

ORACLE ADVANCED SECURITY

KEY FEATURES AND BENEFITS

ORACLE[®] 11g DATABASE

- Transparently encrypt SSN, credit card numbers and other privacy data
- Transparently encrypt entire application tables with tablespace encryption
- Encrypt entire database backups with RMAN and TDE
- Transparently encrypt SQL*Net network traffic
- Enable strong authentication (Kerberos, PKI, RADIUS)
- Regulatory compliance - PCI, SOX, HIPAA
- Standards compliant (3DES 168, AES 256, SHA-1, x.509v3, PKCS #7/10/11/12, TLS 1.0)

Oracle Advanced Security helps customers address regulatory compliance requirements by protecting sensitive data on the network, on backup media or within the database, from unauthorized disclosure.

Oracle Advanced Security Transparent Data Encryption provides the industries most advanced encryption capabilities for protecting sensitive information without requiring any changes to the existing application.

Transparent Data Encryption

Oracle Advanced Security transparent data encryption (TDE) provides robust encryption solutions to safeguard sensitive data against unauthorized access at the operating system level or through theft of hardware or backup media. TDE helps address privacy and PCI requirements by protecting personally identifiable information such as social security numbers and credit card numbers. With a simple `alter table` command an administrator can encrypt sensitive data within an existing application table.

```
SQL> alter table customers modify (credit_card_number encrypt)
```

Unlike most database encryption solutions, TDE is completely transparent to existing applications with no triggers, views or other application changes required. Data is transparently encrypted when written to disk and transparently decrypted after an application user has successfully authenticated, and passed all authorization checks.

Authorization checks include verifying the user has the necessary `select` and `update` privileges on the

application table and checking Database Vault, Label Security and Virtual Private Database enforcement policies. Existing database backup routines will continue to work, with the data remaining encrypted in the backup. For encryption of entire database backups, TDE can be used in combination with Oracle RMAN.

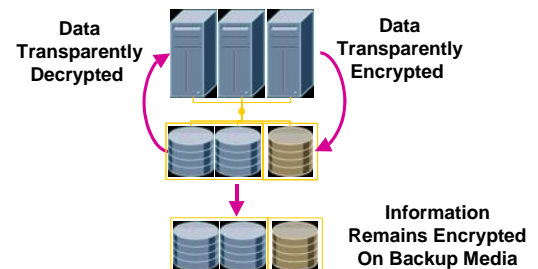


Fig 1. Transparent Data Encryption Overview

Tablespace Encryption

Oracle Advanced Security in Oracle Database 11g Release 1 includes support for tablespace encryption. When a tablespace is created through Enterprise Manager or on the command line, an option now exists to specify that the file be encrypted on the file system. When new data is added to the new tablespace using the `insert` command or datapump, entire tables will be transparently encrypted. When the database reads data blocks from the encrypted tablespace it will transparently decrypt the data blocks.

ORACLE ADVANCED SECURITY

RELATED PRODUCTS:

The following products provide additional security to help meet security, privacy and regulatory requirements:

- Oracle Database 10g Release 2 - Oracle Database Vault
 - Protects application data from DBA and privileged users
 - Controls access to applications and databases
 - Protects against Database changes
- Oracle Label Security
 - Label based access control
 - Multi-level Security
 - Protect sensitive data
 - Integrated with Oracle Database Vault through label factors
 - Common Criteria Evaluation at EAL4
- Oracle Secure Backup
 - Encrypt database and file system data during tape backup
 - Integrated with Oracle Recovery Manager (RMAN) and supports up to 256 bit AES

Hardware Security Modules

TDE has been enhanced in Oracle Database 11g Release 1 to support storing the TDE master encryption key externally on a hardware security module (HSM) device. This provides an even higher level of assurance for protecting the TDE master key. Oracle Database 11g Release 1 communicates with the HSM device using the PKCS#11 interface. The existing wallet based storage mechanism for the master key will continue to be supported.

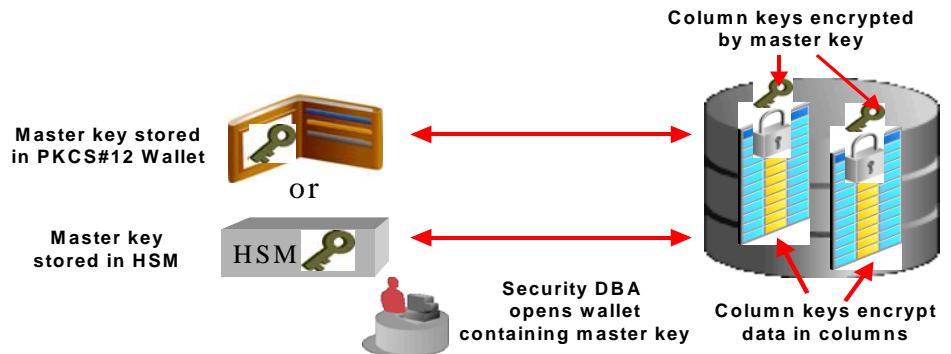


Fig 2. TDE Key Management Architecture

Strong Protection For Data In Transit

Oracle Advanced Security provides an easy-to-deploy and comprehensive solution for protecting all communication to and from the Oracle Database, providing both native network encryption and SSL based encryption. SSL based encryption and authentication is available for businesses that have deployed Public Key Infrastructure. Support for the TLS 1.0 protocol (including AES cipher suites) was introduced with Oracle Database 10g Release 1. The Oracle Database can be configured to reject connections from clients with encryption turned off, or optionally allow unencrypted connections for deployment flexibility. Configuration of network security is simplified using the Oracle Network Configuration administration tool, allowing businesses to easily deploy network encryption, as there are no changes required in the application.

Strong Authentication Replaces Password Based Authentication

Oracle Advanced Security provides database support for Kerberos, PKI and RADIUS strong authentication services. Certificate Revocation Lists can be stored on the file system, Oracle Internet Directory or using CRL Distribution Points. Support for smart cards is provided using the PKCS #11 standard. Credentials can be shared using the PKCS #12 standard.