

## L'hard disco esterno più sicuro mai realizzato

Hard disco esterno, ultra-sicuro, USB 3.1 super veloce, autenticato con PIN e con crittografia hardware, dotato dell'esclusiva tecnologia iStorage EDGE™

### Protezione costantemente garantita grazie alla sicurezza dati avanzata (Advanced Data Security)

Il diskAshur DT<sup>2</sup> è un hard disco esterno, semplice da utilizzare, ultra-sicuro, con crittografia hardware e capacità fino a 10TB. È sufficiente attivare l'alimentazione, collegare il cavo USB 3.1 a qualsiasi computer e immettere un PIN a 7-15 cifre. Se il PIN è corretto, tutti i dati memorizzati sul drive saranno decodificati e accessibili. Per bloccare il drive e crittografare tutti i dati, è sufficiente estrarre il diskAshur DT<sup>2</sup> dal computer host. Tutti i contenuti del drive saranno crittografati (crittografia di tutto il disco) mediante crittografia hardware AES a 256 bit di livello militare (modalità XTS). In caso di perdita o furto del drive, qualora si immetta un PIN errato per 15 volte consecutive, il drive sarà azzerato, la chiave di crittografia sarà cancellata e tutti i dati precedentemente memorizzati sul drive saranno persi irrimediabilmente.

Una delle funzioni di sicurezza esclusive e basilari del diskAshur DT<sup>2</sup> conforme a GDPR è il microprocessore dedicato e sicuro su base hardware (idoneo secondo lo standard Common Criteria EAL4+), che utilizza dei meccanismi di protezione fisica incorporati, ideati quale difesa dal rischio di manomissioni esterne, attacchi bypass e fault injection. A differenza di altre soluzioni, il diskAshurDT<sup>2</sup> reagisce ad eventuali attacchi automatizzati attivando lo stato di blocco, che rende vano qualsiasi attacco.

**In parole chiare e semplici, senza PIN, nessun accesso!**

### Indipendente dal SO e dalla piattaforma

Con funzionamento e configurazione libera del software, il diskAshurDT<sup>2</sup> è indipendente da piattaforma/dispositivo e funziona su tutti i sistemi operativi, fra cui tutte le versioni di MS Windows, macOS, Linux, Android, Chrome, Thin Client, Zero Client e sistemi integrati. Si può infatti utilizzare su qualsiasi dispositivo dotato di porta USB.

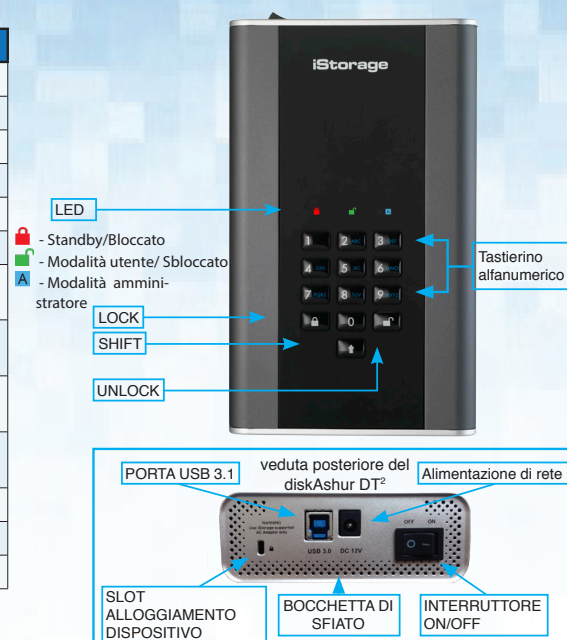
Il diskAshur DT<sup>2</sup> è stato ideato per essere certificato secondo gli accreditamenti governativi FIPS 140-2 Livello 2, NCSC CPA-Livello base, Common Criteria e NLNCSA. Sarai l'invidia dei tuoi compagni, amici e familiari, oltre ad essere certo che i tuoi dati rimarranno personali e saranno sempre protetti.



### Caratteristiche principali

- |  |  |
|--|--|
| ✓ Microprocessore sicuro incorporato idoneo secondo lo standard Common Criteria EAL4+          | ✓ FIPS 140-2 Livello 2, NCSC CPA (livello base), Common Criteria & NLNCSA - Tutte le certificazioni in attesa di registrazione |
| ✓ Crittografia hardware in tempo reale di tutto il disco AES-XTS a 256-bit di livello militare | ✓ Nessuna necessità di software o driver - Crittografia 100% hardware  |
| ✓ Algoritmo di crittografia convalidato FIPS PUB 197   | ✓ Modalità Solo lettura (protezione da scrittura) e Lettura/Scrittura  |
| ✓ I PIN e le chiavi di crittografia sono sempre crittografati quando non in funzione           | ✓ Accesso tramite PIN - PIN indipendenti Amministratore e Utente, lunghezza 7-15 cifre   |
| ✓ Meccanismo di difesa contro attacchi di forza bruta  | ✓ Funzione di autodistruzione  |
| ✓ A prova di manomissione  | ✓ Funzione di ripristino del drive, a garanzia di semplicità di riutilizzo   |
| ✓ Immune a BadUSB  | ✓ USB 3.1 super veloce   |
| ✓ Tastierino resistente all'usura, con rivestimento in resina epossidica                       | ✓ Funzione di autoblocco automatico  |
| ✓ Nessuna riduzione di velocità - rapido come qualsiasi USB 3.1 HDD non crittografato          | ✓ Nessuna necessità di diritti di amministratore   |
| ✓ Slot alloggiamento dispositivo   | ✓ Indipendentemente da sistema operativo e piattaforma - Funziona su qualsiasi dispositivo dotato di porta USB                 |
| ✓ Tutti i componenti sono rivestiti da uno strato di resistente resina epossidica              |  |

Caratteristiche tecniche	
Capacità	1TB, 2TB, 3TB, 4TB, 6TB, 8TB & 10TB
Velocità di trasferimento dati	Lettura 225 MBps / Scrittura 223 MBps
Alimentazione	Adattatore CA 12 V
Dimensioni (L, P, A)	185,5 mm x 112 mm x 43,5 mm
Peso	1238 grammi circa (basato su drive da 8TB. Altre capacità potrebbero variare)
Autorizzazioni	Convalidato FIPS PUB 197, conforme a FCC, CE, RoHS, WEEE, TAA
Accreditamenti	FIPS 140-2 Livello 2, NCSC CPA (livello base), Common Criteria e NLNCSA Certificazioni in attesa di registrazione
Interfaccia	USB 3.1 super veloce - fino a 5 Gbps. Parte posteriore compatibile con USB 3.0/2.0/1.1
Compatibilità con i sistemi operativi	MS Windows, macOS, Linux, Android, Chrome, Thin Client, Zero Client e sistemi integrati
Crittografia hardware dei dati	Crittografia hardware in tempo reale di tutto il disco AES-XTS a 256-bit di livello militare
Garanzia	2 anni
Codice iStorage	IS-DT2-256-XXXX-C-G (xxxx = capacità)
Contenuto della confezione	Drive, adattatore di rete universale, cavo USB e Guida rapida



## Funzioni di sicurezza EDGE™

- ✓ Garanzia di elevata sicurezza dei dati in modalità portatile mediante sistema incorporato di crittografia hardware AES-XTS a 256-bit convalidato FIPS PUB 197. La chiave di crittografia dati viene generata casualmente da un generatore casuale di numeri idoneo secondo lo standard Common Criteria EAL4+ e protetta da algoritmi di wrapping convalidati NCSC, FIPS e Common Criteria.
- ✓ Dotato di un esclusivo microprocessore sicuro integrato certificato secondo lo standard Common Criteria EAL4+ , a garanzia di maggiore sicurezza grazie alla generazione casuale dei numeri e alla crittografia incorporata. Il componente di sicurezza utilizza dei meccanismi di protezione fisica per proteggersi da manomissioni esterne, attacchi laser bypass e fault injection e adotta una tecnologia anti-iniezione di tipo "active-shield". In modo più specifico, il microprocessore sicuro reagisce a qualsiasi forma di tentativo di attacco automatizzato attivando lo stato di blocco, dove il dispositivo può essere riattivato solamente mediante una procedura di ripristino dell'alimentazione (vale a dire spegnimento/accensione).
- ✓ Tutti i parametri di autenticazione sono codificati e fisicamente protetti dalla codifica della memoria (scrambler) e dagli schemi di controllo accessi del microprocessore.
- ✓ La funzione di blocco di sicurezza protegge il dispositivo da qualsiasi modifica non autorizzata al firmware dal lato host (protezione totale da BadUSB)

## Spiegazione delle principali funzioni di sicurezza

**Meccanismo di difesa contro attacchi di forza bruta:** L'iStorage diskAshur DT<sup>2</sup> è programmato in modo intelligente per garantire la protezione da qualsiasi forma di attacco di forza bruta. Dopo cinque tentativi consecutivi di immissione di PIN errati, il drive si "congela" e dovrà quindi essere scollegato e ricollegato per ritentare l'immissione di ulteriori cinque PIN. In caso di ulteriori cinque (10 in totale) tentativi consecutivi di immissione di PIN errato, il diskAshur DT<sup>2</sup> si bloccherà nuovamente. Per effettuare gli ulteriori e ultimi cinque tentativi di immissione PIN (15 in totale), premere il pulsante "shift" durante la disattivazione del diskAshur DT<sup>2</sup>, quindi riattivarlo prima di immettere il PIN iStorage predefinito. Dopo la quindicesima immissione consecutiva del PIN errato, il diskAshur DT<sup>2</sup> presuppone la presenza di un attacco, cancellerà quindi la chiave di cifratura e si bloccherà, perdendo irrimediabilmente tutti i dati precedentemente memorizzati sul drive. A questo punto, ipotranno essere ripristinate le impostazioni di fabbrica predefinite, quindi il drive verrà riavviato.

**Funzione di autodistruzione:** è possibile pre-programmare il diskAshur DT<sup>2</sup> con il proprio PIN di autodistruzione esclusivo che, una volta implementato, cancellerà immediatamente la chiave di cifratura, tutti i PIN e i dati, creando quindi una nuova chiave di crittografia.

**Funzione di autoblocco automatico:** impostare la funzione di blocco automatico del diskAshurDT<sup>2</sup> per bloccarlo automaticamente dopo un periodo predefinito di non utilizzo del drive.

**Design a prova di manomissione:** oltre al microprocessore sicuro incorporato, la crittografia dei dati e la chiave di crittografia, il diskAshur DT<sup>2</sup> aggiunge un'altra barriera fra i dati e gli hacker. Tutti i componenti del diskAshur DT<sup>2</sup> sono totalmente rivestiti da uno strato di resina epossidica super-resistente, praticamente impossibile da rimuovere senza causare danni permanenti ai componenti. Questa barriera impedisce ad eventuali hacker di accedere ai componenti critici per lanciare una serie di futuri attacchi.

**Tastierino rivestito di resina epossidica resistente all'usura:** ideato pensando alla protezione, il tastierino rivestito di resina epossidica resistente all'usura del diskAshur DT<sup>2</sup> nasconde i tasti per evitare di insospettire eventuali hacker circa l'utilizzo di tasti di uso comune.



Progettato, sviluppato e assemblato nel Regno Unito.

## Gamma di prodotti iStorage - Soluzioni innovative per la sicurezza dei dati



FC CE RoHS



Conforme al Trade Agreements Act (TAA)



Tutti i marchi di fabbrica e nomi commerciali sono di proprietà dei rispettivi detentori.

[www.istorage-uk.com](http://www.istorage-uk.com)

info@istorage-uk.com | Tel.: + 44 (0) 20 8991 6260 | Fax: + 44 (0) 20 8991 6277  
iStorage Limited, iStorage House, 13 Alpertown Lane, Perivale, Middlesex, UB6 8DH, Regno Unito

**iStorage®**