

SECURE STORAGE SERVER

*Network File Server Protected with NSA Type 1
Encryption for Data-At-Rest*

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
1.0	EXECUTIVE SUMMARY	1
2.0	PRODUCT DESCRIPTION.....	2
2.1	Overview	2
2.2	Network File Server	3
2.3	KG-202.....	4
2.4	Storage Controller	5
2.5	Disk Drives.....	5
2.6	Concept of Operation.....	6
2.6.1	Startup Sequence with Diskless Client Workstations.....	6
2.6.2	Emergency Overrun Response	7
2.6.3	Zeroize Recovery	7
2.6.4	Data Export and Import by Physical Media Exchange	7
3.0	PERFORMANCE	8
4.0	SUMMARY.....	9

LIST OF FIGURES

<u>Figure</u>	<u>Page</u>
Figure 1. Environment for the Secure Storage Server	1
Figure 2. Modular Elements Support the Secure Storage Server.....	2
Figure 3. Modular Network File System.....	3
Figure 4. Modular Type 1 Fibre Channel Encryption/Decryption	4
Figure 5. Modular Controller Supports RAID 0/1 or RAID 5	5
Figure 6. Secure Storage Server Supports Multiple Disk Drives	6

LIST OF TABLES

<u>Table</u>	<u>Page</u>
Table 1. Performance of the Secure Storage Server	8
Table 2. Benefits of a Secure Storage Server	9

1.0 EXECUTIVE SUMMARY

The vulnerability of data in transit has long been understood. Network encryptors are used to protect critical information – voice, data, and video – sent from one location to another. These encryptors share confidential key material, ensuring that only those intended to receive the information are capable of deciphering the data.

In today's net-centric environment, however, information needs to be protected not only in transit, but also at the many nodes where it is stored within a network. This information, or data-at-rest, can be at the heart of a network on an enterprise server, at the tactical edge on a single PC, or anywhere in between. All of these storage points are vulnerable to threats from insiders or overruns when forward deployed. Data-at-rest is data at risk.

General Dynamics C4 Systems is developing several NSA-certified, Type 1 products to protect data-at-rest. The first product is a Secure Storage Server, shown in Figure 1, that combines the elements of an enterprise file server (processor blades hosting file server software, storage controller and multiple disk drives) with the protection of the KG-202 embedded media encryptor into an integrated, modular turn-key system.

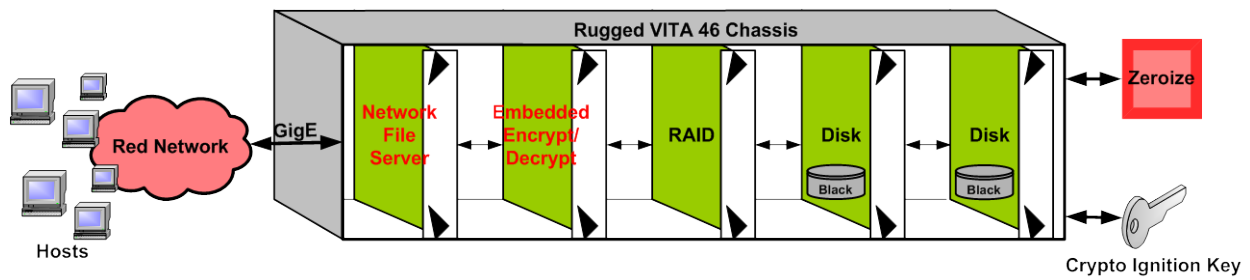


Figure 1. Environment for the Secure Storage Server

The Secure Storage Server uses industry-standard file architectures and protocols to provide transparent operation to users. Additional media can easily be added to grow with mission needs. The shelf can also be provisioned so that the media can be shared between servers. This modular solution provides all authentications required to meet stringent NSA certification requirements. Through a single action, the stored data can be rendered instantly inaccessible, yet still available for recovery later.

The Secure Storage Server will be available for demonstration at General Dynamics C4 Systems starting in early 2009.

2.0 PRODUCT DESCRIPTION

2.1 Overview

Designed for data-critical applications, the Secure Storage Server is an integrated file server appliance that simplifies data sharing in a network environment, while providing the protection of NSA-certified Type 1 encryption for the stored data-at-rest.

The Secure Storage Server, shown in Figure 2, offers the same ease of access that commercial file servers provide to multiple network client computers accessing a common pool of storage. In addition, the integrated KG-202 embedded media encryptor provides Type 1 encryption for the data-at-rest in the Secure Storage Server so that the non-volatile media is protected up to TOP SECRET/Sensitive Compartmented Information (TS/SCI).

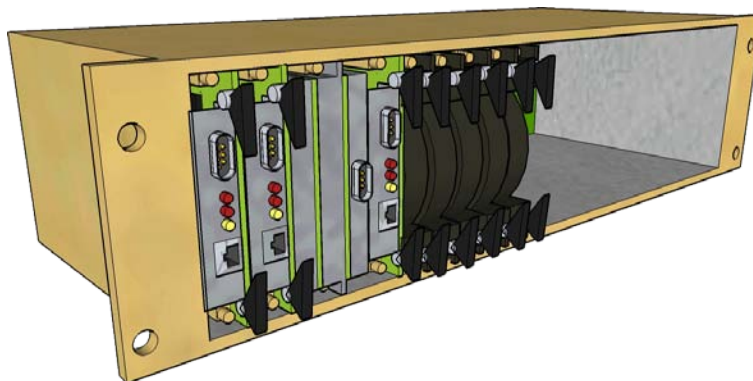


Figure 2. Modular Elements Support the Secure Storage Server

The Secure Storage Server provides heterogeneous data sharing and ease of use based upon mature commercial network file access protocols. Data stored on the Secure Storage Server is accessed using commercial standard open protocols (Network File System (NFS) and Common Internet File System (CIFS)) over standard Ethernet network connections. The NFS and CIFS protocols use client programs that reside on the user's host computers to gain access to the encrypted files. The user computer performs normal file and directory transactions with this client software (routinely part of Windows and Unix/Linux systems). The client software interacts with the server software provided by the Secure Storage Server to gain access to the user's data. The software within the Secure Storage Server converts the client file accesses into actual media device reads and writes.

The encryption function is invisible to the client computers as well as to the media devices attached to the Secure Storage Server. The cryptographic keys used to encrypt the data are stored within the KG-202. All necessary security functions for protecting the encryption keys are provided by the design of the KG-202.

All the functions needed to configure and manage the embedded KG-202 media encryptor are incorporated within the Secure Storage Server. Management options for the Secure Storage Server provide for the assignment of file access privileges to different users, the allocation of storage capacity to different logical volumes, and the association of specific encryption keys with specific logical volumes. Once keys have been associated with a logical volume, this association is automatically detected and the correct keys are used to access the data. This automatic detection is particularly useful for media that is moved from a mobile platform to a ground station, or for media that is shipped from one location to another (e.g., mobile-to-mobile or ground-to-ground).

For routine operations such as an overnight shutdown, the Secure Storage Server can easily be made inoperative (unclassified) and can just as easily be returned to full functionality. This routine deactivation and reactivation is accomplished by removing the Crypto Ignition Key (CIK) from the Secure Storage Server's front panel, then later reinserting it. When the CIK is removed, the Secure Storage Server's cryptographic functions are disabled and the stored data is no longer accessible for reading or writing. Returning the CIK to the Secure Storage Server restores its cryptographic functions and restores access to all protected data.

In an emergency, with or without power, the media encryption keys can be zeroized within a fraction of a second. The Secure Storage Server makes available a manually operated zeroize switch as well as a zeroize discrete for remote placement of a zeroize switch in the event that the Secure Storage Server is not conveniently accessible to the operator. Once zeroized, the server and the data it protects are inaccessible for reading and writing and are unclassified, even if classified data (up through TS/SCI) has been stored on the media. When the emergency is resolved, the original keys can be obtained through key management channels and re-filled into the Secure Storage Server. Once the keys have been restored, full access to the original data is also restored.

A discussion on each of the modules that compose the Secure Storage Server follows:

- Network File Server
- KG-202
- Storage Controller
- Disk Drives

2.2 Network File Server

The Secure Storage Server provides a journaling file system using a dedicated processor, shown in Figure 3. Data stored on the Secure Storage Server is accessed using commercial standard open protocols (NFS and CIFS) over standard Ethernet network connections.

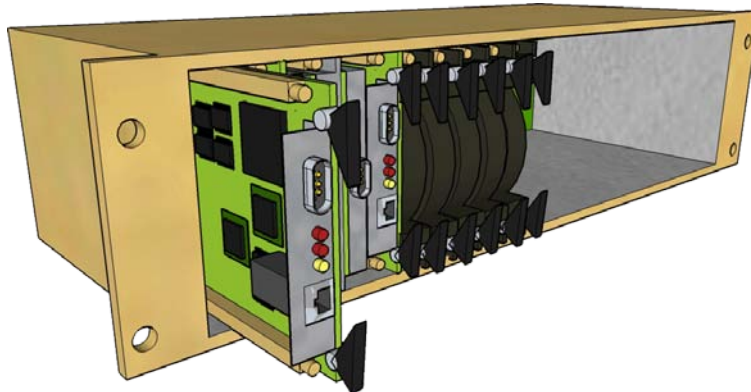


Figure 3. Modular Network File System

The Secure Storage Server provides access for Windows, Linux/Unix, and MacOS clients. The Secure Storage Server can be configured to provide NFS file access for Linux/Unix MacOS clients and for Microsoft systems using Microsoft's Services for Unix. NFS is an open standard, cross-platform file system utility with implementations available for a wide range of operating systems, architectures, platforms, and appliances, from embedded systems to mainframes and high-performance clusters. The Secure Storage Server can also be configured to use Windows Server Message Block (SMB) and CIFS protocols for Windows clients, and provides an interface for networks using Microsoft's Active Directory. The Secure Storage Server provides Windows and NFS file access concurrently. This dual system can be more effective than using the protocols in separate servers.

Windows users can access files and storage space through the Secure Storage Server via “My Network Places” or “Map Network Drive”, just as they do with Windows-based file servers. Unlike Windows-based file servers, a Secure Storage Server does not require any client licenses.

This approach provides rapid recovery from improper shutdowns and drastically reduces the chances of file system corruption, even from severe events such as a power failure. In contrast, a file server not using a journaling file system must have its directory structures checked for consistency after an unexpected power failure or system crash.

2.3 KG-202

Protection for the Secure Storage Server is provided by the KG-202 (Figure 4). This module is a Type 1 cryptographic device used to protect an enclave's data filed in a storage subsystem. User data may include data files, videos, or host-generated management data. The KG-202 encrypts user data before the data is written to the data storage subsystem. This renders the data as “black” on the media. When the users' data is read from the data storage subsystem, the KG-202 automatically decrypts the data. Multiple enclaves at different classifications may share a single data storage subsystem when multiple KG-202 and NFS modules are installed.

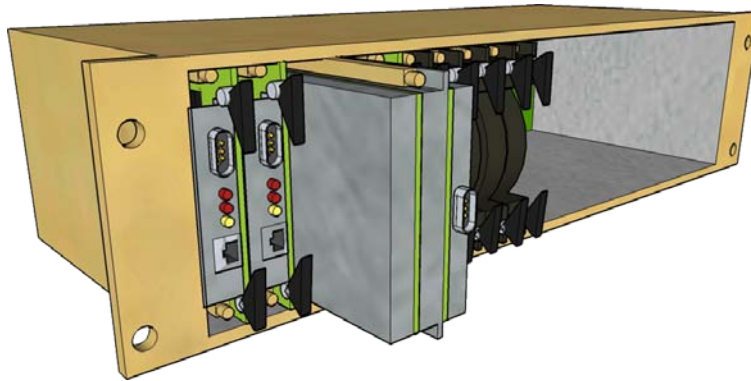


Figure 4. Modular Type 1 Fibre Channel Encryption/Decryption

Key management for the KG-202 is based on the Government's Electronic Key Management System (EKMS). Traditional keys are loaded using either red or benign fill techniques. Data stored on a disk drive within one Secure Storage Server can be shared with other Secure Storage Servers by using the same media encryption key.

A significant feature of the KG-202 is that all data in the storage subsystem of a Secure Storage Server can be quickly rendered cryptographically unintelligible in three ways. The first method is simply to remove the CIK. Without the CIK, the encryptor is rendered unusable and becomes an unclassified, Cryptographic Controlled Item (CCI). The data may be quickly recovered and the Secure Storage Server returned to operation by reinserting the CIK. The second method is for the host system to activate the discrete zeroize signal into the encryptor. After the signal has been activated, the data may still be recovered by refilling the media encryption keys. Lastly, the administrator may log into the web based Secure Storage Server configuration manager and send a zeroize command. Again, the zeroize recovery procedure will recover the data.

Interfaces through the VITA-46 backplane to the KG-202 include:

- One plaintext (PT) port and one ciphertext (CT) port. The PT and CT ports support Small Computer System Interface (SCSI) protocol over Fibre Channel (FC) to transfer user data between a host and a storage partition in the data storage subsystem. The KG-202 operates at the SCSI block level and does not interpret the meaning of user data contained within the SCSI blocks.

- An Ethernet management interface through which the NFS hosted system manager can monitor and control the KG-202, using Management Information Base (MIB) elements via Simple Network Management Protocol Version 3 (SNMPv3) commands.
- A DS-101 key fill bus interface designed to support multiple KG-202s.
- A CIK interface to accept its crypto ignition key.
- Discrete signal interfaces to the backplane provide the capability to command zeroization, set classification level, provide KG-202 status, set the IP address for management, and set power shutdown warnings.

As with all of the Secure Storage Server components, the KG-202 is a replaceable unit. During storage and transit, the encryptor receives power from its transport battery attachment, which is removed after the KG-202 is installed in the chassis assembly.

2.4 Storage Controller

The storage controller used in the Secure Storage Server, shown in Figure 5, provides management of the data across several disks. This module supports the operations of standard RAIDs including 0/1 or 5. The front end of the storage controller interfaces to the KG-202 with Fibre Channel, and the back end provide Serial Attached SCSI (SAS) ports to the disk drives. The SAS interface allows for external memory expansion to many terabytes (TBytes).

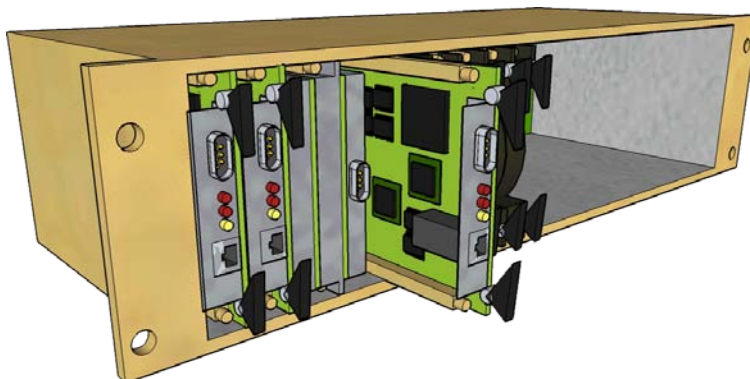


Figure 5. Modular Controller Supports RAID 0/1 or RAID 5

The storage controller supports RAID 5's striped parity, distributed across several disks, which allows the system to recover automatically after the failure of any disk. User traffic is processed and the data stored is unaffected.

The storage controller can also be configured with stand alone "removable" media which allows a disk with encrypted data to be shipped to another location, where the data can be decrypted. These encrypted disk drives are considered cryptographic "black" material and can be handled as Cryptographic Controlled Item (CCI) devices.

2.5 Disk Drives

The Secure Storage Server uses industry-standard SAS drives. Figure 6 illustrates that multiple drives can be supported in the rugged chassis for a storage capacity into TBytes. With the storage controller acting as a RAID 5, any disk can be removed and repaired without interrupting users' operations.

Although initially designed for moving head media, the Secure Storage Server is compatible with solid state media as well.

A single array of disks can be used to store multiple levels of security by using multiple NFS servers and KG-202 encryptors filled with different keys. For those data centers that handle multiple classification levels, this helps reduce the costs of integrating and provisioning multiple storage arrays as well as saving data center power.

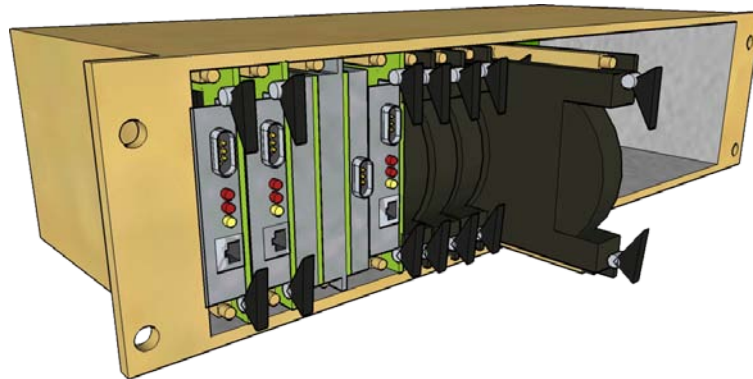


Figure 6. Secure Storage Server Supports Multiple Disk Drives

2.6 Concepts of Operation

2.6.1 *Startup Sequence with Diskless Client Workstations*

1. Following application of power, the Secure Storage Server initializes the attached storage, boots the file server from local flash memory, and initializes the KG-202.
2. Diskless workstations boot from local flash memory to a point that enables the download of the remainder of their operating systems and the application software from the Secure Storage Server.
3. The user inserts the CIK and logs into the Secure Storage Server web based configuration page to unlock the KG-202.
4. The KG-202 becomes active and compares internally stored media encryption keys to the keys needed to access the stored data within the Secure Storage Server.
5. The KG-202 associates media encryption keys with the correct storage partitions and restores media access to the Secure Storage Server.
6. The file server allows the files stored on the Secure Storage Server to be visible to the diskless clients.
7. Diskless clients complete their boot process and load application software.
8. Application software reads and writes files within the Secure Storage Server as network-attached files.

2.6.2 *Emergency Overrun Response*

In an emergency, the stored data can be quickly protected:

1. Zeroize switch on Secure Storage Server (or the remotely located zeroize discrete) is activated.
2. KG-202 destroys all media encryption keys within a small fraction of one second. This process can be performed with or without system power.
3. Without the media encryption keys, the data stored in the Type 1 Secure Storage Server is unintelligible. All read and write accesses to the Secure Storage Server's storage media will fail.

2.6.3 *Zeroize Recovery*

After a zeroize, access to the stored data can be easily restored:

1. The user fills the KG-202 through the front panel DS-101 fill port with the same media encryption keys originally used from a data transfer device (e.g., DTD or Simple Key Loader (SKL)).
2. The user logs into the Secure Storage Server to unlock the KG-202.
3. The KG-202 automatically associates media encryption keys with the correct storage partitions and restores media access to the server.
4. The Secure Storage Server restores the file systems to the last self-consistent journal state and allows the files stored on the Secure Storage Server to be visible to the clients.

2.6.4 *Data Export and Import by Physical Media Exchange*

Data stored on the Secure Storage Server may be transferred to a different location:

1. Remove the media blade to be transported (as with any removable disk, removing media during read or write activity may corrupt the disk).
2. Because the media blade containing the encrypted classified data is UNCLASSIFIED, they may be transported by any method compatible with CCI handling.
3. Install the media blades into the destination Secure Storage Server.
4. KG-202 compares the internally stored media encryption keys to the keys needed to access the stored data within the Secure Storage Server.
5. KG-202 automatically associates media encryption keys with the matching storage partitions and restores media access to the server.
6. If the KG-202 does not automatically perform the key associations, the user logs into the Secure Storage Server configuration page to identify the short title of the additional media encryption key(s) needed to access data on the storage blades. The user then fills the KG-202 through the front panel DS-101 fill port with the needed media encryption key(s).
7. File server allows the files stored on the Secure Storage Server to be visible to the clients.

3.0 PERFORMANCE

The Secure Storage Server provides enterprise level performance in a compact rugged chassis as shown in Table 1.

Table 1. Performance of the Secure Storage Server

Characteristic	Performance
Security Features <ul style="list-style-type: none"> • Encryption algorithm • Methods of key fill • CIKs • Media encryption keys 	<ul style="list-style-type: none"> • AES-256 • Benign fill, red fill • Up to 6 CIKs, all equivalent • Maximum 31 keys; up to 16 may be active, the rest are spares
Data Transfer <ul style="list-style-type: none"> • Secure Storage Server • KG-202 Fibre Channel I/O • Throughput between media and NFS • Data frame latency through KG-202 • Concurrent exchanges (data transfers) • Devices on KG-202 PT loop • Devices on KG-202 CT loop • Number of disk partitions (logical units) 	<ul style="list-style-type: none"> • Gigabit Ethernet data rates in each direction • Up to 2 Gbps in each direction, simultaneously • Up to 1.6 Gbps in each direction, simultaneously • 200 microseconds • 16 concurrent exchanges • Up to 5 hosts • One • 16, each may use a different media key
Startup Time <ul style="list-style-type: none"> • Power up 	60 seconds
Power <ul style="list-style-type: none"> • Input power • Power consumption 	<ul style="list-style-type: none"> • 120 VAC (28 VDC optional) • Wattage determined by storage configuration

4.0 SUMMARY

Table 2 summarizes the benefits of the Secure Storage Server to a user. The Secure Storage Server is designed to work as a complete, turn-key solution. The Secure Storage Server is a low cost storage approach that provides enterprise-level performance, scalability, and availability, combined with NSA-certified Type 1 security. The Secure Storage Server is a specialized appliance optimized for storing, retrieving, and serving files, which also provides advantages over direct-attached storage, including improved scalability, reliability, availability, and performance.

Table 2. Benefits of a Secure Storage Server

Feature of Secure Storage Server	Benefit to Users
Transparent Operation	Secure Storage Server's use of open standards and high speed encryption provides network users secure Type 1 storage without meaningful performance impact.
Type 1 Encryption	Use of Type 1 encryption allows for three major advantages for sensitive data up to TS/SCI: <ul style="list-style-type: none"> • Sharing of "black" media across multiple security domains • Quick cryptographic erasure in case of overrun • Simplified data handling.
Support for RAID 5	Increased system reliability with data and parity striped across multiple disks. Replacement of a faulted disk is accomplished without user's traffic interruption.
Automated, User Friendly Support for Removable Media	Transportation of classified data using CCI device restrictions only. Supports archiving data off site with CCI restrictions only.
Modularity for TBytes of Storage	SAS media, either rotating head or solid state, can be added to the VITA-46 chassis. The modular design supports growth as system or mission changes.
Standardized Front End	The use of a standard Gigabit Ethernet and Network File System (NFS or CIFS) allows integration into existing or new storage systems.
Ruggedized Environments	Allows for enterprise level storage in forward deployed platforms such as wheeled vehicles or airframes.

The Secure Storage Server can support multi-level security systems. One method is to provide a separate Secure Storage Server for each classification level; encrypted data is stored on separate storage subsystems per classification. Another method is to configure one Secure Storage Server with a KG-202 and NFS pair for each classification level; encrypted data from each classification level is stored on the same storage subsystem (storage controller and disk array).

The Secure Storage Server enables files to be shared easily by multiple users and enables storage to be allocated quickly and easily. The amount of available storage can also be increased more cost-effectively than by adding storage to individual workstations.

For more information on the system or the roadmap for the Secure Storage Server, please contact: INFOSEC@GDC4S.com