Securing Oracle with Primus Hardware Security Module

libC Technologies SA
Avenue d’Ouchy 18
1006 Lausanne

December 2017

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. libC Technologies SA does not warrant that this document is error free.

Securing Oracle with the Primus Hardware Security Module (HSM)

With the help of the Securosys Primus HSM, a physical device to safeguard your digital cryptographic keys, and its supporting libraries implementing the standard APIs such as Microsoft's Cryptographic Service Provider (CNG), Java JCE and PKCS#11 we have the necessary means to implement integrity, confidentiality and availability for any existing or new Oracle based application environment. Oracle requires the PKCS#11 interface to integrate with an HSM.

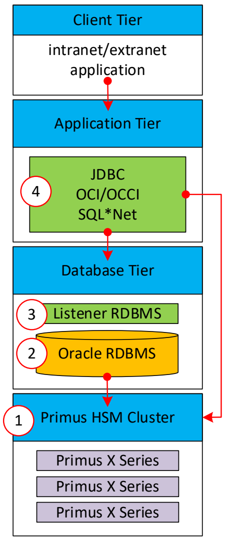
To address physical storage, communication, operational and sys-admin related security issues integrating the Primus HSM in an Oracle environment, we will consider the following traditional application deployment illustrated here for our walk-through:

1 Primus HSM cluster for safekeeping the encryption and authentication keys

2 RDBMS with ciphered content at the file system level

3 RDBMS listener requiring strong client authentication

4 Application tier communicating using strong client authentication



1 The Primus HSM enables you to centralize the encryption and authentication keys, both when migrating or generating the Oracle key material.

The choice of the HSM architecture is adjustable to your environment as it permits a deployment in various forms: single or multi-tenant, on premises or in the cloud; single HSM or HSM cluster supporting transparent object replication, connection failover and backup.

The standard role-based management of the HSM and keys is delegated to the CSO team. HSMs and keys are managed remotely using the Decanus Remote Control Terminal using one or two factor authentication or directly at the HSM console.

2 You integrate the Primus PKCS#11 interface on each RDBMS server and configure the DB instances to encrypt and decrypt sensitive data using Transparent Data Encryption (TDE). This secures your data on the operating file system.

Using the standard Oracle RBAC mechanisms, you control R/W access to your encrypted storage (columns or table space). This operation does not affect the existing applications.

Oracle offloads the data cipher operations to the RDBMS monitor process. The processing performance of the shared or dedicated Oracle processes is not affected, nor is the availability of the applications and RDBMS.

3 In addition to the data encryption, you can take advantage of the HSM and its centralized key management to secure the communication channels between RDBMS server and the application tier by enabling strong client authentication on the RDBMS listener process.

Deploying a hardware RSA key and associated certificate on the RDBMS listener process, you enforce authentication of the connecting clients and benefit from the SSL/TLS protocol between application and DB tier.

4 For each JDBC, SQL*Net, OCI or OCCI client, you issue a hardware based RSA key and associated certificate to authenticate the connection from the application tier to the RDBMS listener to benefit from the SSL/TLS protocol between client and server.

Oracle implements TLS with RSA/AES/SHA algorithms supported by the Primus HSM. For this, you install and configure the PKCS#11 interface on each application server connecting to the RDBMS listener.

Benefits

- ✓ Seamless integration with Oracle environment: transparent to backup, restore and replication
- ✓ Centralized key management performed by CSO team: remotely via Decanus Remote Control Terminal or via Primus HSM console
- ✓ DBA management tasks not affected by the implementation of RDBMS encryption and/or authentication. Any existing software key is removed from the server infrastructure
- ✓ No impact on existing application environment: no application code modification necessary to implement data encryption.
- ✓ No performance loss and side-effect: cipher operations are performed asynchronously by the Oracle monitoring process
- ✓ Application availability is ensured: HSM cluster enables safe failover and asynchronous cipher operations do not impact application availability in case of network failure between the monitoring process and the HSM cluster
- ✓ Low setup, configuration and maintenance footprint: deploy the Primus PKCS#11 interface and configure the connection settings.

Platforms

Oracle 12c, Oracle 11g Standard and Enterprise versions
Oracle Linux 7, Solaris 11.3, Windows x64