DIGISTOR®

SECURE DATA STORAGE

Building a Citadel of Trust in a Zero Trust World

Data must be safe, but available

Your challenge is to secure your network. That really means secure your data. At the same time, to fulfill your mission, your network and data have to be readily available from anywhere: at headquarters, at known satellite offices, and increasingly, at a dynamically changing variety of field locations.

Your attention has to be on your external adversaries, as it always has been, but you must also include insider threats, which account for a large number of data loss incidents. Zero trust must be your operating principle. The issues of data protection, endpoint security and user authentication all apply at every level of your organization regardless of role—and regardless of location.

You need to deliver a security architecture to fully protect against all threats. It starts with a highly secure data at rest solution. Without that, you have no foundation upon which to build.

The problem is well understood

Data is most secure when it is properly encrypted on a storage device that has been powered all the way down and whose data encryption key (DEK) is unavailable. Ideally the SSD is also locked when powered down. This means that even if the drive falls into the wrong hands, the contents are not accessible until unlocked. Such a mechanism renders it impossible for the drive to be replicated. Should your equipment come into the possession

of a well-funded, organized, and determined adversary, a likely first step is for them to attempt to make multiple copies of your drives. This enables your adversary to mount parallel attacks, while having backups against the measures that you have taken to destroy the data following repeated failed login attempts.

Software encryption exists of course. However, the system must be booted and active before software encryption can be engaged. That is a lot of capability to put online, already exposed, before your security measures are fully active. While the algorithm is active, the DEKs for software encryption are almost always stored in plain text in system memory while active. This is a very broad attack surface to provide to your adversary. It is easy for software encryption DEKs to be copied. Indeed, DEK duplication is common during normal operation for many secure data implementations. Even if these duplicate DEKs are in obscured form, cryptographic erasure is rendered far less than certain. Moreover, encryption is computationally intensive, therefore the overhead of software encryption uses precious system processing power.

Hardware encryption is efficient

Hardware encryption on a self-encrypting drive (SED) is much more elemental. It has a much smaller attack surface. The hardware encryption engine uses no system processing resources. The security functionality around releasing the DEK to the SED's Encryption Engine (EE) must occur as the system is coming up. Indeed, if the SED is a boot device, key release must be a pre-boot activity. The DEK never leaves the SED. Upon power down, the key is removed from volatile memory and it is only ever stored in non-volatile memory in a cryptographically protected form. Accessing the DEK is therefore a much tougher challenge for the aggressor. When the DEK is deleted from the EE, or replaced, the data on the SED is irretrievably unrecoverable.

AES-256 is part of the Commercial National Security Algorithm suite of cryptographic algorithms approved by the NSA to protect our nation's most critical secrets. A correct implementation of AES-256 can be independently certified. It is readily commercially available. There is really no excuse for you not to use an SED whose EE fully implements this algorithm.

Pre-boot authentication (PBA)

The critical step then is the unlocking of the SED, a key element of which is releasing the DEK to the EE. Optimum security makes authenticating your users central to this process. Adding multi-factor authentication can increase your confidence in the user's identity and allow you to gain confidence in other aspects of the end-equipment's configuration and environment. In the secure storage world, this process is known as Authorization Acquisition (AA). Ensuring that this happens

DAR Solution Checklist

- ☐ Lock Feature
- ☐ H/W AES 256 Crypto
- ☐ Pre-Boot Authentication
  - ☐ Built-in
  - ☐ Multi-Factor
  - ☐ Least privilege role enforcement
  - ☐ Erase on repeated AA failure
  - ☐ Configuration management
- ☐ 3rd Party Certifications
  - ☐ TAA
  - ☐ FIPS 197
  - ☐ FIPS Validated
  - ☐ Common Criteria validated
  - ☐ NIAP-Listed
  - ☐ CSfC-Listed
- ☐ Current technology
  - ☐ 2.5-inch (7mm) & M.2
  - ☐ SATA III & NVMe
  - ☐ Up to 2TB
  - ☐ up to 3.4 GB/s

prior to booting the OS is called Pre-Boot Authentication (PBA).

Simple passwords that unlock functionality may be adequate for some applications, but much more secure is a password, or passphrase that can be hashed to provide a value that is itself used to cryptographically unlock the DEK. Of course, the user must use a sufficiently complex password. It must be known only to them. It must not be written down anywhere. By these means and others it should be withheld from an adversary. However, the many case histories of hackers succeeding with phishing scams are a reminder that, despite all of our warnings and training, not all users are as careful as they need to be with password security. The ability to add two factor authentication to the AA process builds confidence in the identity of the person attempting to access the SED. A simple

mechanism to delete the DEK after a maximum number of failed logins further enhances the solution. Providing a mechanism to allow the user to trigger such cryptographic erasure should they be operating under duress adds yet another layer of security.

When PBA is employed, particularly on endpoint equipment, it brings additional values. By properly maintaining role separation between system administrators and users, you can have confidence that the systems and applications software on the boot drive are fully authentic. This adds to the confidence that you have in your other trusted boot mechanisms. Said software can then check that the endpoint equipment is properly configured and in an acceptable environment before accessing your network in a secure and approved fashion.

Implementing all of these measures is complex. Third party certifications establish confidence that your solution will deliver on its security promise. The Federal Information Processing Standards (FIPS), administered by the National Institute of Standards and Technology (NIST), go a long way here. FIPS 197 assures correct implementation of the complicated AES crypto algorithm. FIPS 140-2 assures that the EE engine has been properly designed and secured. FIPS 140-2 L2 is the accepted minimum level for most applications and ensures that there is visible evidence of any physical tampering of the SSD.

The Common Criteria (CC) standard maintained by NIAP, and related international bodies, assures that the AA and EE functions have been properly engineered and that the interfaces between AA and EE are free from critical information leaks. Certification to these standards is a requirement for US Government IT deployments and security sensitive commercial applications are also increasingly demanding their adoption. President Biden's Executive Order of May 12, 2021 reinforced that requirement and included retrofitting certified encrypted and authenticated Data at Rest (DAR) to existing installations.

All storage devices in your zero-trust network must be SEDs whose critical security mechanisms have been independently certified to meet a standard at least equal to the sensitivity of your data. Their capabilities should

be understood by your team and fully leveraged by your systems administration and operational security policies.

Seeking a solution

While adopting these measures is central to your needs, they are not proving easy to find off the shelf.

There are commercial solutions that claim security properties yet have no third-party certifications.

There are full military-grade, NSA-approved solutions that may carry all of the certifications that matter, but they have failed to keep up with commercial densities, interfaces and formats. In addition, they are extremely expensive, making them impractical beyond a very narrow set of highly specialized applications.

AES 256 cryptography is almost universally available from commercial SSD vendors. There are even a steadily increasing number of vendors who have successfully certified their EE solutions to the FIPS 140-2 level 2 standard, but they lack an out of the box AA solution.

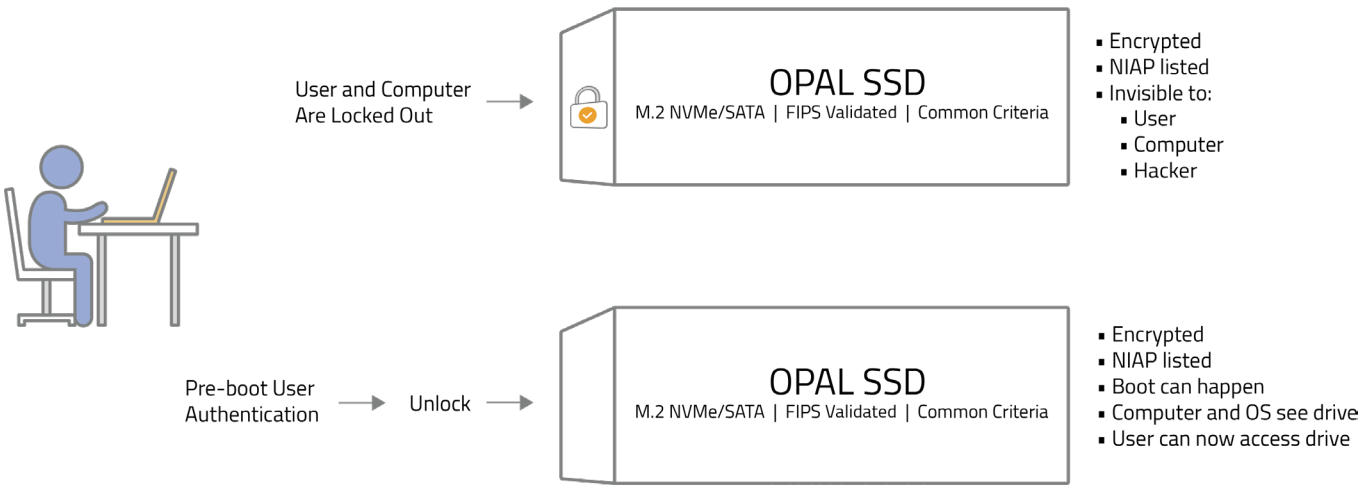
There are finally a few SSDs emerging that claim to support the TCG Opal 2.0 standard for SEDs. This standard includes a shadow Master Boot Record (MBR) mechanism that can support an AA function, which on a boot device would have to be PBA. Furthermore, the Opal standard supports a lock mechanism that prevents the SSD from being replicated.

Frustratingly, the vendors who claim to have implemented Opal have only implemented the EE side of securing data at rest. None of them have available software to place in the shadow MBR and implement the PBA functionality. These vendors simply state that all things are possible—all you need is someone to write the code.

In the face of these challenges, it may look like you might have to develop your own solution. Something for which you have not the time, staffing, budget, bandwidth nor ambition to do.

DIGISTOR Citadel™ SSDs for Securing Data at Rest (DAR)

The DIGISTOR Citadel family of secure SSDs, complement existing DIGISTOR offerings, suited for securing data at rest (DIGISTOR FIPS 140-2 L2 self-encrypting SSDs, DIGISTOR TCG Opal 2.0 self-encrypting SSDs). Citadel SSDs solve many of the problems that kept people from implementing robust security solutions



for Data at Rest. Citadel is a complete solution leveraging commercial technology from TAA compliant sources that you can make central to your zero-trust environment.

Citadel SSDs are engineered to be deployed in secure military systems—and integrate all the features that you need in a readily configurable package.

A Citadel SSD is automatically locked when powered off. There is no possibility to replicate the SSD unless the PBA process has been fully executed. Should an adversary somehow get around that obstacle, the SSD contents are protected with a FIPS 197 certified AES 256 encryption engine embedded in a cryptographic module that is fully certified to FIPS 140-2 L2.

With built in, fully configurable PBA software, a full user authentication process, with optional two factor authentication, must occur before your OS or hypervisor even begins to boot. Moreover, the PBA software is completely agnostic as to your choice of runtime OS.

Citadel Solution Checklist

- ☑ Lock Feature
- ☑ H/W AES 256 Crypto
- ☑ Pre-Boot Authentication
  - ☑ Built-in
  - ☑ Multi-Factor
  - ☑ Least privilege role enforcement
  - ☑ Erase on repeated AA failure
  - ☑ Configuration management
- ☑ 3rd Party Certifications
  - ☑ TAA
  - ☑ FIPS 197
  - ☑ FIPS Validated
  - ☑ Common Criteria validated
  - ☑ NIAP-Listed
  - ☑ CSfC-Listed
- ☑ Current technology
  - ☑ 2.5-inch (7mm) & M.2
  - ☑ SATA III & NVMe
  - ☑ Up to 2TB
  - ☑ up to 3.4 GB/s

The Citadel configuration management and PBA software supports four operating roles – System Administrator, Help Desk Technician, Security Officer, and Login User–each with different privileges.

This entire package conforms to the Common Criteria requirements, are NIAP listed and forms the very heart of your zero-trust layered security solution.

By adopting commercial technologies, the Citadel SSD product family can be readily incorporated into standard laptop and desktop systems. Thes SSDs support SATA 3.2 and NVMe 1.3 (PCIe 3.1) interfaces; 7mm 2.5" and M.2 formats; densities up to 2TB and speeds up to 3.4GBps. The pre-installed FIPS- and CC-certified PBA software ensures that Citadel SSDs are ready for rapid deployment right out of the box.

DIGISTOR Citadel SSDs are NIAP-and CSfC-listed. They are thoroughly tested and represent a full CSfC layer of protection. Learn about the importance of CSfC in this blog.

By creating a virtual cybersecurity stronghold, DIGISTOR Citadel SSDs will protect your secrets even against an adversary who has possession of your SSD.

For further information about Citadel SSDs, please visit digistor.com/citadel.