The Krypt

Date:	27 May '15
Frequency:	Daily
Circulation:	Unavailable

The iStorage datAshur

Posted by Michael in Cryptography ≈ Leave a comment

Last year a small team of us at Security-Forensics had a good look at the datAshur USB drive, and I was almost tempted to order the datAshur Personal at £30 for 8GB. While both appear to be the same product with a different casing, there are technical differences potential buyers need to be aware of. To summarise, I ended up ordering the original datAshur because its level of security is pretty damn impressive – the datAshur Personal maybe less so.

To recap, the datAshur we looked at was basically an encrypted storage device that works differently to most other encrypted USB drives on the market. It uses an onboard Hardware Security Module (HSM, or 'crypto-processor'), whereas other devices typically interact with a software application. It's quite compact and feels expensive. I like it, but is it actually secure enough?
Apparently the datAshur has 'military grade encryption'. While that's technically a marketing term that doesn't really mean anything, the hardware-based AES 256 would be *practically* unbreakable *depending on* how the encryption key is managed. This is where the FIPS standard becomes important.

The main thing I was concerned about is the datAshur personal is stated as simply having a 'FIPS PUB 197 Validated Encryption Algorithm', while the older device is 'FIPS Security 140-2 Level 3 Certified'. Essentially the cheaper datAshur Personal is missing a layer of security that was in the original product, being merely 'tamper evident' rather than 'tamper resistant'.

It's worth exploring why that's important, because consumer reviews don't even touch on this, and it took some digging to find the technical details of the device. Both products work by using a Hardware Security Module (HSM) to mediate the I/O and encrypt/decrypt whatever's stored on the main memory chip. The HSM itself is unlocked with the user's PIN, so the datAshur can't be mounted directly.

But that's still not secure, if the casing can be opened, the encrypted data pulled off the chip and decrypted. With the older datAshur product, this would be an extremely awkward task, as its circuitry is sealed in epoxy and both chips have a 'memory protect fuse' to prevent them being read externally. The datAshure Personal doesn't have that level of protection, apparently, for some reason. The salient point here is the HSM appears to be generating and storing a random encryption key each time the device is reset, so the high tamper resistance would offset the disadvantage of having a stored key. If the casing was somehow opened the data would most likely be unrecoverable, as it's extremely unlikely the main storage and HSM could be accessed without one or both being destroyed.

So, I bought the older datAshur product because I'm dead certain nothing can be recovered from it without considerable resources, expertise and determination – this is definitely worth the admittedly large trade-offs for the security. The datAshur personal, on the other hand, is probably okay if you want privacy of non-sensitive files at a lower cost.