**James Chad Ballay**

**Locate the description of a self-encrypting drive product. Identify the encryption algorithm and cipher mode used. Describe how the drive manages encryption keys. Identify any product certifications held by that product (FIPS 140, for example).**

# Product: DT4000G2 Encrypted USB Flash Drive

<https://www.kingston.com/us/usb-flash-drives/datatraveler-4000g2-encrypted-usb-flash-drive>

Encryption Algorithm and Cipher Mode: 256 bit AES using XTS cipher mode

A screenshot of a cell phone

Description automatically generated

<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

<https://en.wikipedia.org/wiki/Disk_encryption_theory#XTS>

Product Certification: FIPS 140-2 Level 3 & TAA

\* TAA may not be directly related to the intent of your question but ensuring that nation state actors don’t introduce a backdoor at the core level for the device is why I included it.

A close up of a logo

Description automatically generated

<https://en.wikipedia.org/wiki/FIPS_140#Security_levels>

<https://en.wikipedia.org/wiki/Trade_Agreements_Act_of_1979>

**For each of the general types of attacks listed in Figure 1.7, describe how volume encryption helps resist that attack. Is there any attack that volume encryption might make more likely to occur?**

Physical Theft – This is the primary attack vector that it protects against. With physical access to a drive or machine you open up a veritable pandora’s box of vectors. Freezing hardware and then using an electron microscope to view the wiring. Tapping the circuits directly. Etc, etc…. All of these are either made harder or blocked completely with the introduction of volume encryption.

Denial of Service – Unfortunately this one gets increased. Tamper resistant hardware creates a larger surface area for an attacker to trigger a fault situation. If the drive self erases when it thinks it is being tampered with then maybe I can trigger that by modifying the voltage to the drive. Or inducing some sort of environmental change that triggers a fault condition.

Subversion – This doesn’t induce it to be any easier. If you have the ability to introduce malicious code, you probably already have access to the physical hardware. Are you have some sort of access that without volume encryption you would still have the same or greater dominion over the hardware.

Masquerade - Volume encryption isn’t meant to prevent this so at worse it doesn’t seem to make this easier.

Disclosure – Volume encryption isn’t meant to prevent this one either. All data coming in or out of the drive is intended to be encrypted so at a minimum it doesn’t make things worse.

Forgery – Volume encryption isn’t concerned with the veracity of the data that flows to and fro. It is focused on the data being what was intended to be. No molestation of the content.