Datakey

Use Case

Ground Control Stations (GCS)

Drone Ground Control Stations (GCS) are used to pilot unmanned systems in contested or remote environments. These GCSs require secure authentication to prevent unauthorized access and may also need to load mission-specific configurations or encryption keys in the field. Datakey memory tokens can function as a secure and reliable credential and can be used for transferring mission data and firmware updates to these critical control units.

Authentication and Access Control

To prevent unauthorized operation of military drones, access to the drone GCS must be restricted to verified personnel. When Type 1 encryption is used, a Crypto Ignition Key (CIK) is used to enable encryption and declassify the GCS when it is not in use.

- Acts as a secure credential enabling encrypted communications.
- Supports secure authentication protocols to verify legitimacy of the credential.
- Allows for safe transport where CIK removal declassifies the unit.

Secure Firmware Updates in the Field

GCS firmware and encryption modules need regular updates to counter evolving threats. Updates must often be delivered to remote, air-gapped installations. The process demands a reliable, controlled means to transport and verify updates without exposing systems to cyber threats.

- Provides a trusted, removable storage medium for securely transporting update files.
- Unique serial numbers enable the base station to authenticate firmware before applying it, reducing the risk of compromise.
- Supports unique identifiers or write-logs for tracking when and where updates occurred.
- Audit trail data, including GCS ID, time-date stamp, update version, etc. can be written back to the token.

Datakey
The power of memory. Secured.

Secure Data Logging in Harsh Environments

After a mission, a GCS may store operational logs such as command sequences, system performance, or incidents. This data is sensitive and may be subject to chain-of-custody requirements. A secure, removable medium is needed to extract, transport, and archive the data without risk of loss or tampering.

- Serves as a robust, field-ready device for recording and transporting high-value mission data.
- Allows secure export of sensitive logs without network exposure.
- Simplifies the process of moving data from deployed systems to centralized intelligence teams.

Geofencing & No-Fly Zone Enforcement

Military drone missions must strictly adhere to pre-defined airspaces to avoid unintended breaches into hostile, civilian, or restricted zones. Geofencing data, such as no-fly zones, mission corridors, and temporary airspace restrictions must be updated regularly to reflect evolving battlefield conditions. In Denied, Disrupted, Intermittent, or Low-Bandwidth (DDIL) environments where remote updates aren't feasible, this data needs to be delivered physically and securely. Datakey memory tokens:

- Enable trusted, tamper-resistant loading of geospatial boundaries directly into the drone GCS in the field.
- Ensures only authenticated tokens can interface with the GCS's receptacle, preventing unauthorized data injection.
- Ensures boundaries are retained even through power cycles or rough handling.