



# DTS1 and DTS1+

## 1-Slot Network Attached File Server

The DTS1 is the embedded industry's first commercial off-the-shelf (COTS) data-at-rest (DAR) network attached storage (NAS) solution that supports two layers of full disk encryption (FDE) in a single device.

Having received Common Criteria (CC) certification, the hardware and software FDE layers used in the DTS1 are now currently listed on the United States NIAP Product Compliant List, NSA's CSfC Components List, the International Common Criteria Certified Products List, and the NATO Information Assurance Product Catalogue (NIAPC). Selecting an approved device enables system architects to greatly reduce the time, cost, and program risk associated with developing an approved encryption solution.

The secure small form factor DTS1 stores and protects large amounts of classified data on helicopters, unmanned aerial vehicles (UAV), unmanned underwater vehicles (UUV), unmanned ground vehicles (UGV), and intelligence surveillance reconnaissance (ISR) aircraft. The DTS1 is an acceptable solution to support unattended Top Secret / Sensitive Compartmented Information (TS/SCI) for DAR. The DTS1 is also the first Common Criteria certified NAS, optimized for deployed ground vehicle operations.

The rugged NAS is easily integrated into network-centric systems and houses one Removable Memory Cartridge (RMC) which is considered unclassified when 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 offloading.

### Key Features

- Full disk encryption - both hardware and software layers
- NSA CSfC Components List approved
- International Common Criteria certified
- ITAR free and NATO Approved
- SWap optimized
- Supports TS/SCI for unmanned
- Network attached storage
  - + Block storage (iSCSI)
  - + Ethernet recording and packet capture (PCAP)
  - + File serving (NFS, CIFS, FTP, HTTP)
  - + Remote boot of network clients (PXE, DHCP)
  - + MPEG2 over RTP

### Applications

- Deployed network-centric systems
- Manned vehicles
- Unmanned vehicles
- Air, Sea and Ground vehicles
- Remote embedded client boot
- Flight test instrumentation

## NEXT GENERATION ANNOUNCEMENT: DTS1+ IS A FORM/FIT/FUNCTION REPLACEMENT FOR THE DTS1 PRODUCT



Next Generation Announcement: The DTS1+ will be a form/fit/function update for the DTS1. The DTS1+ will have an updated encryption ASIC, the same 2 layers of encryption inside with Commercial Solution for Classified (CSfC) approval along with a significant improvement of the data throughput speed. The DTS1+ provides nearly double the data throughput performance as before, with 190 MB/s combined Write speeds and 220 MB/s combined Read speeds. The existing Removable Memory Cartridges (RMCs) and external cables will continue to work with the DTS1+. The order information is listed on the last page of this data sheet.

## Secure Data-At-Rest

The DTS1 is designed around the Commercial Solutions for Classified (CSfC) two-layer encryption program, an NSA-approved approach for protecting classified National Security Systems (NSS) information in aerospace and defense applications. The NSA established the CSfC program as an alternative approach to Type 1 encryption in order to accelerate the protection of top secret data. The two DTS1 encryption layers have each been certified under NIAP's Common Criteria (CC) program, and are listed as NSA approved CSfC components, International Common Criteria Certified Products, and has been approved for listing in the NATO Information Assurance Product Catalogue (NIAPC). As result, the DTS1 can be proposed as a NAS solution in applications for NATO countries. The DTS1 is an acceptable solution to support unattended or unmanned TS/SCI for DAR. With its certified software and hardware encryption layers, the DTS1 reduces program risk while easing and speeding the ability of system designers to protect data-at-rest with an approved, cost-effective NAS.

### DTS1 Common Criteria Certifications

- Hardware Encryption Common Criteria Certificate
- Software Encryption Common Criteria Certificate

## Net-Centric Architecture

Modern unmanned vehicles, ISR aircraft, and mobile ground vehicles are built around a network-centric architecture. The backbone of such systems is Gigabit Ethernet (GbE) operating at 1.25 gigabits per second. With a network switch (or redundant switches) in the middle of the system, any network-enabled device can

communicate with any other similar device. NAS devices like the DTS1 allow any client to retrieve stored files or save new captured files. A NAS device provides size, weight, and power (SWaP) advantages by negating the need for local storage in each computer, display, or management device. These network clients can use the DTS1 to store sensor or maintenance data and to retrieve the latest mission and digital map data. Supporting industry standard NAS protocols like NFS, CIFS, FTP, or HTTP, enables the clients to use different operating systems (Linux®, VxWorks®, Windows®, etc) or CPUs (PPC, Intel®, Arm®, etc), permitting system design flexibility.

## Flexible, Partitioned Storage

The DTS1 supports one RMC which houses one physical disk. Storage capacities range from 256 GB to 8 TB. Each disk consumes about 2.5W and weighs only 0.7 lb (318 g). An RMC is small enough to fit in a shirt or flight-suit pocket. NAND flash memory can be selected to balance cost and endurance.

The RMC can appear like several virtual disks with partitioning. Separate partitions can be configured for NAS files, iSCSI blocks, PCAP data, and PXE boot files. Different software encryption pass phrases can be used on each partition for in-depth security.

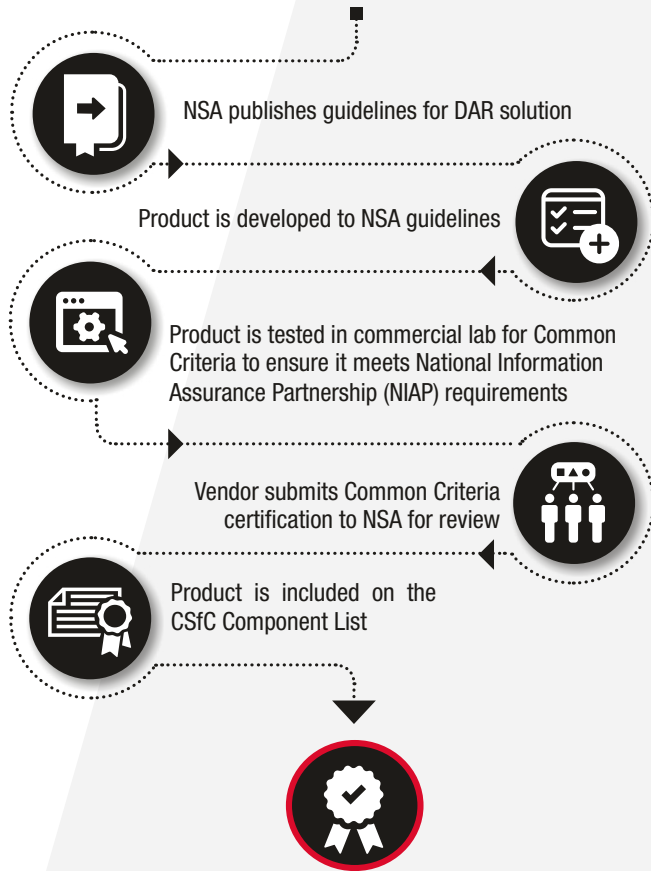
White Paper: [Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions](#)

## DTS1 and DTS1+

## Video Stream Capture

In addition to supporting the NAS protocols, the DTS1 also supports the capture of video streams from cameras. Two MPEG2 streams (via RTP) can be easily handled at one time. The video files are encrypted prior to storage on the RMC.

### Curtiss-Wright Starts Here



## You Start Here

Purchase Certified COTS Product

Figure 1: Shorten encryption development time with approved COTS solutions

## iSCSI Block Storage

The DTS1 supports iSCSI protocol, enabling network clients to use the DTS1 as a block storage device. With the DTS1 acting as an iSCSI target, a network client can be the iSCSI initiator. The initiator has full control over how and where the blocks are stored.

All iSCSI data would be encrypted in the DTS1 prior to storage. A separate partition must be set up for use by the iSCSI initiator. That partition can be equipped with its own unique software encryption passphrase if needed.

## Network Client Boot with PXE

The DTS1 provides the additional protocol called Pre-boot Execution Environment (PXE). Upon power up, PXE allows client devices to obtain boot files from the DTS1. These boot files will be up-to-date when the RMC is loaded by the commander or pilot prior to deployment. With this approach, there is no need to add the extra weight of local storage in each client. Eliminating all the local client drives can result in considerable platform SWaP savings.

In addition to SWaP savings, remote boot also provides the benefit of faster maintenance of the client software. Instead of requiring each client to be physically removed from the platform and transported back to the depot for software updates, the RMC can be loaded with the latest software for each client. This approach reduces software maintenance risk and can provide a huge cost savings over a long program life.

All PXE boot files would be encrypted in the DTS1 prior to storage. A separate partition can be set up for storage of the PXE files. That partition can be equipped with its own unique software encryption passphrase if needed, restricting access to these important boot files.

White Paper: [Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems](#)

## DTS1 and DTS1+

## Flexible Mounting Options

The DTS1 provides two mounting options that make it easy to integrate into your platform: DZUS panel or L-brackets. The DZUS flange allows the unit to be mounted in a standard panel mount. Alternatively, the DTS1 comes with four L-brackets attached to threaded holes on the sides. With the L-brackets, the DTS1 can be bottom-mounted, top-mounted, or side mounted. This flexible option allows the use of a conduction-cooled plate for severe environments.



Figure 2: DTS1 with L-bracket mounting



Figure 3: DTS1 with DZUS mounting

## Removable Memory Cartridge

The DTS1 RMC was uniquely designed to avoid obsolescence issues and increase insertion cycles. The RMC is based on industry standard 2.5" SATA SSDs enabling the RMC to take advantage of the broad industrial base and incorporate any of the widely available 2.5" SSDs up to 8TB currently. As a result, the RMC design allows DTS1 to leverage the dynamic and fast paced technical developments of the SSD industry. Read the white paper "[Choosing the Best Location for Your Data-At-Rest Encryption Technology](#)".



Figure 4: RMC rear and front views

The RMC has also been designed for long program life with a 100,000 insertion cycle connector that includes a SATA interface. The RMC is well suited for deployed applications requiring the storage of data and then the removal and transport to another location. Such applications include ISR applications, any mobile application (ground radar, ground mobile, or airborne ISR pods), any heavy industrial application (steel, refinery), cockpit data, or video/audio data collection.

Optionally, an empty RMC can be purchased and the SSD of your choice can be added. This could include SSDs certified to encryption standards needed for your program, or SSDs providing a specific MIL secure erase function (NSA 9-12 for instance). DTS1 supports an `rmcpurge` command for such drives.

When transporting the RMC from a platform to the ground station, the data is consider unclassified. Due to the complexity of the two certified encryption layers, it is recommended that a DTS1 be used for the ground station.

## DTS1 and DTS1+

## Voltage Protection

The DTS1 is the only NSA and International Common Criteria certified NAS solution with a MIL-STD-1275 compliant filter. The DTS1's filter applies test conditions to the input from the ground vehicle's 28V electrical power system to mitigate against high voltage spikes, long voltage surges, and ripples that can reduce performance and reliability. Compliance with MIL-STD-1275 ensures system integrators that the DTS1 can be used dependably in deployed land vehicle applications.

## Ethernet Packet Capture

In addition to standard NAS, iSCSI, and PCAP operation, the DTS1 has a special mode that allows the capture of Ethernet packets. This is essentially a sniffer mode where every character is captured and stored into a \*.PCAP file. Packet capture is a handy feature for flight test instrumentation (FTI) systems like Curtiss-Wright's Acra KAM-500 to support trouble shooting of Ethernet problems.

The user can specify which of the two DTS1 Ethernet ports is dedicated to packet capture. All the stored packets are encrypted like normal NAS files. When the \*.PCAP files are read, the data is decrypted for analysis. The \*.PCAP files can be opened with shareware like Wireshark®.

A separate partition can be set up for storage of PCAP files. That partition can be equipped with its own unique software encryption passphrase providing access control if required.



Figure 5: Acra KAM-500

## DTS1 and DTS1+

## DTS1 Specifications

### Physical

- Dimensions (H x W x D)
  - 1.5 x 5.0 x 6.5” (38.1 x 127 x 165.1 mm)
- Weight
  - DTS1: 3.08 lb (1.40 kg) (with 1 RMC installed)
  - RMC: 0.7 lb (0.317 kg)
- Mounting options
  - L-bracket
  - DZUS panel

### Power

- Input power: +28 VDC (MIL-STD 704F)
  - Optional MIL-STD-1275 external filter available
- Power: Dissipation: 14 Watts average with RMC
- Peak inrush current: 1.3 Amps
- Performance (128 KB transfers)
  - Both Ethernets
    - » Writing: 60.09 MBps and 59.84 MBps = aggregate of 120 MBps
    - » Reading: 60.49 MBps and 60.54 MBps = aggregate of 121 MBps
  - Single Ethernet
    - » Writing: 108 MBps
    - » Reading: 111 MBps
- Performance (DTS1+)
  - Both Ethernets (HWFDE + SWFDE)
    - » Write: 95 MB/s and 95 MB/s = 190 MB/s
    - » Read: 110 MB/s and 110 MB/s = 220 MB/s
  - Single Ethernet
    - » Write: 110 MB/s
    - » Read: 110 MB/s

### Removable Storage Cartridge (RMC)

- NAND Flash
- User capacities
  - Unformatted: 256 GB, 1 TB, 2 TB, 4 TB, 8 TB
  - Formatted: 235 GB, 940 GB, 1.8 TB, 3.8 TB, 7.8 TB
- Protocols supported:
  - iSCSI
  - NFS
  - CIFS
  - FTP
  - HTTP
  - PXE
  - DHCP
  - PCAP
  - MPEG2

## Security and Encryption

- Hardware full disk encryption (HWFDE), always enabled
  - AES256 bit
  - FIPS 140-2 certified ASIC (#1472)
- Software full disk encryption (SWFDE), customer option
  - Linux Unified Keying System (LUKS)
  - AES256 bit (dmccrypt)
- Common Criteria collaborative Protection Profiles (cPP)
  - Full Disk Encryption - Encryption Engine
  - Full Disk Encryption - Authorization Acquisition

- NSA CSfC Capability Package (CP)
  - Data-At-Rest CP
  - Commercial National Security Algorithm (CNSA) Suite (formerly Suite B)
    - Confidentiality (Encryption) AES256
    - Authentication (Digital Signature) ECDSA over the curve P-384 with SHA-384
    - Integrity (Hashing) SHA-384
  - Can protect up to Top Secret
- Encryption Key(s) Clearance
  - Command
  - Front panel push button
  - Rear panel connector discreet input
- NATO Information Assurance Product Catalogue (NIAPC)
  - NATO Classification = NATO Restricted
  - MCM Reference Number = USA NSA endorsement letter Serial: 2019-07072
  - Product Categories = Disk/File Encryption, Storage and Disaster Recovery
  - Security Mechanism Groups = Cryptography, Interruptibility and Availability, Storage and Digital Preservation

## DTS1 and DTS1+

## Environmental Compliance

- Temperature
  - Operating: -45 to 55°C (71°C for 120 minutes), MIL-STD-810G, Method 501.5 Procedure II and 502.5 Procedure II
  - Non-operating: -45 to 85°C, Method 501.5 Procedure I and 502.5 Procedure I
  - Active cooling: Operating: -40 to +85°C for 90 minutes
- Humidity
  - Operating: 0% to 95%, MIL-STD-810G, Method 507.5
- Vibration, operating
  - Vibration - Narrowband Random over Broadband Random, MIL-STD-810G, Method 514.6 Procedure I
  - Vibration - Endurance Frequency Sweep, DEF STAN 0035, Part 3, Chapter 2-01
- Shock
  - Shock, operating, 20g peak, 11ms wide, 3 shocks in each direction per each axis, MIL-STD-810G, Method 516.6, Procedure I
  - Crash Safety, Non-operating, 40g peak, 11ms wide, 2 shocks in each direction per each axis, MIL-STD-810G, Method 516.6, Procedure V
  - Bench Handling, MIL-STD-810G, Method 516.6, Procedure VI

## EMI compliance: evaluated with respect to MIL-STD-461F

- CE101: conducted emissions, power leads, 30 Hz to 10k Hz
- CE102: conducted emissions, power leads, 10k Hz to 10 MHz
- RE101: radiated emissions, magnetic field, 30 Hz to 100k Hz

- RE102: radiated emissions, electric fields, 2 MHz to 18 GHz
- CS101: conducted susceptibility, power leads, 30 Hz to 150k Hz
- CS114: conducted susceptibility, bulk cable injection, 10k Hz to 200 MHz, Curve 5
- CS115: conducted susceptibility, bulk cable injection, impulse excitation
- CS116: conducted susceptibility, damped sinusoid transients, cables and power leads, 10k Hz to 100 MHz
- RS101: radiated susceptibility, magnetic fields, 30 Hz to 100k Hz
- RS103: radiated susceptibility, electric fields, 2 MHz to 18 GHz, 200 volts/meter

## MIL-STD-704F

### Normal, aircraft electrical operation

- LDC101: Load measurements
- LDC102: Steady state limits for voltage (Tested to 22-29VDC)
- LDC103: Voltage distortion spectrum
- LDC104: Total ripple
- LDC105: Normal voltage transients

### Transfer, aircraft electrical operation

- LDC201: Power interrupt abnormal, aircraft electrical operation
- LDC301: Abnormal steady state limits for voltage (Tested to 20-31.5VDC, 30 Min duration)
- LDC302: Abnormal voltage transients (overvoltage/undervoltage)

### Emergency, aircraft electrical operation

- LDC401: Emergency limits for voltage starting, aircraft electrical operation
- LDC501: Starting voltage transients

### Power failure, aircraft electrical operation

- LDC601: Power failure
- LDC602: Polarity reversal

## Ordering Information

- VS-DTS1SL-F: DTS1 L-bracket chassis, 2-layer encryption, Common Criteria certified, NSA approved , NATO approved
- VS-DTS1SL-FD: DTS1 DZUS chassis, 2-layer encryption, Common Criteria certified, NSA approved , NATO approved
- VS-DTS1SL-0: DTS1 L-bracket chassis, 2-layer encryption, not certifiable
- VS-DTS1SL-0D: DTS1 DZUS chassis, 2-layer encryption, not certifiable
- VS-DTS1+SL-F: DTS1+ L-bracket chassis, 2-layer encryption, CSfC Certifiable
- VS-DTS1+SL-FD: DTS1+ DZUS chassis, 2-layer encryption, CSfC Certifiable
- VS-DTS1+SL-0: DTS1+ L-bracket chassis, 2-layer encryption, not certified
- VS-DTS1+SL-0D: DTS1+ DZUS chassis, 2-layer encryption, not certified
- VS-RMC256M-00: RMC, 256 GB
- VS-RMC1024M-00: RMC, 1 TB
- VS-RMC2048M-00: RMC, 2 TB
- VS-RMC4096M-00: RMC, 4 TB
- VS-RMC8192M-00: RMC, 8 TB



## DTS1 and DTS1+