Data-At-Rest Encryption Guide
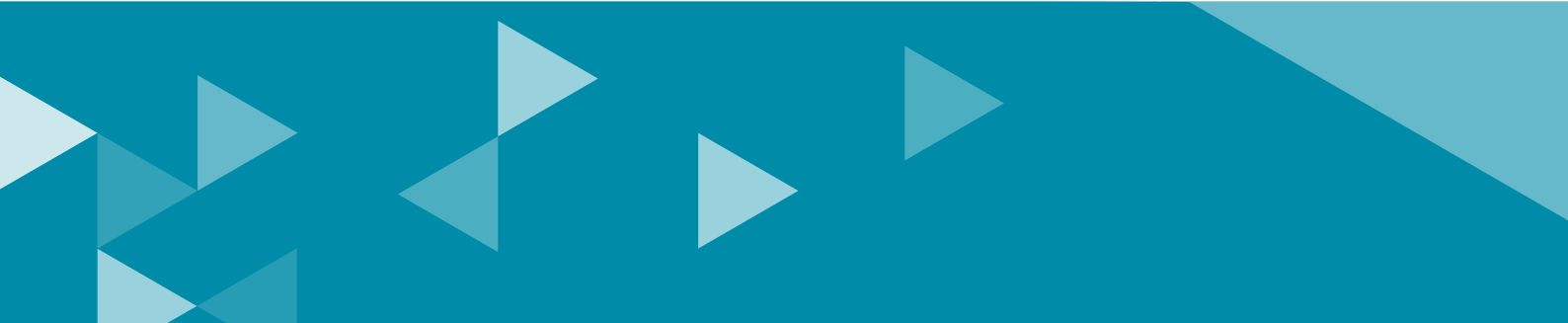
CURTISS-WRIGHT

LAND   AIR   SEA

DATA-AT-REST ENCRYPTION SOLUTIONS

Today's defense and aerospace platforms are required to protect critical data-at-rest (DAR) from unauthorized access. Curtiss-Wright offers cost-effective, proven, and certified commercial off-the-shelf (COTS) storage solutions that match various data security requirements, including National Security Agency (NSA) Type 1, NSA Commercial Solutions for Classified (CSfC), Common Criteria (CC), NATO Information Assurance (NIAPC), and FIPS 140-2.
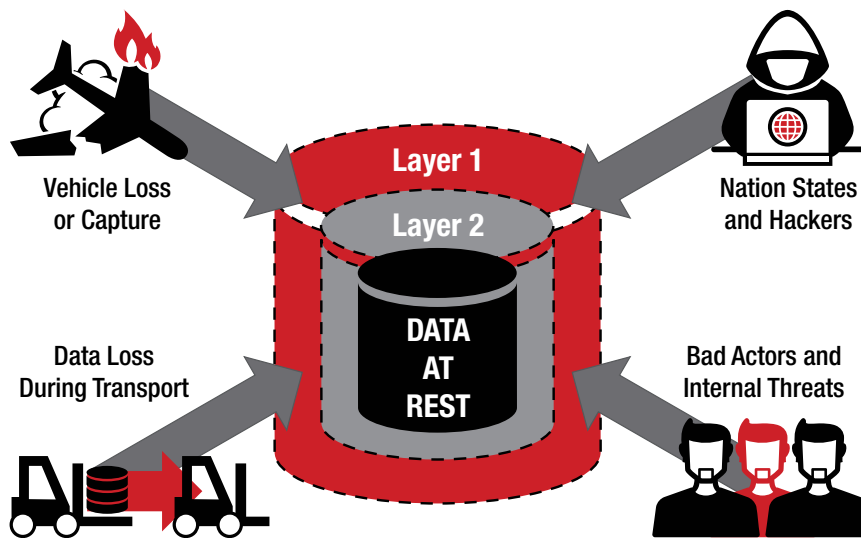
ENCRYPTION STANDARDS

- NSA Type 1
- NSA CSfC
- Common Criteria
- FIPS 140-2
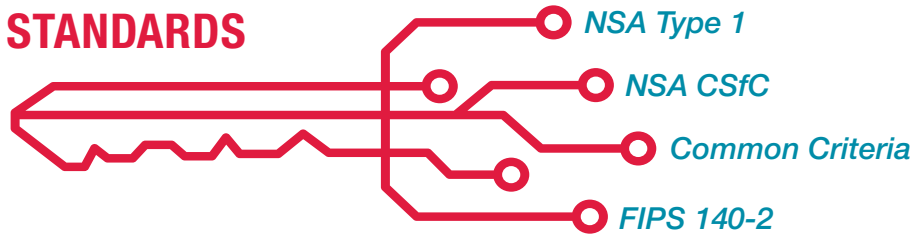
CHOOSING AN ENCRYPTION APPROACH

Classified data-at-rest faces both internal and external threats that can subject sensitive data to exploitation. DAR is particularly at risk during missions if the deployed vehicle is lost, but is also at risk during transport to and from the vehicle. Nation-states and hackers put networked DAR at risk. At the same time, internal threats, such as bad actors with their own agendas, are also a threat to sensitive DAR. This important and urgent matter is further explored in the following white paper, DAR Series Part 1: Data Threats and Protection.

When evaluating or considering an encryption approach, many factors may be used. For each application, the importance of each factor will vary. For deployed applications, 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. The NSA sponsors two basic methods of DAR encryption, and either can be used to protect DAR–Type 1 and CSfC. When deciding how to protect DAR, many factors should be considered like export, certification length, cost, size, weight, and power. As a provider of both NSA Type 1 and NSA CSfC NAS solutions, Curtiss-Wright has a broad and unique perspective. The white paper DAR Series Part 4:NSA CSfC vs. Type 1 Encryption provides an objective, practical, and unbiased comparison between these two NSA programs used to encrypt DAR.

Vehicle Loss or Capture

Data Loss During Transport

Layer 1

Layer 2

DATA AT REST

Nation States and Hackers

Bad Actors and Internal Threats

CURTISS-WRIGHT DAR ENCRYPTION SOLUTIONS

As a developer and manufacturer of network-attached storage (NAS) devices for the commercial and defense industries, Curtiss-Wright offers multiple rugged NAS systems that incorporate NSA Type 1 and Commercial Solutions for Classified (CSfC). In addition, Curtiss-Wright offers FIPS encryption DAR solutions as well.

Unless otherwise noted, the NAS and storage area network (SAN) products listed support the following industry standard protocols:

▶ File serving (NFS, CIFS, FTP, HTTP)

▶ Block storage (iSCSI)

▶ Video stream with real-time protocol (MPEG2 over RTP)

▶ Ethernet recording and packet capture (PCAP)

▶ Remote boot of network clients (PXE, DHCP)

Curtiss-Wright DAR Encryption Solutions

NSA APPROVED ENCRYPTION - TYPE 1 AND CSFC

NSA TYPE 1

A Type 1 product is a Classified or Controlled Cryptographic Item (CCI) endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain approved NSA algorithms and are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with ITAR. In addition to the U.S., Type 1 devices may also be used in the other 5 Eyes countries (UK, Canada, Australia, New Zealand). Additional insights about NSA Type 1 are included in the white paper DAR Series Part 3: NSA Type 1 Encryption.

Unattended Network Storage (UNS)

The Curtiss-Wright UNS leverages the first DAR encryptor on the market certified by the NSA for protection of Top Secret and below DAR in unattended operations. The UNS accommodates two ProtecD@R Multi-Platform Encryptors (KG-204) from General Dynamics Mission Systems (GDMS) behind a secured panel. The incoming plain text (PT) data is encrypted by the KG-204 devices and then stored on the Removable Storage Module (RSM) as cypher text (CT). The RSM is considered unclassified when unpowered and in transport. The UNS protects data from adversaries in forward-deployed locations and in autonomous vehicle operations. The fully rugged, off-the- shelf solution significantly lowers costs and program risk while speeding time to deployment.

UNS KEY FEATURES

+ 2 x KG-204 encryptors
+ 4 x 10 GbE ports
+ 8 x 1 GbE ports
+ 1 x RSM with 32 TB storage capacity

2019 **Military & Aerospace** Electronics
Innovators Awards
SILVER HONOREE

UNS Ground Station (UNS-GS)

The Curtiss-Wright Unattended Network Storage (UNS) system is intended for deployed vehicles requiring Type 1 encryption, high throughput, and massive storage. The UNS is a rugged network attached storage (NAS) system that supports industry standard network storage protocols (NFS, CIFS, iSCSI, HTTP, and FTP) through four 10 GbE (Gigabit Ethernet) and four 1 GbE ports. The UNS Ground Station (UNS-GS) is intended for use in conjunction with the UNS. The UNS-GS accommodates the same Removable Storage Module (RSM) that is used in the UNS.

UNS-GS KEY FEATURES

+ 2 x NSA Type 1 encryption units
  ‣ Top secret and below data protection
+ 32 TB removable solid state memory module
+ Up to 2 GB/s throughtout
+ 4 x 10 GbE and 4 x 1 GbE ports
+ 2 x USB 2.0 ports
+ 1 x RS-232 port

2020 **Military&Aerospace Electronics** INNOVATORS AWARDS

SILVER HONOREE

NSA CSFC AND COMMON CRITERIA

CSfC is essential to NSA's commercial cybersecurity strategy to deliver secure solutions that leverage commercial technologies and products to provide cybersecurity solutions quickly. The CSfC program allows system designers to utilize COTS solutions that have already been verified to satisfy national security standards. The CSfC program is founded on the principle that properly configured, layered solutions can provide robust protection of classified data in various applications. NSA has developed, approved, and published solution-level specifications called Capability Packages (CPs) and works with technical communities from across industry, governments, and academia to develop and publish product-level requirements in U.S. Government Protection Profiles (PPs). The white paper DAR Series Part 2: Commercial Solutions for Classified (CSfC) discusses the CSfC program in depth. System integrators often face budget and time constraints when searching for a solution. Thanks to CSfC, system designers can deploy a COTS solution with encrypted data protection in a matter of months and at a fraction of the cost typically required to achieve certification for more sensitive Type 1 products. As an alternative, CSfC defines an approach for protecting critical data using two-layer commercial encryption technologies. In many cases, system integrators considering a Type 1 approach may be pleasantly surprised to find that their application can instead use the pre-approved and less-costly CSfC approach. CSfC components can be purchased (or loaned) without NSA approval and can be purchased more easily than Type 1 devices. Since it is not International Traffic in Arms Regulation (ITAR) controlled, a CSfC solution (and the components used in it) can be used by more U.S. allies than a Type 1 device (which is ITAR controlled).
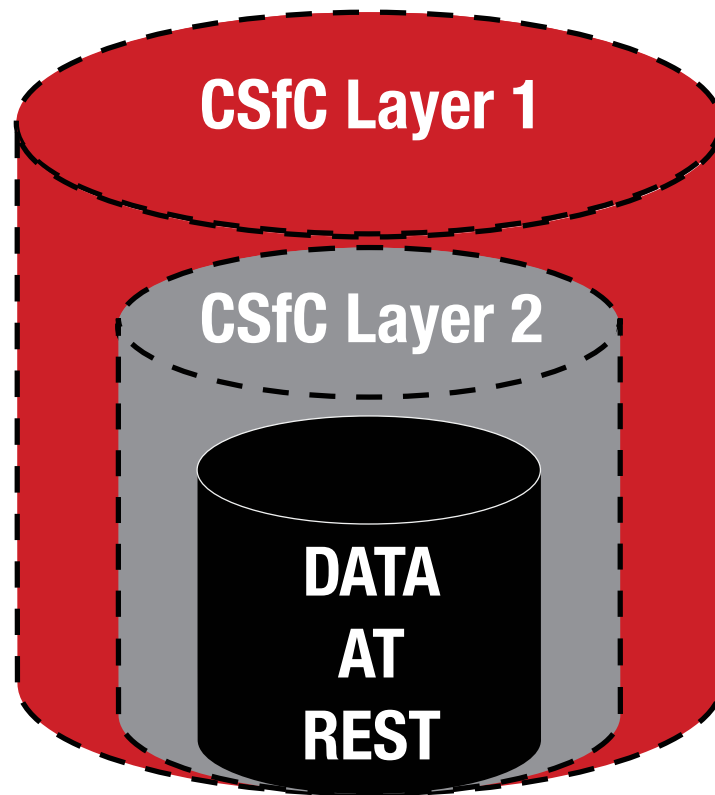
Data Transport System 1-Slot (DTS1)

The DTS1 is the embedded industry's first COTS DAR NAS solution designed with two layers of full disk encryption (FDE) in a single device. Both encryption layers are approved CSfC components. CSfC is an NSA-approved, COTS approach for protecting classified National Security Systems (NSS) information. As a requirement for NSA approval, the two DTS1 encryption layers have each been certified by NIAP under the Common Criteria program. The DTS1 was the first NAS solution to incorporate two layers of full disk encryption into a single device. This provides significant program risk reduction, cost, and time savings.

Selecting a pre-approved device from the CSfC Components List enables system architects to greatly reduce the time and cost needed to design a COTS encryption solution, while also reducing program risk.

The DTS1 is a small form-factor file server that weighs just three pounds, occupies less than 50 cubic inches, and provides scalable storage of up to 8 TB on a single removable memory cartridge (RMC). The RMC is considered unclassified while in transport. The RMC can be easily removed from one DTS1 and installed into any other DTS1 providing full, seamless data transfer between one or more networks in separate locations (e.g., from ground to vehicle to ground), providing quick data off-loading.

DTS1 KEY FEATURES

+ Full disk hardware and software encryption
+ TWO CSfC encryption layers inside
  ‣ International Common Criteria certified
  ‣ NSA approved as CSfC components
  ‣ NATO Information Assurance Product Catalogue (NIAPC)
+ Option MIL-STD-1275 power filter for ground vehicles
+ 2 x 1 GbE ports
+ 1 x RMC with up to 8 TB storage

2 CSfC
ENCRYPTION LAYERS INSIDE

DTS1

2017 Military & Aerospace Electronics
Innovators Awards
GOLD HONOREE

Compact Network Storage 4-Slot (CNS4)

The CNS4 is a flexible storage device designed to meet the challenging programs with changing requirements. Designed around a flexible I/O front end, scalable storage, and advanced encryption options, CNS4 chassis is easily re-configured, mitigating schedule and cost risk when new or changing requirements are introduced. The flexibility of the CNS4 allows it to serve as a technology base across multiple platforms, providing a future-proof solution.

CNS4 KEY FEATURES

+ Full disk hardware and software encryption
+ Both layers
  ‣ International Common Criteria certified
  ‣ NSA approved as CSfC components
+ 4 x 1 GbE ports
+ 4 x Flash Storage Module Carriers with 2 TB storage capacity each

NIST FIPS 140-2

Federal Information Processing Standard (FIPS) Publication 140-2 issued by National Institute of Standards and Technology (NIST) is used to accredit cryptographic modules. Products are FIPS validated using the Advanced Encryption Standard (AES) and a 256-bit encryption key; sensitive data can be protected as prescribed by the FIPS criteria. FIPS 140-2 is used to secure sensitive but unclassified (SBU) information.

Data Transport System 3-Slot (DTS3)

The DTS3 rugged NAS system has been designed for use in mobile vehicles, field ground stations, and aircraft. Similar to but larger than the DTS1, the DTS3 is easily integrated into network centric systems. It supports three RMCs that provide seamless data transfer and quick off-loading. The DTS3 comes standard with SWFDE; optional HWFDE is provided through a module that includes three FIPS-certified ASICs.

DTS3 KEY FEATURES

+ 3 x FIPS 140-2 certified encryption ASICs, one for each RMC
+ 3 x RMC with up to 2 TB each
+ 4 x 1 GbE ports

Compact Network Storage 2-Slot With Fibre Channel (CNS2-FC)

The CNS2-FC comes standard with two 1 GbE ports and two Fibre Channel (FC) ports. The FC ports are particularly useful when upgrading a legacy FC system to modern Ethernet-based NAS where the CNS2-FC can provide a bridge between FC and Ethernet. For data storage and protection, the CNS2-FC hosts two FIPS validated, 2 TB, removable Flash Storage Modules (FSM2). For more information, read the white paper: Bridging Legacy Fibre Channel with Modern Ethernet.

CNS2-FC KEY FEATURES

+ 2 x FSM2 removable storage modules
  ‣ FIPS 140-2 validation in process
  ‣ 2 TB storage capacity each
+ 2 x 1 GbE ports
+ 2 x Fibre Channel ports
+ Fibre Channel target emulation

Data Transport System 1-Slot Non-Certified (DTS1)

For programs that require a SWaP-optimized NAS solution, 4 TB of storage capacity or less, and FIPS-certified hardware, a DTS1 version is available without CC certification or NSA CSfC approval. Similar to the DTS3, this version of the DTS1 comes standard with SWFDE; HWFDE is standard and is provided by one FIPS-certified ASICs.

DTS1 KEY FEATURES

+ FIPS 140-2 certified encryption ASIC
+ 2 x 1 GbE ports
+ 1 x RMC with up to 4 TB

Compact Network Storage 4-Slot Non-Certified (CNS4)

For programs with changing requirements that require flexible storage and FIPS-certified hardware, a CNS4 version is available without CC certification or NSA CSfC approval. Designed around a flexible I/O front end, scalable storage, and advanced encryption options, CNS4 chassis is easily re-configured, mitigating schedule and cost risk when new or changing requirements are introduced. The flexibility of the CNS4 allows it to serve as a technology base across multiple platforms, providing a future-proof solution.

CNS4 KEY FEATURES

+ 4 x FIPS 140-2 validated encryption ASICs, one for each FSM-C
+ 4 x 1 GbE ports
+ 4 x FSM-C with 2 TB storage capacity each
+ Protocol Support: NAS only (NFS, CIFS, FTP, HTTP)

	DTS1	DTS3	HSR10	UNS	CNS2	CNS4
L x W x H (in)	6.5 x 5.0 x 1.5	6.5 x 5.0 x 3.0	9.00 x 8.50 x 3.60	18.95 x 17.80 x 7.10	12.62 x 4.88 x 4.84	12.50 x 10.00 x 7.62
Weight (lb)	3.2	5.5	20	<52	12.1-13.3	39
Cubic Inches	48.75	97.5	275.4	2394.9	298.07	952.5
Network Speed	1 GbE	1 GbE	10 GbE	10 GbE	10 GbE	10 GbE
Encryption	CSfC Two layers (HWFDE & SWFDE)	Two layers AES-256	Two layers HWFDE & SWFDE via Self Encrypting Drives	Type 1	AES-256 FIPS 140-2	Type 1

White Papers	Case Studies	Blogs
COTS Encryption for Data-at-Rest	A COTS Approach to Data-at-Rest Encryption Onboard an Unmanned Underwater Vehicle (UUV)	DTS1 - A Data Transfer Unit (DTU) Replacement with Encryption
What's New? Commercial Solutions for Classified Data-at-Rest Capability Package 5.0 Review	Unmanned Underwater Vehicle NAS Protects Terabytes of Top Secret Mission Data	Leveraging Commercial Encryption to Reduce Risk and Cost.
Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions	Driving Forward the Development of Next Generation UUVs	Meeting the Challenge of Managing Both Data-in-Motion and Data-at-Rest Devices
Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems	Unmanned Surface Vehicle Requires NetBoot and Commercial Encryption	Can Top-Secret Data Be Transported Unclassified?
Choosing the Best Location for Your Data-At-Rest Encryption Technology	Unmanned Surface Vehicle Requires Encrypted Storage for the Autonomy System	Edge Computing, Encryption, and DAR
DAR Series Part 1: Data Threats and Protection	Aircraft Developer looks to Modernize Storage of Sensitive Data	Data-at-Rest Build vs. Buy: Why Export Matters
DAR Series Part 2: Commercial Solutions for Classified (CSfC)	Protecting Data-at-Rest with NSA CSfC Approved Encryption on a UAV	First in Flight, First in Two Layer Commercial Encryption
DAR Series Part 3: NSA Type 1 Encryption	Airplane Developer Looks to Protect ISR Data with Encryption	
DAR Series Part 4: NSA CSfC vs. Type 1 Encryption	Rugged, Encrypted Data Storage for an ISR Pod	
Data-At-Rest Build vs. Buy Considerations for Deployed Storage Devices		
Seaborne Applications & Protecting Data-at-Rest		

CURTISS-WRIGHT

Find Your Sales Representative

curtisswrightds.com

ds@curtisswright.com

Technical Support

curtisswrightds.com/support

dtn_support@curtisswright.com

Additional Contact Details

Curtiss-Wright Defense Solutions
20130 Lakeview Center Plaza, Suite 200
Ashburn, VA 20147
+1.703.779.7800