

Oracle Advanced Security

An Oracle White Paper
September 2008

Oracle Advanced Security

INTRODUCTION

In recent years there have been numerous incidents of identity theft and credit card fraud resulting in damages reaching into the tens of millions of dollars. In other cases lost or misplaced media have touched off well-publicized searches that have made international headlines. Recent cases of network sniffing have shown that sensitive information stolen in transit can be even more costly than lost media. As a result of these and other widely publicized cases, the payment card industry data security standard (PCI-DSS) and numerous privacy breach notification laws have been put in place. The U.S. State of California passed one of the first such breach notification laws back in 2003. Known as California Senate Bill 1386, passage of the bill resulted in many organizations investigating encryption technology for the very first time. Today, more than 40 states in the U.S. have similar such laws. As a result, numerous organizations ranging from universities to health care organizations have realized the urgency to deploy strong security controls around sensitive data. Oracle Advanced Security provides transparent, standards-based security that protects data through network encryption, data-at-rest encryption, and strong authentication services.

ORACLE ADVANCED SECURITY ENCRYPTION

Oracle Advanced Security Transparent Data Encryption (TDE) is the industry's most advanced encryption solution. First introduced in Oracle Database 10g, TDE uses industry standard encryption algorithms and built-in key management to provide transparent encryption of sensitive application data. Unlike 3rd party database encryption offerings, no database triggers, views or other application changes are required. TDE automatically encrypts data before it is written to disk and automatically decrypts data before it is returned to the application. The encryption and decryption process is completely transparent to applications and users.

Flexible Protection Granularity

TDE offers the ability to protect at the individual attribute level or at the full table level. Examples of individual attributes include items such as credit card numbers and social security numbers. These types of attributes are typically spread throughout many commonly used business applications. For customers running Oracle Database 10g Release 2, TDE provides support for encrypting at the attribute level. Customers upgrading to Oracle Database 11g TDE can choose to skip the process of identifying which attributes to encryption and simply use the new TDE table space encryption functionality to protect entire applications. All database objects created in the new table space will be automatically encrypted.

Using TDE table space encryption to encrypt entire application tables provides even more transparency and cost savings. The need to identify individual attributes that need encryption is completely eliminated. In addition, TDE table space encryption provides even greater transparency as all data types are supported and there are no performance costs associated with complex index range scans on encrypted data. When the database is backed up, the encrypted files remain encrypted on the destination media, protecting the information even when the media is lost or stolen.

Customers wishing to simply encrypt their backups can achieve protection by using Oracle RMAN in conjunction with Oracle Advanced Security. Encrypting backups protects data should the backup media fall into the wrong hands or be lost during transit. Encrypted backups are automatically decrypted during restore and recover operations, as long as the required decryption keys are available. Oracle recommends backing up the Oracle Advanced Security Wallet on separate media and storing the keys in multiple secure locations.

Protection for data exports from the Oracle database can be achieved using TDE with Oracle Data Pump. The Oracle Advanced Security TDE master key or a pass phrase can be used as the encryption key.

Oracle Advanced Security TDE supports the industry standard AES and 3DES encryption algorithms with key sizes up to 256 bits.

Oracle Advanced Security and applications

As part of Oracle's commitment to helping customers comply with regulations and insider threat concerns, Oracle Advanced Security Transparent Data Encryption has been certified with numerous applications.

APPLICATION	CERTIFICATION AND OUT-OF-THE-BOX POLICIES
ORACLE E-BUSINESS SUITE 11/R12	DONE
PEOPLESOFT APPLICATIONS	DONE
SIEBEL	DONE
I-FLEX CUBE	DONE
ORACLE INTERNET DIRECTORY	DONE

Table 3 – Oracle Advanced Security and Applications

ORACLE ADVANCED SECURITY ENCRYPTION KEY MANAGEMENT

Transparent key management is critical to deploying encryption successfully. TDE automatically creates an encryption key behind the scenes. 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 password supplied either by the designated security administrator or DBA during setup. New in Oracle Database 11g Advanced Security is the ability to store the master key in a hardware security module (HSM) device for higher assurance. Oracle uses the industry standard PKCS#11 interface to communicate with numerous HSM and external key management systems, including those provided by RSA, nCipher, and Safenet.

ORACLE ADVANCED SECURITY NETWORK ENCRYPTION

Oracle Advanced Security protects privacy and confidentiality of data over the network by preventing data sniffing, data loss, replay and person-in-the-middle attacks. All communication with an Oracle Database can be encrypted with Oracle Advanced Security. Oracle Advanced Security protects all communications to and from the Oracle Database. Businesses have a choice between using Oracle Advanced Security's native encryption/data integrity algorithms and SSL to protect data over the network. Some of the typical scenarios requiring network level encryption include:

- Database Server is behind a firewall and users access the server via client server applications
- Communication between the application server in a DMZ and the Database must be encrypted

Native encryption and data integrity algorithms in Oracle Advanced Security require no PKI deployment. With each subsequent release of the database, newer

encryption algorithms are included as they gain industry approval. The latest addition is the Advanced Encryption Standard (AES), an algorithm improved in security and performance over DES. The complete list of Encryption and Data integrity algorithms are

- 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 release 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 (formerly known as Net8), LDAP, thick JDBC, and IIOP format. SSL encryption provides users with an alternative to the native Oracle Net Services encryption. A benefit of SSL is that it is a de facto Internet standard, and can be used with clients using protocols other than Oracle Net Services.

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. Sun Microsystems defined the JDBC standard, and Oracle Corporation, as an individual provider, implements and extends the standard with its own JDBC drivers. 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 Oracle 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 leveraging a business's existing security framework including Kerberos, Public Key Cryptography, and RADIUS. The ability for Oracle Database Servers or Database Clients /Users to use PKI credentials stored in smart cards or other hardware storage modules using industry's PKCS#11 standard. This is especially useful for users as it provides roaming access to the database via client server applications or web applications. Storing server credentials in a hardware module provides an additional level of security that some deployments require. Both Kerberos and PKI are supported for Oracle Database Enterprise User Security (EUS). EUS enables database users to be managed in the Oracle Internet Directory (OID).

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. Once an Oracle database is registered with a Kerberos Server and configured to support a Kerberos Service, enterprise users can authenticate to the database without any additional complications. Organizations that are already using a Kerberos Server and Oracle Advanced Security's Kerberos adapter can migrate their external database users to the directory to benefit from centralized user management.

Oracle Database 11g Advanced Security Kerberos enhancements include support for principal names up to 2000 characters in length. In addition, Oracle Database 11g 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 in any PKI that is industry standards compliant and accept standard PKCS7 certificate requests and issue X509v3 certificates. Oracle Advanced Security's provides an Entrust adapter that allows business applications to leverage Entrust's PKI with the Oracle Database.

Oracle Wallet Manager continues to be the tool to use for certificate requests and other certificate management tasks for the end user. 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 by Oracle's SSL infrastructure.

Oracle supports PKI integration and interoperability through:

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

Oracle Enterprise Security Manager creates user wallets as part of the user enrollment process. The wallet is stored in Oracle Internet Directory, or other LDAP-compliant directory. Oracle Wallet Manager can upload wallets to—and retrieve them from—the LDAP directory.

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

Oracle Wallet Manager Version 3.0 supports multiple certificates for a single digital entity in a persona—with multiple private key pairs in a persona (each private key can match only one certificate). This enables consolidation of and more secure management of users' PKI credentials.

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 modes and is part of Oracle configuration for RADIUS support.

Oracle Advanced Security provides authentication, respects authorizations stored in RADIUS and basic accounting services to RADIUS users when accessing the Oracle database.

SUMMARY

Data encryption and strong authentication are key components of the defense-in-depth principle. Oracle has long been the leader in data 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. Strong authentication services such as Kerberos and PKI are gaining in popularity for high assurance user identification.



Oracle Advanced Security
September 2008
Author: Paul Needham
Contributing Authors: 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

Copyright © 2008, Oracle. 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.