Verschlüsselungsmodul übertragen, um dort die Ver- und Entschlüsselung zu ermöglichen. Die generierten Schlüssel können über den Datenträger auf weitere Smartcards kopiert werden. Mit Hilfe der Smartcard-PIN können die Krypto-Schlüssel auf der Smartcard erstellt, geändert oder bei Bedarf vernichtet werden.

Die Funktionen zur Verwaltung der kryptografischen Schlüssel (Erstellen, Zerstören und Kopieren) sind nur mit Smartcards möglich, die über das DIGITTRADE HS256 S3 Java Card Applet verfügen. Standardmäßig wird die HS256 S3 mit zwei Kartenexemplaren des Typs NXP J2E081_M64 R3, CC EAL 5 ausgeliefert.

Hinweis: *Die HS256 S3 wird bereits einsatzbereit und vorkonfiguriert ausgeliefert. Aus Sicherheitsgründen ist es dringend erforderlich, dass die kryptografischen Schlüssel geändert und die Smartcards für die HS256 S3 neu initialisiert werden.*

4.1 Erstellen kryptografischer Schlüssel

Mit Hilfe der DIGITTRADE HS256 S3 können kryptografische Schlüssel auf einer zugelassenen Smartcard erstellt werden. Der integrierte zertifizierte Zufallszahlen-generator erzeugt sichere Zufallszahlen. Um zwei kryptografische Schlüssel zu erstellen, gehen Sie wie folgt vor:

1) Stecken Sie eine funktionierende Smartcard in den entsprechenden Steckplatz (siehe Kapitel 1.4 und 3.1).

2) Wenn die Smartcard keine kryptografischen Schlüssel enthält, leuchtet sowohl die „ERROR"-LED als auch die „STATUS"-LED rot.

Enthält die Smartcard bereits zwei kryptografische Schlüssel, die nicht für die HS256 S3 initialisiert sind, blinkt die rote „ERROR"-LED und das Keypad leuchtet. Ist die Smartcard bereits initialisiert, leuchtet das Keypad.

3) Drücken Sie die „ADMIN"-Taste und anschließend die Nummer 2.

4) Drücken Sie „ENTER". Die „STATUS"-LED blinkt mehrmals grün.

5) Geben Sie Ihre 8-stellige Smartcard-PIN ein und drücken Sie „ENTER".

Hinweis: *War die PIN-Eingabe nicht korrekt, blinkt die „ERROR"-LED. Drücken Sie die Taste „ESC" und beginnen Sie erneut mit dem 3. Schritt zum Erstellen der kryptografischen Schlüssel. Sie haben 8 Versuche. Danach wird die eingelegte Smartcard gesperrt und ist nicht mehr verwendbar.*

6) Die „STATUS“-LED blinkt mehrmals grün während die DIGITTRADE HS256 S3 die kryptografischen Schlüssel auf der Smartcard erstellt. Ist dieser Vorgang erfolgreich abgeschlossen, leuchtet die „STATUS“-LED grün und es sind drei Signaltöne zu hören.

7) Trennen Sie die USB-Verbindung der DIGITTRADE HS256 S3 und verbinden Sie diese erneut, um diese Funktion zu verlassen.

Die Krypto-Schlüssel wurden somit erstellt bzw. geändert und die vorherigen eingesetzten Schlüsselpaare dadurch unwiderruflich zerstört. Mit dieser Smartcard ist dann kein Zugriff auf die zuvor gespeicherten Daten mehr möglich. Erstellen Sie daher vorher ggf. eine Sicherungskopie Ihrer Daten.

Wenn Sie diese kryptografischen Schlüssel für die HS256 S3 verwenden wollen, müssen diese für die HS256 S3 initialisiert werden. Folgen Sie dazu der Anleitung in Kapitel 5.4.

Hinweis: *Bitte entfernen Sie die Smartcard **nicht** während der Erstellung der kryptografischen Schlüssel (Schritt 6, „STATUS“-LED blinkt mehrmals* grün*), da die Smartcard sonst beschädigt werden kann.*

4.2 Zerstören beider kryptografischer Schlüssel

1. Die Krypto-Schlüssel können auf zwei Weisen zerstört werden:

a) Zerstörung durch Erzeugung neuer kryptografischer Schlüssel

Führen Sie dazu die Schritte, wie in Kapitel 4.1 beschrieben, durch. Bei dieser Methode können die kryptografischen Schlüssel schnell und unauffällig in Gefahrensituationen zerstört werden, da sich der Vorgang kaum von der normalen Anmeldung unterscheidet. Der Zugriff auf die Daten ist dadurch mit dieser Smartcard auch für den Benutzer nicht mehr möglich.

b) Zerstörung der kryptografischen Schlüssel durch 8-malige Falscheingabe der PIN

Diese Vorgehensweise ist aufwendiger, sie kann jedoch intuitiver und ohne Wissen der Smartcard-PIN umgesetzt werden. Führen Sie dazu folgende Schritte durch:

1) Stecken Sie eine funktionierende Smartcard in den entsprechenden Steckplatz. (siehe Kapitel 1.4 und 3.1).

2) Geben Sie eine falsche 8-stellige PIN ein und drücken Sie „ENTER“.

3) Anschließend blinkt die rote „ERROR“-LED und es ist ein akustisches Signal zu hören.

4) Drücken Sie die Taste „ESC“ und führen Sie den 2. Schritt noch sieben Mal durch.

5) Wurde die falsche PIN 8 Mal eingegeben, sind die kryptografischen Schlüssel zerstört sowie die Smartcard gesperrt und kann nicht mehr verwendet werden.

2. In beiden Fällen handelt es sich nur um die Zerstörung der Kryptoschlüssel auf der jeweiligen Smartcard. Auf der Festplatte vorhandene Daten werden dabei nicht beschädigt und bleiben weiterhin verschlüsselt gespeichert. Liegt dem Benutzer die zweite Smartcard mit den passenden Kryptoschlüsseln und gültiger PIN vor, so kann er auf diese Daten problemlos wieder zugreifen.

3. Falls eine der Smartcards verloren, verlegt oder entwendet wurde, ist es notwendig, die Kryptoschlüssel vollständig zu zerstören. Führen Sie dazu folgende Schritte durch:

1) Nehmen Sie die DIGITTRADE HS256 S3 in Betrieb (siehe Seite 11-12).

2) Sichern Sie alle benötigten Daten von der HS256 S3 auf einen anderen Datenträger.

3) Nach Abschluss dieser Prozedur trennen Sie die USB-Verbindung der HS256 S3 und verbinden Sie diese erneut.

4) Erstellen Sie jetzt zwei neue Krypto-Schlüssel (siehe Kapitel 4.1).

5) Anschließend initialisieren Sie die Smartcard (siehe Kapitel 5.3).

6) Initialisieren und Formatieren Sie die DIGITTRADE HS256 S3 an Ihrem Betriebssystem (siehe Kapitel 6-8).

7) Überschreiben Sie die HS256 S3 vollständig mit Zufallsdaten. Nach Abschluss dieser Prozedur können Sie diese Daten löschen und die DIGITTRADE HS256 S3 normal verwenden.

Jegliche Kopien der alten Kryptoschlüssel auf anderen Smartcards sind anschließend unbrauchbar.

5. Geräte-PIN-Funktionen

Die Geräte-PIN ermöglicht nicht den Zugriff auf die gespeicherten Daten. Mit Hilfe der Geräte-PIN können Sie folgende administrative Funktionen durchführen:

- Ändern der Geräte-PIN

- Aktivieren/Deaktivieren des Lock-Out Modus

- Kopieren von kryptografischen Schlüsseln

- Initialisieren einer neuen Smartcard für die DIGITTRADE HS256 S3

Die bei der Auslieferung voreingestellte Geräte-PIN lautet: **8-7-6-5-4-3-2-1**.

Aus Sicherheitsgründen empfehlen wir Ihnen diese zu ändern. Die Geräte-PIN muss vertraulich behandelt werden. Damit vermeiden Sie die Ausführung der oben genannten Funktionen an Ihrer Festplatte durch Unbefugte.

Die Anzahl der Versuche für die Eingabe der Geräte-PIN ist nicht begrenzt.

Hinweis: *Merken Sie sich Ihre Geräte-PIN. Ohne diese Zahlenfolge ist die Initialisierung neuer Smartcards und somit weitere Benutzung der HS256 S3 nicht möglich.*

5.1 Ändern der Geräte-PIN

Um die Geräte-PIN zu ändern, gehen Sie wie folgt vor:

1) Stecken Sie eine funktionierende Smartcard in den entsprechenden Steckplatz (siehe Kapitel 1.4 und 3.1). Stellen Sie sicher, dass das Keypad leuchtet.

Hinweis: *Leuchten beim Einsetzen der Smartcard die „ERROR"-LED rot und das Keypad, führen Sie bitte die Initialisierung dieser durch (siehe Kapitel 5.4).*

2) Drücken Sie auf dem Keypad die Taste „CHANGE-PIN" und anschließend die „0".

3) Bestätigen Sie die Eingabe mit „ENTER".

4) Geben Sie die aktuelle 8-stellige Geräte-PIN ein und bestätigen Sie die Eingabe mit „ENTER". Die „STATUS"-LED blinkt zwei Mal grün.

5) Geben Sie die neue 8-stellige Geräte-PIN ein und bestätigen Sie die Eingabe mit „ENTER". Die „STATUS"-LED blinkt zwei Mal grün.

6) Geben Sie die neue 8-stellige Geräte-PIN nochmals ein und bestätigen Sie die Eingabe mit „ENTER“.

7) Während der Änderung blinkt die „STATUS“-LED mehrmals grün und es sind zum Abschluss drei Signaltöne zu hören.

8) Die Smartcard kann jetzt entfernt werden. Trennen Sie die USB-Verbindung der HS256 S3 um diese Funktion zu verlassen.

War die PIN-Änderung nicht erfolgreich, blinkt die rote „ERROR“-LED auf. Drücken Sie die Taste „ESC“ und beginnen Sie erneut mit dem 1. Schritt der Änderung der Geräte-PIN.

Hinweis: *Die DIGITTRADE HS256 S3 akzeptiert nur 8-stellige PIN. Die Zahlenfolge sollte zufällig gewählt werden. Verwenden Sie keine Trivial-PIN wie z.B. aufsteigende bzw. absteigende Ziffernreihen oder benutzerbezogene Zahlenfolgen wie Ihr Geburtsdatum oder Ihre Telefonnummer.*

5.2 Aktivieren/Deaktivieren des Lock-Out Modus (Geräte-PIN erforderlich)

Im aktivierten Lock-Out Modus wird der Zugriff auf die Daten nach dem Entfernen der Smartcard aus dem Gehäuse sofort unterbrochen.

Bei der Auslieferung der HS256 S3 ist der Lock-Out Modus aktiviert.

Die „STATUS“-LED leuchtet rot im authentifizierten Zustand. Für eine sichere Benutzung der HS256 S3 muss der Lock-Out Modus aktiviert sein. Ein Betrieb der HS256 S3 mit ausgeschaltetem Lock-Out Modus befindet sich außerhalb des Geltungsbereiches der BSI-Zertifizierung.

Der Nutzer kann in besonderen Fällen diese Funktion deaktivieren. Dies ist erforderlich, wenn nur eine Smardcard den Zugriff zeitgleich auf mehrere Datenträger mit gleichem Krypto-Schlüssel freischalten soll. Ist der Lock-Out Modus deaktiviert, leuchtet die „STATUS“-LED grün im authentifizierten Zustand.

Bitte verwenden Sie in diesem Fall nach dem Beenden der Benutzung die physikalische Trennung (Kapitel 15), da die logische Seperation im deaktivierten Lock-Out Modus nicht möglich ist.

Führen Sie folgende Schritte für die Aktivierung oder Deaktivierung des Lock-Out Modus durch:

1) Stecken Sie eine funktionierende Smartcard in den zugehörigen Steckplatz (siehe Kapitel 1.4 und 3.1). Stellen Sie sicher, dass das Keypad leuchtet.

Hinweis: *Leuchten beim Einsetzen der Smartcard das Keypad und die "Error"-LED dauerhaft, führen Sie bitte die Initialisierung der Smartcard durch (siehe Kapitel 5.4).*

2) Drücken Sie die „ADMIN"-Taste und anschließend die Nummer 1.

3) Drücken Sie „ENTER". Die „STATUS"-LED blinkt mehrmals grün.

4) Geben Sie Ihre 8-stellige Geräte-PIN ein und drücken Sie „ENTER".
Wurde die richtige Zahlenfolge eingegeben, blinkt die „STATUS"-LED mehrmals grün und es sind drei Signaltöne zu hören.

Hinweis: *War die PIN-Eingabe nicht korrekt, blinkt die rote „ERROR"- LED. Drücken Sie die Taste „ESC" und beginnen Sie erneut mit dem 2. Schritt.*

5) Der Lock-Out Modus wird aktiviert / deaktiviert. Die „STATUS"-LED leuchtet im authentisierten Zustand rot, wenn die Funktion aktiviert ist. Im Falle der deaktivierten Funktion leuchtet die „STATUS"-LED grün.

6) Trennen Sie die USB-Verbindung der HS256 S3 und verbinden Sie diese erneut, um diese Funktion zu verlassen.

Hinweis: *Der Lock-Out Modus ist voreingestellt aktiviert. Entfernen Sie in diesem Modus die Smartcard* ***nicht*** *während auf die DIGITTRADE HS256 S3 zugegriffen wird, da dies zu Datenverlust führen kann.*

5.3 Kopieren von kryptografischen Schlüsseln (Geräte-PIN erforderlich)

Mit dieser Funktion können Sie die kryptografischen Schlüssel einer Smartcard auf eine weitere Smartcard übertragen. Sie benötigen dazu zwei Exemplare: Eine Smartcard, die die zu kopierenden Krypto-Schlüssel enthält, und eine Zweite, auf die das Schlüsselpaar kopiert werden soll. Um die kryptografischen Schlüssel zu kopieren, gehen Sie wie folgt vor:

1) Stecken Sie eine funktionierende und initialisierte Smartcard A in den dafür entsprechenden Steckplatz (siehe Seite 12).

Ist die Smartcard bereits initialisiert, leuchtet das Keypad. Enthält die Smartcard bereits zwei kryptografische Schlüssel, die nicht für die HS256 S3 initialisiert sind, blinkt die rote „ERROR"-LED und das Keypad leuchtet. Danach leuchtet die „ERROR"-LED. Initialisieren Sie zunächst diese Smartcard (siehe Seite 22).

2) Drücken Sie die „ADMIN"-Taste und anschließend die Nummer 3.

3) Drücken Sie „ENTER". Die „STATUS"-LED blinkt mehrmals grün.

4) Geben Sie Ihre 8-stellige Geräte-PIN ein und drücken Sie „ENTER". Die „STATUS"-LED blinkt zwei Mal grün. Geben Sie die 8-stellige PIN der Smartcard A ein und drücken Sie „ENTER".

Hinweis:
1. *War die PIN-Eingabe nicht korrekt, blinkt die rote „ERROR"-LED. Drücken Sie die Taste „ESC" und beginnen Sie erneut mit dem 2. Schritt zum Kopieren der kryptografischen Schlüssel.*
2. *Die Smartcard A wird automatisch gesperrt und unbrauchbar, sobald die 8-stellige PIN acht Mal falsch eingegeben wurde.*

5) Die „STATUS"-LED blinkt mehrmals grün während die DIGITTRADE HS256 S3 die kryptografischen Schlüssel der Smartcard A liest. Ist dieser Vorgang erfolgreich abgeschlossen, leuchtet die „STATUS"-LED grün und es sind drei Signaltöne zu hören.

6) Entfernen Sie Smartcard A und stecken Sie Smartcard B in die DIGITTRADE HS256 S3. Das Keypad leuchtet nach dem Einsetzen.

7) Geben Sie Ihre 8-stellige PIN der Smartcard B ein und drücken Sie „ENTER".

Hinweis:
1. *War die PIN-Eingabe nicht korrekt, blinkt die rote „ERROR"- LED. Drücken Sie die Taste „ESC" und geben Sie die 8-stellige PIN der Smartcard B erneut ein.*
2. *Die Smartcard B wird automatisch gesperrt und unbrauchbar, sobald die 8-stellige PIN acht Mal falsch eingegeben wurde.*

8) Die „STATUS“-LED blinkt mehrmals grün während die DIGITTRADE HS256 S3 die kryptografischen Schlüssel auf Smartcard B schreibt. Ist dieser Vorgang erfolgreich abgeschlossen, leuchtet die „STATUS“-LED grün und es sind drei Signaltöne zu hören.

9) Zum Beschreiben weiterer Smartcards mit diesen kryptografischen Schlüsseln trennen Sie die Festplatte und beginnen Sie wieder mit Schritt 1.

Hinweis: *Entfernen Sie die Smartcard **nicht** während der Lese- und Schreibprozesse (Schritt 5 und 8, „STATUS“-LED blinkt mehrmals* grün*), da die Smartcard sonst beschädigt werden kann.*

5.4 Initialisieren einer neuen Smartcard (Geräte-PIN erforderlich)

Das Initialisieren einer neuen Smartcard ist erforderlich, wenn die kryptografischen Schlüssel der Smartcard geändert wurden und die DIGITTRADE HS256 S3 damit betrieben werden soll (z.B. aus Sicherheitsgründen, sowie bei Verlust einer oder mehrerer Smartcards).

Beim Initialisieren einer neuen Smartcard ändern sich die kryptografischen Schlüssel des Krypto-Systems. Die HS256 S3 muss dadurch im Anschluss mit dem Anwenderbetriebssystem neu initialisiert und formatiert werden. Ein Zugriff auf die zuvor gespeicherten Daten ist mit den neuen Krypto-Schlüsseln nicht möglich.

Zum Initialisieren einer neuen Smartcard gehen Sie bitte wie folgt vor:

1) Stecken Sie eine neue funktionierende Smartcard in den entsprechenden Steckplatz (siehe Kapitel 1.4 und 3.1). Vergewissern Sie sich, dass die rote „ERROR“- und das Keypad leuchten.

2) Drücken Sie die „ADMIN“-Taste und anschließend die „0“.

3) Drücken Sie „ENTER“. Die „STATUS“-LED blinkt mehrmals grün.

4) Geben Sie Ihre 8-stellige Geräte-PIN ein und drücken Sie „ENTER“.

Hinweis: *War die PIN-Eingabe nicht korrekt, blinkt die rote „ERROR”-LED. Drücken Sie die Taste „ESC“ und beginnen Sie erneut mit dem 3. Schritt zum Initialisieren einer Smartcard.*

6) Wurde die richtige Geräte-PIN eingegeben, leuchtet die „STATUS“-LED grün und es sind drei Signaltöne zu hören. Die eingesetzte Smartcard wurde für diese DIGITTRADE HS256 S3 initialisiert.

7) Trennen Sie die USB-Verbindung der DIGITTRADE HS256 S3, um diese Funktion zu verlassen.

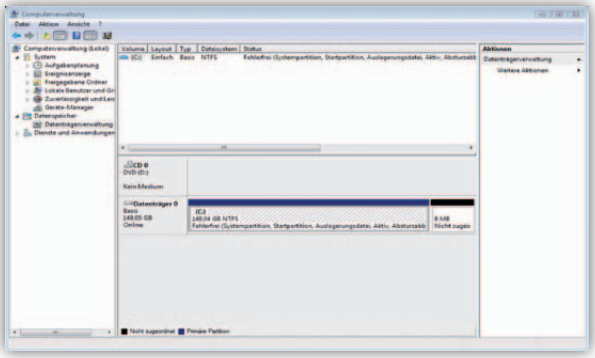
8) Führen Sie eine Initialisierung und eine Formatierung der DIGITTRADE HS256 S3 an Ihrem Betriebssystem durch. Beachten Sie dazu die Hinweise in den folgenden Kapiteln.

Hinweis: *Merken Sie sich Ihre Geräte-PIN. Ohne diese Zahlenfolge ist die Initialisierung neuer Smartcards und somit weitere Benutzung der HS256 S3 nicht möglich.*

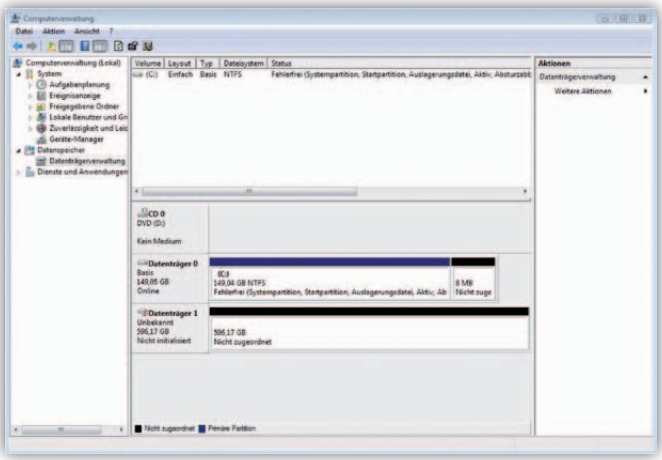
6. Initialisierung/Partitionierung und Formatierung unter Windows

Um die HS256 S3 unter Windows zu initialisieren, gehen Sie wie folgt vor:

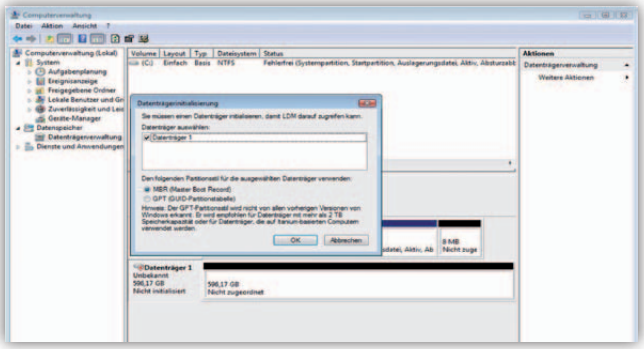
- Nehmen Sie die DIGITTRADE HS256 S3 in Betrieb (siehe Seite 11-12).
- Gehen Sie in die Systemsteuerung und unter der Rubrik Verwaltung wählen Sie anschließend “Computerverwaltung” aus.
- Klicken Sie auf “Computerverwaltung” und anschließend auf „Datenträgerverwaltung“. Hier finden Sie eine Übersicht über alle Festplatten und Laufwerke:



- Die HS256 S3 wird nach erfolgreicher Anmeldung im unteren Teil der Datenträgerverwaltung angezeigt:



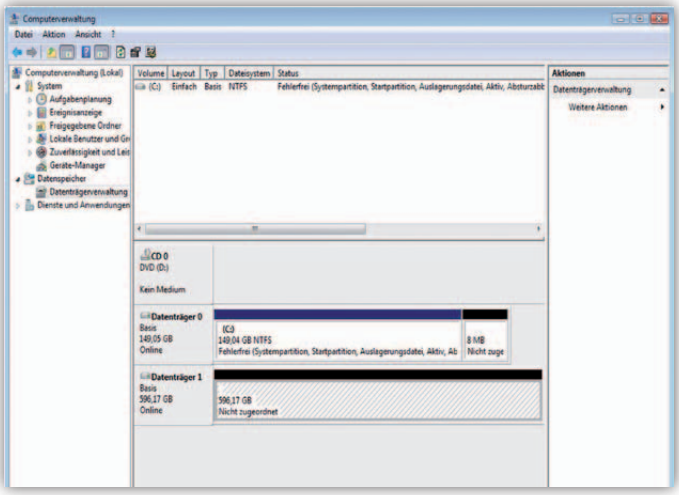
- Wird die Datenträgerverwaltung zum ersten Mal seit dem Anschließen der HS256 S3 gestartet, erscheint folgendes Fenster:



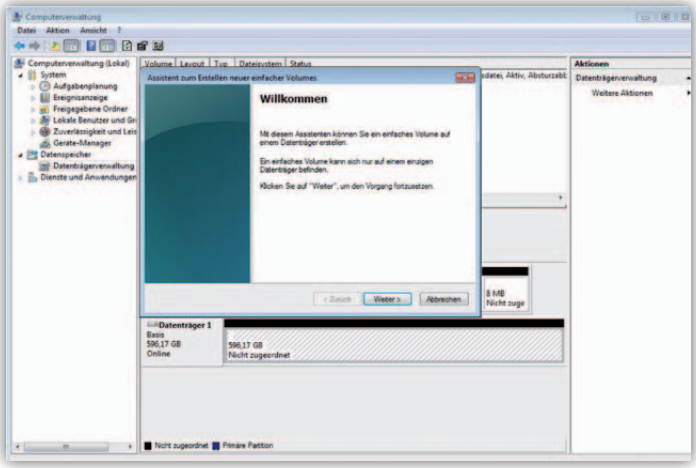
- Hier können Sie mit einem Klick auf „OK“ das neue Laufwerk initialisieren.

Hinweis: *Falls die Initialisierungsaufforderung nicht automatisch erscheint oder diese mit einem Klick auf „Abbrechen“ beendet wurde, können Sie die Initialisierung auch mit einem Rechtsklick auf dem Datenträgerfeld („Nicht initialisiert“) ausführen.*

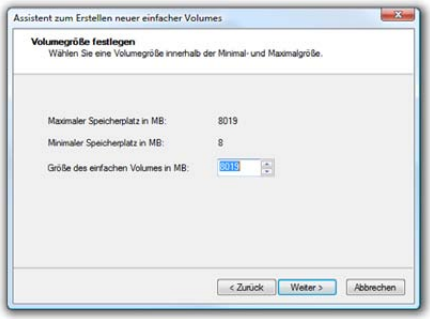
- Anschließend wechselt der Status des Datenträgers von „Nicht initialisiert“ zu „Online“:



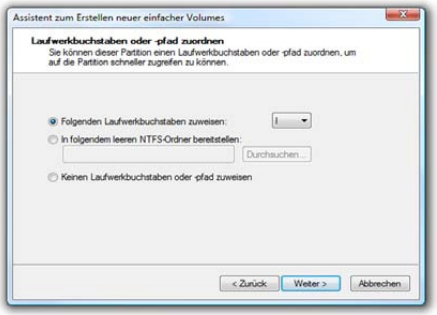
- Klicken Sie mit der rechten Maustaste auf den „Nicht zugeordneten“ Bereich und wählen Sie im Kontextmenü den Eintrag „Neues einfaches Volume…“ aus. Im startenden Assistenten können Sie alle erforderlichen Einstellungen bis zur Formatierung vornehmen.
- Klicken Sie auf „Weiter“, um den Vorgang zu beginnen:



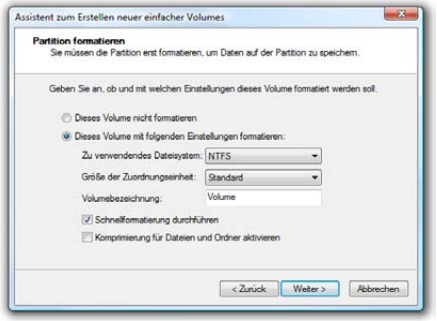
- Tragen Sie die gewünschte Größe der Partition in MB ein und klicken Sie dann auf „Weiter“:



- Sie können der Partition einen Laufwerksbuchstaben zuweisen. Klicken Sie anschließend auf „Weiter“:



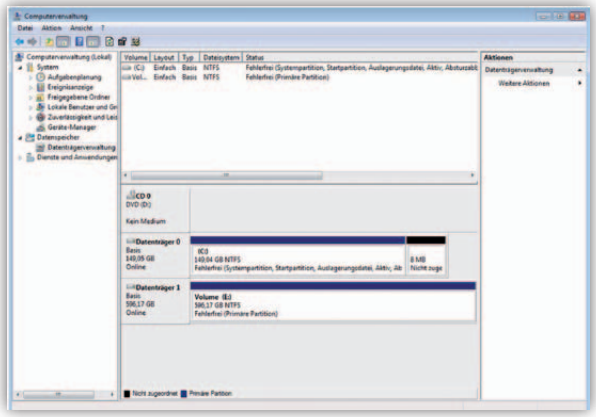
- Wählen Sie das gewünschte Dateisystem, die Art der Formatierung und klicken Sie auf „Weiter“:



- Die Formatierung wird abgeschlossen. Bestätigen Sie diesen Vorgang, indem Sie auf „Fertig stellen“ klicken.

Die Dauer der Formatierung kann je nach Festplattengröße variieren.

Wurde die Formatierung abgeschlossen, wird die HS256 S3 als „Fehlerfrei“ angezeigt und kann verwendet werden:

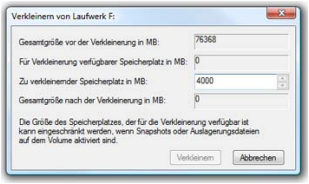


Es besteht zudem die Möglichkeit, über die „Datenträgerverwaltung“, die DIGITTRADE HS256 S3 in mehrere Partitionen einzuteilen.

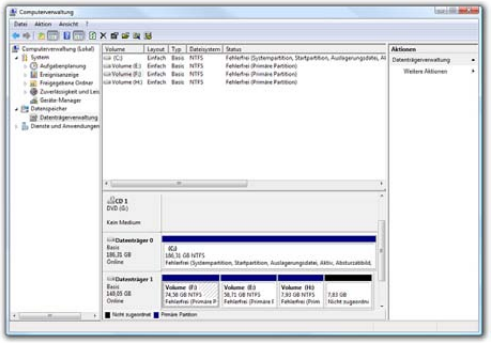
Um die HS256 S3 zu partitionieren, gehen Sie wie folgt vor:

- Wählen Sie mit der Maus die HS256 S3 aus und öffnen Sie mit der rechten Maustaste das Kontextmenü.

- Wählen Sie den Punkt „Volumen verkleinern“ aus.
- Tragen Sie den gewünschten Speicherplatz in MB ein, auf den die Partition verkleinert werden soll:



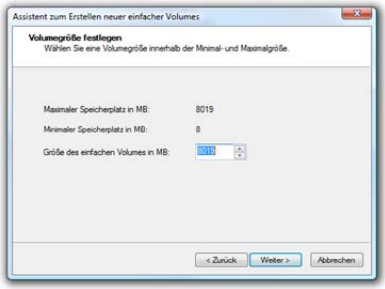
- Es wird jetzt ein nicht zugeordneter Bereich im Verwaltungsbildschirm angezeigt:



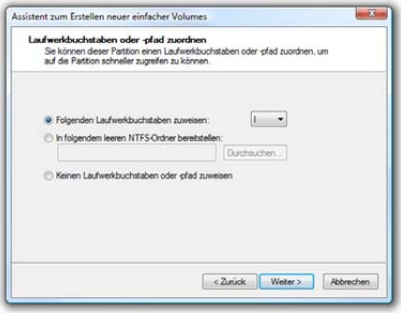
- Markieren Sie den nicht zugeordneten Bereich mit der Maus, öffnen Sie das Kontextmenü mit der rechten Maustaste und wählen Sie den Punkt „neues einfaches Volumen“.
- Es öffnet sich der Partitionierungsassistent:

- Klicken Sie auf „Weiter“.
- Tragen Sie die gewünschte Größe der Partition in MB ein und klicken Sie

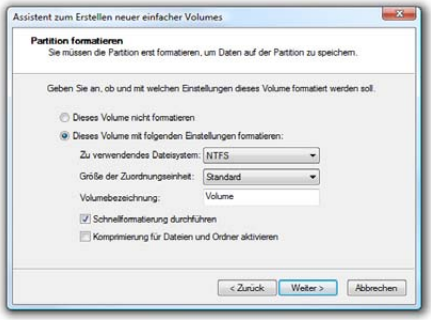
dann auf „Weiter“:



- Sie können der Partition einen Laufwerksbuchstaben zuweisen. Klicken Sie anschließend auf „Weiter“:

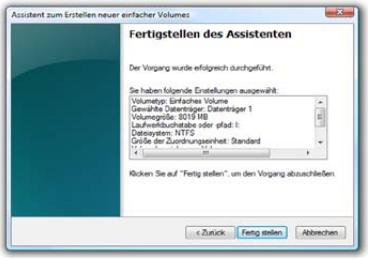


- Wählen Sie das gewünschte Dateisystem, die Art der Formatierung und klicken Sie auf „Weiter“:



- Die Partitionierung wird abgeschlossen. Bestätigen Sie diesen Vorgang indem Sie auf „Fertig stellen“ klicken:

Hinweis: *Der neu partitionierte Bereich wird formatiert. Nach Abschluss der Formatierung wird die neue Partition automatisch vom System erkannt.*



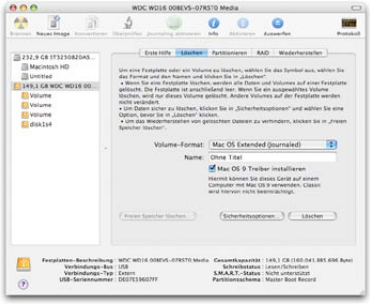
7. Initialisierung/Partitionierung und Formatierung unter MAC OS X

- Nehmen Sie die DIGITTRADE HS256 S3 in Betrieb (siehe Seite 11-12).

Zum Verwalten externer Festplatten unter MAC hilft das „Festplatten Dienstprogramm“. Dazu öffnen Sie „Programme“ und anschließend den Punkt „Dienstprogramme“.

- Wählen Sie das „Festplatten-Dienstprogramm“ aus. Es öffnet sich das Verwaltungsprogramm zum Initialisieren, Partitionieren und Formatieren von Festplatten.

- Wählen Sie aus der Laufwerksübersicht auf der linken Seite die HS256 S3 Festplatte aus. Im Menü lässt sich mit dem Menüpunkt „Löschen“ die HS256 S3 komplett initialisieren und formatieren.



Neben dem Namen lässt sich auch das Dateisystem angeben, mit dem die HS256 S3

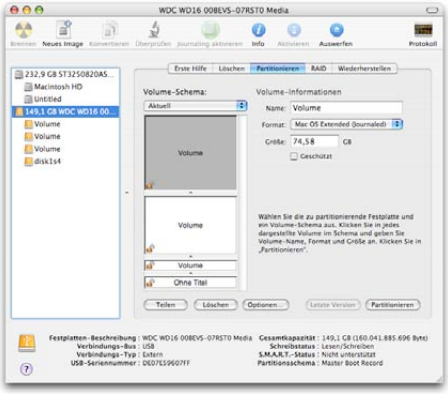
verwendet werden soll. Für MAC OS X sollte „Mac OS Extended (Journaled)“ gewählt werden, für das klassische MAC OS 9 das HFS Format (Mac OS Extended).

- Bestätigen Sie die Initialisierung/ Formatierung durch das Anklicken der Schaltfläche „Löschen“.

Das Partitionieren der HS256 S3 Festplatte erfolgt ebenfalls über das „Festplatten-Dienstprogramm“.

Nach Auswahl der HS256 S3 in der Laufwerksübersicht lassen sich im Menüpunkt „Partitionieren“ einzelne eigenständige Partitionen und die jeweilige gewünschte Partitionsgröße einstellen.

- In der Mitte sehen Sie die aktuelle Partitionierung der Festplatte. Klicken Sie auf das Pulldown-Menü „Aktuell” direkt unter „Volume-Schema”.
- Nun können Sie die Zahl der Partitionen festlegen.
- Nachdem Sie alle Partitionen angelegt haben, können Sie anschließend über die „Volume-Informationen” den Namen und die Größe der einzelnen Partitionen bestimmen.



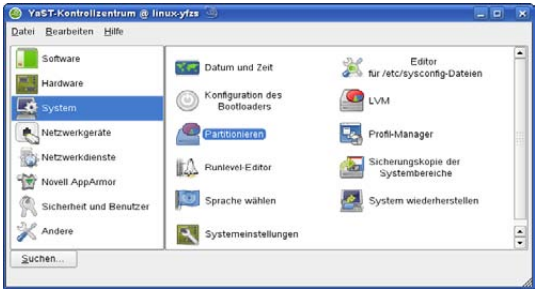
- Bestätigen Sie die durchgeführten Einstellungen durch das Anklicken der Schaltfläche „Partitionieren“.

8. Initialisierung/Partitionierung und Formatierung unter Linux

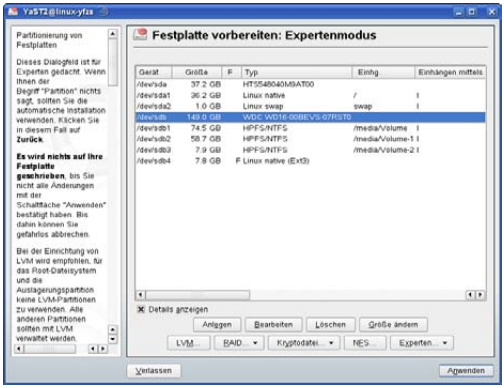
- Nehmen Sie die DIGITTRADE HS256 S3 in Betrieb (siehe Seite 11-12).

Es besteht die Möglichkeit, die HS256 S3 Festplatte unter Linux in mehrere Partitionen einzuteilen. Dabei muss zunächst die HS256 S3 für das korrekte Dateisystem initialisiert werden. Die Vorgehensweise wird hier auf der Basis von YaST von Suse Linux beschrieben. Dieser Vorgang ist unter anderen Linux-Distributionen ähnlich.

- Öffnen Sie zuerst YaST. Sie werden ggf. dazu aufgefordert, sich zu authentisieren.



- Wählen Sie auf der linken Seite „System" und im rechten Feld „Partitionieren" aus.
- Aus Sicherheitsgründen öffnet sich ein Fenster und Sie werden gefragt, ob Sie mit der Partitionierung bereits vertraut sind. Bestätigen Sie diese Meldung mit „Ja".
- Die Datenträgertabelle Ihres Systems wird geöffnet.



- Hier können Sie den gewünschten Datenträger auswählen,partitionieren oder

bereits vorhandene Partionen bearbeiten bzw. löschen.

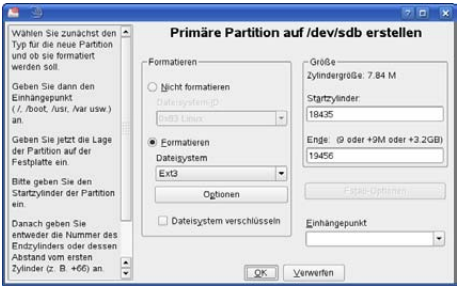
- Zum Löschen der standardmäßig vorhandenen NTFS-Partition wählen Sie diese mit dem Cursor aus und klicken anschließend auf „Löschen".

- Sie werden vom System gefragt, ob Sie die Partition wirklich löschen wollen. Vergewissern Sie sich, dass Sie die richtige Partition ausgewählt haben und bestätigen Sie, indem Sie auf „Ja" klicken.

Hinweis: *Beim Löschen der Partition werden auch alle auf der Partition befindlichen Dateien unwiderruflich gelöscht.*

- Um eine neue Partition auf dem freien Speicher des Datenträgers anzulegen, klicken Sie auf „Erstellen".

- Legen Sie fest, auf welchem Datenträger Sie eine neue Partition erstellen möchten.
- Im nächsten Schritt werden Sie nach der Art der Partition gefragt. Hier empfiehlt es sich in den meisten Fällen, die „Primäre Partition" auszuwählen.

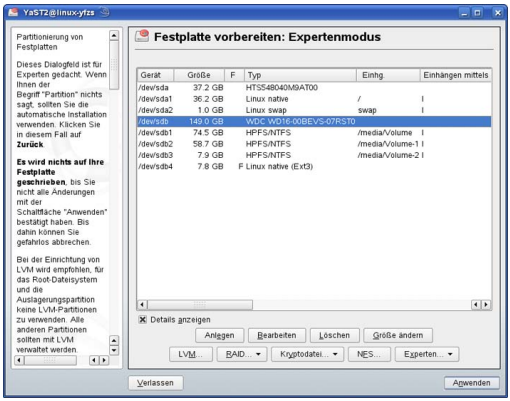


- In diesem Fenster legen Sie alle Merkmale für die Partition fest. Sie können zwischen verschiedenen Dateisystemen wählen, die Größe bestimmen und

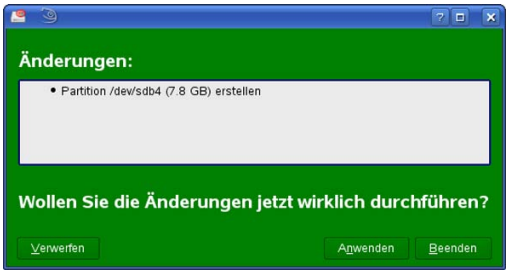
bei Bedarf sogar den Einhängepunkt in Ihr Linux-System festlegen.

- Bestätigen Sie abschließend alle Ihre Angaben mit „OK".

- Die Formatierung erfolgt ähnlich. Wählen Sie hierzu die gewünschte Partition aus und klicken Sie auf „Bearbeiten".
- Setzen Sie anschließend den Haken bei „Formatieren" und wählen Sie ein passendes Dateisystem aus. Bestätigen Sie alle Angaben mit „OK".



- Damit Ihre Änderungen wirksam werden, klicken Sie auf „Anwenden".



- In einem neuen Fenster werden alle Ihre Änderungen aufgelistet. Vergewissern Sie sich erneut, dass alle Änderungen Ihrem Wunsch entsprechen und bestätigen Sie Ihre Einstellungen, indem Sie auf „Anwenden" klicken.

Hinweis: *Sollten Sie sich bei der Wahl des richtigen Dateisystems und der jeweiligen Partitionsgröße unsicher sein, empfiehlt es sich, die automatisch eingetragenen Werte zu übernehmen.*

9. Das richtige Dateisystem

In der nachstehenden Tabelle sehen Sie die Kompatibilität zwischen den Betriebs- und Dateisystemen.

	NTFS	FAT32	HFS+	EXT3
Windows 98	X	L, S	X	X
Windows NT, 2000, ME, XP, Vista, 7, 8, 10	L, S	L, S	X	X
Mac OS X	L	L, S	L, S	X
Linux	L	L, S	X	L, S

Bezeichnung: L - Lesen, S - Schreiben, X - Keine Kompatibilität

Mit Erweiterungsprogrammen können ggf. auch Daten auf Dateisysteme geschrieben werden, bei denen dies sonst nicht möglich ist.

Die DIGITTRADE HS256 S3 ist zum Zeitpunkt der Auslieferung bereits für Sie im NTFS-Dateisystem vorformatiert. In der vorherigen Tabelle sehen Sie die Kompatibilität von NTFS mit Ihrem Betriebssystem. Sollte NTFS nicht zu Ihrem Betriebssystem passen, so müssen Sie die Festplatte erneut formatieren (siehe ab Kapitel 6).

Für Windowsnutzer wird empfohlen, NTFS zu verwenden. Für Mac OS X ist HFS+ das leistungsstärkste Dateisystem und bei Linux sollten Sie EXT3 verwenden. Selbstverständlich ist es auch möglich, die DIGITTRADE HS256 S3 mit jedem anderen Dateisystem zu formatieren. Dies beeinflusst die Verschlüsselung der Daten nicht.

Wenn Sie die Festplatte unter verschiedenen Betriebssystemgruppen verwenden wollen, so empfehlen wir die Formatierung im FAT32-Dateisystem, da dieses von fast allen Betriebssystemen gelesen und beschrieben werden kann. Jedoch gibt es hierbei Einschränkungen in der maximalen Datei- und Partitionsgröße. Des Weiteren gibt es auch leichte Performance-Unterschiede.

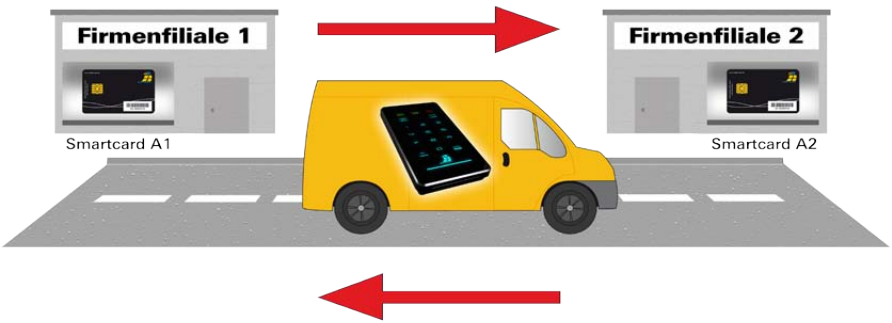
10. Anwendungsmöglichkeiten der HS256 S3

1) Sicherer und kosteneffizienter Datentransport

Die HS256 S3 kann für den Transport vertraulicher Daten verwendet werden. Dazu werden beim Sender und beim Empfänger der Daten Smartcards mit gleichen kryptografischen Schlüsseln hinterlegt. Der Absender versendet nur die HS256 S3. Die Krypto-Schlüssel sind auf der Smartcard unabhängig von der Festplatte gespeichert. Sie sind somit beim Transport phyisch nicht vorhanden und können auch während des Versands nicht ausgelesen werden. Außerdem kann die HS256 S3 mit vertraulichen Daten dem Empfänger kostengünstig und versichert durch einen Paketdienstleister oder Kurier zugestellt werden.

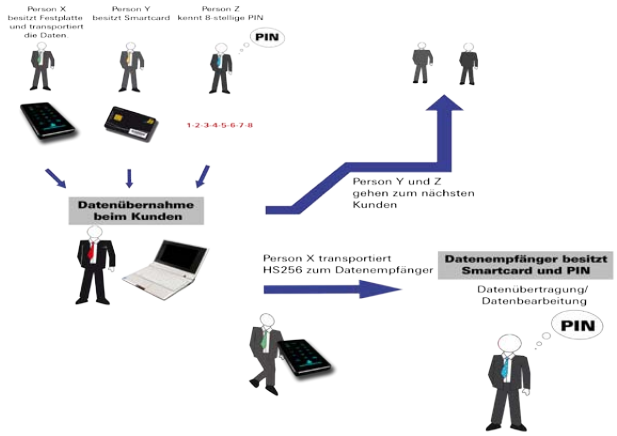
Der Sender und der Empfänger müssen bei jedem Datentransport sicherstellen, dass sie eine Manipulation an der HS256 S3 erkennen können. Hierzu empfiehlt sich, wie in Kapitel 1.8 beschrieben, die Verwendung von versiegelten Sicherheitstaschen. Dies gilt auch für alle anderen Datentransportmöglichkeiten mittels HS256 S3.

Zusätzliche Sicherheit bietet die Verwendung mehrerer Smartcards mit unterschiedlichen kryptografischen Schlüsseln, die beim Sender und Empfänger hinterlegt sind und in bestimmter Reihenfolge oder nach Absprache zur Ver- und Entschlüsselung der Daten verwendet werden.



2) Trennung von Datenträger und Authentifizierungen

Der Zugriff auf die Daten kann so reglementiert sein, dass er nur durch das Zusammenführen von z.B. drei Personen möglich ist. Person X besitzt die HS256 S3, die Person Y verfügt über die Smartcard und die Person Z kennt die Smartcard-PIN. Die drei Personen kommen nur zur Datenübernahme an der Empfängerstelle zusammen und trennen sich anschließend wieder. Die Personen X, Y und Z haben dabei einzeln nicht die Möglichkeit auf die Daten zuzugreifen.



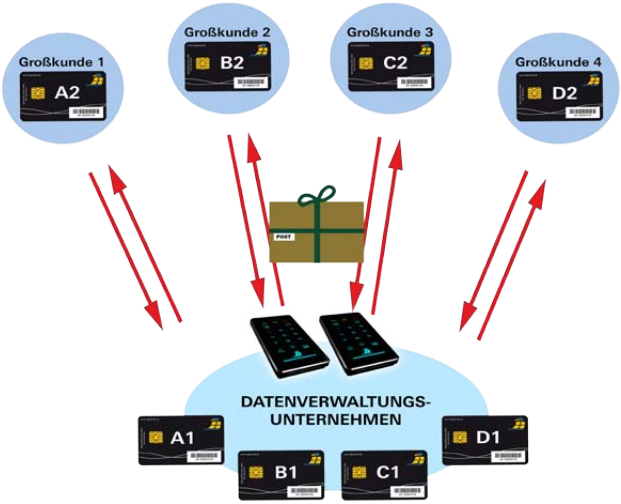
3) Verwendung weniger Datenträger bei großem Kundenkreis

Steht ein Unternehmen (z.B. ein Datenverarbeitungsunternehmen oder eine Datenzentrale von Großunternehmen oder Behörden) in ständigem Datenaustausch mit vielen Datenempfängern, so kann dieses mit Hilfe der HS256 S3-Festplatten Daten mit wenigen Speichermedien sowie kostengünstigen Aufwendungen sicher transportieren. Jeder Datenempfänger erhält eine Smartcard mit seinen eigenen Krypto-Schlüsseln. Bei dem Datenversender werden Zweitexemplare der Smartcards mit den Krypto-Schlüsseln der jeweiligen Datenempfänger angelegt.

Für den Datenversand wird eine Smartcard mit den kryptografischen Schlüsseln des jeweiligen Empfängers für eine HS256 S3 initialisiert (Geräte-PIN erforderlich). Dafür ist jede verfügbare HS256 S3 geeignet. Anschließend führt der Datenversender mit den neuen kryptografischen Schlüsseln eine Schnellformatierung der HS256 S3 durch, die nur wenige Minuten dauert. Aufwendige Datenlöschungen und mehrmaliges Überschreiben des Datenträgers entfallen, da die verbliebenen Daten mit den vorherigen Krypto-Schlüsseln verschlüsselt sind. Somit sind diese ggf. nur vom Besitzer des zugehörigen kryptografischen Schlüssels wiederherstellbar und können im Anschluss gelesen werden. Voraussetzung ist, dass die Daten nicht überschrieben wurden.

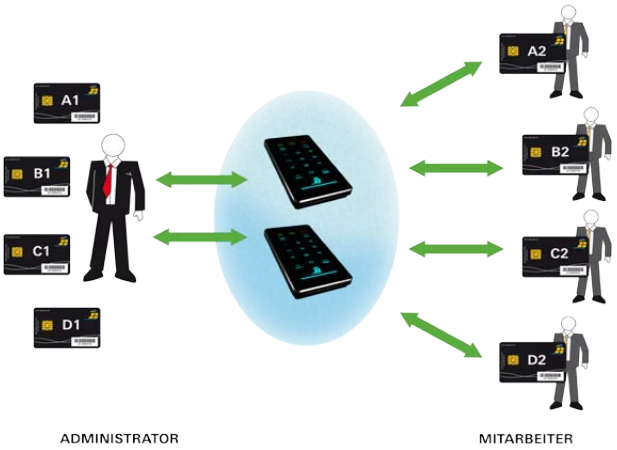
Sollen Daten in kurzen zeitlichen Abständen an den gleichen Empfänger verschickt werden, ist es nicht erforderlich, auf die Rücksendung einer personalisierten HS256 S3 zu warten. Es kann jede, im Unternehmen verfügbare HS256 S3 verwendet werden. Diese wird dazu vor der Datenspeicherung mit den kryptografischen Schlüsseln des entsprechenden Empfängers initialisiert und schnell formatiert.

Die Stückzahl der Datenträger kann jeder Zeit reduziert werden, da nicht für jeden Datenempfänger eine eigene HS256 S3 benötigt wird. Dabei ist es irrelevant, welche der im Unternehmen verfügbaren hoch sicheren Festplatten für den Datentransport verwendet werden. Entscheidend ist, mit welchen kryptografischen Schlüsseln die Daten auf die HS256 S3 geschrieben werden.



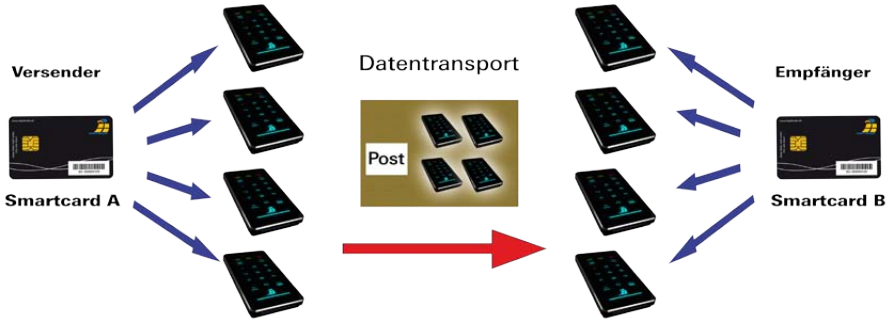
4) Verwendung weniger Datenträger im Außendienst und bei Behörden

In einem Unternehmen kann jeder Außendienstmitarbeiter über seine personalisierte Smartcard mit seinen eigenen kryptografischen Schlüsseln verfügen. Für die Tätigkeit außerhalb des Unternehmens erhält der Mitarbeiter eine beliebige HS256 S3, die zuvor für den Mitarbeiter initialisiert wurde. Der Außendienstler speichert die Daten mit seinen eigenen kryptografischen Schlüsseln.
Nach der Benutzung gibt der Mitarbeiter die HS256 S3 zurück. Diese wird anschließend einer Schnellkonfiguration unterzogen. Innerhalb weniger Minuten ist die HS256 S3 für den nächsten Kollegen einsatzbereit. Es wird daher nicht für jeden Mitarbeiter eine eigene HS256 S3 benötigt und die Anzahl der erforderlichen Datenträger im Unternehmen kann enorm reduziert werden.



5) Betreiben mehrerer Datenträger mit nur einer Smartcard

Es werden dazu Smartcards mit den gleichen kryptografischen Schlüsseln für mehrere HS256 S3 initialisiert. Von besonderem Interesse ist das Betreiben von mehreren Datenträgern mit nur einer Smartcard für die Arbeit mit Datenvolumen, die die Kapazität einer HS256 S3 übersteigen. Hier können die Daten auf mehrere HS256 S3-Geräte verteilt werden. Auch wenn Daten sehr häufig, z.B. täglich verschickt werden, bietet es sich an, mehrere Speichermedien mit den gleichen kryptografischen Schlüsseln zu verwenden.
Es kann täglich eine neue HS256 S3 mit den gleichen Krypto-Schlüsseln versendet werden, ohne dass auf eine personalisierte HS256 S3 gewartet werden muss. Der Empfänger kann stets mit der gleichen Smartcard, die die entsprechenden kryptografischen Schlüssel enthält, auf den Datenträger zugreifen.



6) Zerstören der kryptografischen Schlüssel

Der Nutzer hat in Gefahrensituationen die Möglichkeit, die kryptografischen Schlüssel unauffällig zu zerstören, wenn ihm die Smartcard-PIN bekannt ist. Dazu werden während des Anmeldevorgangs drei zusätzliche Tasten bedient (siehe Kapitel 4.2).

Der Zugriff auf die Daten ist dadurch mit dieser Smartcard auch für den Benutzer nicht mehr möglich.

Falls die Smartcard-PIN nicht bekannt ist, können die Schlüsselpaare auf der Smartcard durch 8-malige Falscheingabe der PIN vernichtet werden.

7) Bootfähigkeit

Auf der DIGITTRADE HS256 S3 können Betriebssysteme, Programme und Daten gespeichert werden. Diese Anwendung ist sowohl für stationäre als auch mobile Computer geeignet. Mit dem Trennen der HS256 S3 vom PC bleiben die Daten, Programme und Betriebssysteme, inkl. temporärer Dateien ausschließlich auf der HS256 S3 verschlüsselt gespeichert und sind für Unbefugte unzugänglich.

8) Verwendung an allen Betriebssystemen

Die HS256 S3 funktioniert durch ihre Hardwareverschlüsselung unabhängig vom Betriebssystem und kann an jedem Gerät verwendet werden, das USB-Datenträger unterstützt.

9) Integration in bereits vorhandene Smartcard-Infrastrukturen in Unternehmen

Wird in einem Unternehmen bereits die Smartcard NXP J2E081_M64 R3, CC EAL 5 verwendet (z.B. Zutrittsmanagement, Nutzerauthentisierung etc.), ist eine Integration der HS256 S3 möglich. Außerdem können weitere Funktionen in die Smartcard integriert werden.

10) Integration von bestehenden Softwarelösungen

Alle im Unternehmen bereits existierenden Softwarelösungen können weiterhin ergänzend verwendet werden, um die Sicherheitseigenschaften und Verwendungsmethoden zu erweitern.

11. Technische Spezifikationen

Transferrate:	USB 3.0 max. 5 GBit/s USB 2.0 max 480 MBit/s
Smartcard:	NXP J2E081_M64 R3, CC EAL 5, JCOP v2.4.2 R3, (NSCIB-CC-13-37761-CR2) mit installiertem DIGITTRADE HS256 S3 Java Card Applet v1.1.0
Verschlüsselung:	256-Bit AES Hardwareverschlüsselung, XTS-Modus, mit 2 x 256-Bit Krypto-Schlüssel

Interne Datenträger:

Die verschlüsselten Daten werden auf internen 2,5 Zoll SATA HDD- oder SSD-Datenträger von Samsung (bevorzugt), Seagate, Western Digital oder Toshiba gespeichert.

Folgende Speichergrößen sind verfügbar: 120GB SSD, 160GB HDD, 250GB SSD, 320GB HDD, 500GB HDD/SSD, 640GB HDD, 750GB HDD/SSD, 1TB HDD/SSD, 1,5TB HDD/SSD, 2TB HDD/SSD, 4TB HDD/SSD.

Die Umrechnung von Byte zu KByte, MByte und GByte erfolgt von Computern und Festplattenherstellern unterschiedlich. Die Festplattenhersteller rechnen im metrischen Zahlensystem (1 KByte = 10^3 Byte = 1000 Byte) und Computer verwenden auf Grund ihrer Bauweise das Dualsystem (1 KByte = 2^{10} Byte = 1024 Byte). Daraus ergeben sich folgende Unterschiede bei der Darstellung der Speicherkapazität:

Kapazität lt. Hersteller	verfügbare Kapazität
120 GB	111,76 GB
160 GB	149,01 GB
250 GB	232,80 GB
320 GB	298,08 GB
500 GB	465,66 GB
640 GB	596,03 GB
750 GB	698,49 GB
1.000 GB	931,32 GB
1.500 GB	1.396,98 GB
2.000 GB	1.862,64 GB
4.000 GB	3.725,29 GB

12. Fehlersuche

Sollte die DIGITTRADE High Security HS256 S3 HDD/SSD einmal Fehler aufweisen, gehen Sie bitte folgende Checkliste durch. Bestehen die Probleme weiterhin, können Sie gern den technischen Support von DIGITTRADE kontaktieren.

Problem	Merkmale	Lösung
Das Eingabefeld ist nicht eingeschaltet	das Keypad ist nicht beleuchtet	Prüfen Sie, ob die USB-Anschlüsse der HS256 S3 und des Computers fest miteinander verbunden sind.
	die„ERROR"-LED blinkt	Prüfen Sie, ob eine gültige Smartcard eingelegt wurde und die Ausrichtung korrekt ist. Die Smartcard muss mit den Kontakten nach unten eingeschoben werden.
Die Sicherheitsabfrage ist fehlgeschlagen	die „ERROR"-LED blinkt	Eine falsche PIN wurde eingegeben. Drücken Sie die „ESC"-Taste um die Sicherheitsabfrage erneut zu starten. (Sie haben max. 8 Versuche).
Das Laufwerk wird nicht erkannt	Laufwerkssymbol wird nicht angezeigt	Stellen Sie sicher, dass die HS256 S3 nicht mit einem USB-Hub oder einem Verlängerungskabel angeschlossen ist.
	fehlende Formatierung/ Partition oder nicht lesbares Dateisystem	Lesen Sie dazu die Kapitel „Initialisierung/ Partitionierung und Formatierung unter..." für weitere Informationen.

Problem	Merkmale	Lösung
Das Laufwerk wird nicht erkannt	es wird ein minder-wertiges USB-Kabel verwendet	Verwenden Sie bitte das im Lieferumfang enthaltene USB-Kabel und verbinden Sie den USB-Stecker mit Ihrem System.
Das Laufwerk arbeitet langsam	Anschluss über USB	Bitte prüfen Sie, ob die HS256 S3 mit einer USB Schnittstelle verbunden ist.
	ein anderes USB-Kabel wird verwendet	Verwenden Sie bitte das im Lieferumfang enthaltene USB-Kabel und verbinden Sie den USB-Stecker mit Ihrem System.
	inkorrekter Anschluss	Prüfen Sie, ob der USB Anschluss fest mit dem USB Anschluss Ihres Computers verbunden ist.
	die HS256 S3 wurde über einen USB-Hub angeschlossen	Stellen Sie sicher, dass die HS256 S3 nicht mit einem USB-Hub oder einem Verlängerungskabel angeschlossen ist.
	es sind andere Geräte mit gleichem Anschluss verbunden	Entfernen Sie bitte alle anderen USB-Geräte und beobachten Sie, ob das Laufwerk anschließend schneller arbeitet.

13. Datensicherheit und Haftungsausschluss

Wir empfehlen, die auf der DIGITTRADE High Security HS256 S3 HDD/SSD befindlichen Daten regelmäßig auf anderen Speichermedien zusätzlich zu sichern. Dies schützt Sie vor einem vollständigen Datenverlust. Die DIGITTRADE GmbH haftet nicht für den Verlust von Daten sowie dadurch entstehende Kosten und Schäden. Zudem trägt das genannte Unternehmen keine datenschutzrechtliche Verantwortlichkeit der gespeicherten Daten.

14. Datenschutzgerechter Umgang mit der HS256 S3

Bitte beachten Sie bei der Speicherung personenbezogener Daten folgende Grundsätze und Anforderungen des Bundesdatenschutzgesetzes (BDSG), der Landesdatenschutzgesetze sowie die entsprechenden Vorgaben der EG-Datenschutz-Richtlinie (95/46/EG):

1) Verbot mit Erlaubnisvorbehalt:
Nach §4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Ähnliches gilt im Hinblick auf Artikel 7 der EG-Datenschutzrichtlinie, wonach die Verarbeitung von personenbezogenen Daten unter einer der folgenden Voraussetzungen zulässig sein soll:

a) die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;
b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;
c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;
f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

2) Datenvermeidung und Datensparsamkeit (§3a BDSG):
Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten bei öffentlichen und nichtöffentlichen Stellen ist nach §3a BDSG an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind dabei Daten – soweit möglich – zu anonymisieren und zu pseudonymisieren.

Bitte bedenken Sie diesen Aspekt bei der Erstellung der Sicherheitskopien. Die alten Backups sollen in regelmäßigen Abständen mit den aktuellen Daten überschrieben werden, anstatt stets neue zu erstellen. Um eine vollständige Löschung der alten Daten vor dem Erstellen eines neuen Backups zu erreichen, wird empfohlen, zuvor den Verschlüsselungsschlüssel zu ändern und die Festplatte mit dem neuen Schlüssel voll zu formatieren.

3) Transparenz und Zweckbindung:
Die betroffene Person ist bei Erhebung bzw. erstmaliger Speicherung oder Übermittlung personenbezogener Daten gem. §§ 4 Abs. 3, 19a und 33 BDSG zu informieren. Gleiches regeln Artikel 10 f. der EG-Datenschutzrichtlinie. Zudem ist bei der Verarbeitung personenbezogener Daten der Grundsatz der Zweckbindung zu beachten (vgl. insbesondere Artikel 6(b) EG-Datenschutzrichtlinie).

4) Besondere Arten personenbezogener Daten:
Nach Artikel 8 der EG-Datenschutzrichtlinie ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben grundsätzlich untersagt.

Eine Verarbeitung dieser Daten ist jedoch dann erlaubt, wenn dies z.B. für das Arbeitsverhältnis oder zum Schutz lebenswichtiger Interessen erforderlich ist. Ferner ist eine Verarbeitung dieser Daten erlaubt, wenn der Betroffene die Daten selbst veröffentlicht hat, diese zur Geltendmachung von Ansprüchen vor Gericht erforderlich sind oder eine Verarbeitung der Daten im Rahmen der medizinischen Versorgung/ Gesundheitsversorgung erforderlich ist.

Entsprechende Regelungen finden sich auch in §28 Abs. 6-9 BDSG.

5) Betroffenenrechte:
Nach §19, 20, 34 und 35 BDSG haben Betroffene ein Recht auf Auskunft, Berichtigung und Löschung oder Sperrung im Hinblick auf die zu ihrer Person gespeicherten Daten.

Gleiches gilt auch nach Artikel 12 der EG-Datenschutzrichtlinie, wonach jedem Betroffenen ein Auskunftsrecht und je nach Fall auch Berichtigungs-, Löschungs- oder Sperrungsansprüche zustehen, sofern die Verarbeitung nicht den Vorgaben der EG-Datenschutzrichtlinie entspricht.

Ferner gibt es nach Artikel 14 der EG-Datenschutzrichtlinie auch ein Widerspruchsrecht des Betroffenen bei einer Datenverarbeitung, wenn überwiegende, schutzwürdige, sich aus ihrer besonderen Situation ergebende Gründe für den Betroffenen bestehen.

6) Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§42a BDSG):
Bei besonders schutzbedürftigen, in §42a Abs. 1 BDSG näher bezeichneten Datenarten besteht grundsätzlich eine Verpflichtung der verantwortlichen Stelle, die Betroffenen über den Datenverlust zu informieren. Ferner ist die zuständige Aufsichtsbehörde unverzüglich über den Vorfall zu informieren.

7) Bußgeldvorschriften:
Die unbefugte Erhebung, Verarbeitung und Nutzung personenbezogener Daten kann nach §43 BDSG mit Bußgeldern von bis zu 300.000,00 € geahndet werden. Im Falle einer vorsätzlichen Begehung bestimmter Bußgeldtatbestände kann zudem eine Straftat vorliegen, die nach §44 BDSG mit einer Freiheitsstrafe bis zu zwei Jahren oder mit einer Geldstrafe geahndet werden kann.

15. Sicheres Beenden nach Benutzung der HS256 S3

Aus Sicherheitsgründen ist eine logische oder physikalische Trennung der Festplatte nach der Benutzung vom Wirtssystem durchzuführen. Dies empfiehlt sich vor allem bei Beendigung, kurzfristiger Unterbrechung sowie beim Verlassen des Arbeitsplatzes.

Die logische Trennung wird durch die Entfernung der Smartcard aus dem Festplattengehäuse erreicht. Diese Funktion steht im aktivierten Lock-Out Modus zur Verfügung, welcher vom Hersteller bei der Auslieferung voreingestellt ist und als Standard-Modus für die sichere Benutzung der DIGITTRADE HS256 S3 gilt.

Für die sichere physkialische Trennung müssen alle Verbindungen von der HS256 S3 entfernt werden.

Hinweis: *Um Datenverlust zu vermeiden, vergewissern Sie sich vor Trennung der Verbindungen, dass die Datenübertragung sowie die Zugriffe auf die Festplatte vollständig abgeschlossen sind.*

16. Aufbewahrung der Smartcard

Zum Lieferumfang der DIGITTRADE HS256 S3 gehören jeweils zwei Smartcards. Bitte bewahren Sie Ihre Smartcards getrennt von der Festplatte auf! Damit gewährleisten Sie einen zusätzlichen Schutz für Ihre Daten.

Bei Defekt einer Smartcard können Sie mit Hilfe der HS256 S3 und einer neuen, von DIGITTRADE zugelassenen Smartcard, eine Kopie der funktionsfähigen Smartcard erstellen. Hinweise dazu finden Sie in Kapitel 5.3. Kompatible Smartcards erhalten Sie über DIGITTRADE.

Bei Verlust einer Smartcard sollten Sie aus Sicherheitsgründen die HS256 S3 mit zwei Smartcards, die zwei neue kryptografische Schlüssel enthalten, betreiben. Neue Smartcards erhalten Sie über DIGITTRADE. Diese können Ihnen bereits mit zwei kryptografischen Schlüsseln beschrieben oder ohne Schlüssel zur eigenen Schlüsselgenerierung an der HS256 S3 zur Verfügung gestellt werden.

Zudem ist es notwendig, den alten Kryptoschlüssel vollständig zu zerstören. Die erforderlichen Schritte finden Sie im Kapitel 4.2 (3). Bei Defekt oder Verlust beider Smartcards besteht keinerlei Möglichkeit, auf die Daten zuzugreifen. Um die Festplatte weiter nutzen zu können, benötigen Sie mindestens zwei neue, von DIGITTRADE zugelassene Smartcards. Sie können mit diesen, wie in Kapitel 4.1 beschrieben, Ihren eigenen kryptografischen Schlüssel erstellen und die HS256 S3 mit diesem neu generierten betreiben.

Bei der Initialisierung der Smartcards wird die Festplatte formatiert und die darauf befindlichen Daten werden unwiderruflich gelöscht. Wenden Sie sich bitte bezüglich neuer Smartcards und bei Fragen an den Support der DIGITTRADE GmbH.

Hinweis: *Merken Sie sich Ihre Geräte-PIN. Ohne diese ist die Initialisierung neuer Smartcards und somit die weitere Benutzung der HS256 S3 nicht möglich.*

Merken Sie sich den Aufbewahrungsort Ihrer Smartcards und die dazugehörigen PINs, da ohne diese kein Zugriff auf die Daten möglich ist. Um die HS256 S3 mit den neuen Smartcards ebenfalls innerhalb des Geltungsbereichs der BSI-Zertifizierung zu verwenden, führen Sie die Schritte von Kapitel 1 durch.

17. Lieferumfang

- DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD) Version 1.0
- Zwei Smartcards NXP J2E081_M64 R3 mit installiertem DIGITTRADE HS256 S3 Java Card Applet version 1.1.0
- Benutzerhandbuch "DIGITTRADE High Security HS256 S3"
- USB-Kabel
- Slimcase

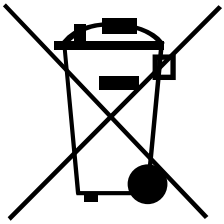
Hinweis: *Zur exakten Identifizierung sind die Bestandteile HS256 S3 (Gerät), Smartcards und das Benutzerhandbuch jeweils mit der eindeutigen Produktbezeichnung und Produktversion "DIGITTRADE High Security HS256 S3 Version 1.0" gekennzeichnet. Die zertifizierten Speicherkonfigurationen der DIGITTRADE HS256 S3 finden Sie in Kapitel 11.*

18. Hinweis zum Schutz und Erhalt der Umwelt

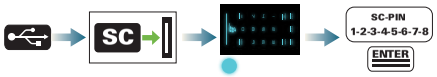
Gemäß der EG-Richtlinie dürfen Elektro- und Elektronik-Altgeräte nicht als kommunale Abfälle entsorgt werden.

Um die Verbreitung der enthaltenen Bausubstanzen in Ihrer Umgebung zu vermeiden und natürliche Ressourcen zu sparen, bitten wir Sie, dieses Produkt nach Ablauf seiner Lebensdauer ausschließlich an einer lokalen Altgerätesammelstelle in Ihrer Nähe abzugeben.

Dank dieser Maßnahmen können die Materialien Ihres Produktes umweltfreundlich wiederverwendet werden.

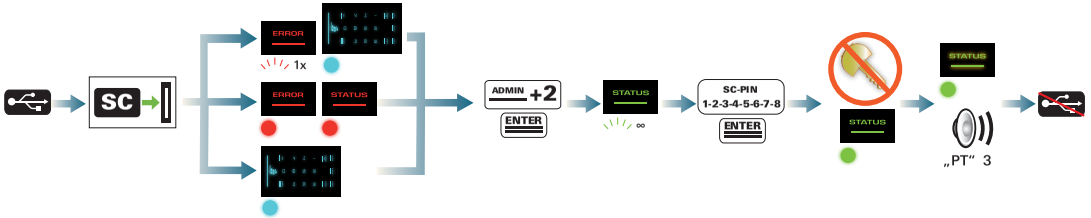


Anmeldevorgang der HS256 S3

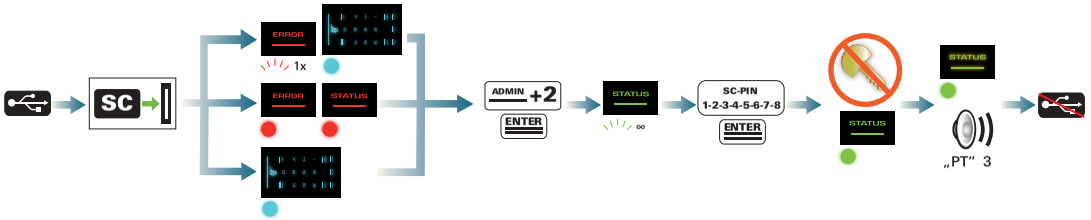


Ändern der Smartcard-PIN

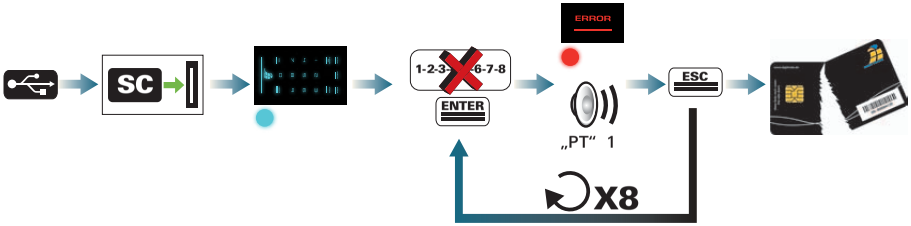
Erstellen von kryptografischen Schlüsseln



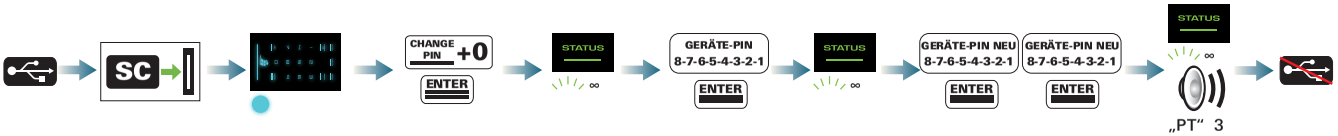
Zerstören von kryptografischen Schlüsseln (Smartcard-PIN bekannt)



Zerstören der kryptografischen Schlüssel (Smartcard-PIN unbekannt)

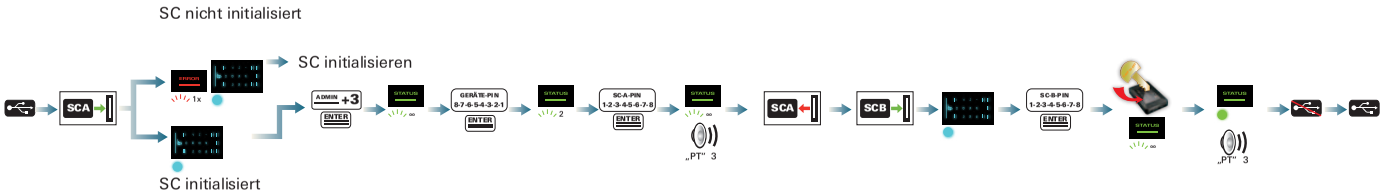


Ändern der Geräte-PIN

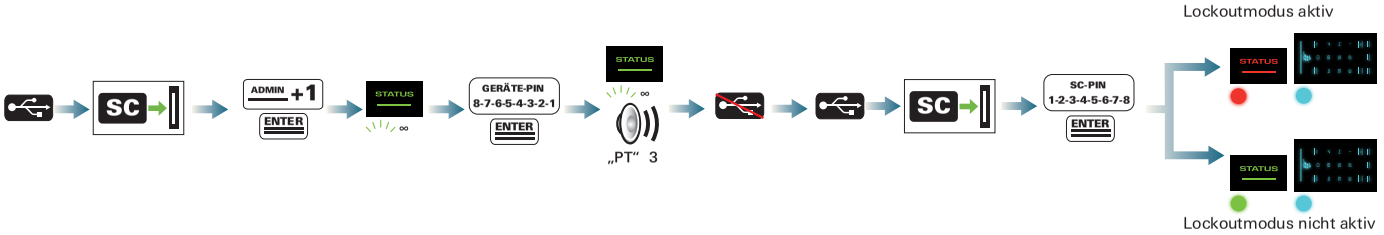


Initialisieren einer neuen Smartcard

Kopieren der kryptografischen Schlüssel



Aktivieren/Deaktivieren des Lock-Out Modus



Verbinden Sie die HS256 S3 mit Ihrem PC

Trennen Sie die HS256 S3 von Ihrem PC

Konnektor

Stecken Sie die Smartcard in den Smartcard-Steckplatz

Stecken Sie die Smartcard A in den Smartcard-Steckplatz

Stecken Sie die Smartcard B in den Smartcard-Steckplatz

Ziehen Sie die Smartcard A heraus

Die Smartcard ist gesperrt und kann nicht mehr verwendet werden

Geben Sie die Smartcard-PIN auf dem Keypad ein

Geben Sie die neue Smartcard-PIN auf dem Keypad ein

Geben Sie die Geräte-PIN auf dem Keypad ein

Geben Sie die neue Geräte-PIN auf dem Keypad ein

Falscheingabe der Smartcard-PIN

Drücken Sie die Tasten “CHANGE PIN“ und „0“ nacheinander (für 0 und 1 entsprechend)

Drücken Sie die Tasten „ADMIN“ und „0“ nacheinander (für 1,2 und 3 entsprechend)

Drücken Sie die Taste „ENTER“

Drücken Sie die Taste „ESC“

Das Keypad leuchtet

Die „STATUS“-LED...

...blinkt 1 mal grün

...blinkt mehrmals grün

...leuchtet grün

Die „STATUS“-LED und / oder „ERROR“-LED...

...blinkt 1 mal rot

...leuchtet rot

„PT“ X

Es ertönen „X“ Pieptöne hintereinander (X= Anzahl der Pieptöne)

Die kryptografischen Schlüssel werden auf die Smartcard geschrieben

Die kryptografischen Schlüssel werden zerstört

Führen Sie diesen Schritt achtmal hintereinander durch

PLEASE READ THE USER MANUAL CAREFULLY AND FOLLOW THE INSTRUCTIONS.

MISUSE CAN LEAD TO DAMAGE AND\OR DATA LOSS OF THE DIGITTRADE HIGH SECURITY HS256 S3 (EXTERNAL ENCRYPTED HDD/SSD).

PLEASE MAKE SURE THAT THE WARRANTY SEAL AND THE SECURITY PACKAGING HAVE NOT BEEN DAMAGED. ESPECIALLY PAY ATTENTION TO THE SECURITY LETTERING “DIGITTRADE SECURITY” ON THE SIDES OF THE SECURITY PACKAGING (SEE CHAPTER 1.8)

The digital copy of the user manual can be downloaded from www.digittrade.de at the download-center.

product version:	DIGITTRADE High Security HS256 S3 (encrypted HDD/SSD) version 1.0
user manual version:	1.8 (08.10.2020)

Table of Content

1. About the DIGITTRADE HS256 S3 **55**
1.1 Encryption 56
1.2 User authentication 56
1.3 Administrating the cryptographic keys 57
1.4 The Smartcard 57
1.5 Extra features 58
1.6 Overview of the most important features 58
1.7 DIGITTRADE HS256 S3 benefits 59
1.8 Security packaging and security seals 59

2. Control panel and USB port **61**

3. Getting started with the HS256 S3 **62**
3.1 Inserting the smart card 63
3.2 Entering the smart card PIN 63
3.3 Changing the smart card PIN 65

4. Administrating the cryptographic keys with the smart card **66**
4.1 Creating the cryptographic keys 66
4.2 Deleting the cryptographic key 67

5. Device PIN features **69**
5.1 Changing the device PIN 69
5.2 Activating/deactivating of the lock-out mode (Device PIN needed) 70
5.3 Copying the cryptographic keys
(Device PIN needed) 71
5.4 Initializing a new smart card (Device PIN needed) 73

6. Initializing/partitioning and formatting with Windows **74**

7. Initializing/partitioning and formatting with
Mac OS X **80**

8. Initializing/partitioning and formatting with Linux **82**

9. The correct file system **85**

10. Possible usage of the DIGITTRADE HS256 S3 **86**

11. Technische Spezifikationen **91**

12. Troubleshooting **92**

13. Data security and disclaimer **93**

14. Appropriate handling of the HS256 S3 for data privacy **94**

15. Safe shutdown after using the HS256 S3 **96**

16. Smart card storage **96**

17. Product contents **97**

18. WEEE Statement **97**

19. Functions diagram **98**

1. About the DIGITTRADE HS256 S3

The DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD) enables the privacy-compliant storage and keeping as well as the safe transport of personal data. Thanks to the security features it is one of the safest solutions to save mobile data.

From the point of the stored data the DIGITTRADE HS256 S3 is secure from unauthorized access even in the case if it will be lost, misplaced or stolen as well as from digital and physical attacks.

The DIGITTRADE HS256 S3 is delivered completely pre-set and is ready to use for the data storage. In the BSI-certified configuration, the user is only allowed to use the hard drive, after he has changed the smart card PIN, the encryption key on the smart card has been generated by himself and the smart card has been initialized.

To use the whole security properties of the HS256 S3 and according to the BSI certification, the following steps are besides necessary:

- Ensure that your host system has a proper protection of all data retrieved from the protected storage of the DIGITTRADE HS256 S3
- Make sure that no malware can be transferred to the hard drive
- Check the security package after the receiving (chapter 1.8)
- Check the range, the completeness and the correctness of the delivery (chapter 17)
- Check all functions of the device after the first start (chapter 3)
- Change the smart card PIN (chapter 3.3)
- Change the device PIN (chapter 5.1)
- Create a new cryptographic keys (chapter 4.1)
- Initialize the smart card with the new cryptographic keys on the HS256 S3 and format the hard drive afterwards (chapter 5.4, 6-9)
- Copy the cryptographic keys on other delivered smart cards (chapter 5.3)
- Check if the login is possible with all smart cards
- Check continuously that the lock-out mode is activated (chapter 5.2)
- For effectively destruction of the encryption key the key must be deleted from all smart card that contains the key. Alternatively the whole hard drive must be overwritten by a new encryption key. (chapter 4.2)
- Keep your authentication data confidential
- The encryption key of the smart card must be used by one hard drive only

Detailed description of the above-named steps is outlined in relevant chapters of this manual.

The information about the type, version and serial number of the hard drive are located on the back of each HS256 S3. Because the hard drive is not updatable, this information is sufficient for determining the version of the delivered HS256 S3.

The DIGITTRADE HS256 S3 ensures the safety of the data through the following security mechanisms:

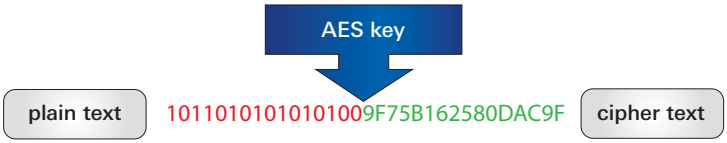
- Encryption
- User authentication
- Administration of the cryptographic keys

1.1 Encryption

- 256 bit AES full disk hardware encryption in XTS mode

The encryption module inside the secure casing encrypts the hard drive/SSD completely. Every saved byte and every written sector on the hard drive/SSD are encrypted according to 256 bit AES (Advanced Encryption Standard) in XTS mode with two 256 bit cryptographic keys.

The DIGITTRADE HS256 S3 encrypts additionally to all stored data temporary files as well as areas that would normally be unnoticed by encryption software.



1.2 User authentication

- 2-factor authentication using smart card and PIN

The user authentication is based on the principal “having and knowing”.

To get an access to the data the user must have the smart card and need to know the correct 8-digit PIN.

If the 8-digit PIN was entered incorrectly 8 times, the smart card is disabled and no longer usable. The cryptographic keys is also irreversibly deleted.

1.3 Administrating the cryptographic keys

With the device PIN the user can copy the cryptographic keys to another smart card, initialize new smart cards on the HS256 S3 and manage the lock-out mode. Instructions to this can be found in chapter 5.

In particular usage scenarios the knowledge of the smart card PIN and the device PIN can be split between two people, with the intention that only one person knows the device PIN and the other one smart card PIN. Knowledge of device PIN only will not enable the individual access to the data.

The cryptographic keys needed for de- and encrypting of the data is externally created and saved encrypted.

This means there is a physical separation between the encrypted data and the cryptographic keys, which makes it impossible to read the cryptographic keys from the DIGITTRADE HS256 S3. After the PIN has been correctly entered the cryptographic keys is transferred to the encryption module of the HS256 S3 to de-/encrypts the data. The external storage of the cryptographic keys enables a number of possible applications which are described in chapter 10.

1.4 The Smartcard

Serially the HS256 S3 works with two java based and Common Criteria EAL5 certified smart cards (NXP J2E081_M64 R3, CC EAL 5). For the use according with the BSI certification only these NXP smart cards are permitted.

These smart cards enable the creating, copying, changing and destroying of the cryptographic keys in use. The administration of the keys is supported by the DIGITTRADE HS256 S3 applet.

For the login on the hard drive are both smart cards needed with the the same cryptographic keys. The smart card PIN can be set differently for each smart card.

The type and the serial number of each smart card are displayed on the front of the smart card. The DIGITTRADE HS256 S3 version number is plotted on the back.

The permitted smart cards can be ordered separately at DIGITTRADE. These will be delivered without the cryptographic keys and have the factory set PIN (see chapter 3.2). To activate new smart cards, please refer to chapter 4.1, 5.3 and 5.4.

Warning: *If an invalid or defective smart card is inserted in the associated slot the "ERROR"-LED will flash three times and illuminate then permanently red. At these findings and accordingly if a smart card behave abnormally or if you identify defects during each operation, please contact DIGITTRADE.*

1.5 Extra features

The 2.5 inch built-in data storage device makes the HS256 S3 small and handy. The optional usage of SSD storage devices makes it shock proof. The data transfer and power supply are solved by USB. The hardware encryption method makes it possible to use the storage device on any OS and occurs transparently.

Accessing the data occurs without the loss of reading/writing speed.

1.6 Overview of the most important features

- 256 bit AES full disk hardware encryption in XTS mode with two cryptographic keys
- 2-factor authentication by smart card and 8-digit PIN
- external and encrypted storage of the cryptographic keys
- creating, copying and deleting the cryptographic keys by the user
- hardware based encryption module
- data encryption of all saved bytes and written sectors
- bootable and independent of the used OS (support for all operating systems, multimedia devices and machines with USB storage device support)
- compatible with USB 3.0 and USB 2.0
- without the loss of reading/writing speed
- handy 2.5 inch format and robust metal enclosure

1.7 DIGITTRADE HS256 S3 benefits

- private and business data are safe from unauthorized access
- easy and safe handling using hardware encryption: connect, log in, use it
- all data are immediately saved with encryption
- no performance loss
- integration into existing smart card infrastructures within companies

1.8 Security packaging and security seals

To avoid manipulation, a special security package is used for the delivery of the DIGITTRADE HS256 S3 and smart cards as well as for additional deliveries of smart cards. The contents will be described on the package.

After receiving, please check the inviolacy of the security lettering “DIGITTRADE SECURITY” on the sides. In addition there is a specific safety closure at the top which shows every manipulation attempts.

On the following images you can see possible indicators:

That's the safety closure when it has been properly closed and not opened again. The blue band at the top of the safety closure and the pale yellow thermal strip is undamaged.

In extreme cold conditions (e.g. use of cold spray) the areas of the blue tape will seperate from the carrier material. The warning "STOP" is readable.

Through extreme heat (e.g. hair dryer), the pale yellow thermal strip turns red.

When using solvents, the blue color of the satey closure dissolves - manipulation is immediately visible.

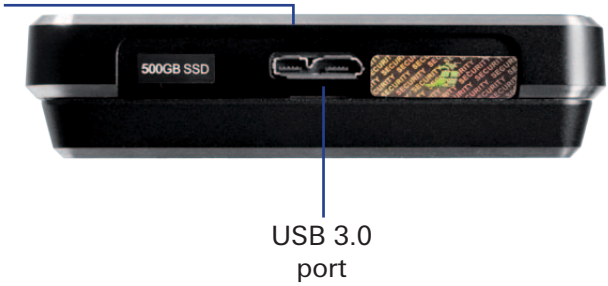
Please check if these indicators have been damaged or removed when you receive the product. Contact your seller if the the security packaging have been manipulated, since the security of the HS256 S3 cannot be guaranteed in this case.

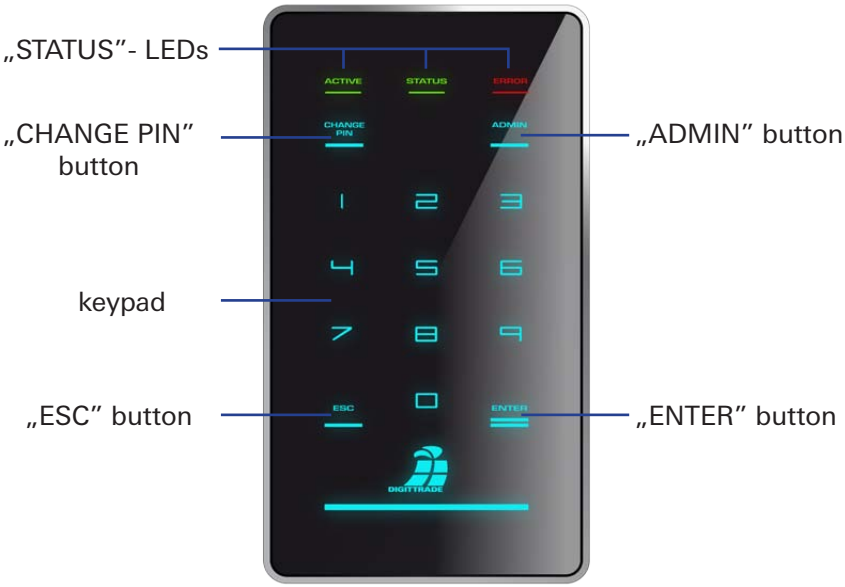
The components are sealed with epoxy resin. In addition there is a warranty seal placed on the opening point as seen below. This sealing is not evaluated by the BSI certification.

Additional warranty seals are inside of the HS256 S3.

2. Control panel and USB port

It is possible to connect the DIGITTRADE HIGH SECURITY HS256 S3 either using USB to the computer.





The HS256 S3 has three status-LEDs: "ACTIVE", "STATUS" and "ERROR".

Possible colors:
"ACTIVE"-LED: green light
"STATUS"-LED: green or red light
"ERROR"-LED: red light

Connect the HS256 S3 to your PC or laptop using the USB cable included in the delivery.

Not only the data will be transmitted through the USB cable but also the HS256 S3 will be energized.

Please make sure that the HDD is connected at all times directly to the USB plug of the PC or laptop.

Note: *Do not use the DIGITTRADE HS256 S3 via a buspowered USB hub or extension cable and ensure it has enough power.*

3. Getting started with the HS256 S3

The necessary power supply for the HS256 S3 is provided by USB.

If the HS256 S3 is connected correctly to the computer, the LED “ACTIVE”, “STATUS” and “ERROR” will flash at the same time.

Now the DIGITTRADE HS256 S3 is ready for use, but still needs to get unlocked.
For this, keep your smart card and smart card PIN ready.

Note: *For security reasons please use only original accessories.*

3.1 Inserting the smart card

After the DIGITTRADE HS256 S3 is ready for use it still needs to get unlocked.

To accomplish this, insert the smart card into the associated slot in direction of the arrow.

If an invalid or defective smart card is inserted in the smart card slot the "ERROR"-LED will flash three times and illuminates then permanently red. In that case please contact DIGITTRADE.

3.2 Entering the smart card PIN

After you have activated the DIGITTRADE HS256 S3 successfully and inserted a valid smart card, the keypad will be lighted and the HDD is ready for PIN entry.

Now you can type in the 8-digit PIN.

The preset factory PIN is:

"1-2-3-4-5-6-7-8".

after you entered the PIN, press the "ENTER" button.

Note: *To guarantee the safety of your data, it is very important to change the factory set PIN (page 65). Change the smart card PIN periodically. It is recommended to use different PINs for different smart cards. The numerical order must be kept confidentially.*

After successful PIN entry, the cryptographic keys are transferred to the encryption module and the "STATUS"-LED illuminates red. The DIGITTRADE HS256 S3 will be identified by the operating system as a removable device and the lighting of the keypad goes out. The "ACTIVE"-LED flashes during the data transfer.

The access is enabled now. The smart card must remain in the DIGITTRADE HS256 S3 whilst in operation. If the smart card will be removed from the slot, the storage device is locked (lock-out mode).
If necessary this function can be deactivated, so that the smart card can be removed after the authentication and you still will have access to the HS256 S3. The "STATUS"-LED illuminates green after successful PIN entry. Please find more information in chapter 5.2. Upon removal of the smart card, the "STATUS" LED turns off and the "ACTIVE" LED is green.

If a wrong PIN was entered, the red "ERROR"-LED flashes and it sounds an acoustic signal. Press the "ESC" button to restart the PIN entry.

Note: *After the PIN was entered eight times incorrectly, the smart card will be irrevocably locked and cannot be used anymore. The cryptographic keys on the smart card are irreversible deleted in the process.*

Note: *In the activated status the HS256 S3 must not be unattended to prevent unauthorized access. Please note, if you are leaving your workplace and if you are not using the DIGITTRADE HS256 S3, it should be locked correctly. All data transfers must be completed and the HS256 S3 must be seperated from the USB connector. If the lock-out mode is activated it is sufficient to remove the smart card from the associated slot.*

For security reasons it is recommended to hide traces upon entry that could allow conclusions about the use of PIN numbers. Possible methods can be:

1. Frequent cleaning of the keypad, so no fingerprints are visible.

2. Frequent tapping of all buttons, so fingerprints are spread evenly.

3. Using special stylus pens that do not leave marks on the surface of the keypad, such as the DIGITTRADE stylus pen.

3.3 Changing the smart card PIN

Follow these steps to change your smart card PIN:

1) Insert a working smart card into the associated slot (see chapter 1.4 and 3.1). The keypad illuminates.

Note: *If the keypad and the red "ERROR"-LED illuminate permanently, please initialize the smart card as described in chapter 5.4.*

2) Press the "CHANGE PIN" button and afterwards the "1" button.

3) Press "ENTER" to confirm. The "STATUS"-LED flashes green several times.

4) Type in the current 8-digit PIN and press "ENTER" to confirm the entry.

5) Type in the new 8-digit smart card PIN and press "ENTER" for confirmation.

6) To confirm, type in the new 8-digit smart card PIN again and press "ENTER".

After a successful PIN change, the "STATUS"-LED flashes green several times and it sounds an acoustic signal at the end. The DIGITTRADE HS256 S3 will be identified from the system as a removable device, the "STATUS"-LED illuminates red (in active lock-out mode) and the lighting of the keypad disappears.

The access to the hard drive is enabled.

If the PIN change was not successful, the red "ERROR" LED flashes and it sounds an acoustic signal. Press the "ESC" button and start again with the first step of the PIN change.

You have 8 attempts for changing the smart card PIN. After this the inserted smart card is locked and no longer usable.

Note: *1. The DIGITTRADE HS256 S3 only accepts 8-digit PINs. Do not use a trivial PIN like ascending or descing series of numbers or user-specific PIN like your phone number or date of birth.*
2. Please change the smart card PIN periodically during the use of the hard drive, plus after receiving the smart card and the transfer to another user.

4. Administrating the cryptographic keys with the smart card

The cryptographic keys are created and encrypted on a certified smart card. After the PIN has been correctly entered the cryptographic keys are transferred to the encryption module of the HS256 S3 to de-/encrypt the data. The cryptographic keys can be copied to other smart cards for using the storage device. The cryptographic keys can be created, changed or deleted using the smart card PIN.

The function of administrating the cryptographic keys (creating, destroying and copying) only works with smart cards that have the DIGITTRADE HS256 S3 Java Card Applet. The HS256 S3 is (by default) distributed with 2 of the following type of smart cards NXP J2E081_M64 R3, CC EAL 5.

Note: *The HS256 S3 is delivered preconfigured and ready-to-use. For security reasons it is very important that the cryptographic keys are changed and the smart cards are re-initialized for the HS256 S3.*

4.1 Creating the cryptographic keys

With the help of DIGITTRADE HS256 S3 the cryptographic keys can be created on a working smart card. The integrated certified random number generator creates random and safe cryptographic numbers.

Follow these steps to create cryptographic keys:

1) Insert a working smart card into the associated card slot (see chapter 1.4 and 3.1).

2) If the smart card has no cryptographic keys, the “ERROR“-LED as well as the “STATUS“-LED illuminate red.

If the smart card already has cryptographic keys that are not initialized for the HS256 S3, the red “ERROR“-LED and the keypad iluminate. The smart card is already initialized the key pad illuminates.

3) Press the “ADMIN“-button and afterwards “2“.

4) Press the “ENTER“-button. The “STATUS“-LED flashes green several times.

5) Type in your 8-digit smart card PIN and press “ENTER“ to confirm the entry.

Note: *If the PIN entry was not successful, the red “ERROR“-LED flashes. Press the “ESC” button and start again with the third step of creating the cryptographic keys. You have 8*

attempts for creating a new one. After this the inserted smart card is locked and no longer usable.

6) The "STATUS"-LED flashes green whilst the DIGITTRADE HS256 S3 is creating and writing the cryptographic keys to the smart card. If the process was successful, the "STATUS"-LED illuminates green and it sounds an acoustic signal.

7) Seperate the USB connection to the DIGITTRADE HS256 S3 to exit this feature.

The cryptographic keys have been created or changed. Now the prior cryptographic keys have been irreversibly deleted. With this smart card you do not have a longer access to the prior stored data. It's necesseary to create a data backup before. If you want to use these cryptographic keys with the HS256 S3, it has to be initialized for the HS256 S3. Please follow the steps in chapter 5.4.

Note: *Please do not remove the smart card during the creation of the cryptographic keys (step 6 "STATUS"-LED flashes* green *several times), otherwise the smart card could be damaged.*

4.2 Deleting the cryptographic key

1. There are two ways to delete the cryptographic keys.

a) Deleting the cryptographic keys by creating a new one

Please follow the steps in chapter 4.1. With this method the cryptographic keys can be quickly deleted without attracting attention in a dangerous situation as the process hardly differs from the normal log-on process. Now the access to the data with this smart card is even for the user impossible.

b) Deleting the cryptographic keys by entering the 8-digit PIN incorrectly 8 times

This method is more complex but can be done intuitive and without the knowledge of the smart card PIN. Please follow these steps:

1) Insert a working smart card into the associated slot (see chapter 1.4 and 3.1).

2) Type in a wrong 8-digit PIN and press "ENTER".

3) The red "ERROR"-LED flashes and it sounds an acoustic signal.

4) Press the “ESC”-button and execute the second step 7 times more.

5) If the wrong PIN had been entered 8 times, the cryptographic keys are destroyed and this smart card is locked and no longer usable.

2. In both cases, only the cryptographic keys are deleted on the respective smart card. The remaining data on the hard drive is not damaged and still stored encrypted. If the user has the second smart card with the appropriate cryptographic keys and valid PIN, he can access this data easily.

3. If one of the smart cards is lost, misplaced or stolen, it is necessary to destroy the cryptographic keys completely. Please follow these steps:

1) Start running the DIGITTRADE HS256 S3 (see page 62 and 63).

2) Back up all necessary data from the HS256 S3 to another storage device.

3) After this process is completed, disconnect the HS256 S3 and connect it again.

4) Now create new cryptographic keys (see chapter 4.1).

5) Initialize the smart card (see chapter 5.3).

6) Initialize and format the HS256 S3 with your OS (see chapter 6-8).

7) Overwrite the HS256 S3 completely with random data. After this process is completed, you can delete the random data and use the DIGITTRADE HS256 S3 normally.

Now any copies of the old cryptographic keys on other smart cards are useless.

5. Device PIN features

The device PIN does not allow the access to the stored data. With the help of this PIN you can execute the following administrative features:

- change the device PIN
- activate/deactivate the lock-out mode
- copy cryptographic keys
- initialize a new smart card for the DIGITTRADE HS256 S3

The preset factory device PIN is: "**8-7-6-5-4-3-2-1**". For security reasons, we recommend that you should change it. The device PIN must be kept confidentially. Therefore avoid the execution of the above functions on your hard drive by unauthorized persons.

The number of attempts to enter the device PIN is not limited.

Note: *Bear your device PIN in mind. Without this PIN the initialization of new smart cards and thus the use of more HS256 S3 is not possible.*

5.1 Changing the device PIN

Follow these steps to change the device PIN:

1) Insert a working smart card into the smart card slot (see chapter 1.4 and 3.1) Make sure that the keypad illuminates.

Note: *If the red „ERROR"-LED and the keypad illuminate, please initialize the smart card as described in chapter 5.4.*

2) Press the "CHANGE-PIN" button on the keypad and afterwards "0".

3) Confirm your entry with "ENTER".

4) Type in the current 8-digit device PIN and press "ENTER" to confirm the entry. The "STATUS"-LED flashes green twice.

5) Type in the new 8-digit device PIN and confirm with "ENTER".

6) For confirmation type in the new 8-digit device PIN again and press "ENTER".

7) During the change, the "STATUS"-LED flashes green several times and it sounds an acoustic signal at the end.

8) The smart card can be removed now. Disconnect the USB connection of the

DIGITTRADE HS256 S3 to exit this features.

If the PIN change was not successful, the red “ERROR“-LED will flash. Press the “ESC“ button and start again with the first step of the PIN change.

Note: *The DIGITTRADE HS256 S3 only accepts 8-digit PIN. The PIN should be chosen at random. Do not use a trivial PIN like ascending or descing series of numbers or user-specific PIN like your phone number or date of birth.*

5.2 Activating/deactivating of the lock-out mode (Device PIN needed)

In the activated lock-out mode access to the data is instantly stopped if the smart card is removed.

The HS256 S3 is preset with activated lock-out mode. The “STATUS“- LED illuminates red during the access mode. For a safe use of the HS256 S3 the lock-out mode must be activated. Using the HS256 S3 with deactivated lock-out mode is outside the scope of the BSI certification.

The user can deactivate this feature in particular situations. This must be done when only one smart card has access to many different storage devices that are supposed to be unlocked at the same time with the same cryptographic keys. When the lock-out mode is deactivated the “STATUS“-LED illuminates green during the access mode.

In that case please use the physical separation after the end of the use (chapter 15) because the logical separation is not possible in the deactivated lock-out mode.

Follow these steps to activate/deactivate the lock-out mode:

1) Insert a working smart card into the associated slot (see chapter 1.4 and 3.1). Make sure that the keypad illuminates.

Note: *If the “STATUS”-LED flashes green shortly and the red “ERROR”-LED illuminates permanently, please initialize the smart card as described in chapter 5.4.*

2) Press the “ADMIN“-button and afterwards “1“.

3) Press the “ENTER“-button. The “STATUS“-LED flashes green several times.

4) Type in your 8-digit device PIN and press “ENTER“. If the PIN was entered correctly, the “STATUS“-LED flashes green several times and it sounds an acousticsignal.

Note: *If the Keypad and the red “ERROR“-LED flashes press the “ESC” button and start again with the third step.*

5) The lock-out mode is now activated/deactivated now. The “STATUS“-LED illuminates red if the mode is activated and green if it is deactivated.

6) Disconnect the USB connection of the DIGITTRADE HS256 S3 to exit this feature.

Note: *The activated lock-out mode is preset. In this mode do **not** remove the smart card from the DIGITTRADE HS256 S3, as it can lead to data loss.*

5.3 Copying the cryptographic keys (Device PIN needed)

With this feature you can copy the cryptographic keys from one smart card to another. For this at least two smart cards are needed: the smart card that has the cryptographic keys that should be copied and one or more smart cards the cryptographic keys should be copied on.

Follow these steps to copy the cryptographic keys:

1) Insert a working initialized smart card into the associated slot (see chapter 1.4 and 3.1).

If the smart card is already initialized, the keypad illuminates. If the smart card has already cryptographic keys that are not initialized with the HS256 S3, the red “ERROR“-LED and the keypad iluminates. Initialize this smart card. (see chapter 5.4)

2) Press the “ADMIN“-button and then the “3“.

3) Press “ENTER“. The “STATUS“-LED flashes entered several times.

4) Type in your 8-digit device PIN and press “ENTER“. The “STATUS“-LED flashes entered twice. Enter the 8-digit PIN from smart card A and press “ENTER“.

Note:
1. If the PIN entry was not successful, the red “ERROR“-LED flashes. Press the “ESC” button and start again with the second step of copying the cryptographic keys.
2. The smart card A is automatically locked and rendered useless as soon as the 8-digit PIN was entered eight times incorrectly.

5) The “STATUS“-LED flashes green several times during the DIGITTRADE HS256 S3 reads the cryptographic keys from smart card A. After this process is completed the “STATUS“-LED illuminates green and it sounds an acoustic signal at the end.

6) Remove smart card A and insert smart card B into the smart card slot. Make sure that the keypad iluminates.

7) Enter the 8-digit PIN for smart card B and press “ENTER“.

Note:
1. If the PIN entry was not successful, the red “ERROR“-LED flashes. Press the “ESC” button and type in the PIN of smart card B again.
2. The smart card B is automatically locked and rendered useless as soon as the 8-digit PIN was entered eight times incorrectly.

8) The “STATUS“-LED flashes green several times when the HS256 S3 is writing the cryptographic keys to smart card B. If the process was successful, the “STATUS“-LED illuminates green and it sounds an acoustic signal.

9) To describe further smartcards with these cryptographic keys disconnect the hard drive and start again with step 1.

Note: *Do not remove the smart card during the reading/writing process (steps 5 and 8, the “STATUS“-LED flashes green several times), otherwise the mart card could be damaged.*

5.4 Initializing a new smart card (Device PIN needed)

Initialising a new smart card is necessary, if the cryptographic keys have been changed and the DIGITTRADE HS256 S3 has to operate with it (for example for security reasons if one or more smart cards are lost).

Whilst initialising a new smart card, the cryptographic keys are changed in the crypto-system. Therefore the HS256 S3 has to be reinitialized and reformatted by the user's OS afterwards. Now the access to the previous stored data is impossible with the new cryptographic keys.

Follow these steps to initialize a new smart card:

1) Insert a working smart card into associated slot (see chapter 1.4 and 3.1). Make sure that the red "ERROR"-LED and the green and the keypad illuminate.

2) Press the "ADMIN" button and afterwards "0".

3) Press "ENTER" to confirm. The "STATUS"-LED flashes green several times.

4) Type in your 8-digit device PIN and press "ENTER".

Note: *If the PIN entry was not successful, the red "ERROR"-LED flashes. Press the "ESC" button and start again with the third step of initialising a smart card.*

6) If the PIN was entered correctly, the "STATUS"-LED flashes green and it sounds an acoustic signal. The inserted smart card is initialized with this DIGITTRADE HS256 S3 now.

7) Disconnect the USB connection to the DIGITTRADE HS256 S3 to exist this feature.

8) Initialize and format your DIGITTRADE HS256 S3 with your OS. Follow the instructions in the following chapters.

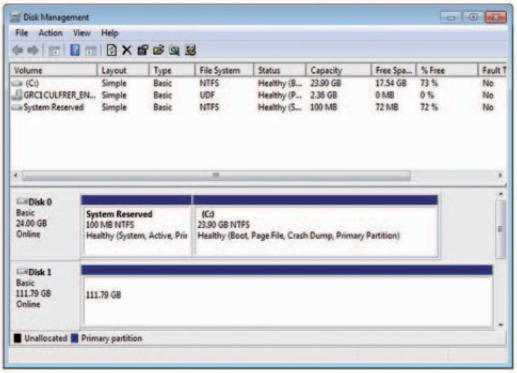
Note: *Keep your device PIN in mind. Without it the initialising of new smart cards is impossible as well as the regular use of your HS256 S3.*

6. Initializing/partitioning and formatting with Windows

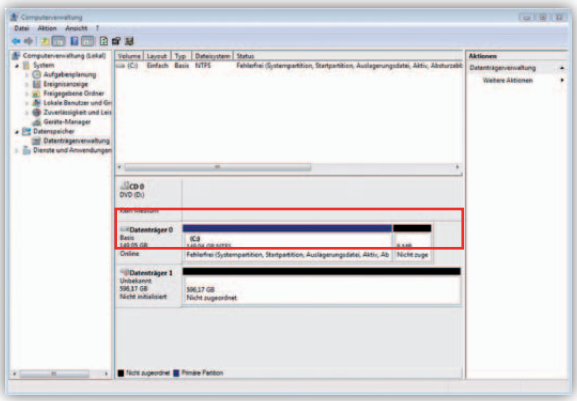
Follow these steps to initialize the DIGITTRADE HS256 S3 with Windows:

- Start running the DIGITTRADE HS256 S3 (see page 62 and 63).
- Enter Disk Management. Right-click on my computer and then click on manage. In Windows Vista or 7 click start, then right-click on my computer, choose manage and then click on Disk Management from the list.

- Here you will find an overview of the different drives:

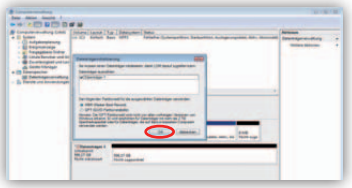


- After successfully initialization the HS256 S3 will be shown in the bottom area of the Disk Management window:



- If the Disk Management is opened for the first time since the HS256 S3 has been

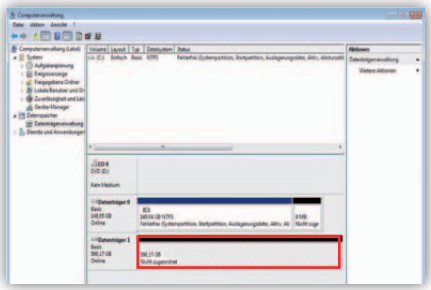
started, the following window will pop-up:



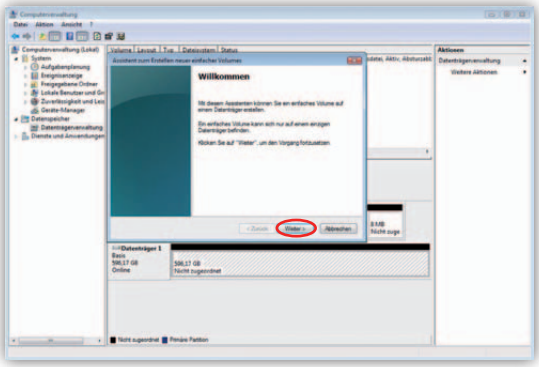
- Here you can initialize the drive by clicking “OK“.

Note: *In case the initialisation window does not automatically pop up, or it was ended by clicking “Cancel“, you can initialize the disk by right clicking on it in the list.*

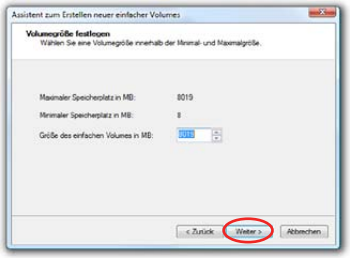
- The status should then change from “not initialized“ to “online“.



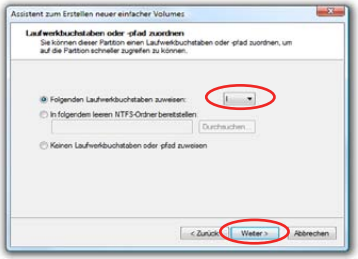
- Right click on the “unallocated“ area and choose “New simple volume“ in the menu. In the started assistant you can change all needed settings and format the drive.
- Click on “next“ to start the process



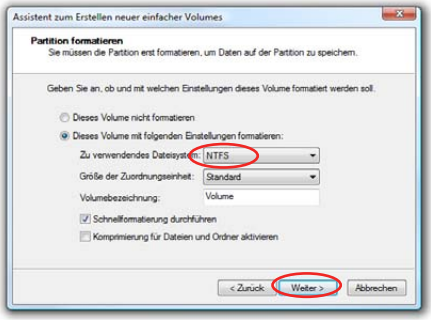
- Enter the desired size of the partition in MB and click “next“:



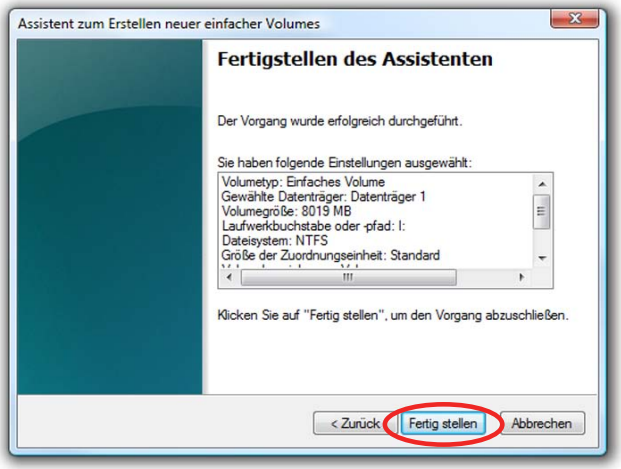
- You may assign a partition letter, then click on “next“:



- Now choose the file system and the type of formatting you would like to use and click “next“:

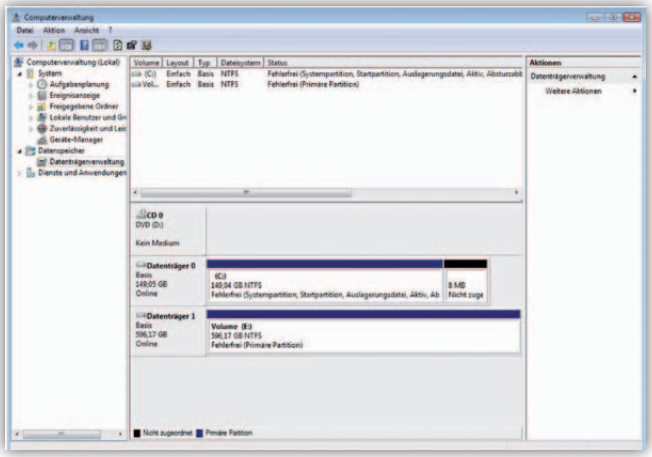


- Click “Done” to complete the formatting:



The duration of the formatting can vary depending on the size of the hard drive.

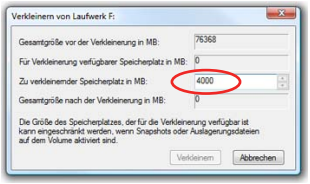
When formatting is completed the HS256 S3 will be shown as “healthy“ and can be used now:



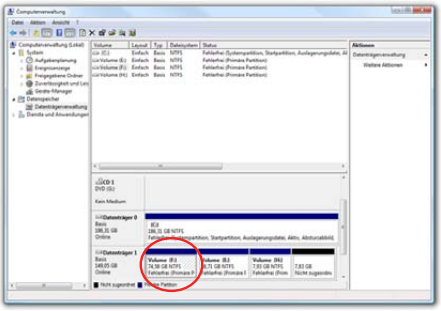
It is also possible to partition the DIGITTRADE HS256 S3 in more than one partition using the Disk Management.

Follow these steps to partition the HS256 S3:

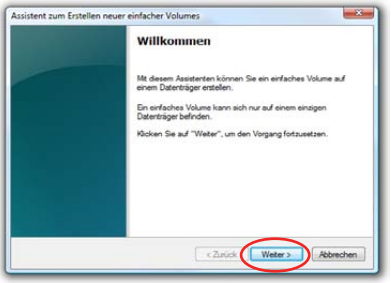
- Scroll to the HS256 S3 with your mouse and click right on it to open the context menu
- Choose “shrink volume“.
- Enter the desired size (in MB) the partition should be shrunk to:



- Then it will show an unlocated space in the management window:

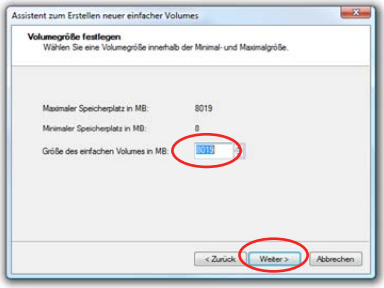


- Scroll to the unallocated space, click right and then choose “new simple volume” from the menu.
- The partition manager opens:

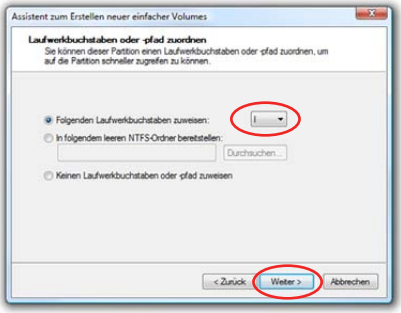


- Click “next” to continue.

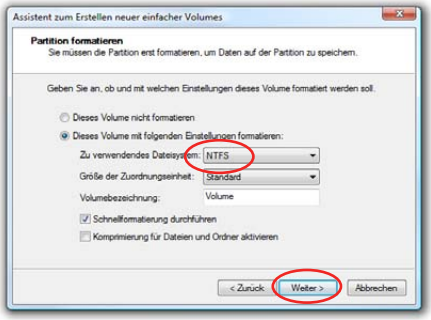
- Enter the desired size of the partition in MB and click “next“:



- You may give the partition a letter then click on “next“:

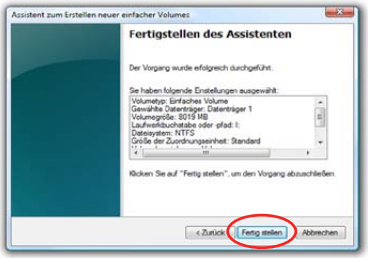


- Now choose the file system and the type of format you would like to use and click “next“:



- Then the format be comlplete, to continue click “done“:

Note: *The newly partitioned area is being formatted. After successfully partitioning, the new partition is automatically recognised by the system.*



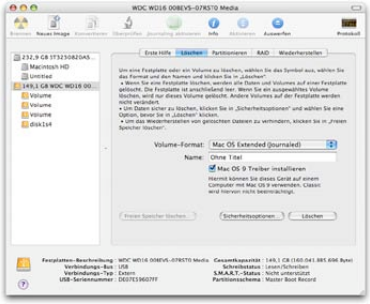
7. Initializing/partitioning and formatting with Mac OS X

- Start running the DIGITTRADE HS256 S3 (see page 62 and 63).

To manage external disks using a MAC you can use the “Disk Utility“. To open it go to “Programs“ and then “Utilities“.

- Choose the “Disk Utility“. The Disk Management for initialising, partitioning and formatting opens.

- Choose the HS256 S3 from the drive list on the left side. Under menu item “delete“ you can initialize and partition the HS256 S3.



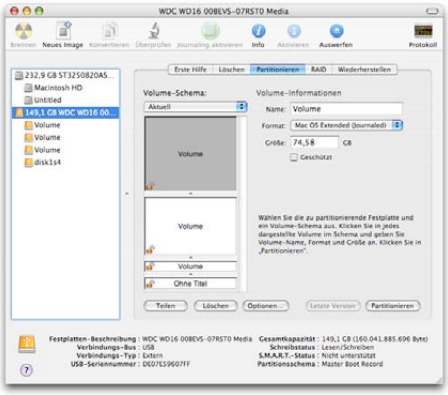
As well as giving the drive a name you can choose the file system to be used. For MAC

OS X you should use “Mac OS Extended (Journaled)“ and for the classic MAC OS 9 the HFS Format (Mac OS Extended).

- Confirm the initialization/formatting by clicking the “DELETE“ button.

To partition the HS256 S3 the “Disk Utility“ is also used. Click on the HS256 S3 and choose ”Partitioning“ you may also choose the size of the partitions.

- In the middle you can see how the disk is currently partitioned. Click on the pulldown menu “current“ right under “volume scheme“.
- Now you may choose the number of partitions you would like to have.
- After you have applied all of the partitions, you can decide the name and size of every partition under “Volume Information“.



- Now you can apply the settings by clicking “apply“.

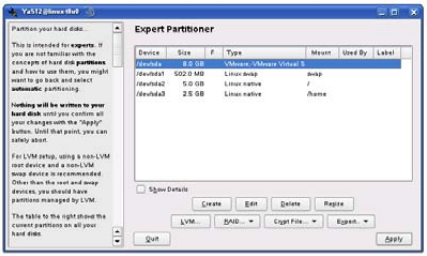
8. Initializing/partitioning and formatting with Linux

It is possible to partition the DIGITTRADE HS256 S3 in more than one partition using Linux. For this the correct file system has to be initialized first.
The process which is described here based on YaST from Suse Linux. The process is similar on other Linux distributions.

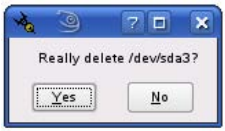
- Start running the DIGITTRADE HS256 S3 (see page 63 and 65).

Then open YaST. If necessary, you will need to authenticate yourself.

- Choose from the left side “System” and from the right field “Partitioner”.
- For security reasons a window will open and you will be asked whether you are familiar with the partitioning. Confirm this with “Yes”.
- The volume table of your system will appear.



- Now you can choose the desired volume, partition it, edit or delete already existing partitions.
- To delete the standard NTFS partition please click on it and afterwards on “Delete”.

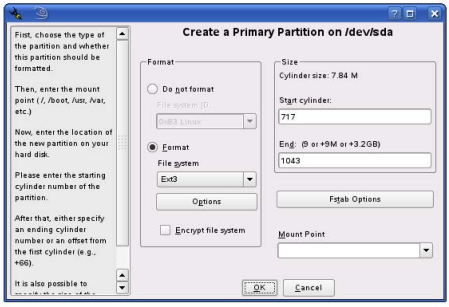


- You will be asked whether you really want to delete the partition. Make sure you have chosen the correct partition and confirm with a click on “Yes”.

Note: *If you delete the partition, you will delete irrevocably all files stored on it.*

- To create a new partition in the free space of your volume click on “Create”.

- Choose a volume to create the new partition.
- You will be asked which type of partition you want to create. It is recommended to use “Primary Partition”.



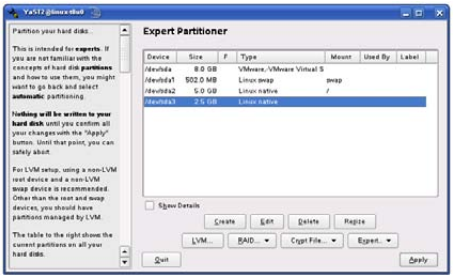
- In this window you configure all features of the partition. You can choose between

different file systems and sizes and if necessary you can configure a mountingpoint for Linux.

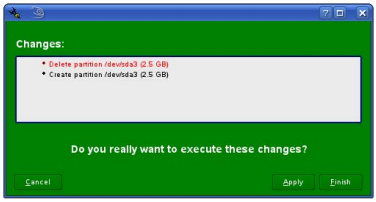
- Confirm your configuration with “OK”.

- Formatting works similarly. Choose the desired partition and click on “Edit”.
- Click on “Formatting” and choose the adequate file system. Confirm your configurations with “OK”.

-



- Click on “Apply” to operate your modifications.



- All modifications will be shown in a new window. Make sure that all modifiacations are correct and confirm the configurations by clicking on “Apply”.

Note: *If you are not sure which file system or partition size you should choose, we recommend taking the automatically entered values.*

9. The correct file system

The table below shows the compatibility between operating systems and file systems.

	NTFS	FAT32	HFS+	EXT3
Win 98	X	R, W	X	X
Win NT, 2000, ME, XP, Vista, 7, 8, 10	R, W	R, W	X	X
Mac OS X	R	R, W	R, W	X
Linux	R	R, W	X	R, W

description: R - read, W - write, X - no compatibility

You may be able to write data to file systems that are usually not compatible by using an external program.

At the time of the delivery the DIGITTRADE HS256 S3 is already formatted for you in the NTFS file system. In the chart above you can see the compatibility of the NTFS file system with your operating system. If NTFS does not work with your operating system, you will have to re-format the hard drive (chapter 6).

For Windows users we recommend NTFS. The most powerful file system for MAC OS X is HFS+ and for Linux you should use EXT3. The DIGITTRADE HS256 S3 can be formatted to any other file system, this does not affect the encryption of the data.

If you would like to use the hard drive with different operating systems, we suggest using the FAT32 file system, as it is supported by nearly all operating systems (Read/Write). However, there are restrictions to the file/partition size. Furthermore there are slight performance differences.

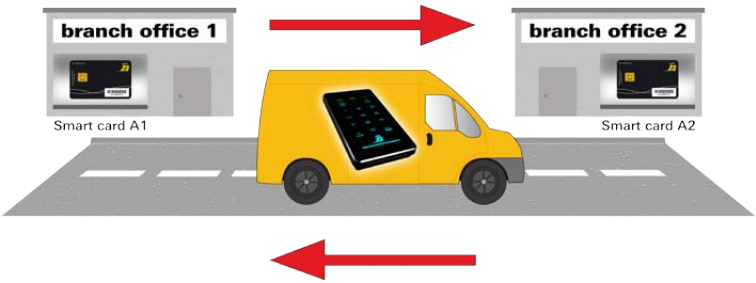
10. Possible usage of the DIGITTRADE HS256 S3

1) Secure and cost-efficient data transport

The HS256 S3 can be used to transport confidential data. For the dispatcher and recipient of the data, have a smart card with identical cryptographic keys. The dispatcher only sends the HS256 S3. As the cryptographic keys do not physically exist (it is on the smart cards), it cannot be read out during the transport. Additionally the HS256 S3 with confidential data can be sent cost-efficiently and insured by a postal service or courier.

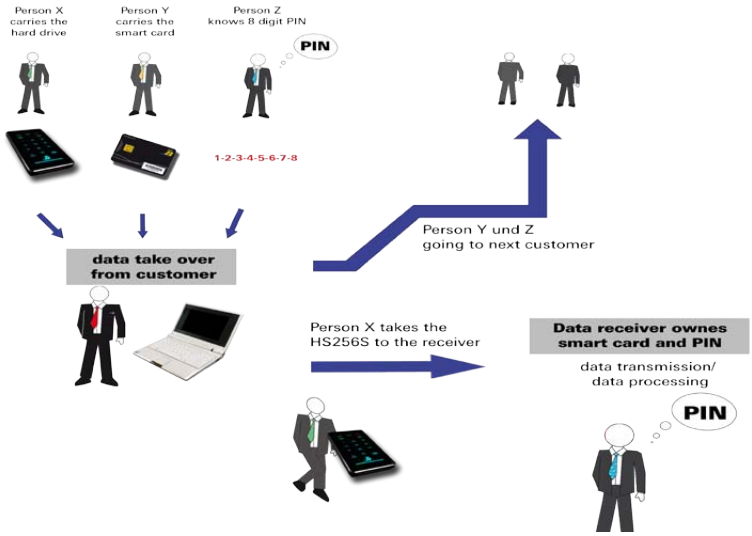
The dispatcher and recipient must check that the HS256 S3 has not been tampered during the transport. For this purpose it is recommended to use security packaging like described in chapter 1.8. This is also effective for all other transport possibilities of the HS256 S3.

For additional security, the use of multiple smart cards with different cryptographic keys, (deposited at the dispatcher and recipient) which can be used to decrypt or encrypt the data in a chosen sequence.



2) Data storage device & authentication separation

The access to the data can be regulated with help of three persons. Person X has the HS256 S3, Person Y has the smart card and person Z knows the smart card PIN. The three people only meet for the data transfer at the recipient and separate again afterwards. Persons X, Y and Z cannot gain access to the data on their own.



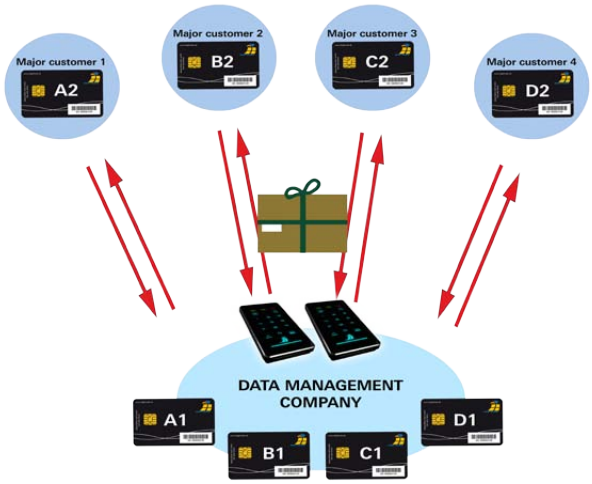
3) Using limited amount of storage devices for a wide range of customers

If a company (i.e. data processing company or data center for large companies or agencies) is in a constant exchange of data with many different data recipients, it can use the benefits of the HS256 S3 to transport data secure and cost-efficiently. Every recipient receives a smart card with his/her own cryptographic keys. The dispatcher has a copy of each of the cards with the cryptographic keys of every recipient.

For the transportation of data a smart card with the cryptographic keys of the recipient is initialized with the HS256 S3 (device PIN required).
Every HS256 S3 is suitable. Subsequently, the data dispatcher does a quick format of the HS256 S3 with the new cryptographic keys which only takes a few minutes. Complicated data deletion or overwriting is not necessary, as the data was encrypted with different cryptographic keys and could only be encrypted and restored by the owner of the old cryptographic keys provided the data has not already been overwritten.

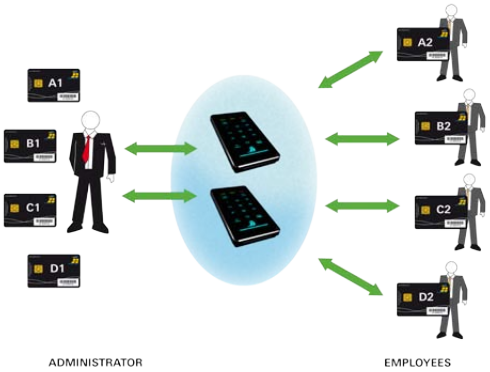
If data is supposed to be sent to the same recipient in short intervals there is no need to wait for a personalized HS256 S3 to return. Every HS256 S3 can be used. All you need to do is initialize it with the recipients cryptographic keys.

The amount can be reduced to the actual amount. Because not every recipient needs their own HS256 S3. It is irrelevant which of the company's HS256 S3 is available and used for transport. Crucial is which cryptographic keys have written the data to the HS256 S3.



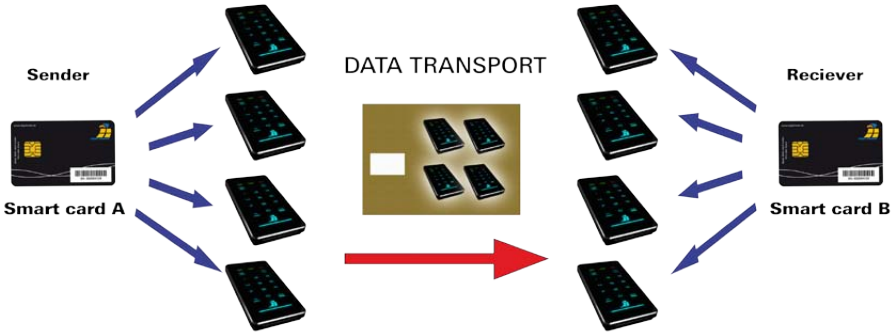
4) Using limited amount of storage devices in the field and public authorities

Within a company every Sales Representative can have his/her own personalised smart card (own cryptographic keys). For their work every employee receives their own HS256 S3 which has been priorly initialized. The employee saves the data with his/her cryptographic keys. After usage the employee gives the HS256 S3 back. Then it goes through a quick configuration and within minutes it is ready for the next employee. Therefore there is no need for a HS256 S3 for every employee and the actual amount of required storage devices is reduced to a minimum.



5) Operating multiple storage devices with a single smart card

To accomplish this multiple HS256 S3 have to be initialized with identical cryptographic keys. It is possible to generate cryptographic keys for one smart card which allows the access to several diffrent hard drives. It offers the advantage that one employee does not know varios numeric codes for the diffrent drives which he/she has an access for. It is only one PIN necessary. Even if the data are sent frequently, it provides a great solution for every time the data are dispatched and an other diffrent HS256 S3 can be used. A Waiting for the return of personalies HS256 S3 is unnecessary.



6) Deleting the cryptographic keys

The user has the possibility to delete the key without attracting attention in dangerous situations, given that he/she knows the PIN. In order to do this three additional buttons must be pressed. (Chapter 4.2)

Now the access to the data is impossible with this smart card and therefore also for the user.

Provided the smart card PIN is unknown, the cryptographic keys are also deleted by entering the 8-digit PIN wrong 8 times.

7) Bootability

Operating systems, programs and data can be saved to the HS256 S3. This usage is compatible with stationary as well as mobile computers. By disconnecting the HS256 S3 from the pc, the data, programs and operating systems are saved and encrypted exclusively on the HS256 S3 and are inaccessible by unauthorized persons.

8) Usage with all operating systems

The HS256 S3 hardware encryption is standalone, which means it can be used on any device that supports data storage devices.

9) Integrating in existing smart card infrastructures within companies.

If a company is already using the smart card Smartcard NXP J2E081_M64 R3, CC EAL 5 (i.e. access management, user authentication) the integration of the HS256 S3 is possible. Further functions can also be implemented into the smart card.

10) Integrating in existing software solutions

All existing software solutions can still be used to additionally expand the security properties and methods of use.

11. Technische Spezifikationen

Data Transfer Rate: USB 3.0 max 5 Gbps
USB 2.0 max 480 Mbps

Smart Card: NXP J2E081_M64 R3, CC EAL 5
JCOP v2.4.2 R3, (NSCIB-CC-13-37761-CR2)
with installed DIGITTRADE HS256 S3 Java Card Applet v1.1.0

Supported Encryption: 256 bit AES hardware based encryption, XTS mode, with two 256 bit cryptographic keys

Internal volume:

The encrypted data are stored on the internal 2.5 inch SATA HDD or SSD drive from Samsung (preferred), Seagate, Western Digital or Toshiba.

The following capacities are available: 120GB SSD, 160GB HDD, 250GB SSD, 320GB HDD, 500GB HDD/SSD, 640GB HDD, 750GB HDD/SSD, 1TB HDD/SSD, 1,5TB HDD/SSD, 2TB HDD/SSD, 4TB HDD/SSD

Computers and HDD manufacturers convert differently from Byte to KByte, MByte and GByte. HDD manufacturers calculate in the metric system (1 KByte = 10^3 Byte = 1000 Byte) and computers use due to their construction the dual system (1 KByte = 2^{10} Byte = 1024 Byte). The outcomes of this are the following differences in the representation of the memory capacity.

HDD manufacturer	available space
120 GB	111.76 GB
160 GB	149.01 GB
250 GB	232.80 GB
320 GB	298.08 GB
500 GB	465.66 GB
640 GB	596.03 GB
750 GB	698.49 GB
1,000 GB	931.32 GB
1,500 GB	1,396.98 GB
2,000 GB	1,862.64 GB
4,000 GB	3,725.29 GB

12. Troubleshooting

If any problems occure with your DIGITTRADE High Security HS256 S3 HDD/SSD please read the following checklist to find a solution. If further technical support is required, please feel free to contact our support team.

Problem	Symptom	Solution
The number pad is inactive	keypad light is turned off	Ensure that the USB connector is firmly connected to your computer's USB port.
	"ERROR" LED lights up	Ensure that a valid card is inserted and that the card orientation is correct by inserting the card with the contacts facing down.
Authentication fails	"ERROR" LED lights up	An incorrect PIN was entered. Press the "ESC" button to restart PIN entry (max. 8 trials).
The drive cannot be identified	no icon for the device is shown on the computer	Ensure that the HS256 S3 is not connected to a bus-powered USB hub or a USB extension cable. Please use the delivered USB cable.
	missing partition or file system cannot be detected	Please refer to Chapter 6 "Partitioning / Formatting", p. 41 et seqq.

Problem	Symptom	Solution
The drive cannot be identified	the wrong USB-cable is used	Please use the delivered USB cable and connect it to your computer.
The drive is performaing very slowly	connection using USB	Please ensure your HS256 S3 is connected to a USB interface.
	the wrong USB-cable is used	Please use the delivered USB cable and connect it to your computer.
	wrong connection to the computer	Ensure the USB cable is connected to your computer.
	the HS256 S3 is plugged in an USB hub	Connect the HS256 S3 directly to your computer.
	other USB devices are connected to the same port	Disconnect any other USB devices and see if performance improves.

13. Data security and disclaimer

We recommend to frequently backup your data saved on the DIGITTRADE High Security HS256 S3 on another storage device. This will protect you from a total data loss. The DIGITTRADE GmbH is not liable for any data loss and/or resulting costs and damages and does not bear the responsibility of data privacy of the stored data.

14. Appropriate handling of the HS256 S3 for data privacy

Please note following principles and requirements of the Federal Data Protection Act (BDSG), State Data Protection Acts and the corresponding standards of the EU Data Protection Directive (95/46/EC) for storaging personal data:

1) Lawfulness of data collection, processing and use
According to §4 para. 1 BDSG the collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.

The same is true in regard to Article 7 of the EU Data Protection Directive, according to which Member States shall provide that personal data may be processed only if:

a) the data subject has unambiguously given his consent; or
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) processing is necessary in order to protect the vital interests of the data subject; or
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

2) Data reduction and data economy (Section 3a)
Personal data shall be collected, processed and used as well as and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.

Please consider this aspect during the creation of backup copies. The old backups should be replaced with the current data regularly instead of providing new ones. To delete the old data before creating a new backup completely before creating a new backup, iit is recommended to change the cryptographic keys and afterwards please format the whole hard drive with a new key.

3) Transparency and purpose
The data subject is to be informed of collection, first-time storage or transmission of the personal data according to §48 Para. 3, §19 and §33 of the Federal Data Protection Act (BDSG). This is also regulated by Article 10 f. of the EU Data Protection Directive (95/46/EC). In addition to processing personal data the principle of the purpose must be regarded (see in particular Article 6 (b) of EU Data Protection Directive).

4) The processing of special categories of data Article 8:
Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life.

Processing is only allowed if e.g. this is required for the employment relationship or to protect the vital interests involved. Further data processing is allowed if the owner has published the data by himself/herself. It is required to assert claims in court or processing the data in the context of medical care / health care is needed.
Appropriate regulations can be found in § 28 para. 6-9 BDSG

5) Inalienable rights of the data subject
According to §19, 20, 34 and 35 BDSG the data subject has the right of access, rectification and erasure or blocking of the stored data concerning them.

The same also applies to Article 12 of the EC Data Protection Directive, in which any interested party has the right to information and, as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive.

Furthermore according to article 14 Member States shall grant the data subject the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him.

6) Section 42a Obligation to notify in case of unlawful access to data:
With very vulnerable data types referred to in §42a para.1 BDSG it is obligatory that the responsible authority informs all parties concerned of the data loss.

7) Administrative offences:
The unauthorized collection, processing and use of personal information can in accordance to §43 BDSG be punished with fines up to € 300,000.00. In the event of an intentional commission of certain offenses fines can therefore be according to §44 BDSG a criminal offense and can be punished with imprisonment up to two years or with a fine.

15. Safe shutdown after using the HS256 S3

For safety reasons, a logical or physical separation of the hard drive is executed from the host system after use. This is recommended especially at the end, short-term interruption and when leaving the workplace.

The logical separation is achieved by removing the smart card from the enclosure. This function is avalaible in the active lock-out mode, which is preset by the manufacturer at the delivery and is the default mode for the safe use of HS256 S3.

For the safe physical separation all connections must be removed from the HS256 S3.

Note: *To prevent data loss, make sure that the data transfer and access are terminated on the hard drive before disconnecting all cables.*

16. Smart card storage

The DIGITTRADE HS256 S3 is delivered with 2 smart cards. Please keep your smart cards separated from the HS256 S3! Doing this guarantees additional protection of your data.

If a card is somehow broken, you can create a copy (DIGITTRADE certified smart card) of the working one using the HS256 S3. You can find tips in chapter 5.3 and compatible smart cards can be purchased at DIGITTRADE.

If lost, we recommend using the HS256 S3 with two new smart cards with new cryptographic keys. You can obtain new smart cards at DIGITTRADE. You can choose between a new one which is already written with cryptographic keys by DIGITTRADE or without new keys. In these case you are able to generate cryptographic keys by yourself for your HS256 S3. Furthermore it is necessary to destroy the cryptographic keys completely. Please follow the steps in Chapter 4.2 (3).

If the smart cards are lost or broken, there is no way of accessing the data. To continue using the hard drive you need at least two new DIGITTRADE certified smart cards. As described in chapter 4.1 then you can create an new cryptographic key pair and operate the HS256 S3 with it. During the process of initialising the hard drive is formatted and the data on the disk is irrevocably deleted. Please contact the support at DIGITTRADE GmbH for new smart cards and other questions.

Note: *Please keep your device PIN in mind. Without this PIN it is not possible to initialize new smart cards and hence to use the HDD.*
Please keep the locations and PINs of your smart cards always in mind, otherwise access to your data would not be possible any more. To use the HS256 S3 with new smart Cards according to the BSI-Certification it is necessary fulfill the procedure of chapter 1.

17. Product contents

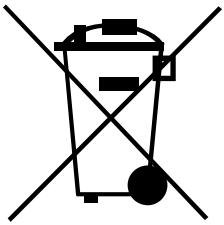
- DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD) version 1.0
- Two smart cards NXP J2E081_M64 R3 loaded with DIGITTRADE HS256 S3 Java Card Applet version 1.1.0
- User manual "DIGITTRADE High Security HS256 S3"
- USB cable
- Slim case

Note: *For the exact identification, the components HS256 S3 (Device), smart cards and user manual are individual marked by the explicit product name and product version "DIGITTRADE High Security HS256 S3 Version 1.0". The certified storage configurations of the DIGITTRADE HS256 S3 are available in chapter 11.*

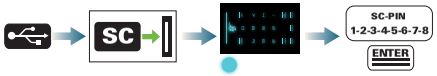
18. WEEE Statement

According to the EC directive, waste electrical and electronic equipment (WEEE) must not be disposed as municipal wastes.
To avoid the spread of the contained fabric components in your environment and to save natural resources we would like to ask you to hand this product after its economic life time only to a collecting point for WEEE in your area.

Thanks to these measures, materials of your product can be reused environmentally friendly.

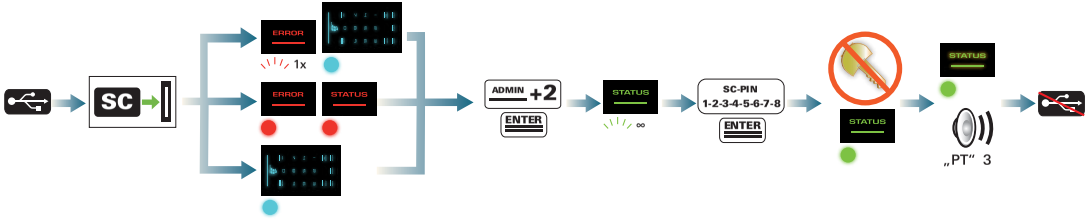


authentication on the HS256 S3

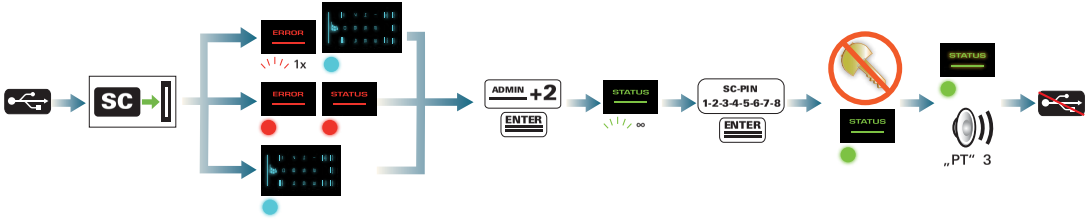


changing the smart card PIN

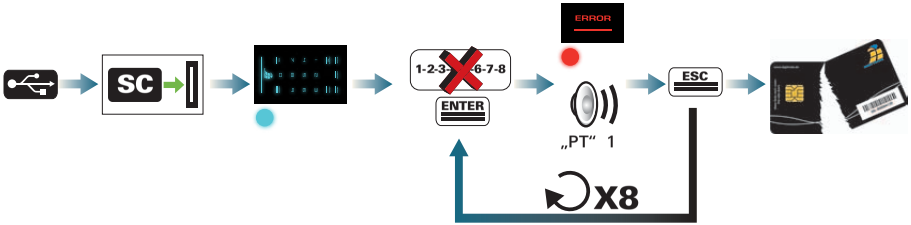
creating the cryptografical keys



delete the cryptografical keys (PIN is be known)



deleting of the cryptographic keys (unkown smart card PIN)

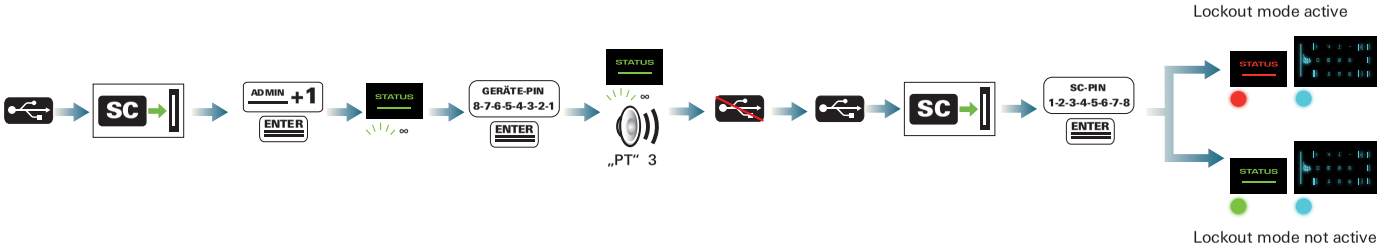


changing the device PIN

initialising a new smart card

Copying the cryptographic keys

activating/deactivating the lock out mode



Connect the HS256 S3 to the PC

Disconnect the HS256 S3 from the PC

Connector

Insert the smart card into the slot

Insert smart card A into the slot

Insert smart card B into the slot

Pull out smart card A

The smart card is locked and unusable

Enter the smart card pin by using the keypad

Enter the smart card PIN by using the keypad

Enter the device PIN by using the device PIN

Enter the new device PIN on the keypad

Misentry of the smart card PIN

Press „CHANGE PIN“ then „0“ (similiar for 0 and 1)

Press „ADMIN“ then „0“ (similiar for 1,2,3)

Press „ENTER“

Press „ESC“

The keypad illuminates

The „STATUS“-LED...

...flashes green for 1-times

...flashes green multiple times

...illuminates green

The „STATUS“-LED and / or the „ERROR“-LED...

...flashes red for 1-times

...illuminates red

You will hear beep tones for x-times

„PT“ X

The cryptographic keys will be written to the smart card

The cryptographic keys will be destroyed

Do this step 8 times in a row

Ihre Notizen / Your Notes

© 2017 DIGITTRADE GmbH

Deutsch
Dieses Handbuch ist urheberrechtlich geschützt und darf nicht (auch nicht teilweise) ohne schriftliche Zustimmung der DIGITTRADE GmbH kopiert werden.

English
This user manual is protected by copyright. No part of this material may be reproduced, transcribed, used or disclosed to any third party in any form or by any means, without the written permission of the DIGITTRADE GmbH.

DIGITTRADE GmbH
Ernst-Thälmann-Strasse 39
06179 Holleben Germany

Fon +49 / 3 45 / 2 31 73 53
Fax +49 / 3 45 / 6 13 86 97
Web www.digittrade.de
E-Mail beratung@digittrade.de