diskAshur DT²®

Secure, Fast & Easy to Use Encrypted Desktop Drive

Ultra-secure, super speed USB 3.1, PIN authenticated, hardware encrypted desktop hard drive incorporating unique iStorage EDGE™ technology

Protecting You Always with Advanced Data Security

The diskAshur DT² is an easy to use, ultra-secure, hardware encrypted desktop hard drive with capacities of up to 10TB. Simply switch the power on and connect the USB 3.1 cable to any computer and enter a 7-15 digit PIN, if the correct PIN is entered, all data stored on the drive will be decrypted and accessible. To lock the drive and encrypt all data, simply eject the diskAshur DT² from the host computer and the entire contents of the drive will be encrypted (full disk encryption) using military grade AES-XTS 256-bit hardware encryption. If the drive is lost or stolen and an incorrect PIN is entered 15 consecutive times, the drive will reset, the encryption key will be deleted and all data previously stored on the drive will be lost forever.

One of the unique and underlying security features of the GDPR compliant diskAshur DT² is the dedicated hardware based secure microprocessor (Common Criteria EAL4+ ready), which employs built-in physical protection mechanisms designed to defend against external tamper, bypass attacks and fault injections. Unlike other solutions, the diskAshur DT² reacts to an automated attack by entering the deadlock frozen state, which renders all such attacks as useless.

In plain and simple terms, without the PIN there's no way in!

OS and Platform Independent

With software free setup and operation, the diskAshur DT² is platform/device agnostic and works across all operating systems including all versions of MS Windows, macOS, Linux, Android, Chrome, Thin Clients, Zero Clients and embedded systems. In fact it will work on any device with a USB port!

The diskAshur DT² is designed to be certified to FIPS 140-2 Level 2, NCSC CPA Foundation Level, Common Criteria and NLNCSA government accreditations. You will be the envy of your peers, friends and family and be safe in the knowledge that your data remains your data and is protected at all times.

Main Features

✔ Common Criteria EAL4+ ready on-board secure microprocessor	✔ FIPS 140-2 Level 2, NCSC CPA (foundation level), Common Criteria & NLNCSA - Certifications all pending
✔ Real-time military grade AES-XTS 256-bit Full-Disk Hardware Encryption	✔ No software or drivers required - 100% Hardware Encryption
✔ FIPS PUB 197 Validated Encryption Algorithm	✔ Read-Only (Write Protect) & Read/Write modes
✔ PINs and encryption keys are always encrypted while at rest	✔ PIN authenticated - Supports Admin and User Independent PINs 7-15 digits in length
✔ Brute Force Hack Defence Mechanism	✔ Self Destruct Feature
✔ Tamper Proof	✔ Drive Reset Feature for easy redeployment
✔ Immune to BadUSB	✔ Super Speed USB 3.1
✔ Epoxy coated wear resistant keypad	✔ Unattended Auto-Lock feature
✔ No speed degradation - as fast as any non-encrypted USB 3.1 HDD	✔ No admin rights needed
✔ Desk Lock Slot	✔ OS & Platform Independent - Works on any device with a USB port
✔ All components covered with a layer of super tough epoxy resin	

www.istorage-uk.com
info@istorage-uk.com I Tel: + 44 (0) 20 8991 6260 I Fax: + 44 (0) 20 8991 6277
iStorage Limited, iStorage House, 13 Alperton Lane, Perivale, Middlesex, UB6 8DH, UK

iStorage®

Technical Specifications	
Capacity	1TB, 2TB, 3TB, 4TB, 6TB, 8TB, 10TB
Data Transfer Speed	Read 225 MBps / Write 223 MBps
Power Supply	12V AC Adapter
Dimensions (W, D, H)	185.5 mm x 112 mm x 43.5 mm
Weight	1238 grams approx. (based on a 8TB drive, other capacities may vary)
Approvals	FIPS PUB 197 Validated, FCC, CE, RoHS, WEEE, TAA Compliant
Accreditations	FIPS 140-2 Level 2, NCSC CPA (foundation level), Common Criteria & NLNCSA- Certifications pending
Interface	Super Speed USB 3.1 - up to 5Gbps. Backward compatible with USB 3.0/2.0/1.1
Operating System Compatibility	MS Windows, macOS, Linux, Android, Chrome, Thin Clients, Zero Clients and embedded systems
Hardware Data Encryption	Real-Time Military Grade AES-XTS 256-bit Full-Disk Hardware Encryption
Warranty	2 Years
iStorage Part Number	IS-DT2-256-XXXX-C-G (xxxx = Capacity)
Box Contents	Drive, Universal Mains Adapter, USB cable & Quick Start Guide

EDGE™ Security Features

- Offering advanced portable data security via built-in FIPS PUB 197 validated AES 256-bit XTS hardware encryption engine. The data encryption key is randomly generated by a Common Criteria EAL4+ ready Random Number Generator and protected by NCSC, FIPS and Common Criteria validated wrapping algorithms.
- Uniquely featuring a dedicated on-board Common Criteria EAL4+ ready secure microprocessor to enhance security through true random number generation and built-in cryptography. The security component employs physical protection mechanisms to protect itself from any external tamper, bypass laser attacks and fault injections and incorporates active-shield violation technology. More specifically, the secure microprocessor reacts to all forms of automated hacking attempts by entering the deadlock frozen state where the device can only restart through a Power On Reset procedure (i.e. power off/power on).
- All authentication parameters are encrypted and physically protected by the microprocessors' memory encryption (scrambler) and access control schemes.
- The security lock feature protects the device against any unauthorised firmware modifications from the host side (fully protected against BadUSB)

Main Security Features Explained

Brute Force Hack Defence Mechanism: The iStorage diskAshur DT² is intelligently programmed to protect against all forms of Brute Force attacks. After five consecutive incorrect PIN entries the drive will freeze, requiring the drive to be powered off and powered back on again in order to get a further five PIN entry attempts. If a further five (10 in total) consecutive incorrect PIN attempts are entered again, the diskAshur DT² will freeze again. To get a further and final five PIN attempts (15 in total), the "shift" button must be pressed whilst powering the diskAshur DT² off and then powering back on before entering the iStorage preset PIN. On the fifteenth consecutive incorrect PIN entry, the diskAshur DT² assumes it is being attacked and will delete the encryption key and lock itself, rendering all data previously stored on the drive as lost forever. At this point the drive can be reset to factory default settings and redeployed.

Self Destruct Feature: You can pre-program the diskAshur DT² with your own unique Self Destruct PIN which, once implemented, instantly deletes the encryption key, all PINs, data and then creates a new encryption key.

Unattended Auto-Lock Feature: Set the unattended diskAshur DT² to automatically lock after a pre-determined amount of time where the drive has not been used.

Tamper Proof Design: In addition to incorporating a secure microprocessor, encrypting the data and the encryption key, the diskAshur DT² adds another barrier between your data and a hacker. All of the components of the diskAshur DT² are completely covered by a layer of super tough epoxy resin, which is virtually impossible to remove without causing permanent damage to the components. This barrier prevents a potential hacker from accessing the critical components and launching a variety of futile attacks.

Wear Resistant Epoxy Coated Keypad: Designed with protection in mind, the diskAshur DT² wear resistant epoxy coated keypad hides key usage to avoid tipping off a potential hacker to commonly used keys.

iStorage Product Range - Innovative data security solutions

FC CE RoHS

Trade Agreements Act (TAA) Compliant

CITRIX

www.istorage-uk.com
info@istorage-uk.com I Tel: + 44 (0) 20 8991 6260 I Fax: + 44 (0) 20 8991 6277
iStorage Limited, iStorage House, 13 Alperton Lane, Perivale, Middlesex, UB6 8DH, UK

iStorage®