Informationsblatt
DIGITTRADE High Security Festplatte HS256S

Datenschutz und Datensicherheit sind äußerst sensible Themen für Unternehmen. Immer wieder erfordern Geschäftsprozesse die mobile Verfügbarkeit von Forschungs-, Finanz-, Kunden- oder Kontodaten. Bei der Datenaufbewahrung und dem Datentransport muss sich ein Unternehmen auf absolute Sicherheit verlassen können. Gelangen sensible Daten in unbefugte Hände, entsteht meist ein irreparabler Schaden. Es ist der Super-GAU für jedes Unternehmen: Hochsensible Daten geraten in fremde Hände, werden eingelesen und verbreitet oder missbraucht.

Um dies zu verhindern und höchste Datensicherheit für den mobilen Datentransport zu gewährleisten, müssen folgende Hauptkriterien beachtet werden:

- **Verschlüsselung**
- **Zugriffskontrolle**
- **Verwaltung des kryptografischen Schlüssels (Erstellung, Speicherung und Zerstörung)**

Metaphorisch gesprochen ist die **Verschlüsselung** wie die Tür eines Hauses. Die Tür kann z.B. aus Holz oder Stahl sein. Übertragen auf die mobilen Festplatten würde das bedeuten, dass zum Beispiel eine einfache XOR-Verknüpfung oder eine Verschlüsselung nach AES mit unterschiedlichen Schlüssellängen und Blockmodi verwendet werden kann.

Die Wahl einer passenden Verschlüsselung entscheidend für die Datensicherheit. Für hohe Anforderungen an die Datensicherheit empfiehlt es sich, mindestens eine AES-Verschlüsselung mit einer Schlüssellänge von 256-Bit im CBC-Modus zu verwenden.
Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptosystem, welches weltweit als berechnungssicher gilt und auch in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen ist.

Die **Zugriffskontrolle** kann mit einem Schloss verglichen werden. Dies kann ein leicht zugängliches Schloss sein, das mit einem Draht geöffnet werden kann oder ein robustes Schloss, das auch gegen große Manipulationen und physische Belastungen geschützt ist.

Somit ist die Verwendung der härtesten Stahltür nichtig, wenn sie durch ein einfaches Schloss gesichert wird.

In Bezug auf die Sicherheitsmedien ist damit gemeint, dass die Zugriffskontrolle von einem einfachen Passwort bis hin zu komplexen mehrstufigen Authentifizierungsmethoden reichen kann. Eine komplexe Zugriffsmethode mit einer Zwei-Faktor-Authentifizierung (z.B. Smartcard und PIN) bietet ein sehr hohes Maß an Datensicherheit.

Bei dem Schlüssel für die Haustür ist es wichtig zu wissen, wer diesen hergestellt hat und wo er abgelegt wird. Dabei bringt es nichts, die härteste Stahltür und das sicherste Schloss zu verwenden, wenn der Schlüssel direkt neben der Tür an einem Schlüsselbrett hängt. Es muss demnach sichergestellt sein, dass sich der Schlüssel an einem sicheren Ort befindet und für Unbefugte unzugänglich bleibt.

Auf die externen Speicher bezogen, sollten Informationen über die **Verwaltung des kryptografischen Schlüssels (Krypto-Schlüssel)** beachtet werden. Dabei sollte bekannt sein, wie der Krypto-Schlüssel hergestellt wurde und ob bei der Herstellung oder auf dem Weg zum Nutzer eine Kopie des Schlüssels angefertigt werden konnte. Außerdem sollte betrachtet werden, wie sicher und wo der Schlüssel für die Verwendung abgelegt ist. Typische Speicherorte des Krypto-Schlüssels sind auf der Festplatte, im Sicherheitscontroller oder außerhalb des Speichermediums, z.B. auf einer Smartcard.

Zudem müssen Informationen darüber bestehen, ob und wie der Krypto-Schlüssel in einer extremen Situation durch den Benutzer schnell zerstört werden kann, damit Unbefugte, auch mittels Zwang, nicht an die sensible Daten gelangen können.

Es müssen für die Wahl eines geeigneten Sicherheitsspeichermediums immer alle 3 Sicherheitskriterien berücksichtigt werden. Hat eine dieser Kriterien eine Sicherheitslücke, so wird dadurch die gesamte Sicherheitskette gefährdet.

Sicher verschlüsselte Daten

DIGITTRADE HS256S - eine hochsichere Speicherlösung

Die externe **High Security Festplatte HS256S** von DIGITTRADE bietet die beste Zusammensetzung drei Sicherheitskriterien.

Die externe High Security Festplatte DIGITTRADE HS256S wurde in Übereinstimmung mit den neuesten Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) an mobile Speichermedien entwickelt und bietet eine der sichersten Möglichkeiten für die Speicherung mobiler Daten.

Dank der Full-Disk-Hardwareverschlüsselung nach AES (Advanced Encryption Standard) mit 256-Bit im CBC-Modus und der Zwei-Faktor-Authentifizierung mittels Smartcard und 8-stelliger PIN vereint sie die Vorteile mobiler Datenträger mit den höchsten Sicherheitsstandards für den Datenschutz.

Die DIGITTRADE HS256S gewährleistet die Vertraulichkeit der Daten durch folgende Sicherheitsmechanismen:

- Verschlüsselung
- Zugriffskontrolle
- Verwaltung des kryptografischen Schlüssels

Die Festplatte hat ein eingebautes Verschlüsselungsmodul. Dieses verschlüsselt alle Daten und einzelne Sektoren der Festplatte in Echtzeit und ohne Performanceverlust. Die Bootfähigkeit erlaubt das Starten kompletter Programme und Betriebssysteme über die Festplatte. Dadurch besteht die Möglichkeit, auch an fremden Systemen alle Anwendungen auszuführen. Zudem kann die HS256S uneingeschränkt und sicher an allen Geräten verwendet werden, die externe Speichermedien unterstützen.

Die Zwei-Faktor-Authentifizierung aus der weltweit einzigartigen Smartcard-PIN-Kombination erfolgt nach dem Prinzip „Besitzen und Wissen“. Nur wer die Smartcard besitzt und die dazugehörige PIN kennt, kann auf die HS256S zugreifen.

Die HS256S bietet die Möglichkeit, den Krypto-Schlüssel unabhängig von PC oder Software auf der Festplatte zu verwalten. Der Nutzer kann den Krypto-Schlüssel erstellen, ändern und bei Gefahr zerstören.

Der Krypto-Schlüssel befindet sich außerhalb der Festplatte und ist verschlüsselt auf der Smartcard gespeichert. Der Zugang zum Schlüssel ist durch eine 8-stellige PIN gesichert und wird nur nach korrekter Eingabe freigegeben. Daraufhin erfolgt die Übertragung des Schlüssels an das Verschlüsselungsmodul der Festplatte. Die Daten können nun gelesen und bearbeitet werden.

Nach 8-maliger Fehleingabe der PIN, wird der Krypto-Schlüssel auf der Smartcard durch die Erzeugung eines neuen Krypto-Schlüssels zerstört. Zusätzlich wird die Smartcard durch das Smartcard-Applet unwiderruflich blockiert. Die Smartcard wird dadurch absolut unbrauchbar gemacht. Die Daten auf der Festplatte werden dabei nicht beeinflusst und bleiben weiterhin verschlüsselt gespeichert. Der Zugang ist weiterhin mit der zweiten, mitgelieferten Smartcard möglich, vorausgesetzt, die richtige PIN ist bekannt.

Serienmäßig wird die Festplatte mit der Smartcard Oberthur Cosmo 64 v5.4 angeboten. Sie ist nach FIPS 140-2 Level 3 zertifiziert und bietet die Möglichkeit, den Krypto-Schlüssel sicher zu verwalten. Diese Smartcard entspricht den hohen Anforderungen an kryptografische Funktionen und Schlüsselsicherheit, denen zivile Regierungseinrichtungen unterliegen.

Es können außerdem die vom BSI zertifizierten Smartcards NXP J2A040 oder Infineon geliefert werden. Diese verfügen über eine Zertifizierung nach EAL5+. Die Sicherheitsfunktionen für die Verwaltung des kryptografischen Schlüssels können zudem in firmeninterne Smartcards integriert werden.

Der Krypto-Schlüssel befindet sich auf der Smartcard und kann bei Verlust oder Diebstahl der Festplatte weder aus dem Gehäuse noch aus der Festplatte ausgelesen werden.

Die Festplatten sind so konstruiert, dass der verwendete Krypto-Schlüssel beliebig verändert werden kann. Bei der Verwendung einer Smartcard mit einem neuen Krypto-Schlüssel muss diese vor der Benutzung auf der Festplatte initialisiert werden. Die neuen Daten werden nach einer Schnellformatierung der Festplatte mit dem neuen Krypto-Schlüssel gespeichert. Der Zugriff auf die alten Daten ist danach nur auf dem Wege der Datenwiederherstellung unter Verwendung der Smartcard mit passendem Krypto-Schlüssel begrenzt möglich.

Die AES-Betriebsart Cypher Block Chaining (CBC) bezeichnet ein komplexes Verfahren, bei dem die einzelnen Klartextblöcke zunächst mit dem im letzten Schritt erzeugten Geheimtextblock verknüpft und erst anschließend mit dem AES-Schlüssel verschlüsselt werden. Auf diese Weise können keine Rückschlüsse auf die Klartexte gezogen werden, was eine extrem hohe Sicherheit garantiert.

Zusätzlich zu den gespeicherten Daten werden selbst temporäre Dateien sowie Bereiche verschlüsselt, die von Verschlüssel-ungssoftware oft nicht beachtet werden.

Die HS256S mit eingebauter Solid State Drive (SSD) bietet einen zusätzlichen Schutz bei physischen Belastungen, da keine beweglichen Teile wie Lese- und Schreibköpfe vorhanden sind. Dank der Verwendung moderner Flashspeicher sind ihre Daten auch bei Erschütterungen sicher. HS256S SSD ist damit äußerst widerstandsfähig gegen Stürze, Stöße und Vibrationen und kann auch in störgefährdeten Umgebungen sicher eingesetzt werden.

Wesentliche Anwendungsmöglichkeiten

1. Sicherer und kosteneffizienter Datentransport

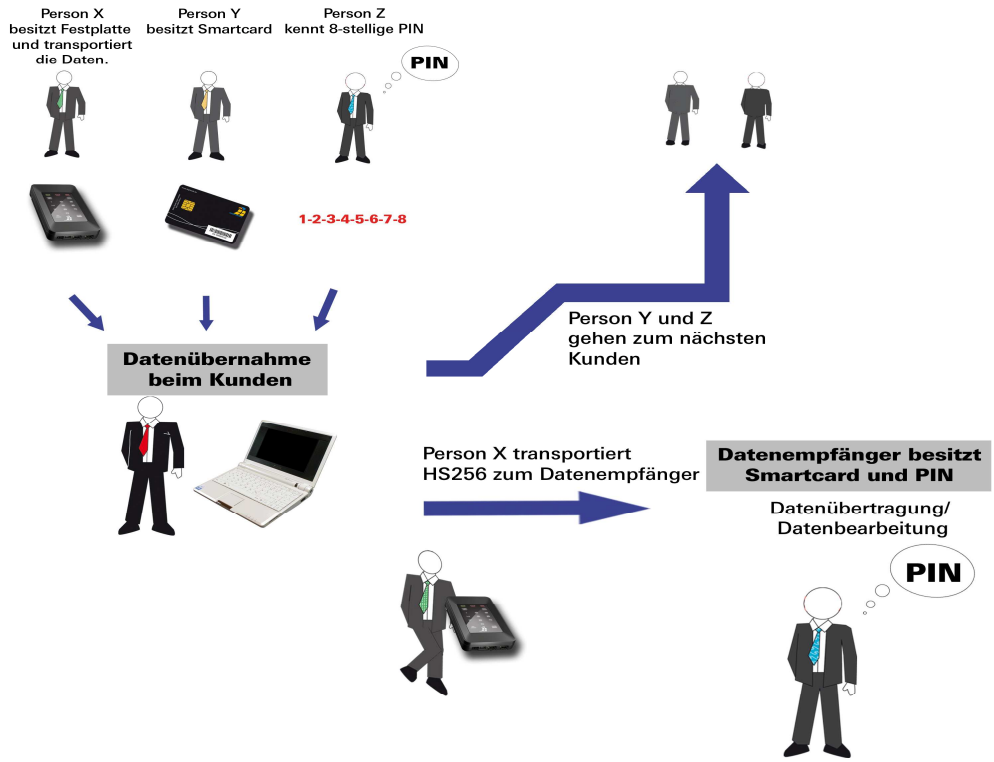
   Die HS256S kann für den Transport vertraulicher Daten verwendet werden. Dazu werden beim Sender und Empfänger der Daten Smartcards mit dem gleichen kryptografischen Schlüssel hinterlegt. Der Absender versendet nur die HS256S. Da der kryptografische Schlüssel physisch nicht vorhanden ist (er befindet sich auf den Smartcards), kann dieser beim Transport nicht ausgelesen werden. Außerdem kann die HS256S mit vertraulichen Daten dem Empfänger kostengünstig und versichert durch einen Paketdienstleister oder Kurier zugestellt werden.

   Der Sender und der Empfänger müssen bei jedem Transport von Daten sicherstellen, dass sie eine Manipulation an der HS256S erkennen können. Es sollte immer darauf geachtet werden, ob die Versiegelungen von DIGITTRADE unversehrt sind. Außerdem können weitere Sicherungsmethoden, wie eine versiegelte Verpackung, angewendet werden. Dies gilt auch für alle anderen Datentransportmöglichkeiten mittels HS256S.

   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 Festplatte und Authentisierungen

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 HS256S, Person Y verfügt über die Smartcard und Person Z kennt die 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.



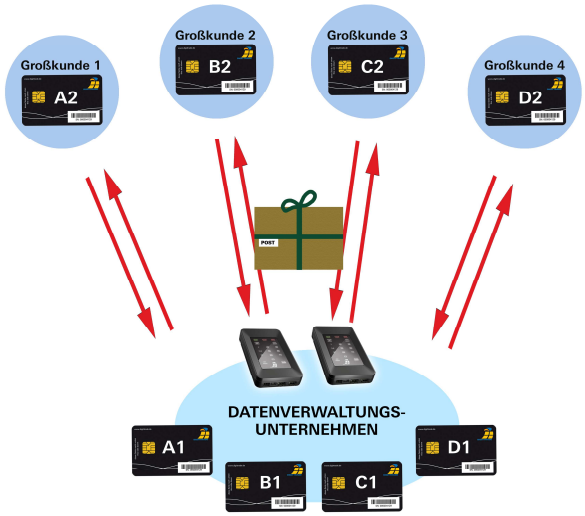
3. Verwendung von wenigen Festplatten bei großem Kundenkreis

Steht ein Unternehmen (z.B. ein Datenverarbeitungsunternehmen oder eine Datenzentrale von Großunternehmen oder Behörden) in ständigem Datenaustausch mit vielen Datenempfängern, so kann dieses unter der Verwendung von HS256S-Festplatten/-SSDs Daten mit einer deutlich geringeren Anzahl von Datenträgern und großer finanzieller Einsparung sicher transportieren. Jeder Datenempfänger erhält eine Smartcard mit seinem eigenen kryptografischen Schlüssel. Bei dem Datenversender werden Zweitexemplare der Smartcards mit den kryptografischen Schlüsseln der jeweiligen Datenempfänger angelegt.

Für den Datenversand wird eine Smartcard mit dem kryptografischen Schlüssel des jeweiligen Empfängers für eine HS256S initialisiert (Admin-PIN erforderlich). Dafür ist jede verfügbare HS256S geeignet. Anschließend führt der Datenversender mit dem neuen kryptografischen Schlüssel eine Schnellformatierung der HS256S durch, die nur wenige Minuten dauert. Aufwendige Datenlöschungen und mehrmaliges Überschreiben des Datenträgers entfallen, da die verbliebenen Daten mit einem anderen kryptografischen Schlüssel verschlüsselt sind und somit ggf. nur vom Besitzer des zugehörigen kryptografischen Schlüssels wiederhergestellt und gelesen werden können, vorausgesetzt, 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 HS256S zu warten. Es kann jede, im Unternehmen verfügbare HS256S verwendet werden. Diese wird dazu vor der Datenspeicherung mit dem kryptografischen Schlüssel des entsprechenden Empfängers initialisiert und schnellformatiert.

Die Stückzahl der Datenträger kann auf die tatsächliche, für den jeweiligen Zeitpunkt notwendige reduziert werden, da nicht für jeden Datenempfänger eine eigene HS256S benötigt wird. Dabei ist es irrelevant, welche der im Unternehmen verfügbaren HS256S für den Datentransport verwendet wird. Entscheidend ist, mit welchem kryptografischen Schlüssel die Daten auf die HS256S geschrieben werden.

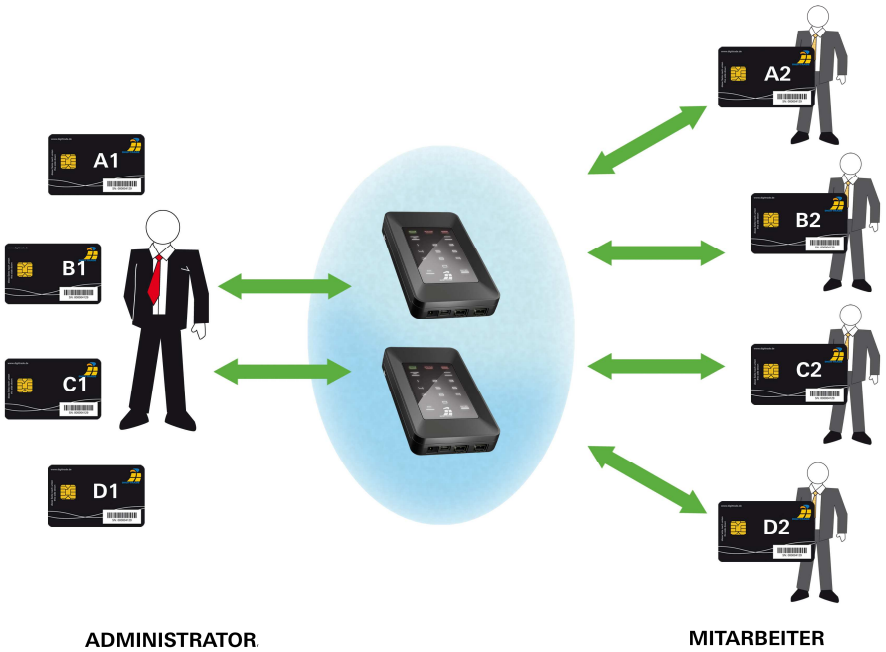


4. Verwendung von wenigen Festplatten im Außendienst und Behörden

Wurde früher für jeden Mitarbeiter eine persönliche Festplatte für vertrauliche Daten benötigt, so ist es mit den HS256S Festplatten möglich, mit bedeutend weniger Festplatten diesen Bedarf abzudecken.

Hierbei wird für jeden Mitarbeiter eine personalisierte Smartcard mit eigenem Krypto-Schlüssel vergeben. Der Administrator, welcher alle vorhandenen Festplatten verwaltet, verfügt über die Gegenstücke der Mitarbeiter-Smartcards. Benötigt nun ein Mitarbeiter eine Festplatte, so initialisiert der Administrator die Festplatte mit der entsprechenden Smartcard und übergibt sie dem Mitarbeiter.

Nach beendeter Benutzung gibt der Mitarbeiter dem Administrator die Festplatte zurück. Diese wird anschließend einer Schnellkonfiguration unterzogen. Innerhalb weniger Minuten ist die Festplatte für den nächsten Mitarbeiter einsatzbereit. Dazu muss die Smartcard des nächsten Mitarbeiters an der Festplatte initialisiert und die Festplatte schnellformatiert werden. Die neuen Daten werden mit dem Krypto-Schlüssel des nächstens Mitarbeiters gespeichert.

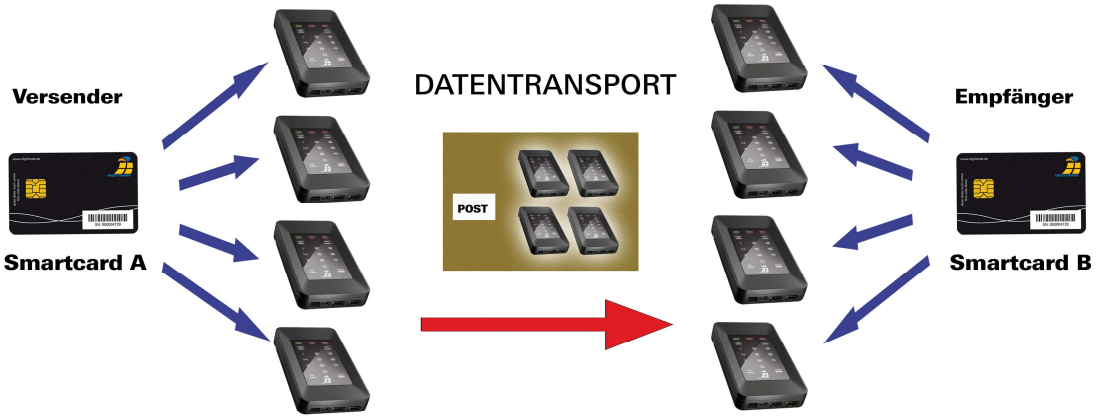


5. Betreiben mehrerer Festplatten mit nur einer Smartcard

Es werden dazu Smartcards mit dem gleichen kryptografischen Schlüssel für mehrere Festplatten initialisiert. Von besonderem Interesse ist das Betreiben von mehreren Festplatten mit nur einer Smartcard für die Arbeit mit Datenvolumen, die die Kapazität einer Festplatte übersteigen, da die Daten auf mehrere Festplatten verteilt werden.

Auch wenn Daten sehr häufig, z.B. täglich verschickt werden, bietet es sich an, mehrere Festplatten mit dem gleichen kryptografischen Schlüssel zu verwenden. Es kann täglich eine neue Festplatte mit dem gleichen kryptografischen Schlüssel versendet werden, ohne dass auf eine personalisierte Festplatte gewartet werden muss.

Der Empfänger kann stets mit der gleichen Smartcard, die den entsprechenden kryptografischen Schlüssel enthält, auf die Festplatten zugreifen.



6. Zerstörung des Krypto-Schlüssels auf der Smartcard.

Der Nutzer hat in Gefahrensituationen die Möglichkeit, den kryptografischen Schlüssel unauffällig zu zerstören, wenn ihm die Smartcard-PIN bekannt ist. Dazu werden während des Anmeldevorgangs zwei zusätzliche Tasten bedient.

Falls die Smartcard-PIN nicht bekannt ist, kann der kryptografische Schlüssel auf der Smartcard durch 8-malige Falscheingabe der PIN vernichtet werden.

7. Bootfähigkeit

Auf der DIGITTRADE HS256S können Betriebssysteme, Programme und Daten gespeichert werden. Diese Anwendung ist sowohl für stationäre als auch mobile Computer geeignet. Mit dem Trennen der HS256S vom PC bleiben die Daten, Programme und Betriebssysteme, inkl. temporärer Dateien ausschließlich auf der HS256S verschlüsselt gespeichert und sind für Unbefugte unzugänglich.

8. Verwendung an allen Betriebssystemen.

Die HS256S 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

Werden in einem Unternehmen bereits Java-basierte Smartcards verwendet (z.B. Zutrittsmanagement, Nutzerauthentisierung etc.), ist eine Integration der HS256S möglich.

10. Integration von bestehenden Softwarelösungen.

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

Die wichtigsten Eigenschaften im Überblick

- 256-Bit AES-Full-Disk-Hardwareverschlüsselung im CBC-Modus
- 2-Faktor-Authentifizierung mittels Smartcard und 8-stelliger PIN
- externe Speicherung des kryptografischen Schlüssels
- Erstellen, Kopieren und Zerstören des kryptografischen Schlüssels durch den Nutzer
- hardwarebasiertes Verschlüsselungsmodul
- Datenverschlüsselung aller gespeicherten Bytes und beschriebenen Sektoren
- unabhängig von Betriebssystemen (Unterstützung aller Betriebssysteme, Multimediageräte und Maschinen mit USB-Datenträger-Unterstützung)
- bootfähig
- kompatibel mit USB 1.1, USB 2.0 und FireWire
- keine Einschränkungen der Lese- und Schreibgeschwindigkeit
- handliches 2,5”-Format

Vorteile der DIGITTRADE HS256S

- 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

Acronis Quick Backup Software

Die DIGITTRADE HS256S, wird wie alle anderen Sicherheitsspeichermedien von DIGITTRADE mit der Acronis Quick Backup-Software geliefert. Dieses Programm ist keine Verschlüsselungssoftware, sondern ein Zusatzfeature für das Backup von Daten.

Acronis True Image OEM Quick Backup ist eine integrierte Programm-Zusammenstellung, mit der der Erhalt aller Informationen auf dem Computer gewährleistet wird. Es kann das Betriebssystem, installierte Anwendungen, Einstellungen und alle Daten sichern. Es können mit dieser Software komplette Festplatten oder einzelne Partitionen gesichert werden. Acronis Online Backup ermöglicht es, die wichtigsten Dateien auf einem entfernten Storage zu speichern, so dass sie selbst dann geschützt sind, wenn die Festplatte verloren geht, defekt oder gestohlen wird.

Sollte die Festplatte beschädigt oder von einem Virus bzw. Schadprogrammen befallen werden, können die gesicherten Daten leicht und schnell wiederhergestellt werden. Acronis True Image OEM Quick Backup enthält alle notwendigen Extras, die zur Wiederherstellung eines Computer-Systems im Desaster-Fall benötigt werden, z.B. bei Datenverlust und versehentlichem Löschen entscheidender Dateien. Wenn Fehler auftreten, die einen Zugriff auf Informationen blockieren oder das Betriebssystem beeinflussen, können das System und verlorene Daten einfach wiederhergestellt werden.

Die einzigartige Snapshot-Technologie ermöglicht die Erstellung exakter Sektor-für-Sektor-Backups von Festplatten, welches alle Betriebssysteme, Anwendungen und Konfigurationsdateien, Software-Updates, persönliche Einstellungen und Daten beinhaltet.