# *Database TDE Master Key Protection*

## *Using Data Privacy Manager to secure Oracle and MS SQL Server native TDE master keys with encryption and access control*

### *The Challenge*

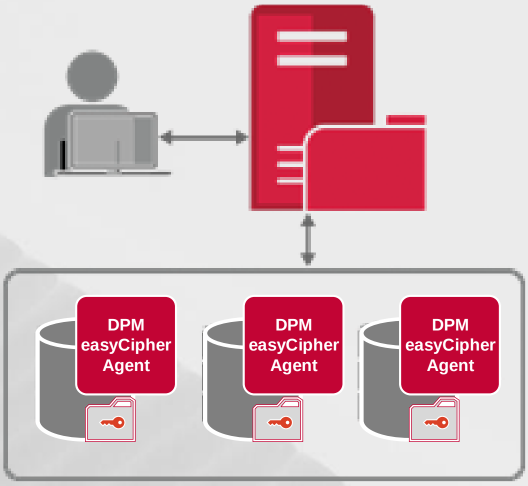
The client required to single policy based solution to protect key wallets and master keys in multi-vendor databases using native transparent data encryption from system administrators. The environment consisted of two database vendor types and versions being Oracle Transparent Database Encryption (TDE) and Microsoft MS SQL Server TDE used to protect credit card data.

The client did not have the financial or technical resources to integrate and maintain proprietary hardware security modules for master keys nor did they want to change established enterprise wide data backup workflow for encryption keys.

### *The Solution*

DPM was used to protect the database key files:

- DPM easyCipher Agent was installed on each database server
- DPM easyCipher Manager was installed on a new virtual machine
- An encryption and access control policy was applied to encrypt the key files or master database with keys to allow only databases to access them



### *The Benefits*

1. No application code changes or database reconfigurations were required – DPM transparently protected the TDE master key files or master database with AES256
2. Protection is managed by the security admin and not the DBA
3. Protection from all users, including the OS admin user. Only the database process user is allowed to access the database folder and decrypt the keys
4. A consistent policy was applied across multi-vendor databases - Oracle 11gR2, 12c, MS SQL Server 2012 and 2014 databases. In the future, the same method would apply to newer versions and different database vendors
5. The same solution can be applied to protect other database secrets such as configuration files, log files, or even databases without TDE
6. Key backups in DPM easyCipher used the same people and processes of backup method as existing database and system backup

*Randtronics*

*For more detailed technical specifications, please visit*
***www.randtronics.com***