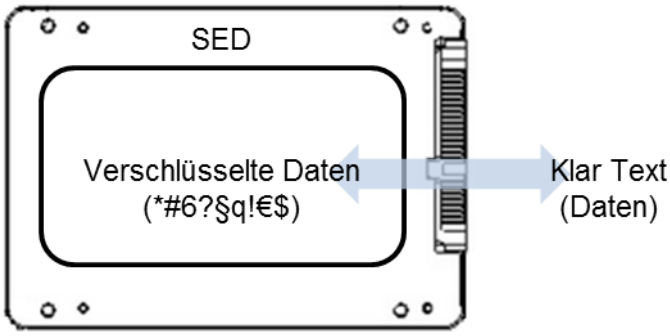
Self-Encrypting Drive (SED)

SEDs sind selbstverschlüsselnde Laufwerke, die auf Hardwareverschlüsselung basieren. Ein SED verschlüsselt stets sämtliche Daten mit einem intern generierten Zufallswert, bevor sie in die Flash-Chips geschrieben werden. Dadurch dass die Ver- und Entschlüsselung selbständig im Controller der SSD erfolgt, wird im Gegensatz zu einer Software-Verschlüsselung die CPU und der RAM von dieser Arbeit befreit. Ein weiterer Vorteil ist, dass die CPU oder der RAM keine möglichen Angriffsziele für Hacker mehr sind. Anders als bei Software-Verschlüsselung funktioniert mit solch einer SED auch die Trim-Funktion; zudem vermeiden solche Laufwerke das Risiko, dass wegen des Wear Levelings unverschlüsselte oder anders verschlüsselte Reste alter Daten in den Flash-Chips zurückbleiben. Daten in den Flash-Chips einer SED lassen sich ohne den Controller nicht mehr lesen, also auch nicht retten.
Indem die Ver- und Entschlüsselung der Daten in einem SED erst im Flash Controller erfolgt, bietet eine SED allein keine umfassende Datensicherheit.



Advanced Encryption Standard (AES)

Eine weitverbreitete Methode zur Verschlüsselung von Daten in Speichermedien wie bei SED‘s ist das AES Verfahren. Der AES-Algorithmus ist eine symmetrische Blockchiffre, welche einen kryptographische Schlüssel von 128, 192 und 256 Bits Länge verwenden kann, um Daten in Blöcken von 128 Bits ver- und entschlüsseln zu können.
Weitere Informationen finden Sie hier:
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

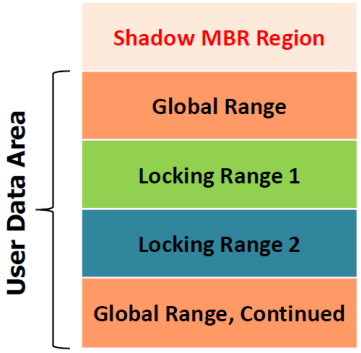
ATA-Passwort

Eine einfache „ältere“ Methode um eine umfassende Datensicherheit her zu stellen ist, das Setzen des ATA-Passworts im BIOS/UEFI. Danach ist ein Zugriff auf die SSD nur noch für Systeme möglich, welche das entsprechende Passwort und Kommando überträgt. Handelt es sich bei dieser SSD um eine SED, bleiben auch Angriffe auf den NAND selbst erfolglos, da enthaltene Daten ausschließlich verschlüsselt gespeichert sind.
Diese umfassende Datensicherheit macht eine Datenrettung bei Verlust des ATA-Passworts unmöglich.

TCG SSC Opal

Die Trusted Computing Group (TCG) ist eine Organisation, die offene Standards für vertrauenswürdige Computerplattformen entwickelt. Der TCG gehören eine Vielzahl von führenden Herstellern von Speicherlösungen, Technologiekonzernen und Software Unternehmen an.
https://trustedcomputinggroup.org/membership/member-companies/
Unteranderem spezifizierte sie den Security Subsystem Class (SSC) Opal Standard.
Die SSC Opal Spezifikation wurde erstellt, um die Vertraulichkeit von gespeicherten Benutzerdaten auf Speichermedien vor unberechtigtem Zugriff zu schützen, sobald diese die Kontrolle des Besitzers verlässt. Diese Spezifikation ist Herstellerübergreifend.
Die SSC Opal definiert eine voll funktionsfähige Schnittstelle zur Verwaltung der Sicherheitsfunktionen auf einem Speichermedium, einschließlich Geräteverschlüsselung. Sie führt die Vorteile einer Software und Hardware Verschlüsselung zusammen. Um dies zu gewährleisten muss das Speichermedium eine SED sein und eine AES-128bit oder AES-256bit Verschlüsselung besitzen.

Spezialisierte „Independent Software Vendors“ (ISV) bieten Software Lösungen an um das Opal Feature zu aktivieren und zu verwalten.
Eine Opal SSD wird in verschiedene Bereiche aufgeteilt. Die Shadow MBR Region bietet einen Ort zum Booten in eine sichere Umgebung zur Authentifizierung vor dem Start, um eine Geräteentsperrung durchzuführen. Hier wird die Pre-boot Umgebung von der ISV Software angelegt, in der die Bereiche und Schlüssel zum Entsperren hinterlegt sind. Jeder einzelne Bereich „LBA Locking Range“ besitzt seinen eigenen Schlüssel.



Es gilt zu beachten, wenn Opal an einer SED SSD aktiviert ist, dann ist die ATA Passwort Funktion deaktiviert.

Sollte bei aktiviertem OPAL die Security ID (SID) oder die Verwaltbarkeit des Speichermediums verlorengegangen sein, kann über die Physical Presence SID (PSID) das Gerät auf den Werkszustand zurück gesetzt werden. Die PSID ist eine durch die TCG spezifizierte Zeichenkette mit 32-Stellen. Die PSID wird bei Xmore® 2,5“ SSD’s auf das Rückseiten Label aufgedruckt. Ein Tool zum Übertragen der PSID und somit zum zurücksetzten des Speichermediums auf Werkszustand kann durch Xmore® zur Verfügung gestellt werden.

eDrive

Der eDrive Standard (Encrypted Drive) von Microsoft® organisiert den Zugriff durch das Betriebssystem mit Hilfe des Bitlockers auf das SED Speichermedium. Der eDrive Standard basiert dabei auf der TCG OPAL und IEEE 1667. IEEE 1667 ist ein Standradprotokoll für die Authentifizierung von Host anhängige Speichermedien. Diese Spezifikationen müssen von einem SED Speichermedium unterstütz werden, damit die eDrive Funktion genutzt werden kann.
Durch das Auslagern der Verschlüsselung auf die Hardware der SED wird die Performance von Bitlocker gesteigert, die Host Auslastung reduziert und der Stromverbrauch reduziert werden.