Data-At-Rest Encryption Guide

CURTISS-WRIGHT

CURTISSWRIGHTDS.COM

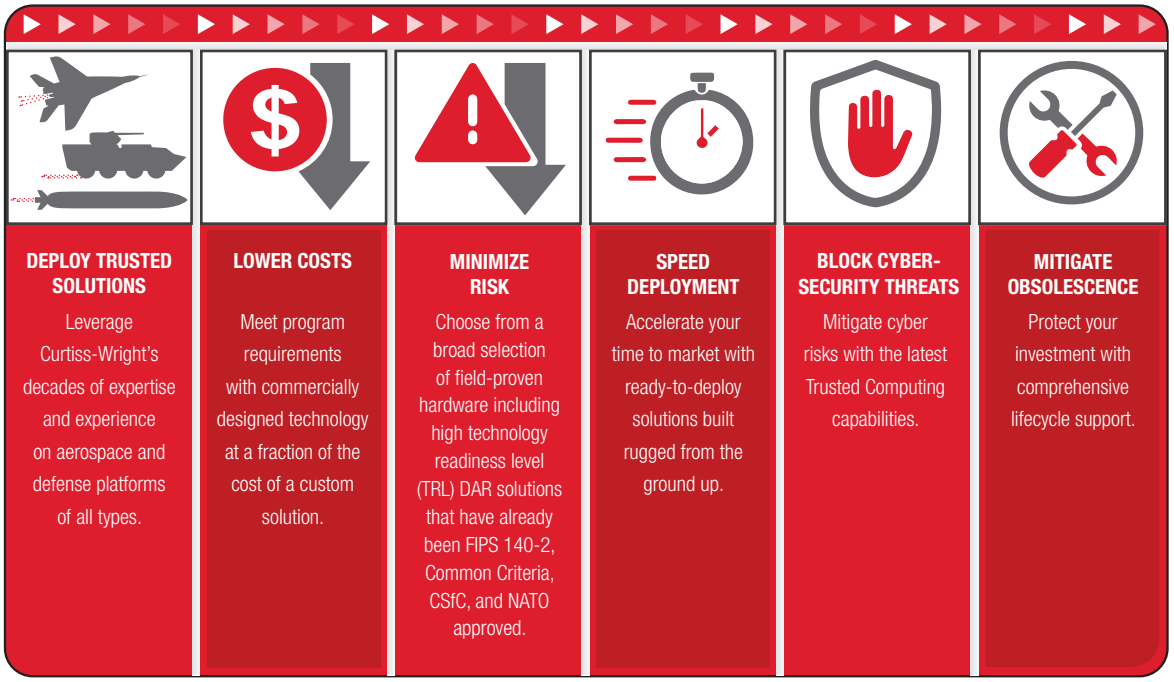
TRUSTED
PROVEN
LEADER

AIR LAND SEA

ABOUT CURTISS-WRIGHT

Curtiss-Wright Defense Solutions, a division of Curtiss-Wright, is an industry-leading supplier of sophisticated electronic products that have been trusted by defense departments, commercial avionics companies, and system integrators around the world for more than 80 years. We are proud to maintain our long historic tradition of innovation that honors the legacy of the company's founders, the Wright brothers and Glenn Curtiss.

Curtiss-Wright continues to lead the way in developing and bringing to market new advanced solutions that address the rapidly evolving requirements of deployed systems and applications. We play a key industry role in the establishment of resources and services that ensure our customers have access to the long lifecycle support required by defense and aerospace programs. As well, Curtiss-Wright offers comprehensive approaches for mitigating obsolescence, blocking the use of counterfeit parts, and developing product roadmaps to ease the integration of future generations of technologies.



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.

CHOOSING AN ENCRYPTION APPROACH

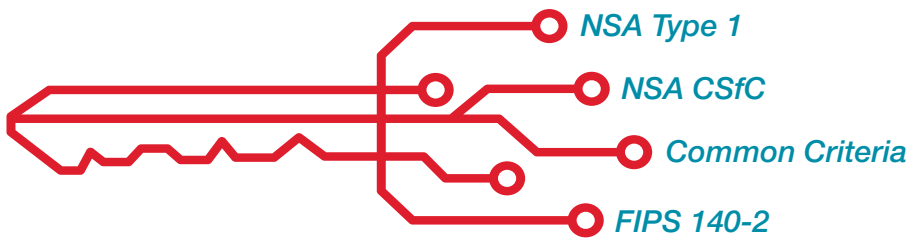
Encryption Algorithms

The strength of the encryption algorithm plays a key role in a DAR system's ability to protect sensitive data. NSA Type 1 encryption devices may use Suite A or B algorithms but the exact type and nature are not publicly known. On the other hand, CSfC encryption devices follow public guidelines set in the DAR Capability Package. The guidelines direct the use of Suite B, now known as Commercial National Security Algorithms (CNSA), which are listed in table 1, below. By using these algorithms and meeting other criteria, the DAR CP states that "up to Top Secret data" can be stored and protected by certified and approved solutions. Older DAR devices may have followed older DAR CP guidelines which allow weaker algorithms like AES-128.

In addition to the encryption algorithm, key generation and management is often an important factor to consider when choosing the right type of encryption technology for DAR applications. The difference between NSA Type 1 and CSfC (or FIPS 140-2) solutions with regards to key management is that the government manages the encryptor keys for Type 1 solutions, whereas a CSfC solution requires the program or customer to decide the best key management solution. Though this can create a challenge for those not particularly experienced with key management, some people prefer to have this responsibility managed in-house. Depending on the level of security required, and program requirements, there are a couple of options available, including outsourcing key management or generating the keys yourself. However, generating the keys yourself requires abiding by a number of strict procedures around when, where, and how they are generated, as well as considering key storage and life cycle management. It's important to note that CSfC provides flexibility around key generation, storage, and management that a Type 1 device does not. Though your CSfC solution provider can help guide you down a key management path that works for your program, ultimately it will be up to you to manage with NSA consultation.

APPROVED COMMERCIAL NATIONAL SECURITY ALGORITHM (CNSA) SUITE FOR DAR		
SECURITY SERVICE	**CNSA SUITE STANDARDS**	**SPECIFICATIONS**
Confidentiality (Encryption)	AES-256	FIPS PUB 197
Authentication (Digital Signature)	Elliptical Curve Digital Signature Algorithm over the curve P-384 with SHA-384	FIPS PUB 186-4
	RSA 3072 (minimum)	FIPS PUB 186-4
Integrity (Hashing)	SHA-384	FIPS PUB 180-4
Can Protect	Up to Top Secret	N/A

ENCRYPTION STANDARDS



Upgrade Path

Another factor to consider when choosing the right encryption solution for your program is the maintenance and upgrade path. A CSfC DAR solution that provides full disk encryption has both software and hardware layers of security. The software layer can be maintained quite easily through secure uploading. So if an issue arises, it can be addressed quickly without returning the system to a depot or to the factory and incurring downtime. Similarly, firmware updates can be completed remotely at the depot level, instead of at the factory. However, like NSA Type 1 devices, when an issue arises with the hardware encryption, both types of devices must be removed from the platform to be fixed. Though this can be an advantage of using a CSfC solution as opposed to a Type 1, the software layer in a CSfC solution is based on open source libraries, which can bring about a new set of issues due to its wide availability. For example, if a weakness is identified, it is publicly available for adversaries to take advantage of. So even though the software may be easier to upgrade and maintain, it is theoretically more vulnerable from a security perspective.

Operation Specific Requirements

When securing DAR on manned platforms, the encrypted NAS is under control of the operator. For unmanned operations, the NAS is unattended, which requires an additional set of considerations. At the time of this publication, the NSA hasn't provided clear guidance on the use of CSfC solutions for unattended operations, though they are working towards providing clarity in a future DAR CP update expected in early 2020. The lack of specific clarity today doesn't mean that CSfC solutions can't be used for unmanned operations, it just means that consideration is needed with regards to the program and application.

Like CSfC, FIPS 140-2 provides no specific guidance regarding unattended operation. On the other hand, Type 1 encryptors are expected to be approved by NSA for unattended operations in 2019.

CURTISS-WRIGHT DAR ENCRYPTION SOLUTIONS

Following the NSA government off-the-shelf (GOTS) approach, Curtiss-Wright offers DAR solutions with Type 1 encryption. As well, following the NSA COTS approach, Curtiss-Wright offers DAR solutions with CSfC and CC encryption. For simpler encryption requirements, Curtiss-Wright offers a FIPS encryption DAR approach. Note that the Type 1-based GOTS solutions are International Traffic in Arms Regulation (ITAR)-controlled, whereas CSfC, CC, and FIPS solutions are not. As such, the CSfC COTS DAR products, and the vehicles in which they are used, may be more widely deployed globally.

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)
- Ethernet recording and packet capture (PCAP)
- Remote boot of network clients (PXE, DHCP)

Curtiss-Wright DAR Encryption Solutions

ENCRYPTION APPROACHES AND PRODUCT SUPPORT

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).

Unattended Network Storage (UNS)

The Curtiss-Wright UNS leverages the first DAR encryptor on the market that is planned to be 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 — certification in process
- 4 x 10 GbE ports
- 8 x 1 GbE ports
- 1 x RSM with 32 TB storage capacity

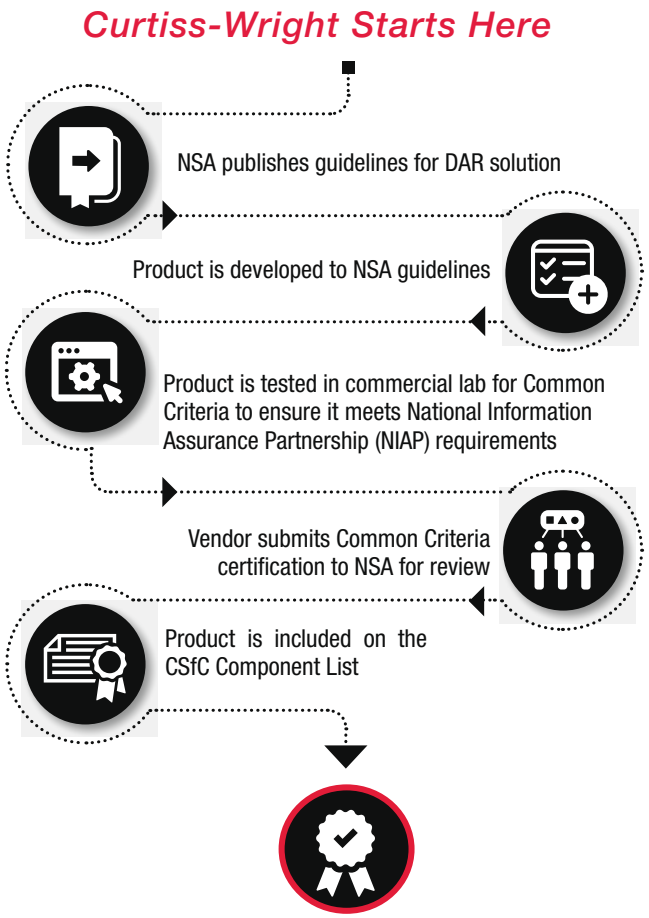
NSA CSFC AND COMMON CRITERIA

CSfC is an important part of NSA's commercial cybersecurity strategy to deliver secure solutions that leverage commercial technologies and products to deliver cybersecurity solutions quickly. The CSfC program is founded on the principle that properly configured, layered solutions can provide robust protection of classified data in a variety of different 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).

For CSfC approval, a DAR component must complete CC certification. In the U.S., the CC certification process is managed by NIAP and the certifications are recognized by 30 other Common Criteria Recognition Agreement (CCRA) member countries. The CCRA was formed to produce a set of stringent standards for IT products and to allow certification in one country, to apply more quickly in another country without re-validation.

Thanks to CSfC, system designers can now 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.

The products below incorporate two COTS full disk encryption layers (hardware and software) which have been certified by NIAP for CC, approved by the NSA for the CSfC Component List and approved by NATO (the DTS1 only)to be listed in the Information Assurance Product Catalogue (NIAPC). These products can protect data at top secret and below as defined by NSA in the DAR Capability Package.

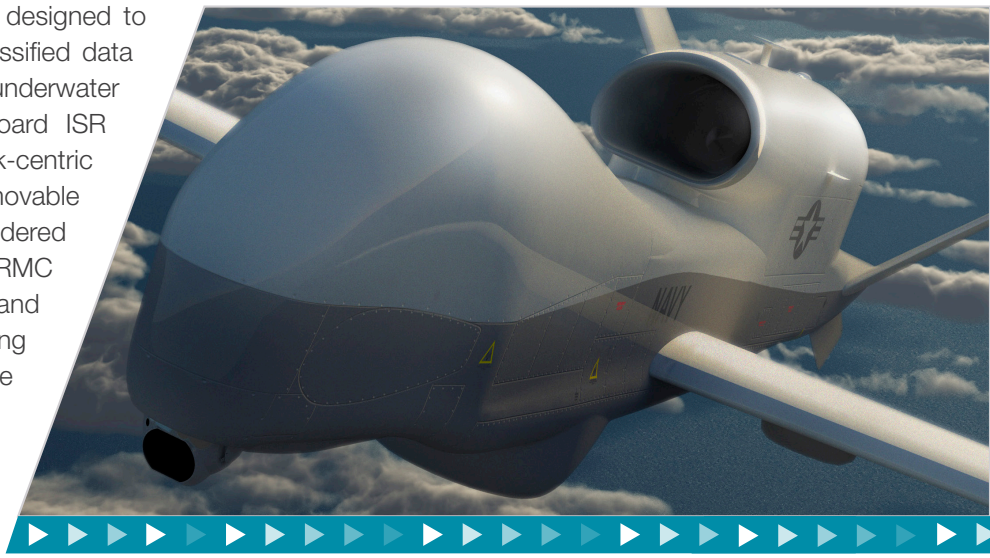


The CSfC Development Process

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. Having received CC certification, the hardware and software FDE layers used in the DTS1 are now currently listed on the United States NIAP Product Compliant List, the NSA's CSfC Components List, International Common Criteria Certified Products list, and the NATO Information Assurance Product Catalogue (NIAPC). 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 greatly reducing program risk.

The rugged small form factor DTS1 is designed to store and protect large amounts of classified data on helicopters, unmanned aerial, underwater or ground vehicles, as well as on-board ISR platforms. Easily integrated into network-centric systems, the DTS1 houses one Removable Memory Cartridge (RMC), which 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
- Both layers
  - International Common Criteria certified
  - NSA approved as CSfC components
  - On the 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 4 TB storage

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.

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

The CNS2-FC comes standard with two 1 GbE ports and two Fiber 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 Fiber 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 Fiber Channel ports
- Fiber Channel target emulation

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

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

+ 1 x 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)

CURTISS-WRIGHT

TRUSTED PROVEN LEADER

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

unitronix
THE EMBEDDED EDGE

9-37 Currans Road, Cooranbong, NSW 2265
+61 (0)2 4977 3511
unisales@unitronix.com.au www.unitronix.com.au