



## Thales keyAuthority®

### KEY BENEFITS

- > Enable encryption across the enterprise
- > Reduce operational costs
- > Maintain access to encrypted data
- > Achieve audit and regulatory compliance

#### Automate key management for enterprise-wide encryption

Fueled by the need to meet compliance and data privacy requirements, organizations are racing to encrypt data. Doing so requires organizations to develop their own encryption key handling processes, which includes determining where keys are deployed and how to recover them.

Ad hoc processes and inadequate key management can lead to higher costs, lost access to data, and barriers to business continuity. Managers who avoid these risks by not encrypting data may face the even worse consequences of data breaches and failed compliance.

#### Move your encryption strategy forward

Thales keyAuthority eliminates the burdens and risks of deploying encryption. It delivers the automation, policy support, and reporting needed to execute your encryption strategy. By enforcing your policy and automating the key lifecycle, Thales keyAuthority eliminates improvised processes that steal resources. It also ensures that data is accessible by securely maintaining encryption keys.

# >> Thales keyAuthority

## Scale across the enterprise

Designed to meet diverse needs, Thales keyAuthority is ready to manage enterprise-wide encryption with support for both symmetric and public key deployments. Thales keyAuthority ensures that policy is enforced and maintains a complete, tamper-proof audit log, which is critical for reporting and auditing.

## Align with the business

As the use of encryption grows, businesses must align policy, reporting, and performance in order to control costs, maintain business continuity, and achieve compliance goals. Thales keyAuthority provides a multi-tiered architecture to fit your organizational and operational structure. Administrator access is controlled and business units are segmented, providing consistent management without sacrificing the benefits of an enterprise-wide approach.

## Enable encryption across the enterprise

Thales keyAuthority manages legacy, current, and future encryption deployments, including storage systems, point-of-sale, application servers, in-house applications, and more.

- > **Multiple key types** – manages both symmetric and asymmetric encryption keys, as well as digital certificates.
- > **Standard application interfaces** – Integrates using standards-based interfaces, including Java JCE, Microsoft CSP (MS-CAPI), and PKCS#11.

## Reduce operational costs

By eliminating redundant or ad hoc management of keys, you reduce costs and risks while freeing your team to work on other projects. Thales keyAuthority manages all encryption key processes.

- > **Key lifecycle management** – Full automation of key creation, distribution, rollover, and replacement.
- > **Partitioned management** – Operate a single deployment across many departments or groups with separate administrators and policies.

## Maintain access to encrypted data

Thales keyAuthority's policy engine works in the background to automate operations.

- > **Complete key history** – Entire history is maintained for active, archived, and pre-generated encryption keys.
- > **Automatic certificate renewal** – Ensure system uptime with managed certificate renewal and replacement before expiration.

## Achieve audit and regulatory compliance

The ability to document policy changes, administrator operations, and encryption key custody is critical to audit and regulatory compliance. Thales keyAuthority was built to operate in the most demanding environments for audit and compliance success.

- > **Tamper-proof logging** – Operations are digitally signed and verified.
- > **Real-time notifications** – Alert administrators, integrate with security information and event management systems.
- > **Trusted key generation, distribution, and storage** – Key generation operations are performed by certified, proven hardware security modules. Keys are transferred and stored in encrypted form.

## Technical Specifications

Managed key types:

- > **RSA, DSA, AES, 3DES**

Management interfaces:

- > **PKCS#11, CSP for Microsoft CryptoAPI (MS-CAPI), Java JCA/JCE CSP, OpenSSL**

For more detailed technical specifications, please visit [www.thalesgroup.com/InfoSysSecurity](http://www.thalesgroup.com/InfoSysSecurity).

**Thales**  
Information Systems Security