



## PacStar 413 HSM Sled

### ENGAGE BLACK



**PacStar 413 HSM Sled with  
BlackVault HSM Installed**

PacStar 413 adapts Engage Black, BlackVault Hardware Security Module (HSM) devices to integrate into PacStar 400-Series compact case solutions. The combination creates a rugged small form factor HSM that provides FIPS 140-2 Level 3+ certified crypto key generation, storage and signing support for use with certificate authorities (CA), while taking advantage of the PacStar 400-Series modularity. PacStar 413 is ideal for forward deployed secure key management for use in public key infrastructure solutions – and is designed to be used in classified and PKI enabled networks powered by commercial solutions, supplementing online CAs.

The sled provides snap-in integration for the BlackVault HSM including:

- Physical adaptation of the HSM into the PacStar 400-Series chassis
- (1) 10/100 copper RJ-45 Ethernet interface, exposed on the front of the HSM
- Integrated smart card reader with card retention device
- PacStar 400-Series standard interconnect enabling modules ‘snap’ together in the field and to share power
- Locking features front and back, for secure transport

PacStar 413 is designed to work in conjunction with PacStar 400-Series communications modules serving the tactical and expeditionary communications needs of small teams that deploy worldwide and have secure communication requirements in austere environments. PacStar 413 enables teams from US DoD, Coalition Forces, Homeland Security, first responders and civilian organizations to easily and securely manage crypto keys.

#### KEY FEATURES - Sled

- Secures and integrates BlackVault HSM into PacStar 400-Series solutions
- Integrated power connectors providing power from tactical radio batteries, or power input provided by PacStar 400-Series chassis
- Continuous runtime with hot swappable batteries
- Snap-together design enables quick expansion with other PacStar 400-Series products
- Compact design for flexible packing and transport

#### KEY FEATURES - BlackVault HSM

- FIPS 140-2 Level 3 Certified Security Architecture
- Tamper Reactive Die Shield
- Suite B Accelerators
- Support for NIST ECC Curves
- Secure Authentication/Access
- Role Based Multi factor authentication
- Backup through Key Cloning
- M of N per role

#### Military Grade Tamper Reactive

The Cryptographic Boundary is within Secure CPU's silicon. The Die Shield has dynamic fault detection with real time environmental and active tamper detection circuitry.

- Achieves Active Level 3+ Tamper
- Eliminates Inadvertent Tamper
- Transport Safe

#### Encryption Capabilities

- Asymmetric public key algorithms:
  - RSA (1024, 2048, 4096)
  - Diffie-Hellman ECDH, DSA, ECDSA
- Symmetric algorithm: AES 128, 192, 256
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512bit)
- Full Suite B implementation with Elliptic Curve Cryptography (ECC)
- Hardware Random Number Generator
- NIST SP 800-90 compliant DRBG

#### Connectors

- (1) RJ45 (10/100 Base-T Ethernet)
- Wide range DC input via PacStar 400-Series standard power interconnectors /radio battery compatibility

#### Physical Specifications

- Dimensions 5.67" x 10.12" x 1.73"
- Weight 3.6 lbs. (with BlackVault HSM)
- Supports PacStar 400-Series standard interconnect enabling modules to be ‘snapped’ together in the field and share power
- Fanless design for quiet operation, higher reliability, and low power draw
- Temperature: operating -10 to 60°C, storage -20 to 70°C
- Humidity: operating 10 to 90%, storage: 0 to 95%

#### Power Specifications

- Battery snap-together connectors for 1-2 each AN/PRC-152/148 snap on radio batteries; hot swappable with 5+ hours runtime per battery
- Wide range DC input 5-30 VDC (when installed in PacStar Smart Chassis)
- Power draw: Nominal 4 watts total

092118