

- > **APPLICATION:** Secure the Dismounted Data Communications Terminal (D-DACT) used to provide situation awareness, command and control, navigation, basic mission planning, and electronic messaging capabilities to the user.



### Device Spotlight



**Talla-Tech Rugged Personal Digital Assistant 5700 series (RPDA-57)**

### Key Features

- Device loss protection with power-on password and data encryption
- One-finger device wipe

### Related Documents

- a. DoD Instruction 8500.2: "Information Assurance Implementation", February 6, 2003
- b. DoD Memorandum: "Data at Rest Encryption", July 3, 2007
- c. Department of the Navy IA Pub-5239-26: "Information Assurance Remanence Security Publication", May, 2000
- d. Dismounted Data Automated Communication Terminal (D-DACT) System Security Authorization Agreement (SSAA): "D-DACT SSAA", February, 2007
- e. National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitation, September, 2006

### Related Application

- Ruggedized PDAs used for factory floor automation

### Challenges

- Meet the Government's Information Assurance requirements in order to use a ruggedized PDA in a Department of Defense deployment
- Offer a mechanism for the assignment and/or enforcement of privileges using the D-DACT provided on the Talla-Tech Rugged Personal Digital Assistant 5700 series (RPDA-57); that employs a single operating system
- Secure the D-DACT while it is employed in an unsecured environment, that is under threat of compromise

### Solution

- Provide security to the device that includes the following features:
  - Password protection
  - Configuration Tools
  - Protection of data-at-rest via NIST FIPS 140-2 compliant encryption
  - Application restriction
  - Provide a self-destruct mechanism through purging of protected data
  - Communication restriction of device IrDA, Wi-fi, and Bluetooth
  - Distribute software via secured digital memory card

### Benefits

- The use of secured mobile devices increases preparedness and communications on the battlefield
- Device loss protection capabilities such as password protection, FIPS 140-2 compliant encryption and self-destruct mechanism protects vulnerabilities and negative effects from enemy hands
- Application restriction prevents implementation of virus', spyware, and improper applications
- Communication restriction protects improper channels of communications
- Software distribution via secured digital memory card prevents information leakage via over-the-air or other mediums