Entrust KeyControl Supports Transparent Data Encryption (TDE)

Get the flexibility you need to speed up processes while mitigating risks and facilitating compliance

Overview

Transparent data encryption (TDE) natively protects data at rest in leading SQL databases. Applied at the file level, the technology secures sensitive data, enabling organizations to address regulatory compliance requirements.

Entrust KeyControl protects data at rest in SQL databases by securely managing the underpinning encryption keys at scale throughout their lifecycle. It enables encryption and delivers certified FIPS 140-2 Level 1 secure key management. Plus, integration with Entrust nShield® Hardware Security Modules (HSMs) provides an additional protection layer and FIPS 140-2 Level 3 compliance.

HIGHLIGHTS

- Enhances the security of SQL TDE deployments
- Simplifies management of master key lifecycle at scale
- Leverages nShield HSMs for a hardware root of trust
- Facilitates compliance with regulatory requirements
- Deploys easily and provides a rapid time to value
- Unmatched maintenance and support ensure easy deployment and operation
- Supports both Transparent Data Encryption (TDE) Mode and Cell-Level Encryption (CLE) Mode

Learn more about Entrust KeyControl at entrust.com

Entrust KeyControl Supports TDE

The Challenge

An organization's databases are a significant repository of sensitive information. They typically contain confidential human resources data, intellectual property, and even customer credit card details. Data breaches put organizations at risk of reputational and brand damage. Data breach disclosure requirements and potential fines and liabilities can have a serious impact.

Transparent data encryption (TDE) protects the information in databases using database encryption keys (DEKs), which are stored in the database boot record. The DEKs are encrypted using a server certificate. TDE provides encryption at the database level so that backups are also encrypted. TDE is supported by leading SQL databases. While TDE protects the files in databases from compromise, the encryption keys that unlock the data are not natively encrypted, making it necessary to add an additional layer of security.

As organizations store growing volumes of sensitive data in databases, protecting and managing the encryption keys that secure the data becomes increasingly challenging. Encryption keys underpin the security of databases, and if stored alongside the database tables, it puts them at increased risk of compromise.

To mitigate risks and eliminate insider threats, master TDE keys should be carefully managed with role-based access controls and stored separately, when possible, in dedicated hardware.
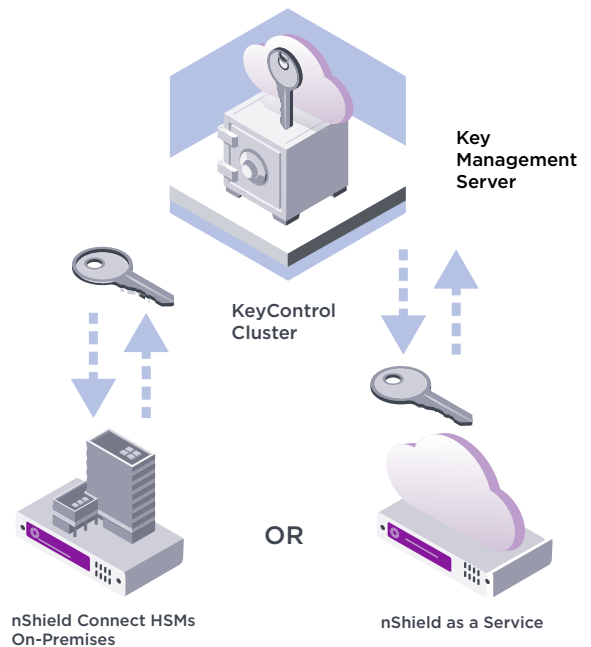
The Solution

Entrust offers a comprehensive and unified database security platform that ensures critical data is always secured from external and internal threats and available for uninterrupted business. KeyControl protects underpinning TDE master keys and provides the flexibility you need to speed up processes – all while helping you mitigate risks and facilitate compliance.

Database Administration

SQL Database

Key Management Server

KeyControl Cluster

nShield Connect HSMs On-Premises

OR

nShield as a Service

Entrust KeyControl manages the lifecycle of SQL database TDE master keys with enhanced security delivered by an nShield HSM root of trust.

Entrust KeyControl Supports TDE

Benefits

KeyControl allows you to:

- Address a range of database security requirements and approaches – all from a single vendor

- Deliver certified encryption and key management to enforce best practices/standards

- Enforce separation of duties isolating master keys from encrypted data, reducing insider attacks

- Keep encryption keys readily available to ensure optimum database and application performance

- Ensure that users and devices have the necessary authentication credentials to access databases

- Streamline the management of user and device certificates

- Simplify authentication, authorization, and risk policy decisions

- Align with data-protection regulations and industry mandates

- Facilitate auditing and reporting for compliance obligations

The Entrust Difference

Entrust combines strong identity management capabilities with robust protection of TDE keys to prevent unauthorized access to, and loss of, sensitive data. Entrust database security products interoperate with leading database vendors to centrally manage encryption keys, reduce complexity, and facilitate compliance with security regulations.

Our solutions address enterprise database security requirements – from managing who and what has access to the data to protecting the data at rest in SQL databases. And it's all paired with professional services and support to help you through your data protection journey, simplify your implementation and maintenance strategy, and ease procurement.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223