Short Public Report

1. Name and version of the IT product or IT-based service:

   DIGITTRADE High Security HDD HS256S

2. Manufacturer or vendor of the IT product / Provider of the IT-based service:

   Company Name:

   DIGITTRADE GmbH

   Address:

   Ernst-Thälmann-Str. 39

   06179 Teutschenthal
   Germany

   Contact Person:

   Leonid Gimbut

3. Time frame of evaluation:

August 1st 2012 to February 28th 2013

4. EuroPriSe Experts who evaluated the IT product or IT-based service:

Name of the Legal Expert:

Stephan Hansen-Oest

Address of the Legal Expert:

Neustadt 56
24939 Flensburg
Germany
sh@hansen-oest.com

Name of the Technical Expert:

Andreas Bethke

Address of the Technical Expert:

Papenbergallee 34
25448 Kellinghusen
bethke@datenschutz-guetesiegel.sh

5. Certification Body:

Name: Unabhaengiges Landeszentrum fuer Datenschutz - ULD
Address: Holstenstr. 98
24103 Kiel
Germany
eMail: europrise@datenschutzzentrum.de

6. Specification of Target of Evaluation (ToE):

The ToE is a portable, self contained storage device with a physical host connection providing encrypted storage of protected data and strong authentication to unlock access to the protected data.

Following components belong to the ToE :

- the Digittrade HS256S Java Card Applet Version 1.3 in usage with the smartcard “NXP P5CD081 J3A081 JCOP v2.4.1 R3, BSI-DSZ-CC-0675-2011” from NXP Semiconductors,
- the ID-One Applet in usage with the smartcard “Oberthur Cosmo 64 v5.4 FIPS-140-2 Level 3”,
- the integrated cardreader,
- the integrated keypad,
- the harddisk-controller-unit,
- the integrated crypto-module,
- the communication between smartcard and controller,
- the host interface (USB & Firewire) and
- the protected storage.

It does not include:

- smart card NXP Semiconductors P5CD081 J3A081 JCOP v2.4.1 R3 , BSI-DSZ-CC-0675-2011 (as such)
- smart card Oberthur Cosmo 64 v5.4 FIPS-140-2 Level 3 (as such)
- Processing of customer data (e.g. when buying the product from the manufacturer)

7. General description of the IT product or IT-based service:

The protected data in the storage area of the storage medium is not accessible to unauthorised individuals in case the medium is lost, misplaced or stolen, as well as in the event of logical or physical attacks. Therefore the ToE provides the following security functions:

- full disc hardware encryption using AES (256 bit, CBC mode);
- two-factor authentication (key on the smart card and knowing the smart card PIN);
- administration of the encryption key

The default power-up state of the device provides only access to the authentication mechanism.

A key aspect of the ToE is that the security functions are completely implemented within the storage device itself. This enables using the TOE with a wide range of host systems since it is not subject to supporting software requirements.

One single authentication process is enough to unlock the protected data on the storage device and to make it accessible to the user. After successful authentication, the storage medium provides its security service transparently without any further access control requirements on the device.

The utilised smart card PIN and the encryption key are stored securely on a smart card.

The TOE provides a keypad, onto which the user can enter his PIN.

The encryption key is generated and stored securely on the smart card. For encryption and decryption of the data, the encryption key will be transmitted to the crypto module inside of the "DIGITTRADE High Security HS256S". Upon completion of usage, the encryption key will be deleted securely on the storage device.

The authorized user possesses an authentication attribute that is split into two parts: the device PIN and the key on the smart card in combination with the smart card PIN. According to the functions the user utilizes the particular PIN either separately or at the same time.

The authentication attributes can be split among two persons. The authentication attribute 1 (person 1): key on the smart card and smart card PIN. Authentication attribute 2 (Person 2): device PIN. If only the device PIN is known, the protected data will not be accessible.

Using the smart card and the smart card PIN, the user is able to generate and change the encryption key. If necessary, he can also destroy and delete the encryption key by generating a new key. After generating a new encryption key on the smart card, the encrypted data on the storage device will only be accessible with the previous, matching encryption key.

Using the device PIN, the user is able to initialize the smart card with a new encryption key onto the storage device. After initialization of a new smart card, the data on the storage device will be encrypted with the new encryption key. Hence the previous data can’t be accessed anymore.

Disconnection of the TOE from the host either physically or logically (by dismounting or power down) will lock the protected user data as well as TSF data and will ensure that no residual data from any active access is available.

The protected data will be locked in case of disconnection of TOE and host if additionally the power supply is disconnected.

The protected data will be locked in case of disconnection of smart card and storage device, if the lock-out mode is activated. Lock-out mode can be de-/activated, using the device PIN. In order to achieve a higher security level, the lock-out mode is recommended.

The security relevant components (e.g. crypto module and controller) are sealed by an epoxy sealing. Additionally, sealing labels are installed at the junction of

the implemented storage and the SATA interface as well as at the opening areas of the enclosure.

Extended Package - Extended Authentication PSMPP-EA is realized in the form of a two-factor authentication by key on the smart card and smart card PIN entry on the Keypad of the HS256S.

8. Transnational issues:

- none -

9. Tools used by the manufacturer of the IT product / provider of the IT-based service:

- Eclipse
- JCOP tools from NXP (containing all tools for developing on a Java Card™ Platform)
- uberSVN – application lifecycle management
- Toshiba IDE

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria May 2011

11. Evaluation results:

Set 1: Overview on fundamental issues

The controller is responsible for the processing of personal data and the purpose of the processing of data. The product is used for data storage and data management.

Data stores on the device is encrypted. Access to data on the device is only possible when the corresponding smartcard is in the possession of the user and if the user has knowledge of the PIN .

Set 2: Legitimacy of Data Processing

Responsibility:

The ToE is a data storage device that can be used to store all sorts of data.

The controller using the ToE is responsible to use the product in a lawful manner and to comply with all legal provisions for the processing of personal data.

The ToE can be used in a data protection compliant manner anyway.

Lawful processing of personal data:

Users of DIGITTRADE HS256S are informed about relevant data protection issues by means of specific notes on data protection in the user manual.

Set 3: Technical-Organisational Measures: Accompanying Measures for Protection of the Data Subject

The ToE includes a so-called certified "crypto module" on the controller that provides the actual encryption and decryption of data.

The encryption method used protects the data stored on the disk against an unauthorized access of third parties. Besides pure encryption of data on the hard drive, a smart card with PIN method is used additionally. The data is encrypted by using a AES-CBC algorithm with a key length of 256 bits. To get

access to the data, the user must hold the hard disk, as well as the smart card, as well as the 8-digit PIN to get the AES key, located on the smart card.

Personal data can be stored on the (mobile) disk, but it is encrypted. Access to the data itself is only possible in combination with the key and the PIN. There are no special rights / roles implemented within the ToE.

The product supports appropriate measures for identification and authentication due to the coupling of a particular smart card to a device and the 8-digit PIN in conjunction with the final destruction of the smart card (and thus a blocking of access to the data) after typing 8 incorrect entries. A real password management does not exist within the product.

The manufacturer has implemented features within the product that guarantee the secure deletion of data. Once all data on smart cards is destroyed there is no possibility to get access to the encrypted data with these cards. Concerning the current technical possibilities a reconstruction is not possible. On the other hand a cryptographic key stored on the smart card could be changed, which causes a deletion of data by initializing the hard drive and reformatting the hard disk

After changing the key for a HS256S old data can not be recovered. It is also impossible if there exists still a smart card with an old key. This “old” key can’t be used any more, because changing a key means always initializing the disk.

In his user documentation the manufacturer recommends always formatting the disk, after the destruction of the key, so that no further data can be reconstructed.

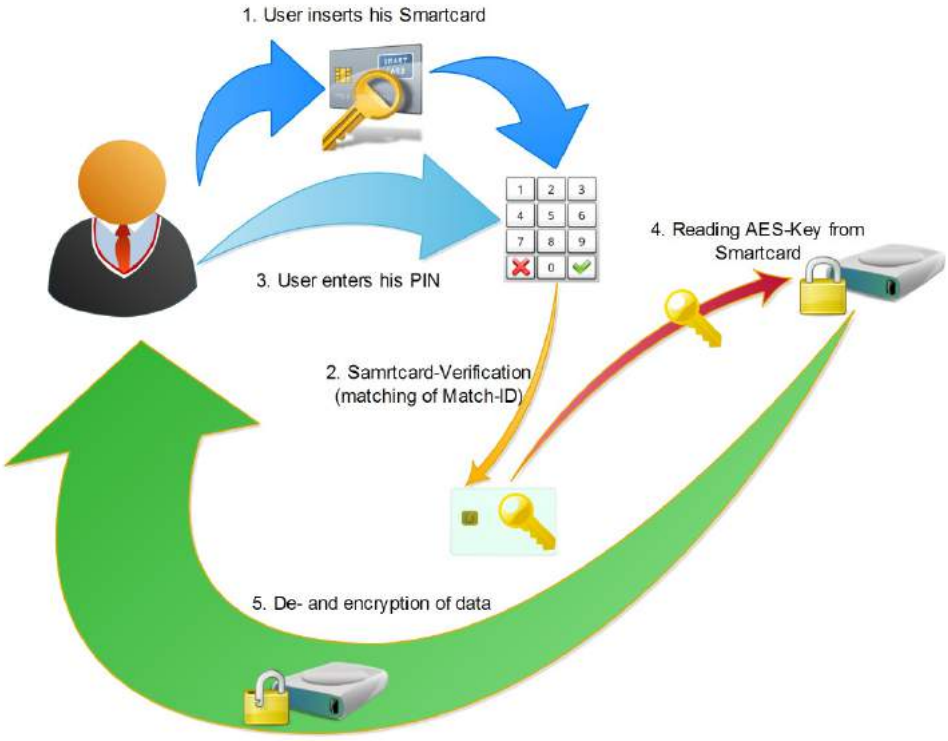
The hard disk can be used for any IT application, and therefore the operation, individual records, as well as individual data will be deleted.

Set 4: Data Subjects Rights

Compliance with Data Subject Rights is the responsibility of the controller that uses to product. The manufacturer has no influence if and how the controller respects the rights.

The decisive factor is whether the protection of the data subjects' rights with the product is possible. However, this is easily possible like using other data stores.

12. Data flow:



13. Privacy-enhancing functionalities:

The products makes uses of advanced encryption technologies that makes use of full disc hardware encryption using AES (256 bit, CBC mode) and a two-factor authentication (key on the smart card and knowing the smart card PIN). This ensures that access to data by unauthorised persons is not possible, even in case of loss or theft of the device.

14. Issues demanding special user attention:

    - none -

15. Compensation of weaknesses:

    - does not apply -

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*adequate*	There is no limitation of processing data with the product. The responsibility rests with the controller who makes use of the ToE.
Transparency	*excellent*	The product comes along with an excellent documentation, which includes hints for a lawful processing of personal data.
Technical-Organisational Measures	*excellent*	The technical-organisation measures taken by DIGITTRADE ensure the protection of data are excellent. It is assured that state-of-the-art measures are in place to protect access to data and programs by unauthorized third parties.
Data Subjects' Rights	*adequate*	The manufacturer has no influence on how each responsible administration respects the rights

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Flensburg, 01.03.2013	Stephan Hansen-Oest	
Place, Date	Name of Legal Expert	Signature of Legal Expert
Kellinghusen, 01.03.2013	Andreas Bethke	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Recertification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Place, Date	Name of Certification Body	Signature