



Thales e-Security keyAuthority®

KEY BENEFITS

- > Automates and centralizes lifecycle encryption key management
- > Lowers the risk of security breaches with a hardened appliance approach
- > Accelerates deployment by enabling pre-qualified partner encryption devices
- > Simplifies audits and policy compliance through federated device management
- > Reduces administrative time and cost with a consistent storage key manager
- > Meets business continuity and data retention goals with increased reliability

Your information is at risk

Organizations are under pressure to protect information and support regulatory mandates that reduce risks to sensitive data. Failing to do so can be devastating, including costly penalties, remediation expenses and damaged business reputation. While encryption is a well-proven method to control exposure of data, application managers must decide how best to deploy and manage encryption across a diverse IT environment, and prove to auditors that effective security controls over encryption keys are in place.

Devices, such as tape libraries, disk arrays and SAN switches, now include embedded cryptography. However, without reliable key management, the cost and complexity of deploying and managing encryption can stall adoption. When planning a data protection strategy, both business continuity and reliable data access cannot suffer. A systematic and simplified approach is needed to automate key lifecycle controls, while ensuring long-term key protection.

Simplified security with a hardened appliance key manager

Thales e-Security keyAuthority® is a standards-based, FIPS-designed key manager that enables confident key management across classes of encrypting devices. The appliance supports standards-based protocols, as well as legacy interoperability, with leading encryption products. Administration is centralized for consistent key lifecycle management and auditing, while ensuring that business continuity and data recovery requirements are met. Pre-qualified support for industry-leading encryption products and devices delivers a comprehensive, integrated solution that grows with enterprise needs.

>> Thales e-Security keyAuthority

Confidently manage encryption

Key manager reliability for key recovery is a top priority to control data access with confidence. Encryption deployment is simplified through pre-qualified device integration.

- > **Device certification** – Tested and validated solutions with partner products accelerate setup and deployment.
- > **Extensible** – A vendor-neutral approach allows new encryption devices to be integrated quickly as industry standards and new products become available.

Meet continuity and data retention needs

The performance-optimized appliance secures keys long-term using a redundant hardware design to help ensure access.

- > **Redundant, FIPS-designed hardware** – Hot-swappable fans and power supplies, mirrored disks, and tamper-resistance features lower risk of downtime.
- > **Key backup** – The key manager ensures access to data with backups to offsite data centers.
- > **Synchronized key replication** – Automated failover helps ensure high-availability among appliances.

Achieve compliance and audit goals

The key manager enforces policies and maintains logs within secure facilities for reporting integrity.

- > **Policy-based controls** – Domains and key groups maintain rules for key access and sharing.



- > **A single point for auditing** – A dedicated auditor role simplifies system and key lifecycle reporting activities.
- > **Alerting and export** – System functions are logged, with the ability to notify through email, SNMP, and syslog, and to securely export audit logs for controls attestation.

Reduce complexity with a unified approach

The key manager simplifies maintenance by enabling standards of due care. Administrator time and cost is reduced through a single approach based on best practices.

- > **Single key manager** – Application, compliance, and security teams manage centrally from a single console to reduce the need for additional key managers.
- > **Role-based access controls** – Defined entitlements and separation of duties maintain accountability.
- > **Current and legacy protocols** – Standards-based and proprietary device interface support provides the flexibility to extend key management to future new applications.

| | |
|-------------------------------------|---|
| Dimensions and Weight | 2U standard rack units. Height 3.47 in. (8.81 cm), width 17.19 in. (43.66 cm), depth 30 in. (76.20 cm). 41 lbs (18.6 kg) without the rack mounting kit. |
| Input Voltage | 100 to 240 VAC (autosensing); input line frequency nominally 50 to 60 Hz; total power consumption 250 W |
| Temperature | Operating temperature 10 to 40° C (50 to 104° F); operating humidity 5% to 85% non-condensing at 40° C (104° F); operating altitude 0 to 6562 feet (2 km) above sea level Non-operating shock 20 G, 11 ms duration, square wave Non-operating vibration 10 G, 5 to 500 to 5 Hz @ 1 octave intervals |
| Shock | Operating shock 5 G, 11 ms duration, half sine; operating vibration 5 G, 5 to 500 to 5 Hz at 1 octave intervals; non-operating temperature -30° to 65° C (-22° to 149° F); non-operating humidity 95% RH maximum; non-operating altitude 0 to 47 250 feet (12 km) above sea level |
| Airflow | Airflow volume 300 ft ³ (8.5 m ³) per minute; airflow direction Intake from front, exhaust to rear |
| Replaceable Components | Hot-swappable redundant fans and power supply units |
| Interfaces | Serial RJ-45 console port for command line interface (setup only) 10/100BaseT Ethernet ports to the LAN Smart card reader (ISO 7816 compliant) for system key and configuration backup Web graphical user interface for role-based administration |
| Certified Encryption Devices | Brocade Encryption Switch and FSB-18 blades TKLM-compatible IBM storage devices (TS-series tape and DS8000-series disk) |

THALES

