WHITE PAPER

Demystifying Hardware Full Disk Encryption Technology for Military Data Storage

BOB LAZARAVICH, TECHNICAL DIRECTOR
PHILIP FULMER, DIRECTOR OF PRODUCT MARKETING
JUNE 2017

mercury systems™

Data Storage for Military Applications

Moore's Law has enabled high-density NAND flash to be mass-produced at price points appropriate for adoption in commodity applications like solid-state drives (SSD) deployed in consumer PCs, enterprise servers, and automotive vehicles. Unlike conventional hard disk drives with rotating magnetic media, SSDs offer substantially higher sustained read and write speeds with lower power consumption. NAND flash media reliability concerns have largely been addressed through (1) advances in error correction code (ECC) and wear leveling algorithms and (2) NAND flash over-provisioning. For the typical person in the 21st century, modern SSDs are nearly the holy grail of long-term consumer data storage. Few of us experience the failure of a SSD in a computer; in the event of such a failure we simply replace the failed drive or use the opportunity to upgrade to the latest device model featuring a faster processor or higher-resolution display, in addition to taking advantage of the latest developments in NAND flash technology. To most consumers, the uncommon SSD failure is of little long-term consequence thanks to the advances discussed above.

Secure SSDs

While the consumer market promotes rapid adoption of new microelectronics with ever-shortening product life cycles, the military market demands risk mitigation and long-term supply continuity -- even for commercial-off-the-shelf (COTS) parts modified or screened to military requirements. Given the advantages of SSD devices that consumers take for granted today, it is not surprising to see SSD devices adopted for military applications. Our previous white paper, Safeguarding Mission Critical Data with Secure Solid State Drives, described the requirements for a military grade SSD with embedded security. In particular, we maintain that security cannot simply be "bolted on" to a commercial- or even an automotive-grade SSD. Security must be rooted in the design of the military-grade SSD from the early concept stages of development. In this particular use case, design references not only the mechanical and electrical specifications, but also the security of the manufacturing location and the judicious selection of components and supply chain partners. As such, we refer to an SSD engineered to military grade standards and manufactured in a secure and trusted environment as a Secure Military Grade SSD, or simply Secure SSD.

Having defined the parameters used for the design and manufacturability of a Secure Military Grade SSD, the next logical subject matter for discussion is the practical implementation of this new class of device for a military application. This white paper discusses the implementation of a commercially available Secure SSD for the storage of classified, secret, and top secret data in accordance with government requirements. Before opening this discussion, however, some additional background is required.

Securing Classified Data

Historically, classified, secret, and top secret data storage could only be accomplished through the implementation of a Government-Off-the-Shelf (GOTS) Type 1 security solution. Following government protocols, the desired end result -- data at rest (DAR) protection – is achieved. Although the detailed steps required for practical implementation of a Type 1 security solution are beyond the scope of this white paper, Type 1 security solutions are broadly associated with lengthy implementation times and significant development costs. For clarity, we do not question the integrity or suitability of a Type 1 security solution for data at rest protection.

Commercial Solutions for Classified (CSfC) Programs

Recognizing that US government customers have an increasing need for the most advanced and highly agile commercial technologies, the National Security Agency (NSA) and the Central Security Service (CSS) launched the Commercial Solutions for Classified (CSfC) Program. A key aspect of the CSfC program is the ability to deploy a security solution in months instead of years[1].

According to the NSA [2], "Instead of building government owned and operated solutions, whenever possible, NSA is moving to a defense-in-depth approach using properly configured, layered solutions to provide adequate protection of classified data for a variety of different capabilities." [emphasis added]

CSfC implementation requirements are defined by Capability Packages published by the NSA. As emphasized in the prior reference, each layer of security technology must be properly configured per the specifications outlined in the appropriate Capability Package. Four Capability Packages are available at the time of this writing: Mobile Access, Campus WLAN, Multi-Site Connectivity, and the subject of this white paper – Data at Rest. Capability Packages serve as detailed sources of information for those who may benefit from the proper implementation of a CSfC solution. These detailed documentation sets allow the reader to make informed decisions about the suitability of a particular CSfC solution for a specific security implementation scenario. Detailed information is available in the appropriate Capability Packages published by the NSA.

The discussion material in this paper is applicable at the time of writing. Readers seeking to implement a CSfC solution must refer to and abide by the latest documents posted on the NSA website as the single source of truth. For the reader's benefit, NSA web page references are provided at the end of this paper.

CSfC Solution Architecture

The CSfC program simultaneously implements two or more independent commercial security components together to provide a layered security approach for the storage of classified data. Each of the security components, or layers, must be validated to CSfC requirements. The two security layers are referred to as the inner layer and the outer layer, as shown in the Figure below.

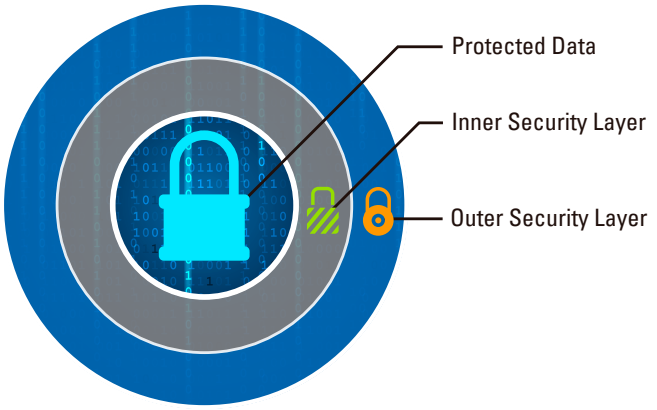

Figure 1: Depiction of two-layer security protection using two independently developed and distinct security layers.

Both the inner and outer security layers must integrate Suite B encryption algorithms. In doing so, the security redundancy provided by the second layer of security renders it unlikely that an adversarial force could penetrate both security layers, provided that all CSfC requirements are successfully met. It is important to note that the CSfC program requires diversity when selecting security components.

At first glance, the diversity requirement may seem puzzling. The intention of redundant security components is to mitigate the risk of failure of any one particular component. However, a single vendor producing multiple security components may use similar, if not identical, design principles for each component's cryptographic algorithm. If a security flaw in two separate components originates from the same fundamental design weakness, infiltration of one security layer quickly provides an adversary with a similar bypass through the second security layer.

Maximum protection, and full compliance with CSfC program guidelines, can only be achieved with proven diversity in the selection of security components.

It should be noted, however, that NSA documentation does permit a single vendor to produce multiple security components. This scenario requires definitive evidence and agreement from the NSA that each cryptographic algorithm was developed using distinct and independently developed resources and design methodologies.

Once a security component is validated and eligible for use as a CSfC security component per NSA guidelines, strict change control procedures must be enforced by the manufacturer. Failure to adhere to copy-exact manufacturing requirements may introduce security threats. For example, consider the scenario where the manufacturer of an ASIC controller introduces a minor change to the ASIC's internal ROM firmware but fails to notify its customers. In the course of implementing the manufacturing change, there is the potential for the integrity of the device to be compromised, intentionally or unintentionally. Suppose that such a change, for example, were to accidently introduce a security bypass mechanism or activate a previously disabled key recovery procedure. A discontinuity in a trusted supply chain may have catastrophic effects far beyond the scope of the intended purpose.

Although there are companies that claim to offer security components engineered to the standards of 2-layer CSfC-types of security solutions, a true CSfC security component must be fully validated per CSfC guidelines. With the rigorous standards defined by the CSfC program and the few number of vendors offering compliant products, there is no substitute for achieving validation and compliance with the requirements of the CSfC program. One can easily argue that if validation to CSfC requirements was a straight-forward engineering exercise, the list of CSfC validated components would be multiple pages long.

True eligibility for a security component to be integrated into a CSfC solution can only be verified by locating the security component on the NSA's CSfC Component List.

Readers are also cautioned against employing a "2-layer CSfC-like" data protection approach. The authors do not question the enhanced security of such commercial 2-layer security approaches over a single layer of security for the storage of unclassified data. However, classified data is marked as such to indicate the consequential nature if an adversary were to secure this information. With the clear NSA requirements outlined in the CSfC program to leverage highly agile, rapidly deployed commercial technologies, there is no valid reason to employ inferior, potentially flawed security components that have not been successfully evaluated according to NSA guidelines.

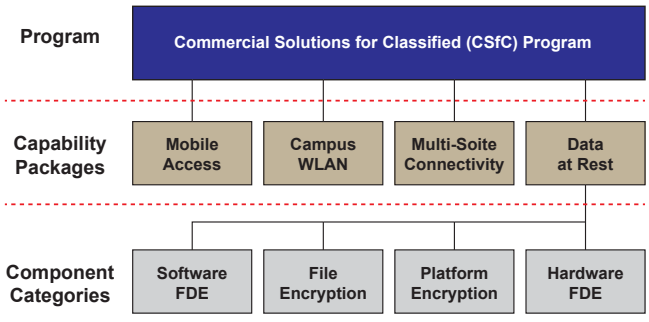

Figure 2: Relationship between CSfC Program, Capability Packages, and Component Categories with emphasis on Data at Rest. Component categories for Mobile Access, Campus WLAN, and Multi-Site Connectivity can be found in the corresponding Capability Packages published by the NSA.

Building CSfC Data at Rest Solutions

The Data at Rest Capability Package published by the NSA classifies security components into four categories, as discussed below. Conformance with CSfC requirements demands that two independent security components be selected while maintaining independence of cryptographic algorithms development. Two of the security components utilize full disk encryption (FDE) while the remaining two employ file or platform encryption.

Solution Designation	Inner Layer	Outer Layer
SF	SWFDE	FE
PF	PE	FE
HF	HWFDE	FE
HS	HWFDE	SWFDE

Figure 3: Possible combinations of inner and outer security layers for DAR solutions.

Software Full Disk Encryption (SWFDE): SWFDE components encrypt all data on the hard drive, including the computer's operating system. The boot sequence and subsequent access to the data can is only permissible after successful authentication.

File Encryption (FE): FE encrypts individual files or sets of files in a device. Access to the encrypted data is only provided after authentication has succeeded. Encryption may be performed by an application, platform, or the host operating system.

Platform Encryption (PE): PE is provided by the operating system for platform-wide data encryption. PE differs from FE in that PE is only an inner layer and FE is only an outer layer. The primary technical difference between the two related to the hardware key protection requirements.[3]

Hardware Full Disk Encryption (HWFDE): HWFDE components use encryption algorithms embedded into the storage controller. An authentication key is used to decrypt the data encryption key (DEK) and provide access to the data. The primary thesis of this paper centers on the application of HWFDE technology.

Data at Rest solution components are the fundamental building blocks required to develop, register, and provide maintenance for a CSfC registered solution. The NSA provides clear instructions for specific combinations of solution components to be integrated as inner and outer layers. Although theoretically 16 combinations are possible with four different security component types, only four solutions are authorized configurations. These four solutions are designated by two letter acronyms, where the first letter represents the inner layer and the second letter represents the outer layer. For example, the HS solution uses HWFDE (Hardware Full Disk Encryption) as the inner layer of protection and SWFDE (Software Full Disk Encryption) as the outer layer of security.

Selection of the appropriate solution – SF, PF, HF, or HS – should be done only after careful consideration of the application and its security requirements. For clarity, the authors do not endorse any single solution design. Readers are encouraged to carefully evaluate the DAR Capability Packages to identify the most appropriate solution designation for their specific security application.

To facilitate the design, integration, testing, documentation, fielding, and maintenance of a CSfC solution, the NSA has developed a program for organizations to become a trusted CSfC integrator. These trusted organizations provide their expertise as a service for hire. Those wishing to implement a CSfC solution may hire one or more trusted integrators based on their application and security requirements. Customers may wish to use multiple integrators to ensure that no single third party entity has access to all of the solution components. It is not necessary to use the services of one or more trusted integrators, although it may expedite the deployment of a security solution for those unfamiliar with CSfC program requirements. The NSA provides a list of trusted integrators and their contact information on the CSfC Trusted Integrator List published online.

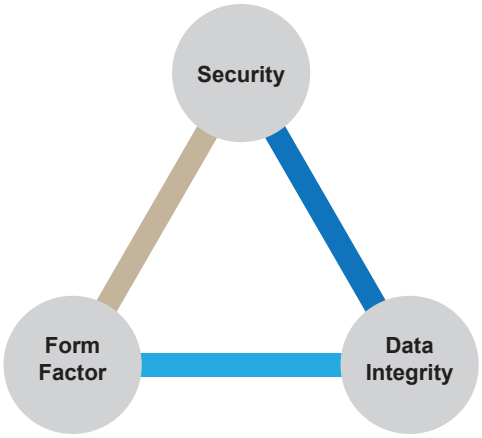

Figure 4: Data storage considerations when selecting a HWFDE component.

HWFDE Component Considerations: Security

Returning to the overriding objective of this white paper, we now discuss the integration of a Secure SSD into a two-layer CSfC solution as a HWFDE inner layer component. Per CSfC program requirements, the outer layer component must be either FE or SWFDE. Before continuing, it is important to note that there is no single universally superior HWFDE component for every security implementation. Readers are encouraged to reference NSA documentation and consult organizations which have achieved the Trusted Integrator designation from the NSA.

HWFDE components may be either a conventional hard disk drive (HDD) with rotating magnetic media or a SSD using NAND flash storage media. Given the reliability and performance differentials between SSDs and HDDs, most applications today select solid-state technology for data storage. Both configurations require self-encryption functionality, which is typically achieved through implementing cryptographic algorithms in the drive's controller and/or processor.

Careful selection of HWFDE components must be made to ensure that the cryptographic algorithm deployed in the inner HWFDE layer is distinct from the selected outer security layer, either File Encryption or Software Full Disk Encryption. Authentication of the HWFDE component can be performed using a randomly generated passphrase or a randomly generated bit-string equivalent to the cryptographic strength of the DEK. Passphrases must comply with requirements outlined in the DAR Capability package, most notably the minimum strength calculations.

There are additional considerations. Data must be protected with the strength of advanced encryption standard (AES) with 256-bit keys and an XTS (XEX with ciphertext stealing), GCM (Galois/Counter Mode) or CBC (Cipher Block Chaining) block cipher mode.

Generally XTS implementations are preferable. In doing so, all classified data must be encrypted on the device without exception.

Additionally, the encryption key for each layer must be distinct. If an adversary were to gain access to one of the encryption keys, unique encryption keys for each layer prevents access to the encrypted data. In the event that the encryption key is purged from the device, there must be no remnants of the key on the device and there must be no way to recover the key from the drive.

HWFDE Component Considerations: Data Integrity

The discussion above highlights the magnitude of considerations that must be addressed before a storage device can be deployed in a CSfC solution. We argue that the same degree of scrutiny should be applied not only to the security of the data but also to any device consideration that impacts the integrity of the data. Any data, classified or unclassified, may be highly valuable and irreplaceable for a military operation. The malfunction of a device during a mission may have disastrous consequences. The following discussion presents considerations for a user when selecting one HWFDE component over another.

First, the NAND flash media type must be matched to the performance demands of the application and its environment. NAND flash manufacturers now offer a myriad of technologies available to the consumer:

- Single-Level Cell (SLC) NAND flash stores only 1 bit per cell yet offers 10X higher data endurance than the next best alternative media type. It also has the most robust operating temperature range, –40 to +85 °C. SLC technology is the media of choice for applications storing data that cannot be replaced in the event of an SSD failure.
- Multi-Level Cell (MLC) NAND flash, in contrast, stores 2 bits per cell, thereby offering a larger data storage capacity at a significantly reduced cost. However, this increased capacity comes at the expense of reduced read/write endurance compared to SLC NAND and shorter data retention.
- Triple-Level Cell (TLC) technology stores three bits per cell, thereby further reducing cost, with additional penalties beyond MLC technology in terms of data endurance and operational lifetime.
- 3D-NAND technology vertically stacks storage cells to surmount the scaling limitations of conventional planar (SLC, MLC, TLC) technologies. At the time of this writing, 3D NAND memories are available only with operating temperatures of 0 to +70 °C. Although 3D-NAND technology does allow further scaling, the vertical integration does present new reliability issues, such as vertical charge loss and lateral charge migration.[4]

With a myriad of NAND technologies, selecting the appropriate SSD for a given application is not a trivial exercise. As a rule of thumb, selecting a SSD based on SLC technology is clearly the safest approach when data integrity is critical and/or operating temperatures are below 0°C or exceed 70 °C. Under commercial operating temperatures where the SSD can be readily replaced as a preventative maintenance operation, MLC technology offers higher storage capacities suitable for high-volume data record recording applications where the data has limited lifetime value. At the time of this writing, TLC and 3D NAND technologies have not yet reached a maturity level where the authors can recommend their consideration for military applications.

Those selecting a HWFDE component are encouraged to inquire with the manufacturer about performance throttling algorithms designed to extend the useful lifetime of a device. Normally these algorithms, activated under heavy duty-cycle operation or high temperature operation, are not advertised by the SSD manufacturer. Extended operational lifetimes sounds like a benefit to the user; however, extended operational lifetime comes at the expense of non-deterministic and reduced read and write speeds. Although potentially acceptable for commercial applications, many military applications demand continuous high-speed data capture at extended temperatures for a successful mission.

Assuming the NAND flash media and controller architecture of the SSD have been addressed, one additional question remains: In the event of a sudden power loss, what happens to the cells that are being read and/or written? A sudden disruption in power may lead to the corruption or loss of data if the device has no mechanism to ensure an orderly and deterministic shut-down procedure. Batteries, supercapacitors, and other means of data preservation can be integrated into the device's architecture. Users are cautioned when selecting any solution deploying batteries or supercapacitors, as their effectiveness is limited in environments requiring low and high temperature operation.

HWFDE Component Considerations: Form Factor

The industry standard 2.5" form factor is the defacto configuration. However, not all 2.5" SSD packages are created equal. The shock and vibration conditions, both expected and unexpected during deployment, must be evaluated. The physical package/enclosure of the SSD must be structurally validated to survive all shock and vibration conditions possible in the given application. Further consideration must be given to the integrity of the mechanically connecting interface between the SSD and the host system. Ruggedized mechanically interlocking connectors minimize the possibility of an accidental disconnect from the host system. Scenarios may arise where a user requires an alternate form factor, such as mSATA or XMC card. Can the SSD manufacturer support the rapid development and qualification procedures to achieve eligibility for use as a CSfC solution component? Is the controller architecture portable and readily adapted to the new form factor? If the manufacturer has not even achieved 3rd party qualifications -- such as FIPS 140-2 and Common Criteria -- on one form factor, it is highly unlikely that the review and qualification process needed for the new form factor can be completed quickly.

Case Study: Speed and Security Matter

The following case study is hypothetical and provided for illustrative purposes only.

The Threat

An overseas military operation receives intelligence that a hostile nation state has begun construction of a mining facility in a remote desert to source a specific raw material. The hostile nation state is known to possess the capabilities required to refine this raw material into the components needed for the development of advanced weapons. Reports indicate that the mining facility will become operational in less than one year. Once mining begins, the material must be transported to a processing facility for purification and further processing before it is suitable for deployment in weaponized applications. If the hostile nation state gains access to this raw material in sufficient quantities, it could pose a significant threat to neighboring ally countries.

The Mission Objective

The orders are clear – gather tangible evidence that the raw material is being mined and transported to a purification facility. Then, an appropriate course of action can be determined given the geopolitical environment at the time.

A fleet of new, highly classified extended range unmanned aerial vehicles (UAVs) is redirected from a prototype evaluation program and assigned to this mission. The operations team must make the fleet of new UAVs deployable in no more than 9 months. The UAV mission computer contains advanced electronic warfare electronics and processing algorithms designed to allow evasion of enemy radar. These UAVs must be retrofitted with advanced sensors and state-of-the-art imaging and night-vision systems as soon as possible. The UAVs will then continuously survey the area of interest around the clock, capturing both (1) optical images of the types and number of vehicles traveling to and from the mine site and (2) sensor data monitoring the surveillance area for traces of the suspected raw material exiting the mine site. The UAV mission computer and sensor processing subsystems employ highly sophisticated algorithms that have been classified Top Secret by the government.

Mission Vulnerabilities

Moving from a controlled test environment in a highly secure facility to field deployment in unfriendly territory necessitates a robust means of protection for the mission computer's control system as well as the sensor data resident in the data storage platform. The design team first considers an existing storage system implemented as two sequential layers of AES-256 encryption. This approach could potentially shorten time to deployment by a few months. The manufacturer's product literature indicates the system is "compliant" to CSfC, however; the individual components of each layer do not appear on the CSfC approved components list and the system solution is not NSA registered as a CSfC End User Device (EUD). Ultimately the team decides that using a non-validated solution for such a mission critical application incurs too much risk should a UAV be lost in unfriendly territory. After careful consideration and lengthy discussions with a series of Trusted Integrators, the team decides that a fully validated CSfC 2-layer security implementation using HWFDE and SWFDE components from the CSfC approved component list provides the most robust security implementation. The ideal HWFDE component in the CSfC component list is an SSD in a 2.5" form factor. Unfortunately, this form factor is too large for installation in the existing electronics bay of the UAV. The team needs to find a creative solution.

Effecting the Mission

The UAV team Program Manager contacts the manufacturer of the HWFDE component, Qubit Drives, Inc (QDI). Following proper security protocols, QDI's cleared engineering team is briefed on the problem at hand. A solution is possible, although it will be challenging to implement in the short time period available. The QDI team suggests taking the Qubit Drives CSfC certified 2.5" SSD and repackaging the design into a small, low profile BGA form-factor. The new BGA device must achieve FIPS 140-2 and Common Criteria certification and then gain inclusion on the HWFDE CSfC approved component list within a 6 month design window.

Fortunately, QDI's SSD engineers had previous begun conversion of their CSfC certified 2.5" SSD product into both BGA and mSATA form-factors. Prototype BGA devices were already undergoing design validation testing in a QDI R&D lab. The QDI engineering team reviews notes from the evaluation of their original 2.5" SSD CSfC HWFDE component. QDI's Program Manager maintained a list of lessons learned during the certification process and this is expected to accelerate the CSfC validation schedule for the BGA device. The BGA device uses the same firmware set as the original 2.5" design and after an initial evaluation by the external FIPS/CC lab, it is determined that the minor changes between the 2.5" and the BGA will definitely speed the certification process. The QDI team updates the FIPS Security Policy and CC Administrative Guide documents and submits them to an approved external lab for review. The external lab conducts on-site code reviews, state machine reviews, a schematic review and an entropy assessment as well as running a thorough suite of tests and debug procedures on the BGA device. The QDI team provides sample BGA devices for destructive physical security testing. The lessons learned from the original 2.5" certification and the similarity between the two designs now pays dividends. The remaining FIPS and CC tests proceed smoothly. There is essentially no learning curve for the external lab, and in less than 2 months, the lab completes its FIPS and CC evaluations and submits final reports to NIST and NIAP for the FIPS 140-2 and CC certifications. In another 4 months the BGA component is fully certified and appears on the CSfC components list as a new HWFDE component.

While QDI worked to achieve FIPS 140-2, CC, and CSfC certification for the BGA device, the UAV design team moved ahead with the effort to create the final two-layer CSfC End User Device (EUD) solution. The UAV design team selected a Trusted Integrator and together the two teams planned a robust CSfC security solution implemented using the BGA device as the HWFDE component and a SWFDE component as the second security layer. Careful consideration is given by the Trusted Integrator to properly select the correct second security layer for this specific mission. Together the two layer solution provides protection for the boot code, sensor processing, and EW algorithms used by the UAV mission computing system. To simplify the implementation, the Trusted Integrator team suggested an identical HWFDE and SWFDE solution to protect the sensor data collected during missions. Of course, the encryption keys for each layer are randomly generated and distinct from each other.

Mission Success

Working together at an accelerated pace, the UAV team, QDI, and the Trusted Integrator complete the security implementation and perform a final review the NSA Data at Rest Capability Package, make some final adjustments, some improvements, and conduct final system testing. After months of effort, the system is ready for EUD registration and review by the NSA. Approval is achieved, and two of the UAVs used during prototype security testing are configured and prepared for trial missions.

In a few days, the first of the sophisticated UAVs successfully launches and guides itself toward the remote mining facility. Hours later, the vehicle returns loaded with Giga-Bytes of sensor data that analysts eagerly review. There are no indications that the UAV had been detected during the mission. A second, then a third mission is completed. In a few weeks, missions are running around the clock. Construction at the mining facility is complete and large amounts of raw ore move every night to a hereto unknown processing facility located near a large rural power plant. As expected, the sensors on the UAV detect minute amounts of a radio-active mineral but surprisingly dust collectors in the UAV also capture large amounts of highly toxic beryllium metal in dust emanating from the mining facility. While Beryllium has some justifiable commercial uses, the element's high melting point, light weight, and strength find numerous uses in defense applications such as missiles, aircraft, spacecraft, and nuclear reactors.

With the mission declared a success the UAV team moves to their next project -- a covert underwater drone. Like the airborne UAV, the underwater drone needs superior protection for data at rest. The lessons learned during the UAV project will easily transfer to the underwater drone application.

Implementing a Secure SSD

The integration of security into a military data storage device is not a trivial task. Mercury's Application Engineering Team assists customers with the design and implementation of custom security solutions.

Mercury has a wide breadth of product offerings for applications requiring various levels of security. Our TRRUST-Stor® portfolio of Secure SSDs is available in multiple form factors, including the industry-standard 2.5", mSATA, XMC, and ultra-compact BGA. The most recent addition to Mercury's SSD portfolio is the ASURRE-Stor™ SSD, available with FIPS 140-2 certification and eligibility to be used as a HWFDE component in a properly configured and deployed 2-layer CSfC registered solution.

Please note that Mercury Systems is not a Trusted Integrator. Contact Mercury's Secure SSD team at secure.ssd@mrcy.com.

[1] https://www.nsa.gov/resources/everyone/csfc/
[2] https://www.nsa.gov/resources/everyone/csfc/assets/files/faqs-non-technical.pdf
[3] For more information, please refer to https://www.niap-ccevs.org/Profile/PP.cfm
[4] R. Micheloni (ed.), 3D Flash Memories, Springer Science + Business Media, 2016, retrieved from https://goo.gl/BdLwcR

Reference Websites

CSfC Website:
https://www.nsa.gov/resources/everyone/csfc/
CSfC Capability Packages:
https://www.nsa.gov/resources/everyone/csfc/capability-packages/
CSfC Data At Rest Capability Package:
https://www.nsa.gov/resources/everyone/csfc/capability-packages/#data-at-rest
CSfC Components List:
https://www.nsa.gov/resources/everyone/csfc/components-list/
CSfC Trusted Integrators List:
https://www.nsa.gov/resources/everyone/csfc/trusted-integrator-list.shtml
CSfC Frequently Asked Questions:
https://www.nsa.gov/resources/everyone/csfc/faq.shtml
National Information Assurance Partnership:
https://www.niap-ccevs.org/Product/
Mercury Systems ASURRE-Stor SSD:
http://www.mrcy.com/CSfC
Mercury Systems Secure SSD Portfolio:
https://www.mrcy.com/military-grade-secure-solid-state-drives/

Acronyms

Acronym	Definition
3D-NAND	Three-Dimensional NAND flash
AES	Advanced Encryption Standard
BGA	Ball Grid Array
CBC	Cipher Block Chaining
COTS	Commercial Off-The-Shelf
CP	Capability Package
CSfC	Commercial Solutions for Classified
CSS	Central Security Service
DAR	Data At Rest
ECC	Error Correction Code
FDE	Full Disk Encryption
FE	File Encryption
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GOTS	Government Off-The-Shelf
HDD	Hard Disk Drive
HF	DAR solution designation for HWFDE and FE
HS	DAR solution designation for HWFDE and SWFDE
HWFDE	Hardware Full Disk Encryption
MLC	Multi-Level Cell NAND flash
mSATA	Mobile SATA
NIAP	National Information Assurance Partnership
NSA	National Security Agency
PE	Platform Encryption
PF	DAR solution designation for PE and FE
SF	DAR solution designation for SWFDE and FE
SLC	Single-Level Cell NAND flash
SSD	Solid State Drive
SWFDE	Software Full Disk Encryption
TLC	Triple-Level Cell NAND flash
WLAN	Wireless Local Area Network
XEX	Xor-encrypt-xor
XMC	Switched Mezzanine Card
XTS	XEX with ciphertext stealing

About the Authors

Bob Lazaravich is the Technical Director for the Secure Solid State Drive product line at Mercury Systems in Phoenix, Arizona. Bob frequently engages with customers to implement security features tailored to address application-specific requirements. Bob received his BSE and MSE degrees in Electrical Engineering from Arizona State University.

Philip Fulmer is the Director of Product Marketing for the Advanced Microelectronics Solutions group in San Jose, California. Philip received his BS degree in Chemistry from the University of Scranton and MSE degree in Materials Science and Engineering from the University of Texas at Austin.

 3318.00E-0617-wp-MSS-CSfC

www.mrcy.com

CORPORATE HEADQUARTERS
50 Minuteman Road • Andover, MA 01810 USA
(978) 967-1401 • (866) 627-6951 • Fax (978) 256-3599

EUROPE - MERCURY SYSTEMS, LTD
Unit 1 - Easter Park, Benyon Road, Silchester, Reading
RG7 2PQ United Kingdom
+ 44 0 1189 702050 • Fax + 44 0 1189 702321