DIGISTOR®

SECURE DATA STORAGE

Use Citadel K-GL SSDs to Secure Downrange Data at Rest (DAR)

Protect against unauthorized access to data on UAVs, tactical edge devices, and appliances

- **Headless Authentication**
- **COTS priced and ITAR free**
- **Windows, Linux, hypervisors like SecureView, and Forcepoint**
- **Meets Defense DAR security requirements**

Citadel K-GL FIPS 140-2 certified self-encrypting SSDs with pre-boot authentication (PBA) are ideal for securing data collected and stored in UAVs, sensor systems, autonomous platforms, appliances, and tactical edge devices that don't have a keyboard or monitor.

Powered by CipherDrive®, the built in PBA of Citadel K-GL locks access to the encrypted OS and data on the drive until a user inserts a USB security key. Once authenticated, the PBA unlocks the SSD and the system boots as intended.

The Citadel K-GL SSD is encrypted by NSA-approved Advanced Encryption Standard (AES) 256-bit encryption at the hardware level. This means Citadel GL has no software overhead and provides read/write access to encrypted data at the full performance of the system.

Citadel K-GL SSD Security Features

- Specialized version for headless applications
- No monitor or keyboard required - System waits for an authorized USB security key to be inserted before unlocking
- Encryption - AES-256, FIPS PUB 197 specification
- Authorization Acquisition (AA) under Common Criteria cPP
- Compliant under collaborative Protection Profiles (cPP)
- Pre-Boot Authentication (PBA) supports booting and chain loading VMs / SecureView and other hypervisors
- PBA Admin and Management capabilities
- Cryptographic Erase (CE)
- User Management
- Trusted Platform Module (TPM) 2.0 support
- Key Management – Custom AK and DEK

NIST Certification #3926

DIGISTOR Citadel K-GL Secure Storage SSDs

Technical Specifications

Form Factors & Interfaces	▪ M.2 2280 PCIe Gen 3x4 NVMe 1.3 ▪ M.2 2280 SATA 6 Gb/s 2.5-inch 7mm SATA 6 Gb/s	Advanced Flash Management	Static & Dynamic Wear Leveling Bad Block Management TRIM S.M.A.R.T.	Authentication Methods	USB Key
Flash Type	BiCS4	MTBF	More than 1,600,000 hours	Confidentiality (Encryption)	AES-256 / FIPS PUB 197
Performance	SATA: Read: up to 550MB/s Write: up to 530MB/s NVMe: Read: up to 3,400MB/s Write: up to 3,100MB/s	Encryption	TCG Opal SSC hardware level AES 256-bit encryption	Authentication (Digital Signature)	Elliptic Curve Digital Signature Algorithm (ECDSA) over the curve P-384 with SHA-384 / FIPS PUB 186-4 RSA 2048-PSS with SHA-256 method / FIPS PUB 186-4
Power Consumption	Active mode: ≤2,300mW Idle mode: ≤110mW	Compliance	RoHS Compliant TAA Compliant	Integrity (Hashing)	SHA-384 / FIPS PUB 180-4
Temperature Range	Operation: 0°C ~ 70°C Storage: -40°C ~ 85°C				

Citadel K-GL SSDs are self-encrypting drives that secure all critical data using strong AES 256-bit encryption, with the encryption/decryption performed by the SSD hardware itself, independent from the host, which maintains the highest host performance by not impacting CPU load. Locked BOMs available.

All available configurations are TAA-compliant, FIPS 140-2 L2 certified (NIST Certification #3926), and NIAP-listed

CipherDrive K-GL Technology is FIPS and Common Criteria Certified

Contact Us

+1 (408) 796-5140
sales@digistor.com
www.digistor.com

1000 SE Tech Center Dr, Suite 160
Vancouver, WA 98683