

General Intelligence and
Security Service
Ministry of the Interior and
Kingdom Relations

Deployment Advisory iStorage diskAshur PRO² and diskAshur DT²

Date February 21, 2018

Colophon

Our reference number	:	8b5aa4ab-or1-1.0
	:	T +31 (0)79 320 50 50
	:	F +31 (0)70 320 07 33
	:	P.O. Box 20010 2500 EA The Hague The Netherlands
Copy number	:	
Author(s)	:	NLNCSA
Number of enclosures	:	0

Table of contents

Statement of Conformity 4
1 Introduction 5
1.1 Scope 5
1.2 Disclaimer 6
1.3 Certification scheme 6
1.4 Copyright information 7
1.5 Contact information 7
2 Product overview 8
2.1 Product version 8
2.2 Product identification 8
2.3 Security functions 8
2.4 Product description 8
2.5 Product category 9
2.6 Product configuration 9
3 The evaluated use-case for the product 10
4 Scope and limitations of the evaluation 11
4.1 Testing company 11
4.2 Test duration and time used 11
4.3 Evaluation process and scope 11
4.4 Product procurement, installation and configuration for evaluation 12
5 Recommendations for the administrator 13
5.1 Procurement of the product 13
5.2 Installation of the product 13
5.3 Configuration of the product 13
5.4 Security risks and countermeasures 13
5.5 Availability risks and countermeasures 14
6 Instructions for the user 15
6.1 Procurement of the product 15
6.2 Installation of the product 15
6.3 Configuration of the product 15
6.4 Security risks and countermeasures 15
6.5 Availability risks and countermeasures 15
6.6 Do's 16
6.7 Don'ts 17

8e6a1c37-or1-1.0

General Intelligence and
Security Service
Ministry of the Interior and
Kingdom Relations

Statement of Conformity

Hereby is stated that evaluation has demonstrated that the product:

iStorage diskAshur PRO² and diskAshur DT²

from
iStorage Limited

iStorage House, 13 Alperton Lane, Perivale, Middlesex UB6 8DH United Kingdom

is in conformity to:
Security Evaluation Target iStorage diskAshur PRO² and diskAshur DT v1.0,

October, 17, 2017

as demonstrated by:
Riscure located in Delft, Netherlands

Applying:
NL Scheme for Baseline Product Assessment, September 14, 2017

This Statement of Conformity (SoC) is part of the Deployment Advisory (DA) and is only valid if the recommendations and obligations in the DA are being followed.

The DA determines the conformity of the product with its SET and the effectiveness of the security features offered by the product.

This SoC declares that the product, when used in accordance with the DA, meets the security specification to a level sufficient to meet the requirements of the BIR.

This SoC relates only to a specific version of a product. If the product is changed, this SoC is not applicable any more. Newer versions of the products need to undergo the BSPA process anew to obtain a new Statement of Conformity.

Issuance of a SoC is no guarantee that the product is free from security vulnerabilities. Also, a SoC is not an endorsement of the IT product by NLNCSA and no warranty of the IT product by NLNCSA or by any other organisation, is either expressed or implied.

Issue date: 21 of February 2018

Head of the National Communications Security Agency of
the General Intelligence and Security Service

1 Introduction

1.1 Scope

Product name	iStorage diskAshur PRO² and diskAshur DT²
Product version	diskAshur PRO^2 Firmware Version: 1.6 diskAshur PRO^2 All Models: IS-DAP2-256-500-C-X, IS-DAP2-256-1000-C-X IS-DAP2-256-2000-C-X, IS-DAP2-256-3000-C-X IS-DAP2-256-4000-C-X, IS-DAP2-256-5000-C-X IS-DAP2-256-SSD-128-C-X, IS-DAP2-256-SSD-256-C-X IS-DAP2-256-SSD-512-C-X, IS-DAP2-256-SSD-1000-C-X IS-DAP2-256-SSD-2000-C-X, IS-DAP2-256-SSD-4000-C-X diskAshur DT^2 Firmware Version: 1.6 diskAshur DT^2 All Models: IS-DT2-256-1000-C-X, IS-DT2-256-2000-C-X IS-DT2-256-3000-C-X, IS-DT2-256-4000-C-X IS-DT2-256-6000-C-X, IS-DT2-256-8000-C-X IS-DT2-256-10000-C-X
Product category	Media and file security and Hardware and embedded software.
Evaluation criteria and version	BNC Evaluation Requirements [8640f72f-or1-1.0] (Pilot version); August 10th, 2015 *This deployment-advisory was made during the pilot-phase of the Baseline Security Product Assessment (BSPA) scheme.*
Vendor	iStorage Limited iStorage House, 13 Alperton Lane, Perivale, Middlesex UB6 8DH United Kingdom quan.xu@istorage-uk.com www.istorage-uk.com
Overseer	General Intelligence and Security Service Ministry of the Interior and Kingdom Relations Netherlands National Communications Security Agency (NLNCSA) P.O. Box 20010 2500 EA The Hague The Netherlands
Evaluation laboratory	Riscure B.V. Delftechpark 49 2628 XJ Delft The Netherlands

The goal of this Deployment Advisory is to inform consumers on:

- the specific use case for which the product has been tested,
- the manner in which the product has been tested and the limitations of this test process,
- the level of security provided by the product when used according to the prescribed use case,
- the residual risks of the product when used according to the prescribed use case.

This Deployment Advisory also gives guidance to users and/or administrators on how to securely use and configure the product.

1.2 Disclaimer

This advisory and associated Statement of Conformity applies only to the specific version of the product in its evaluated configuration (see section 2.1).

The Statement of Conformity is not a guarantee that the product is free from security vulnerabilities. Neither is it a guarantee that the product protects against adversaries with a high attack potential like (for example) intelligence organisations, organised (cyber-) crime organisations, terrorist organisations and capable security researchers.[1]

Exploitable vulnerabilities may be discovered after issuance of the Statement of Conformity. The organisation or individual using the product should check regularly if security vulnerabilities have been discovered and whether updates are provided by the vendor. Installation of updates must be compliant with the risk management policy[2] and risk appetite of the organisation or individual using the product. Updates should only be installed if there is sufficient trust or assurance that they improve the security of the product.

This advisory does not supersede or make redundant the (security-) instructions and documentation of the vendor. It is still necessary to consult these before installing and using the product.

All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

1.3 Certification scheme

The Dutch *Baseline Security Product Assessment* evaluates the security features of hardware and software security products for use in the "sensitive but unclassified" domain that is covered by the Dutch *Baseline Informatiebeveiliging Rijksdienst* (Dutch government security baseline, short: BIR). The main goals of the evaluation are:

- Establishing that the product conforms to the security specification in the Security Evaluation Target,
- Establishing the effectiveness of the security features offered by the product,

---

[1] For organisations and users from Dutch government organisations this implies that the maximum security level implied by the Statement of Conformity is the level of the Baseline Informatiebeveiliging Rijksdienst (BIR). The Statement of Conformity is not an accreditation of the product for protection of classified information.

[2] Organisations and users from Dutch government organisations will find risk management and update instructions in the BIR.

- Establishing that the product has a limited impact on the security of the host system.

Documentation and procedures of the Baseline Security Product Assessment scheme are available at the following Internet site: www.aivd.nl/informatiebeveiliging/bspa[3].

1.4 Copyright information

This report is published by the GISS / NLNCSA under the terms of the Creative Commons Attribution+Noncommercial+NoDerivativeWorks license, CC BY-NC-ND.

1.5 Contact information

All correspondence regarding this deployment advisory should be addressed to:

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations
NLNCSA
P.O. Box 20010
2500 EA The Hague
The Netherlands
bspa@nlncsa.nl

[3]During the BSPA pilot-phase this website will not be on-line. The URL is subject to change.

2 Product overview

2.1 Product version

This deployment advisory is limited to version iStorage diskAshur PRO² and iStorage diskAshur DT² with release version 1.6.

2.2 Product identification

The firmware version of the iStorage diskAshur PRO² and iStorage diskAshur DT² can be checked with the following procedure:

1. Unlock the unit as user or admin
2. Press and hold the keys "3" and "8" until the green and blue LEDs blink together.
3. Press "UNLOCK" button. All the LEDs (red, green and blue) become solid for one second.
4. The red LED blinks indicate the integral part of the firmware version number.
5. The green LED blinks indicate the fractional part of the firmware version number.
6. All the LEDs (red, green and blue) become solid for one second and the unit resumes its normal operation.

2.3 Security functions

The evaluated security functions of iStorage diskAshur PRO² and iStorage diskAshur DT² are:

- Access control to the protected data.
- User Data encryption with AES-XTS-256.
- Decryption key destruction when brute force attack is detected
- Security functions that are not evaluated are:
- The use of data encryption algorithms other than AES.
- Protection of unencrypted data while the system is active and the drive is unlocked.

2.4 Product description

The diskAshur PRO^2 and DT^2 secure storage drives feature a dedicated on-board Common Criteria EAL5+ ready hardware processor to enhance security through true random number generation and built-in cryptography protected by FIPS validated wrapping algorithms. Data is stored encrypted in the physical media using AES-XTS-256. The encryption and decryption process is transparent to the host system.

With software free setup and operation, the diskAshur PRO^2 and DT^2 are cross-platform compatible and work across various operating systems. The diskAshur PRO^2 and DT^2 enable user to access the data on the drive, by entering his own unique 7-15 digits PIN and with fast USB 3.1 he can access the data.

All the critical components of the devices are completely covered by a layer of epoxy

resin. This barrier is intended to prevent a potential attacker from accessing the critical components.

The diskAshur PRO^2 and DT^2 provides the following measures against brute force attacks: after fifteen consecutive incorrect PIN entries, the device assumes it is being attacked and will delete the encryption key, rendering all data previously stored on the drive as lost forever.

2.5 Product category

- 01 – Network security
- 02 – Network filtering, detection and response
- 03 – Secure messaging
- ☑ 04 – Media and file security
- 05 – Identity and access management
- 06 – Secure OS execution environment
- ☑ 07 – Hardware and embedded software

2.6 Product configuration

The user sets up an administrative PIN, and optionally a standard user PIN on diskAshur PRO^2 and DT^2 drives during the first-time use. By entering the correct PIN, the user can view the protected storage media from the host, and write the data to or read data from the media. Only the legit user knows the PIN therefore having the exclusive privilege to access the protected storage media.

The diskAshur PRO^2 and DT^2 goes to admin mode when the user executes the admin mode entering procedures using a valid administrative PIN. In the admin mode, the user can set up unattended auto lock time, standard user PIN policy, set the drive as write protect, etc. These administrative features offer different access levels for diskAshur PRO^2 and DT^2 thus improving the drive overall security.

If an incorrect PIN is entered 15 consecutive times, then all Admin/User PINs associated security parameters, the encryption key and all data will be deleted and lost forever. The diskAshur PRO^2 and DT^2 will then need to be formatted and partitioned before it can be reused.

3 The evaluated use-case for the product

The product has been evaluated for BSPA Security Evaluation secure storage of confidential information intended to ascertain the suitability of IT security products for use in the "sensitive but unclassified" domain that is covered by the Dutch Baseline Informatiebeveiliging Rijksdienst (Government security baseline, in short: BIR2017 up to level 2).

- The user needs to purchase iStorage diskAshur PRO² and iStorage diskAshur DT² from iStorage or one of its resellers. Upon receipt the device is ready for usage no additional software is required.
- The user sets up an administrative PIN, and optionally a standard user PIN on diskAshur PRO^2 and DT^2 drives during the first-time use. By entering the correct PIN, the user can view the protected storage media from the host, and write the data to or read data from the media. Only the legit user knows the PIN therefore having the exclusive privilege to access the protected storage media.
- If an incorrect PIN is entered 15 consecutive times, then all Admin/User PINs associated security parameters, the encryption key and all data will be deleted and lost forever. The diskAshur PRO^2 and DT^2 will then need to be formatted and partitioned before it can be reused.
- The user can set up a self-destruct PIN in admin mode. When used, the self-destruct PIN will delete the encryption key, ALL data, Admin/User PINs and then unlock the drive. Activating this feature will cause the self-destruct PIN to become the new User PIN and the diskAshur PRO^2 and DT^2 will need to be partitioned and formatted before any new data can be added to the drive.

4 Scope and limitations of the evaluation

4.1 Testing company

The security test has been performed by:

Riscure B.V.
Delftechpark 49
2628 XJ Delft
The Netherlands
https://www.riscure.com/

4.2 Test duration and time used

The vulnerability analysis and the security tests have been performed between the 16th of October, 2017 and 1st of December, 2017.

4.3 Evaluation process and scope

The following time-boxed evaluation process was employed:

- Analysis of the iStorage diskAshur PRO² and iStorage diskAshur DT² platform based on the provided documentation.
- Functional verification of the iStorage diskAshur PRO² and iStorage diskAshur DT².
- Comparison of equality between different models of the iStorage diskAshur PRO² and iStorage diskAshur DT².
- Cryptographic verification of the content encryption used by the iStorage diskAshur PRO² and iStorage diskAshur DT².
- Security evaluation based on the identified assets and provided documentation.
- Reporting of the evaluation.

The evaluation uses a gray-box approach, where all relevant functional details and security related details are made available by iStorage. The full datasheets and user manuals of the security relevant parts are not available due to NDAs. The source code is available under request, but no review was initially planned.

Logical and simple hardware attacks are considered in scope of the evaluation. More elaborated hardware attacks like fault injection or side channel attacks are out of the scope.

Target is evaluated to protect the confidentiality of the stored data against an attacker trying to access the information but without knowledge of the PIN's or data encryption key. Attack scenarios where the adversary could have access to the hard drive and install backdoors (i.e. "evil maid attacks") are not in the scope of the evaluation.

4.4 Product procurement, installation and configuration for evaluation

The product can be purchased from iStorage exclusive distributor in the Netherlands, which is E-quipment (https://e-quipment.eu). No special installation steps are required. Upon usage the user needs to set up an administrative PIN, and optionally a standard user PIN on diskAshur PRO^2 and DT^2.

5 Recommendations for the administrator

In the evaluated use-case the user and the administrator will often be the same person (see chapter 3). That's why we combined the recommendations for the administrator and the user (see chapter 6).

In some use cases the administrator and the user will be different persons. In this situation there are minor difference in recommendations. Please refer below to section 5.3.

5.1 Procurement of the product

iStorage diskAshur PRO² and iStorage diskAshur DT² can be purchased from iStorage exclusive distributor in the Netherlands, which is E-quipment (http://e-quipment.eu). No special installation steps are required. Upon delivery of the product the user needs to set up an administrative PIN, and optionally a standard user PIN on diskAshur PRO^2 and DT^2.

It is important to acquire the product from reputable and trusted sources e.g. the manufacturer's exclusive distributor, E-quipment (http://e-quipment.eu). If the user suspects that the product could have been manipulated by potential adversary during the distribution, for example, if the security seal has been removed or evidently manipulated, the product should be discarded.

5.2 Installation of the product

No installation steps are required upon delivery of the iStorage diskAshur PRO² and iStorage diskAshur DT².

5.3 Configuration of the product

In addition to what is written in section 6.3 the administrator shall configure the administrator private PIN different from the user PIN. The administrator PIN shall be only known to the administrator and not to the user. After administrator and the user PIN are configured the administrator can distribute the device to the user and inform the user about the user PIN.

5.4 Security risks and countermeasures

At the moment there are no countermeasures against the following risks:

- The iStorage diskAshur PRO^2 contains mechanisms that mitigate – but not fully prevent – the threat of tampering. There is a risk of an attacker installing a hardware or firmware backdoor in the hard disk without leaving physical external evidences.

5.5 Availability risks and countermeasures

The availability of the iStorage diskAshur PRO² and iStorage diskAshur DT² is not resistant against physical theft. However, the data contents cannot be retrieved without the correct pin, due to the encryption used.

At the moment there are no countermeasures against the following risks:

- The availability of the data after 15 incorrect PIN attempts.

6 Instructions for the user

6.1 Procurement of the product

iStorage diskAshur PRO² and iStorage diskAshur DT² can be purchased from iStorage exclusive distributor in the Netherlands, which is E-quipment (http://e-quipment.eu). No special installation steps are required. Upon delivery of the product the user needs to set up an administrative PIN, and optionally a standard user PIN on diskAshur PRO^2 and DT^2.

It is important to acquire the product from reputable and trusted sources e.g. the manufacturer's exclusive distributor, E-quipment (http://e-quipment.eu). If the user suspects that the product could have been manipulated by potential adversary during the distribution, for example, if the security seal has been removed or evidently manipulated, the product should be discarded.

6.2 Installation of the product

No installation steps are required upon delivery of the iStorage diskAshur PRO² and iStorage diskAshur DT².

6.3 Configuration of the product

Consult the most recent (security-) instructions and documentation of the vendor before configuring the product.

- The default administrator PIN should be changed before usage.
- The user pin policy should be set appropriately before usage.
- The unattended lock should be set appropriately before usage.
- Depending on the operation environment, the self-destruct PIN should be set appropriately.

Updates
This advisory and associated Statement of Conformity applies only to the specific version of the product in its evaluated configuration (see section 2.1) and not to any updates of the product.

6.4 Security risks and countermeasures

At the moment there are no countermeasures against the following risks:

- The iStorage diskAshur PRO^2 contains mechanisms that mitigate – but not fully prevent – the threat of tampering. There is a risk of an attacker installing a hardware or firmware backdoor in the hard disk without leaving physical external evidences.

6.5 Availability risks and countermeasures

The availability of the iStorage diskAshur PRO² and iStorage diskAshur DT² is not resistant against physical theft. However, the data contents cannot be retrieved without the correct pin, due to the encryption used.

At the moment there are no countermeasures against the following risks:

- The availability of the data after 15 incorrect PIN attempts.

6.6 Do's

- This product may only be used in an environment that protects against physical and logical attacks on the operating system and the computing devices used.
- Verify if the product is intact after procurement. The product should correspond to the picture below. If there is any damage to the case or signs of manipulation discard the hard disk.

	Description device 1	**Description device 2**
Model description	diskAshur PRO²	diskAshur DT²
Picture (external)		

- Change the default administrator PIN to a different unique and strong PIN (only numbers and "SHIFT" key can be used).
- Use a unique, strong PIN (only numbers and "SHIFT" key can be used) of at least 8 random digits and use at least one special digit combination ("SHIFT" key). Using 15 digits is recommended.
- Set the user pin policy to contain a minimum of 8 digits, and enforcing the use of at least 1 special digit combination ("SHIFT" key). Using 15 digits is recommended.
- Set the unattended lock to a recommended 5 minutes delay to lock the iStorage diskAshur PRO² and iStorage diskAshur DT² after 5 minutes of inactivity.
- The self-destruct PIN should only be set by the administrator in cases in which it is required to be able to quickly destroy the content of a hard disk.
- Be aware of people shoulder surfing and/or technical monitoring (for example surveillance camera's) to retrieve the PIN.
- Be alert for signs of physical tampering (Scratches or deformities in the metal case, rubber pieces and screws) of the iStorage diskAshur PRO² and iStorage diskAshur DT².
- Verify that firmware version is 1.6. Version can be verified by pressing a combination of keys. This is described in the user manual.
- Discard the hard disk if you suspect that it could have been manipulated by an adversary. In that situation, copy the information to a trusted device, wipe the suspicious hard disk and destroy it physically.

6.7 Don'ts

- Do not buy any version of the iStorage diskAshur PRO² and iStorage diskAshur DT² from any other distribution channel than E-quipment or E-quipment approved resellers.
- Do not use the default administrator PIN as either the administrator or user PIN.
- Do not use a PIN that corresponds to an easily identifiable password, i.e. the alphanumerical PIN combination of the name of the company, employee, or other commonly used passwords.
- Do not set the unattended lock to longer than 5 minutes.
- Do not disable the unattended lock.
- Never leave the hard disk unattended and physically accessible to an attacker.
- Do not use the hard disk if there is any suspicion that it could have been manipulated by an attacker. If you notice signs of physical tampering (scratches or deformities in the metal case, rubber pieces and screws) of the iStorage diskAshur PRO² and iStorage diskAshur DT² discard it.
- Do not use the iStorage diskAshur PRO² and iStorage diskAshur DT² in situations where there are risks of eavesdropping or shoulder surfing.
- Do not use the iStorage diskAshur PRO² and iStorage diskAshur DT² in situations where there is a risk of physical manipulation of the device.

* * *