

Oracle White Paper  
September 2009

# Oracle Advanced Security with Oracle Database 11g Release 2

Introduction .....	1
Oracle Advanced Security.....	2
Transparent Data Encryption .....	2
Oracle RMAN Encryption .....	3
Oracle Data Pump Encryption.....	3
Oracle Advanced Security Encryption Key Management .....	3
Oracle Advanced Security Network Encryption .....	3
Secure Sockets Layer .....	4
JDBC Security.....	4
Oracle Advanced Security Strong Authentication .....	5
Kerberos Authentication.....	5
PKI Support.....	5
RADIUS (Remote Dial In User Service).....	6
Oracle Advanced Security and Applications .....	6
Conclusion .....	7

## Introduction

Protecting personally identifiable information, intellectual property, financial results, and other sensitive information is a top priority for all organizations. Universities, healthcare organizations, and retailers are just a few of the organizations that have vast amounts of sensitive data ranging from social security numbers to personal health information to credit card numbers. In fact the amount of sensitive information collected and transmitted continues to increase dramatically and will continue to do so as organizations strive to achieve increased efficiencies and consumers continue to embrace Internet based commerce. At the same time, the value of sensitive information to those attempting to commit identity theft and other types of fraud continues to increase. Over the past four years the number of reported data breaches has continued to increase, resulting in damages reaching into the tens of millions of dollars. As a result, numerous privacy breach notification laws have been put in place that mandate the use of encryption technologies to provide a defensive shield for sensitive data. In 2003, the U.S. State of California passed the first such law known as Senate Bill 1386. Since 2003 numerous similar laws have been put in place and additional laws are scheduled to go into effect that mandate even stricter requirements for the use of encryption technologies, including a new law in the U.S. State of Massachusetts scheduled to go into effect in early 2010. The payment card industry data security standard (PCI-DSS) is an industry driven initiative that mandates the use of encryption technology to provide protection for credit card data stored by retailers. The Health Insurance Portability and Accountability Act (HIPAA) requires encryption to protect sensitive information in transit from unauthorized access. Oracle Advanced Security provides transparent, standards-based security that protects data through data-at-rest encryption, network encryption, and strong authentication services.

“Valuable content belongs in a secure, central database where it can be easily managed, automatically backed up—ideally, with minimal man hours. There is nothing more important to us than our customer’s content, which is why we chose Oracle to secure our information and support our growth strategy.”

Andy Barrett, Chief Technology Officer, Yuntaa

## Oracle Advanced Security

Oracle Advanced Security transparent data encryption (TDE) provides the industry's most advanced database encryption solution. TDE automatically encrypts data written to storage by the Oracle database and automatically decrypts the data after the requesting user has authenticated to the Oracle database and passed all access control checks such as those enforced by Oracle Database Vault, Oracle Label Security, and virtual private database. Database backups retain the data as encrypted, providing protection for backup media. Both logical and physical standby databases can be configured with TDE to provide complete protection for sensitive data in high availability architectures. Oracle Advanced Security network encryption provides both SSL based and native network encryption capabilities to protect data in transit. Oracle Advanced Security strong authentication services support PKI, Kerberos and RADIUS for an alternative to existing password-based authentication.

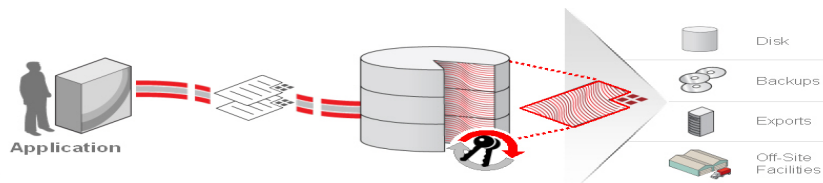


Figure 1. Oracle Advanced Security Transparent Data Encryption

### Transparent Data Encryption

Oracle Advanced Security TDE provides both full tablespace encryption as well as encryption of individual application table columns such as credit card and social security numbers. TDE tablespace encryption eliminates the need to identify and encrypt individual columns and provides increased efficiencies resulting in higher performance. Customers upgrading to Oracle Database 11g can use the new TDE tablespace encryption functionality to protect entire applications. All data stored in encrypted tablespaces will be automatically encrypted. When the database is backed up, the encrypted files remain encrypted on the destination media, protecting the information even when the backup media is lost or stolen. TDE tablespace encryption

works seamlessly with Oracle Streams, Oracle Compression and Oracle Exadata Smart Scans. Storage savings achieved as a result of compression remain the same because data is encrypted after the compression process completes.

## Oracle RMAN Encryption

Existing backup procedures will backup the TDE encrypted tablespaces as encrypted and table columns encrypted using TDE column encryption will remain encrypted on backup media. Encryption of all database files, including the SYSTEM tablespace, can easily be achieved by using Oracle RMAN and TDE together. Oracle RMAN provides the ability to use the TDE encryption algorithms and keys to encrypt the entire database backup. Encrypting backups protects data should the backup media fall into the wrong hands or be lost during transit.

## Oracle Data Pump Encryption

By default data exported from an Oracle Database using the Oracle Data Pump utility will be exported in clear text. Encrypted exports can be created using Oracle Data Pump with TDE. The Oracle Advanced Security TDE master key or a pass phrase can be used to encrypt the export file.

## Oracle Advanced Security Encryption Key Management

Transparent key management is critical to deploying encryption successfully. TDE automatically creates an encryption key behind the scenes. TDE uses a 2-tier key architecture where each key is protected using another key called the TDE master encryption key. The master encryption key is stored outside of the database, in an Oracle Wallet, a PKCS#12 formatted file that is encrypted using a pass phrase supplied either by the designated security administrator or DBA during setup. Oracle RMAN encrypted backups are automatically decrypted during restore and recover operations using the master encryption keys stored in the Oracle Wallet. Oracle recommends backing up the Oracle Advanced Security TDE Wallet on separate media and storing the wallets in separate locations. Oracle Advanced Security with Oracle Database 11g introduced support for storing the master key in a hardware security module (HSM) device for higher assurance, including those provided by RSA, Thales/nCipher and Safenet.

## Oracle Advanced Security Network Encryption

Oracle Advanced Security protects privacy and confidentiality of data over the network using encryption. Encryption of data in transit prevents data sniffing, data loss, replay and person-in-the-middle attacks. All communication with an Oracle database can be encrypted with Advanced Security. Oracle Advanced Security provides both native encryption/data integrity algorithms and support for secure socket layer (SSL) to protect data over the network.

Oracle Advanced Security network encryption is completely transparent, easy to setup and requires no X.509 certificates. Advanced Security supports the following encryption algorithms:

- AES (128, 192 and 256 bits)
- 3DES (2 and 3 keys; 168 bits), RC4 (256 bits)
- SHA1

### Secure Sockets Layer

SSL based encryption is available for businesses that have elected to provide public key infrastructure to their IT deployments. Oracle Advanced Security 10g introduced support for the TLS 1.0 protocol. Oracle Advanced Security provides AES cipher suites with the TLS 1.0 protocol starting in Oracle Database 10g.

Oracle implements the SSL protocol for encryption of data exchanged between database clients and the database. This includes data in Oracle Net Services, LDAP, thick and thin JDBC, and IIOP format. SSL encryption provides users with an alternative to Oracle Advanced Security native encryption.

In a three-tier system, SSL support in the database means that data exchanged between the middle tier and the database can be encrypted using SSL. Oracle's implementation of SSL supports the three standard modes of authentication, including anonymous (Diffie-Hellman), server-only authentication using X.509 certificates, and mutual (client-server) authentication with X.509.

### JDBC Security

JDBC is an industry-standard Java interface that provides a Java standard for connecting to a relational database from a Java program. Oracle implements two types of JDBC drivers: Thick JDBC drivers built on top of the C-based Oracle Net Services client, and thin (pure Java) JDBC drivers to support downloadable applets.

Since thick JDBC uses the full Oracle Net Services communications stack on both client and server, it can take advantage of existing Oracle Advanced Security encryption and authentication mechanisms. Because the thin JDBC driver is designed for use with downloadable applets used over the Internet, Oracle includes a 100% Java implementation of Advanced Security encryption and integrity algorithms for use with thin clients. Configuring the network parameters for the server and/or client enables the network encryption/integrity function. Most businesses can therefore easily uptake this technology as there are no changes required in the application.

## Oracle Advanced Security Strong Authentication

Oracle Advanced Security provides strong authentication solutions as an alternative to traditional password based authentication. Oracle Advanced Security supports Kerberos, PKI and RADIUS solutions. Oracle Advanced Security enables database users to achieve single sign-on to the Oracle database in Windows environments in conjunction with a Microsoft KDC. Database users can use their PKI credentials stored in smart cards or other hardware storage modules to authenticate to the Oracle database. This is especially useful for users as it provides roaming access to the database via client server applications. Both Kerberos and PKI are supported with Oracle database enterprise user security (EUS). EUS enables database users to be managed centrally in the Oracle Internet Directory or an existing enterprise LDAP repository in conjunction with Oracle Virtual Directory.

### Kerberos Authentication

Oracle Advanced Security includes a Kerberos client that is compatible with a Kerberos v5 ticket that is issued by any MIT v5 compliant Kerberos server or Microsoft KDC. Businesses can continue to operate in a heterogeneous environment using Oracle Advanced Security's Kerberos solution. Oracle Advanced Security Kerberos includes support for principal names up to 2000 characters in length. Oracle Advanced Security provides Kerberos cross realm support allowing Kerberos principals in one realm to authenticate to Kerberos principals in another realm.

### PKI Support

Oracle Advanced Security's SSL client can be used with industry standard X.509v3 certificates. Oracle Wallet Manager can be used to create certificate requests and manage other certificate management tasks. Additional command line utilities that assist in managing Certificate Revocation Lists (CRLs) and other Oracle Wallet operations are also available. Certificate Revocation Lists published to an LDAP server, a file system or a URL are supported.

Oracle supports PKI integration and interoperability through:

- PKCS #7, #11 support
- Wallet storage in Oracle Internet Directory
- Multiple certificates per wallet
- Strong wallet encryption

Storing the wallet in a centralized LDAP-compliant directory supports user roaming, allowing users to access their credentials from multiple locations or devices, ensuring consistent and reliable user authentication, while providing centralized wallet management throughout the wallet life cycle.

Oracle Wallets support multiple certificates per wallet, including:

- S/MIME signing certificate
- S/MIME encryption certificate
- Code-signing certificate

## RADIUS (Remote Dial In User Service)

Oracle Advanced Security provides a Remote Authentication Dial In User Service (RADIUS) client that allows the Oracle Database to respect the authentication and authorizations asserted by a RADIUS server. This feature is especially useful for businesses that are interested in two-factor authentication that establishes your identity based on what you know (password or PIN information) and what you have (the token card) provided by some token card manufacturers. RADIUS is a distributed system that secures remote access to network services and has long been established as an industry standard for remote and controlled access to networks. RADIUS user credentials and access information are defined in the RADIUS server to enable this external server to perform authentication, authorization and accounting services when requested.

Oracle RADIUS support is an implementation of the RADIUS client protocols that enables database to provide authentication, authorization and accounting for RADIUS users. It sends authentication requests to RADIUS server and acts upon the server's responses. The authentication can occur either in synchronous or asynchronous authentication mode and is part of Oracle configuration for RADIUS support.

## Oracle Advanced Security and Applications

Oracle Advanced Security TDE has been certified with numerous applications. Information on how to turn on Oracle Advanced Security TDE for these applications can be found on Oracle Metalink.

### ORACLE ADVANCED SECURITY CERTIFIED WITH ORACLE APPLICATIONS

TDE COLUMN ENCRYPTION IN ORACLE DATABASE 10G RELEASE 2	TDE TABLESPACE ENCRYPTION IN ORACLE DATABASE 11G RELEASE 1
Oracle E-Business Suite 11.5.9	Oracle E-Business Suite 11.5.10 and 12.0.4
Oracle PeopleSoft Enterprise 8.46	Oracle PeopleSoft Enterprise 8.48
Oracle Siebel CRM 7.7+	Oracle Siebel CRM 8.0
SAP 6.40 and 7.00	JD Edwards EnterpriseOne

## Conclusion

Data encryption and strong authentication are key components of the defense-in-depth principle. Oracle has long been the leader in database security innovation and continues to develop new and exciting solutions to help customer's address rapidly emerging requirements around privacy and regulatory compliance. Retailers can use Oracle Advanced Security TDE to address PCI-DSS requirements while university and healthcare organizations can use TDE to address Health Insurance Portability and Accountability Act (HIPAA) requirements as well as safeguard social security numbers and other sensitive information. Oracle Advanced Security TDE protects sensitive data on disk drives and backup media from unauthorized access, helping reduce the impact of lost or stolen media. Oracle Advanced Security Network encryption plays an especially important role in safeguarding data in transit, preventing unauthorized sniffing of sensitive data traveling over the intranet. Oracle Advanced Security Strong authentication services such as Kerberos and PKI provide an alternative to traditional password based authentication.



Oracle Advanced Security with  
Oracle Database 11g Release 2  
September 2009  
Author: Paul Needham, Peter Wahl

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
oracle.com



| Oracle is committed to developing practices and products that help protect the environment

Copyright © 2009, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.