Professional solution for authorities and companies

The HS256S3 is an external hard drive with hardware encryption. Its design is adapted to the needs of companies and authorities and is particularly suitable for the secure transport of data and for the creation of backups. The HS256 S3 ensures the confidentiality of the data through the following security mechanisms:

1. Encryption

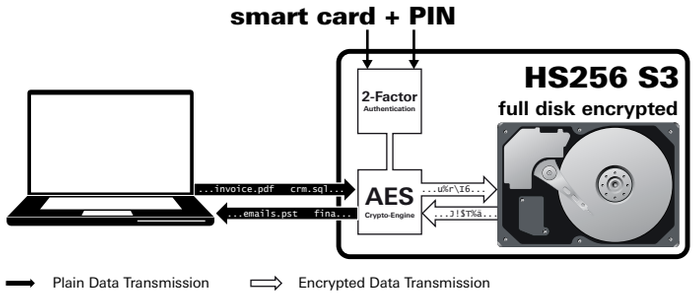
256-bit AES full-disk hardware encryption in XTS mode using two 256-bit crypto keys

2. Access control

Two-factor authentication using a smart card and 8-digit PIN based on the principle of "owning and knowing"

3. Management of cryptographic keys

The cryptographic keys can be created, changed, copied and destroyed by the user on the smart card.



Other features:

- elegant metal case
- support of USB 3.0 and 2.0
- OS independent and bootable
- storage Capacity SSD: 250GB, 500GB, 1TB, 2TB und 4TB; HDD: 500GB, 1TB, 2TB und 4TB
- laser engraving of logo, inventory numbers, scannable QR codes, name o.a. according to customer specifications

Requirements of the GDPR and BDSG

Art. 15 (1) GDPR Data protection through technology design

Taking into account the state of the art, the controller and the processor shall take appropriate technical and organizational measures to ensure a level of protection commensurate with the risk.

Art. 83 (4) GDPR Imposition of fines

In the event of a breach of Article 25, fines of up to € 10,000,000 or, in the case of an entrepreneur, up to 2% of its total annual turnover in the preceding financial year will be imposed, whichever is greater.

§42 BDSG (2018) Penal Code 42§ BDSG (2018) Penal Code

Penalties of up to three years or a fine are imposed on those who knowingly give access to, or otherwise make accessible to, third-party personal information of a large number of persons, and in doing so make commercial use of it.

§43 BDSG (2018) penalty regulations

The offense can be punished with a fine of up to 50,000 euros.

The HS256S3 hard disk is state-of-the-art. BSI certification allows it to store personal data.

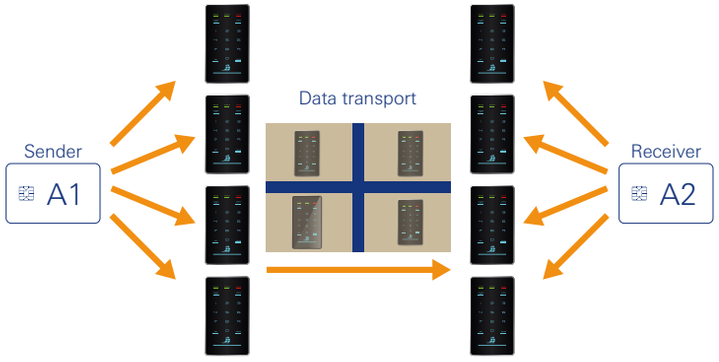
The use of the HS256S3 enables users to fully comply with the strictest requirements of the Federal Data Protection Act (BDSG) and the latest EU Data Protection Regulation (EU-DSGVO) with regard to the storage of personal and sensitive data.

HS256 S3

DIGITTRADE High Security HDD

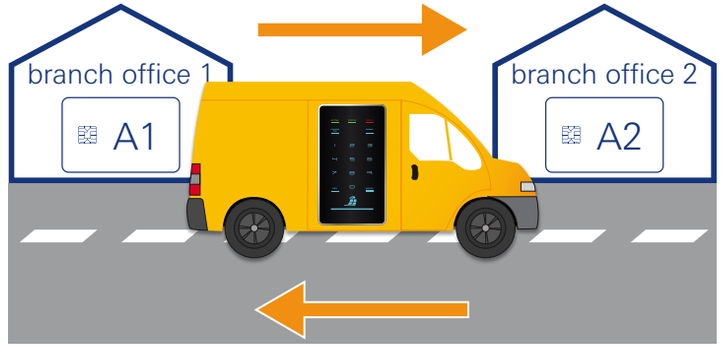
External hard drive with BSI certification according to CC EAL 2 BSI-DSZ-CC-0825-2017

Run multiple disks with one smart card



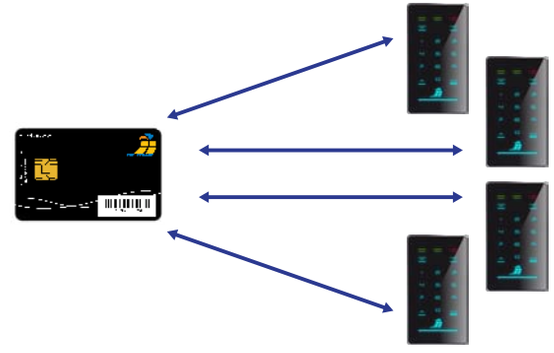
- suitable for data volumes that exceed the capacity of an HS256 S3
- data can be distributed to several HS256 S3s
- multiple HS256 S3 can be used with the same cryptographic keys for frequent or daily shipping

Secure and cost-efficient data transport



- sender and recipient have smart cards with the same crypto key
- sender stores encrypted data on the HDD with the help of his smart card and sends the HS256 S3 cost-effectively by mail or courier to recipient
- recipient receives the hard disk and decrypts the data using his smart card

Secure backup storage



- protects data against unauthorized access
- provides full control over sensitive and personal information
- several hard drives can be operated with the same smart card

Operating system independent

All security features are fully implemented in the HS256 S3. Therefore, this hard drive works with all known operating systems and multimedia devices.

It is also bootable and can be used for the simultaneous storage of operating systems and data.

Security bags

This special security packaging can be used to determine whether tampering has taken place during delivery of the HS256 S3. These bags can be used in addition to the HS256 S3 for secure data transport.

Smartcard Manager SM2

The Smartcard Manager enables:

- centralized registration of all DIGITTRADE hard drives, smart cards and crypto-keys of the company
- classification of all employees, departments and locations to the respective information
- adding new hard drives and smart cards to each employee or department
- to create, change and delete cryptographic keys as well as changing the smart card PIN