Data-At-Rest Encryption Series: Type 1

Read About

Introduction

This white paper is the third in a series of four discussing data-at-rest (DAR) encryption. The first paper in the series, Data Threats and Protection, explores the reasons to protect DAR, encryption basics, and possible encryptor options. The second paper in this series, Commercial Solutions for Classified, focuses on Commercial Solutions for Classified (CSfC), an option offered by the National Security Agency (NSA) that uses two layers of commercial off-the-shelf (COTS) encryption to protect classified data. This third paper discusses the NSA program known as Type 1 encryption, which is a government off-the-shelf (GOTS) option. Much of the data regarding Type 1 encryption is classified, so this paper will only deal with publicly available information.

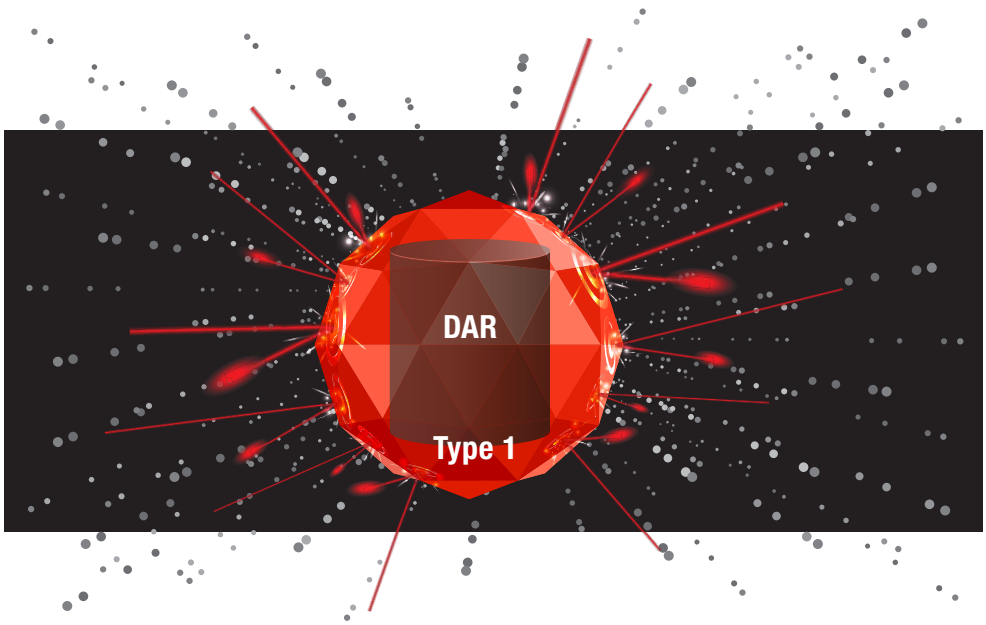

Figure 1: NSA Type 1 Encryption

A Type 1 encryption product is a device or system certified by the NSA for use in cryptographically securing classified United States Government (USG) information, when appropriately keyed. The USG classified data may range from Confidential to Secret to Top Secret.

The fourth white paper in this series compares CSfC and Type 1 encryption when deciding on protection of DAR in deployed applications.

Why Protect Classified Data?

Since 1952, the NSA has been responsible for all USG encryption systems. Over the intervening decades, the mission of protecting USG classified data has not changed. Methods and technology have certainly changed during that time, advancing from vacuum tubes to discreet transistors to integrated circuits to microprocessors and software. In recent years, the threat landscape has been constantly evolving and becoming more sophisticated, and so the protection response must also evolve.

The basic principle of encryption is to convert plain text data (also known as Red data) into cipher text data (also known as Black data). Plain text data can be read by ordinary means and is not protected. Red data is vulnerable to exploitation by an adversary if obtained. In a deployed system, the vehicle such as a fighter, helicopter, or tank may be lost during a mission. As described in the first white paper in this series, many deployed vehicles have been lost over the last few decades. Certainly, more will be lost due to enemy action or accidents in the future.

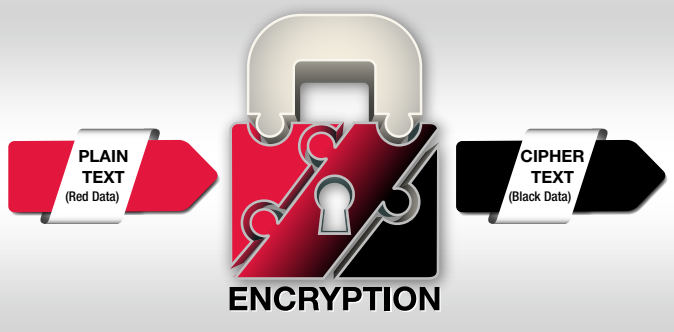

Figure 2: Basic Encryption Concept

This simple encryption representation works for DAR and for data-in-transit (DIT). This paper (and the series) focuses only on DAR; therefore, all references to encryption will be from the DAR perspective.

Threats During and After Missions

For deployed applications, data is likely to be transferred before and after missions. Prior to a mission, plans and maps (generated at a base or ground station) may be loaded from the ground station onto the vehicles. After a mission, sensor data may be off-loaded from the vehicle back to the ground station for post-mission analysis. During transport to/from the deployed vehicle, this data is vulnerable to capture and must be protected with encryption and other means.

Data at the ground station is subject to attack by hackers, either nation-states or individuals. Networks and the data on them are being attacked continually from a variety of advanced persistent threats (APT). Internal bad actors are also a threat. These people have their own agenda and are often team members that no one suspects. Adversaries are simply any individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. This threat landscape can be dissected into smaller elements, but suffice it to say that the threats are increasing in number and sophistication.

APT

An APT is an adversary with sophisticated levels of expertise and significant resources. APT threats are often multiple in number and coordinated. They use a full spectrum of sophisticated attack vectors, including deception, cyber, or physical attacks. These multiple attack vectors provide an APT with many opportunities to achieve its objectives, such as undermining critical missions and establishing footholds in the information technology infrastructure. APTs try to extend their footholds to retrieve the collected data and will persistently repeat their attacks, varying them in response to countermeasures.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

For all these reasons and more, it is important to protect classified data. Encryption of DAR is one measure that should be taken. Other security measures may be required that are commensurate with the risk and the magnitude of harm resulting from the loss, misuse, and unauthorized access to or modification of the information.

KEY TAKEAWAY

Classified DAR in deployed applications is at risk from advanced persistent threats (both internal and external) and must be protected from these adversaries who wish to exploit it.

What Are Type 1 Devices?

This paper will only discuss publicly available information. As mentioned earlier, a Type 1 product is a device or system certified by the NSA for use in cryptographically securing classified USG information, when appropriately keyed. The USG classified data may range from Confidential to Secret to Top Secret.

The term "Type 1" refers only to products and not to information, keys, services, or controls. Type 1 products contain NSA-approved algorithms. Two families of algorithms are used: one classified and one public. These algorithms will be further explored in the section titled Type 1 Encryption Algorithms.

Type 1 devices are available to USG users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation (ITAR). As cryptographic security devices, Type 1 encryptors are communications security (COMSEC) equipment. For effective COMSEC, sound cryptographic systems must be combined with transmission security, physical security, and emission security.

For decades, Type 1 was the only NSA cybersecurity designation regarding encryption. However, there is now an alternative in the NSA's commercial encryption program: CSfC. The second white paper in this series discussed the CSfC program in detail. Each program has advantages and disadvantages, but both are fully supported NSA programs. The fourth paper in this series will make some of those comparisons.

KEY TAKEAWAY

Both Type 1 and CSfC are NSA approved programs for the protection of DAR.

From its black budget, the NSA spends many millions of dollars every year to develop Type 1 equipment. These Type 1 devices are not publicly known or available for general use. Many Type 1 DAR products are developed by commercial companies (like L3Harris, General Dynamics, and ViaSat) and are generally publicly known and advertised. In both development processes, very strict requirements are applied, and these requirements are classified. For a new Type 1 device to be developed, normally the sponsorship by a significant program of record is essential for both funding and eliciting NSA support.

The use of Type 1 devices is also controlled by very strict requirements. Type 1 devices may be considered classified themselves and thus may require special handling, including transporting, securing, and storing. Serious consequences may apply for loss of a Type 1 device.

Type 1 Layers

As opposed to CSfC solutions, which require two layers of encryption, Type 1 encryption solutions require only one layer of encryption, as shown in Figure 2. This can prove advantageous when developing a DAR solution for a deployed vehicle since less equipment may be required.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

Type 1 Levels or Designation

Type 1 encryption devices perform critical COMSEC functions. Special accounting controls may be required, and the requirements may vary depending on the level.

Type 1 encryptors may be considered either a controlled cryptographic item (CCI) device or a cryptographic high value product (CHVP) device. Depending on that level or designation, different shipping and handling may apply to a Type 1 device. That aspect will be examined more closely in the section titled: Shipping and Handling.

Type 1 Encryption Algorithms

The specific algorithm(s) used in a Type 1 encryption device are not usually publicly known. Some devices will state the algorithm used but most do not. The Type 1 algorithms can be from either Suite A or Commercial National Security Algorithm Suite (CNSA) (formerly Suite B).

Suite A

Suite A algorithms are classified and only to be used in Type 1 CCI devices. These algorithms cannot be used in a CSfC device.

Suite A algorithms are believed to include (but may not be limited to) the following[i]:

+ ACCORDION
+ BATON
+ FIREFLY
+ Enhanced FIREFLY
+ JOSEKI
+ KEESEE
+ MEDLEY
+ SHILLELAGH
+ SKIPJACK

CNSA (formerly Suite B)

The CNSA algorithms are publicly known and readily available to anyone. CNSA algorithms are specified for use in CSfC encryption devices, but are used in some Type 1 devices (CCI and CHVP) as well.

CNSA algorithms include:

+ Advanced Encryption Standard (AES)
+ Elliptic Curve Diffie-Hellman (ECDH) Key Exchange
+ Elliptic Curve Digital Signature Algorithm (ECDSA)
+ Secure Hash Algorithm (SHA)
+ Diffie-Hellman (DH) Key Exchange
+ RSA

Type 1 DAR Product Vendors

A number of vendors publicly offer Type 1 DAR encryption devices. This list may not be complete, as each vendor may have additional Type 1 products not listed on their respective websites.

NSA

The NSA may have commissioned Type 1 DAR encryption devices to be developed or may have developed devices themselves for their own use. If such a list exists, it is not public but may be available to the appropriate authority.

General Dynamics Mission Systems (GDMS)[ii]

GDMS, located in Dedham, Massachusetts, has been developing and offering Type 1 encryption devices for decades. While most of their Type 1 devices are targeted for DIT, they have a few DAR offerings, most notably the recently certified KG-204.

+ ProtecD@R Multi-Platform Encryptor (KG-204)
  - › An example usage of this encryptor is shown in a file server in Figure 3.
+ ProtecD@R PC Encryptor (DaR-400)
+ ProtecD@R Embedded (DaR-400E)
+ ProtecD@R High Speed (KG-540A)
+ ProtecD@R High Speed (KG-540B)

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

ViaSat[iii]

ViaSat notes 30 years of experience in developing cyber systems. Their global headquarters is located in Carlsbad, CA. They have two public DAR offerings, including:

+ KG-200M 6U single slot hard drive encryptor
+ KG-200R Inline Media Encryptor

L3Harris[iv]

L3Harris provides advanced defense and commercial technologies across air, land, sea, and cyber domains. Their global headquarters is located in Melbourne, FL. They have one public DAR offering, including:

+ UnityCP® ASIC

Other Possible Vendors and Products

In addition to vendors possibly not listing all their Type 1 DAR encryption products publicly, there may also be other vendors of Type 1 DAR encryption products that are just not publicly known.

Consideration Factors for a Type 1 DAR Application

When evaluating or considering Type 1 devices, many factors may be used. For each application, the importance of each factor will vary, and some factors important to a unique application may not even be listed below. However, this list is a great foundation for any evaluation of potential DAR solutions.

Look at the Entire DAR Solution

One important note to keep in mind is that a Type 1 encryptor by itself does not make a complete DAR solution. A deployable DAR solution, like the example NAS shown in Figure 3, is composed of three basic components – a chassis, removable storage, and one or more encryptors.

+ The chassis will include a processor, operating system, application software, and inputs/outputs (I/O).
+ The removable storage will include a solid state drive(s) and structure to support and transport it.
+ The DAR encryptor will be a device like those noted in the section: Type 1 DAR Product Vendors

KEY TAKEAWAY

A Type 1 DAR encryptor is only one part of a deployed DAR storage solution.

Unit Cost

Keep in mind that the DAR encryptors noted earlier are only encryptors, not file servers or solid state storage. These encryptors are not complete solutions by themselves; in order to use them in deployed storage applications, each encryptor must be integrated into a network attached storage (NAS) system or device.

Figure 3: Curtiss-Wright Unattended Network Storage

Figure 3 shows just such a complete example NAS device that incorporates two Type 1 DAR encryptors. Used by USG entities today, this example NAS also includes a high-speed processor, operating system, application software, I/O, and removable solid-state storage.

The two Type 1 encryptors that are housed in the example NAS in Figure 3 represent only 19% of the entire NAS cost.

Size

The same issues mentioned previously come into play with regard to size. In order to use any encryptor, these must be integrated into a complete NAS system. The two Type 1 encryptors that are housed in the example NAS in Figure 3 represent only 8.5% of the entire NAS size (in cubic inches). That example NAS is a large system for use in ISR type applications requiring high data throughput and large data storage capacity.

Power

Again, the same solution issues mentioned previously are true with regard to power. In order to use any of the encryptors, they must be integrated into a complete NAS system. Additional power will be used to run the entire NAS system, which is much more than just the encryptors' power requirements. The two Type 1 encryptors that are housed in the example NAS in Figure 3 represent only 24% of the entire NAS power dissipation.

Weight

Once again, the same system issues mentioned previously are true with regard to weight. The two Type 1 encryptors that are housed in the example NAS in Figure 3 represent only 22% of the entire NAS weight.

KEY TAKEAWAY

When evaluating an encryptor to protect DAR in a deployed application, look at the total storage solution, not just the encryptor itself.

Export

As mentioned earlier, Type 1 devices are available to USG users, their contractors, and federally sponsored non-USG activities subject to export restrictions in accordance with ITAR. Any NSA Type 1 device will most certainly be ITAR controlled or restricted. As ITAR-controlled devices, it is possible (subject to review) to export Type 1 devices to the other Five Eyes countries (United Kingdom, Australia, New Zealand, and Canada).

If you intend to export the vehicle in which the Type 1 DAR encryption is being used, then careful consideration must be given to this export factor. For instance, a vehicle using Type 1 encryption may not be exportable to even friendly allies such as Japan, France, or Germany. Even North Atlantic Treaty Organization (NATO) countries (other than the United Kingdom) may not be able to use NSA Type 1 devices.

If only intending that the deployed vehicle be used by the USG (even overseas), then the export factor will likely not be a concern.

KEY TAKEAWAY

Make sure that you understand your company's export goals before committing to a DAR solution for a vehicle.

Non-Recurring Engineering Cost

In most cases, Type 1 DAR encryption devices are initially paid for by a USG DoD entity (Navy, Army, Air Force, or other agency) or by the NSA itself. So the first end user must pay for the development and certification process. This development process can be quite expensive and can take a significant amount of time.

If a USG entity has already funded the DAR encryptor development, like for the KG-204, then no additional development cost for the encryptor will be incurred. However, a NAS system is still required in order to utilize such an existing Type 1 encryptor in a deployed application. The NAS shown in Figure 3 was also paid for by the same USG entity that paid for the KG-204 development. So that example NAS system exists and could be used again by another USG entity without further development investment or schedule impact.

However, if the example NAS is too large and must be reduced in size, weight, or power, then additional NRE will be required to develop that new, smaller NAS system. This scenario assumes re-using a previously certified Type 1 encryptor which needs no further development.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

Any modifications to an existing Type 1 encryptor will, of course, require NRE in order to accomplish the task.

Any new development (new or modified Type 1 encryptor or new or modified NAS system) brings in the element of NRE cost and also brings in the element of technical and schedule risk.

KEY TAKEAWAY

You can save NRE cost if you use an existing Type 1 encryptor and NAS system.

Technical and Schedule Risk

As mentioned earlier, the development of Type 1 DAR encryption devices is typically paid for by a USG DoD entity or the NSA itself. This development and certification process can be quite lengthy, characterized by a developer at 18 months to two years. This development time is true not only for the encryptor but also for the NAS in which it will be used.

Any technical development for such an encryptor or NAS has a certain amount of risk. Such risk must be evaluated prior to any development as any program manager knows.

If, however, a USG entity has previously funded the development, like for the KG-204, then no additional schedule impact will be incurred, unless the NAS must be altered or modified.

KEY TAKEAWAY

Any engineering development has a certain amount of risk involved. So be sure to recognize this factor in your evaluation.

Keys

A key is a numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in cryptographic equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures (ECCM) patterns, or for producing other key.[v]

Some of the Type 1 encryption devices, like the DAR-400E, internally generate the encryption keys. For others in which a pre-place key is used, like the KG-204, the keys come from the NSA. Those keys are considered classified. Handling of the key material must be part of the evaluation.

Shipping and Handling

If the Type 1 device is termed CCI, then the following applies:

"Part of the physical security protection given to COMSEC equipment and material is afforded by its special handling and accounting. CCI equipment must be controlled in a manner that affords protection at least equal to other high value equipment, such as money, computers, and Privacy Act-controlled. There are two separate channels used for the handling of such equipment and materials: 'the COMSEC channel' and 'the administrative channel.' The COMSEC channel, called the COMSEC Material Control System, is used to distribute accountable COMSEC items such as classified and CCI equipment, keying material, and maintenance manuals. Some military departments have been authorized to distribute CCI equipment through their standard logistics system. The COMSEC channel is composed of a series of COMSEC accounts, each of which has an appointed COMSEC Custodian who is personally responsible and accountable for all COMSEC materials charged to his/her account. The COMSEC Custodian assumes accountability for the equipment or material upon receipt, then controls its dissemination to authorized individuals on job requirements and a need-to-know basis. The administrative channel is used to distribute COMSEC information other than that which is accountable in the COMSEC Material Control System."[vi]

CHVP devices are handled in less restrictive manner than CCI devices.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

Certification Level

Another important factor in Type 1 encryptor evaluation is the level of data to be handled. Encryptors are certified for certain levels of classified data. For instance, the KG-204 is certified to handle Top Secret/ Special Compartmentalized Information (TS/SCI). On the other hand, the older DAR-400E is certified to handle Secret and below data.

Unattended vs Attended Operation

One critical factor in any future DAR evaluation will be whether the vehicle will be unattended. Most of the Type 1 encryptors identified are not certified for unattended operation. Some examples of unattended vehicles are Unmanned Aerial Vehicles (UAV) like the Predator, Reaper, Global Hawk, or Triton. There are also many Unmanned Underwater Vehicles (UUV) like the XLUUV.

Newer unattended solutions will likely include Type 1 encryptors like the KG-204. This encryptor has been recently certified to handle TS/SCI data and more importantly for unattended operations. This factor can be very important moving forward.

Unattended vehicles (such as UAVs and UUVs) are being deployed in ever increasing numbers, even in swarms of many vehicles, so this key distinction of unattended operation certification can be a key factor in a trade study.

KEY TAKEAWAY

Unattended vehicles like UAV, UUV, and USV have special DAR requirements since no person will be with the vehicle while deployed. No one can 'push the panic button' or pull the plug during an emergency.

Type 1 Certification

A Type 1 encryptor may be developed by the NSA itself or by a commercial vendor. For a commercial company, the NSA works in conjunction with the commercial developer and ultimately certifies the device. Given different levels of data to be handled (secret vs. top secret) and given different applications (attended vs. unattended), different factors will be used during each certification process.

The Type 1 certification is a rigorous process that includes testing and formal analysis of (among other things) cryptographic security, functional security, tamper resistance, emissions security (EMSEC/ TEMPEST), and security of the product manufacturing and distribution process. For a new Type 1 device, the engineering design, development, and testing can be a lengthy process itself, but the Type 1 certification process may take even longer. The time period varies from device to device but often is 18 months or longer.

The benefit of this rigorous process may be in the certification time length.

Certification Time Period

NSA Type 1 encryption devices have a virtually unlimited certification time period. A new Type 1 certification is a necessarily lengthy and detailed process. Once completed, the Type 1 device does not have to be re-certified on a periodic basis, unless a vulnerability is discovered.

NOTE: Some of the descriptions and phrasing are taken directly from NSA documents and website in order to preserve the exact meaning and not misinterpret important information. The NSA does not copyright its documents and allows re-use of its material.

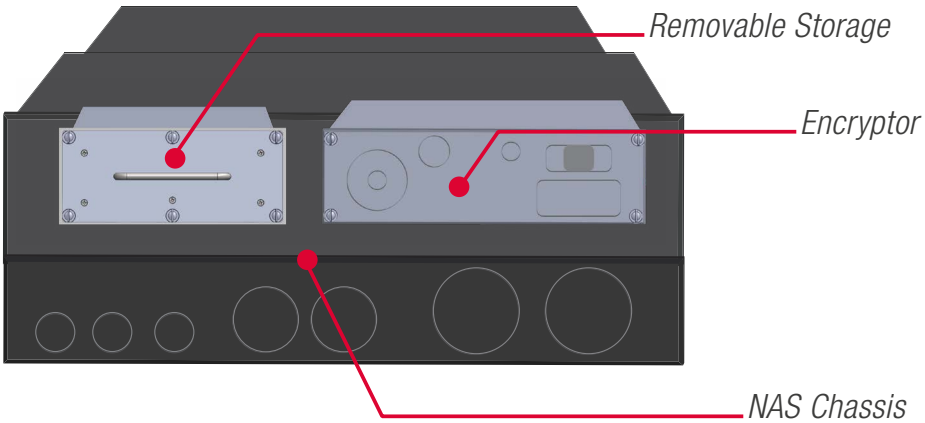

Figure 4: Notional Deployed DAR Storage Solution Components

Conclusion

It is critical in today's world that DAR be protected. Internal and external threats are increasing, which dictates the physical security and encryption of DAR. For deployed applications, the vehicle (fighter, helicopter, UUV, UAV, etc.) may be lost during the mission, putting the critical DAR at risk to exploitation by an adversary. Unattended vehicles may be more at risk to loss than attended vehicles, especially when used in swarms. Critical data is also at risk during transport between the ground station and the deployed vehicle. Even after the mission, advanced persistent threats from nation-states and individuals are attempting to collect and exploit classified DAR.

For many years, NSA Type 1 DAR encryptors have been a very important element in the protection of critical USG data. In the future, Type 1 encryptors will continue to be a major factor in deployed applications especially with the recent introduction of an encryptor certified for unattended operations, which is an increasing application segment for deployed vehicles.

When deciding how to protect DAR, many factors should be considered like export, certification length, cost, size, weight, and power. When considering funding a new Type 1 development (of an encryptor or of a NAS), schedule and technical risk should be honestly considered and not underestimated. There may be other factors unique to a given deployed application, but those factors presented in this paper are a basic set that should be included as part of any such investigation. The next white paper in this series will compare Type 1 and CSfC DAR solutions.

Authors

Steven Petric
Senior Product Manager, Data Solutions
Curtiss-Wright Defense Solutions

Paul Davis
Director, Product Management, Data Solutions
Curtiss-Wright Defense Solutions

Learn More

Products

- Data-at-Rest Encryption Guide
- DTS1 - Network Attached Storage Device

White Papers

- Data-at-Rest Encryption Series

- Part 1: Data Threats and Protection
- Part 2: Commercial Solutions for Classified (CSfC)
- Part 3: NSA Type 1 Encryption
- Part 4: NSA CSfC vs. Type 1 Encryption

- CSfC Series

- CSfC Series: Inner vs. Outer Layer
- CSfC Series: Data-at-Rest Capability Package 4.8

- Choosing the Best Location for Your Data-At-Rest Encryption Technology
- Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions
- COTS Encryption for Data-at-Rest

Case Studies

- Upgrading an Electronic Warfare Suite with an Integrated System Solution
- Rugged Encrypted Data Storage for an ISR Pod

More Resources

- Committee on National Security Systems (CNSSI) Glossary Document CNSSI No. 4009 April 6, 2015
- NIST Publication 800-111 Guide to Storage Encryption Technologies for End User Devices

Endnotes

i. General Dynamics Mission Systems POET ACM Data Sheet
ii. General Dynamics Mission Systems Data At Rest Encryption
iii. ViaSat Data at Rest Encryption for Governments
iv. L3 Harris UnityCP® ASIC
v. Committee on National Security Systems (CNSS) Glossary
vi. Controlled Cryptographic Item (CCI) Briefing

1 (low) 2 3 4 5 (high)

How would you rate this white paper?

TRUSTED PROVEN LEADER

CURTISSWRIGHTDS.COM