Appendix 07
Storage Media

Electronic storage media for MKD with internal hardware encryption and access protection began in the 1980s with smart cards featuring a processor compliant with ISO/IEC 7816. While smart cards can provide very high security—highly certified (e.g., CC EAL 4+) and having proven their security on the market for decades in passports, payment cards, etc.—their storage capacity is currently limited to a few megabytes at most, making them suitable only for mathematical cryptographic methods.

For a one-time pad—and thus consistently absolute data security—storage capacities in the gigabyte and terabyte range are required. Portable storage media with these capacities, internal hardware encryption, and access protection only entered the mass market in this century; their application was, and still is today, highly secure data backup.

This made MKD, in combination with a one-time pad, feasible at a cost of less than a thousand euros per device. MKD gained a whole new dimension in terms of applicability, and absolute security in data encryption and integration protection became possible even in the low-cost segment. With TCG Opal 2.0, an industry standard for external storage media with self-encryption has also been established.

1 Market Overview

Comparison of products available on the European market (the list is not exhaustive), specifications in bytes

Product Name	Type, Interface	Storage capacity in bytes	Approx. price in US dollars	AES-256 integrated	Input device for PIN, etc.,	Read/ write speed
Apricon Aegis Padlock / Fortress	USB	1 to 2 TB	270 to 600	Yes	PIN	500 MB/s
Data Traveller 2000	Flash drive, USB	64 GB	80	Yes, with XTS	PIN	100–150 MB/s
Kingston IronKey Vault Privacy 80	Flash drive, USB	1 to 4 TB	400 to 480	Yes, with XTS	PIN	250 MB/s
Kingston XS2000	Flash drive, USB	2 TB	190	Yes, XTS	PIN	100–150 MB/s
iStorage diskAshur Pro3 SSD	Flash drive, USB	512 GB to 4 TB	310 to 1,300	Yes, with XTS	PIN	450 MB/s
Digitrade HS256 S3	SSD, USB	500 GB to 4 TB	1,100 to 1,800	Yes	PIN, chip card	200 MB/s
KOBRA Stick VS	Flash drive, USB	16 GB to 512 GB		Yes	PIN, chip card	120 MB/s
KOBRA Drive VS	SSD, USB	1 TB to 16 TB	1,100	Yes	PIN, chip card	250 MB/s

All products are security-certified, e.g., the Kobra Drive VS with BSI-VS NfD (classified information), EAL 2, EU restricted, NATO restricted.

Most products available on the market are dustproof, waterproof, and shock resistant. Some products erase all stored key bits after several failed PIN entry attempts.

Some SSDs also include their own non-deterministic random number generator. SSDs that feature a built-in random number generator (TRNG) include, for example,

the Samsung 970 EVO Plus NVMe M.2 SSD, the Western Digital WD Black SN850X NVMe SSD, and the Crucial P5 Plus NVMe M.2 SSD. However, these random number generators are relatively slow and not suitable for generating the non-deterministic key bits required for an MKD application using a one-time pad.

SSDs are characterized by high storage capacity—currently up to 16 TB with MKD capability—and are quiet, compatible, and shock-resistant. NVMe SSDs also feature extremely high read/write speeds. However, they typically have an external PCIe 3.0 to 5.0 interface, generate higher temperatures, and are more expensive than traditional SSDs.

2 NVMe (Non-Volatile Memory Express)

NVMe is an advancement in SSD technology that uses the PCIe protocol to significantly increase storage access speeds. Compared to SATA SSDs, NVMe drives can read and write data at speeds of up to 7 GB/s. NVMe drives not only offer fast read and write speeds but also extremely low latency, making them particularly efficient. However, they require modern hardware that supports the M.2 or PCIe standard. The higher heat generation during intensive use can be a drawback, which is why heat sinks are often used.