Enterprise Data Protection

Hardware Encrypted USB Flash Drive with Second Factor Authentication

CRYPTonKEY

www.cryptonkey.com

Content:

What is CryptOnKey?

CryptOnKey is a Hardware Encrypted USB Flash Drive specially designed to enable Secure Team Collaboration.

CryptOnKey utilizes some simple techniques, that put together, produce an extremely strong data protection mechanism.

CryptOnKey is specially designed for a shared working environment, where few team members are collaborating together by exchanging sensitive business or private information.

CryptOnKey ensures Information is securely and reliably exchanged between team members, mitigating the risk of data leakage.

Protection Layers

1. **Password Protection**
   Users must authenticate using a Password

2. **Second Authentication Factor**
   The drive will only work on a pre-authenticated computer and its designated user account

3. **Data Encryption**
   New generation encryption techniques are used to prevent - brute attacks, hackers or malware – unauthorized access to data

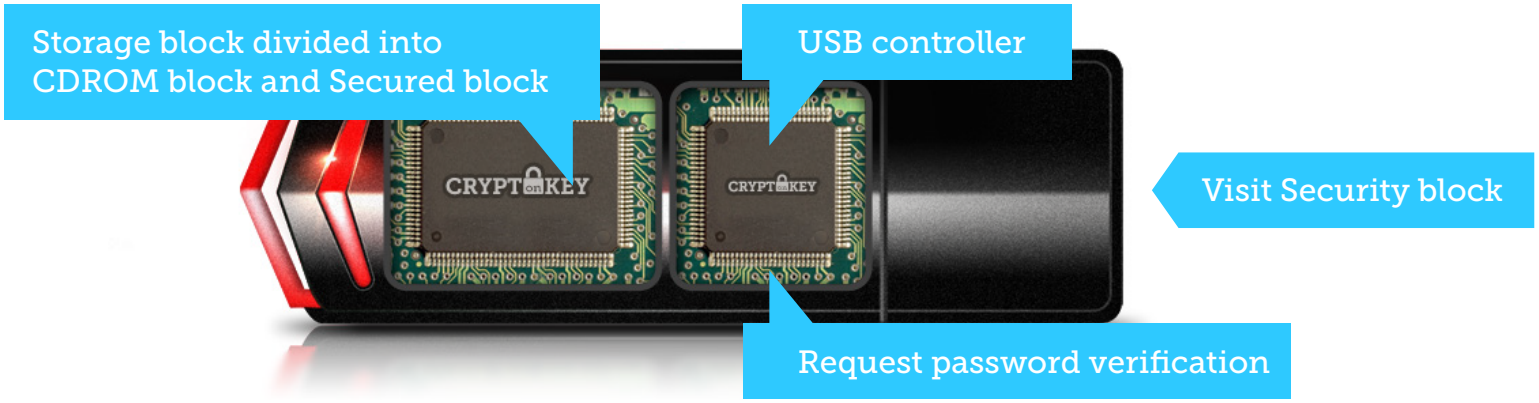
4. **Randomizing Encryption Key**
   New data on the disk is encrypted with fresh 128 bit encryption keys, making unauthorized access virtually impossible !

How it Works?

1 Password Protection

The drive is divided to 3 separate zones. First zone for a special SMI USB controller responsible for writing and reading information to and from the USB memory chip.

The USB memory itself consists of two zone blocks, a CDFS block holding the Secure Client Software and the secured User data zone. User Password is encrypted and saved within the controller, which permits access to the secured user zone only upon proper authentication procedure.



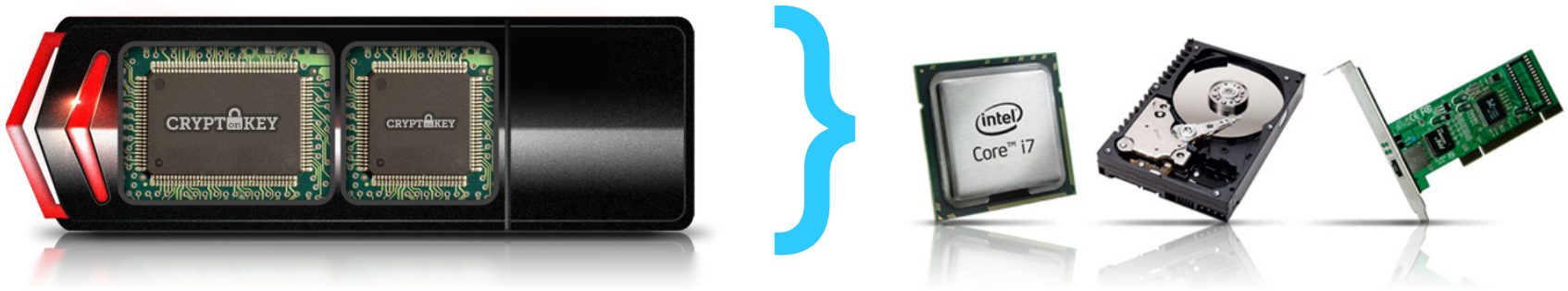
How it Works?

2 Second Authentication Factor

The controller identifies unique Hardware IDs of the user's computer - CPU ID, Hard Drive ID and Network Card ID. These IDs are used along with the user password to produce the encryption key.

Access to the Secured Zone is only allowed if the controller identifies an authorized computer with the correct hardware IDs.

Failing to authenticate the hardware IDs will cause the controller to shut down the power supply responsible for allowing access to the Secured User Zone.

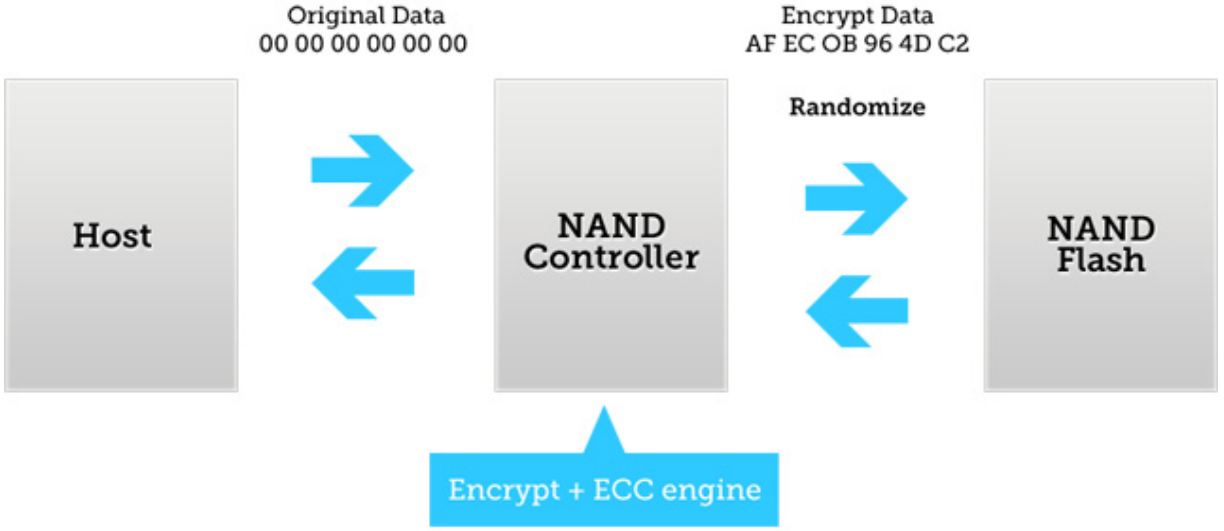


How it Works?

3 Data Encryption

Data written to the Secured Zone is encrypted by the controller, with a 128Bit symmetric encryption algorithm. Every 128 pages of written data, the encryption key is randomized.

The drive is also equipped with an Error Correction Code engine for verifying the consistency of read data.



Even More Secure!

Randomizing the Encryption Key on every 128 pages of written data is an additional layer of security, preventing repetition and hardening the strong 128bit encryption.