Fortanix®

Integration Guide

USING DATA SECURITY MANAGER WITH ORACLE TDE - INTRODUCTION

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052| United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This article describes the TDE process, key hierarchy, prerequisites, and steps to configure **Fortanix Data Security Manager (DSM) for Transparent Data Encryption (TDE)**.

2.0 TERMINOLOGY REFERENCES

1. **Fortanix Data Security Manager**

   Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

2. **TDE – Transparent Data Encryption**

   Transparent Data Encryption (TDE) enables you to encrypt sensitive data that you store in tables and tablespaces. Oracle Database uses authentication, authorization, and auditing mechanisms to secure data in the database, but not in the operating system data files where data is stored. To protect these data files, Oracle Database provides Transparent Data Encryption (TDE). To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a keystore. *For more information, see Introduction to Transparent Data Encryption*.

3.0 TDE KEY HIERARCHY

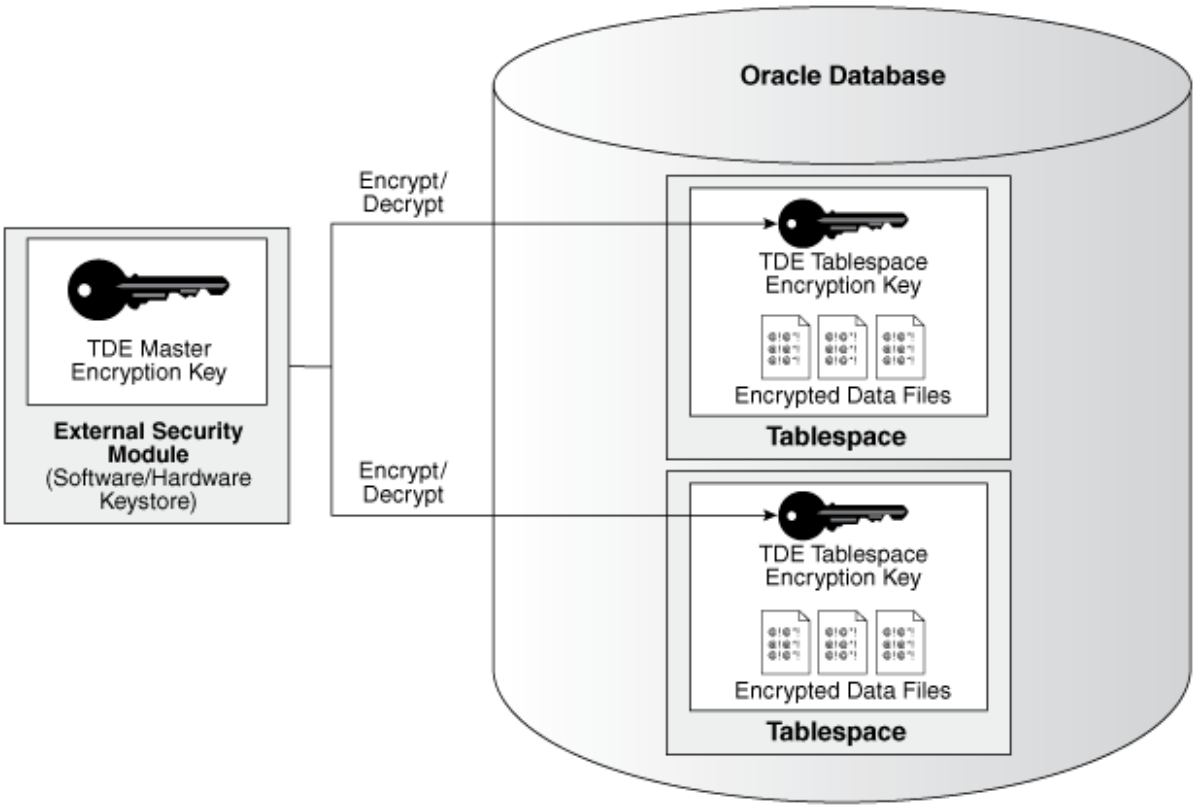

FIGURE 1: TDE KEY HIERARCHY

TDE encryption uses a two-tiered, key-based architecture to transparently encrypt and decrypt data. The TDE master encryption key (KEK) is stored in a security module (such as an Oracle wallet or Hardware Security Module (HSM) such as Fortanix DSM). This TDE master encryption key is used to encrypt the TDE table or tablespace encryption key (DEK), which in turn is used to encrypt and decrypt data in the database files.

Fortanix DSM separates ordinary program functions from encryption operations, making it possible to assign separate, distinct duties to database administrators and security administrators. Security is enhanced because the keystore password can be unknown to the database administrator, requiring the security administrator to provide the password.

4.0 PREREQUISITES

- Oracle Database must be on Fortanix DSM-supported versions. Currently, the supported database versions are: **11g R2, 12c, 18c, 19c**. For Oracle 11g, make sure Oracle Database patch **18948524** is applied. This patch enables the Auto-login mode of the HSM wallet.

- Download the latest Fortanix PKCS#11 library from here. Copy it to the database server.

5.0 CONFIGURING FORTANIX DATA SECURITY MANAGER FOR TDE

5.1 OBTAINING ACCESS TO FORTANIX DATA SECURITY MANAGER

1. Create an Account in Fortanix DSM if you do not have one already. *See Getting Started for more information*.
2. Create a new Group, for example: "ORACLE TDE", for storing the TDE master keys.
3. Create an App in Fortanix DSM in the group created in *Step 2* and copy the API key.
   a. In your Fortanix DSM account, go to the **Applications** tab, and create a new App in the same group as *Step 2*.
   b. After the app is created, click **COPY API KEY** to copy the API key and save it in a notepad.

6.0 VERIFY CONNECTIVITY

1. Validate the connectivity from the database node(s) to the Fortanix DSM endpoint.

```
curl -v https://DSM_ENDPOINT
```

You must receive a 200 status code.

6.1 KNOWN CONNECTIVITY ISSUES

- Port 443 is blocked between the database server and Fortanix DSM.
- The root CA certificate used to sign the Fortanix DSM Cluster certificate is not present in the database server trust store.

7.0 REFERENCES

For steps to integrate Fortanix DSM with Oracle TDE, refer to Using Fortanix DSM with Oracle TDE guide.

1.0 DOCUMENT INFORMATION

1.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:
https://support.fortanix.com/hc/en-us/articles/16378084356884-Using-Fortanix-Data-Security-Manager-with-Oracle-TDE-Introduction

1.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.
For any urgent document updates, please send an email to: support@fortanix.com