

# ORACLE ADVANCED SECURITY

## KEY FEATURES AND BENEFITS



### ADD SECURITY TO YOUR APPLICATIONS

- Easy to configure network encryption/integrity
- Leverage existing security framework – Kerberos, Public Key Infrastructure (PKI), RADIUS or DCE
- Use Smart Cards to protect the clients and/or server private key
- Improve Privacy and Confidentiality in your IT deployments

*Oracle Advanced Security protects privacy and confidentiality of data over the network by eliminating data sniffing, data loss, replay and person-in-the-middle attacks. All communication with an Oracle Database can be encrypted with Oracle Advanced Security. Databases contain extremely sensitive information and restricting access by strong authentication is one of first lines of defense. Oracle Advanced Security provides strong authentication solutions for Oracle Database 10g.*

### Industry Standard Encryption and Data Integrity

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 are listed below:

- 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 which is behind a second firewall 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 Key)
- RC4 (40, 56, 128, 256 Key)
- 3DES (2 Key and 3 Key)
- MD5
- SHA1

SSL based encryption is available for businesses that have elected to provide Public Key Infrastructure to their IT deployments. New in this release is the support for TLS 1.0 protocol. Oracle Advanced Security provides AES cipher suites with the TLS 1.0 protocol in Oracle Database 10g.

### Easy Configuration, No Changes to your Applications

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.

### **Strong Authentication Services for Oracle Database 10g**

Unauthorized access to information is a very old problem. Business decisions today are driven by information gathered from mining terabytes of data. Protecting sensitive information is key to a business's ability to remain competitive. Access to key data repositories such as the Oracle Database 10g that house valuable information can be granted once users are identified and authenticated accurately. Verifying user identity involves collecting more information than the usual username and password. Oracle Advanced Security provides the ability for businesses to leverage their existing security infrastructures such as Kerberos, Public Key Infrastructure (PKI), RADIUS and Distributed Computing Environment (DCE) for strong authentication services to the Oracle Database 10g.

New in this release is

- The ability to check X509v3 certificate revocations using Certificate Revocation Lists stored in the file system, Oracle Internet Directory or using CRL Distribution Points.
- 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.

### **Industry Standards, Interoperable**

Oracle Advanced Security's SSL client can be used in any **PKI** that is industry standards compliant. For instance, certificates issued by Verisign, Thawte, RSA Keon and Oracle Certificate Authority can be used for authentication to Oracle Database 10g as they 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 Oracle Database 10g.

Oracle Advanced Security includes a **Kerberos** client to integrate the Kerberos security framework with Oracle Database 10g. When configured, it allows users to authenticate to an Oracle Database using a Kerberos v5 ticket that is issued by any MIT v5 compliant Kerberos server and Microsoft KDC. Businesses can continue to operate in a heterogeneous environment using Oracle Advanced Security's Kerberos solution.

Oracle Advanced Security provides a **RADIUS** client that allows Oracle Database 10g 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.

**KEY BENEFITS AND RELATED PRODUCTS**

Oracle Advanced Security can be deployed with the Oracle Database 10g Enterprise Edition. It protects privacy and confidentiality of data in motion and allows businesses to leverage existing security frameworks including RADIUS, Kerberos and PKI with the Oracle Database 10g.

**RELATED PRODUCTS**

The following products provide additional security capabilities for the enterprise:

- Oracle Label Security, an Oracle Database 10g Enterprise Edition option
- Oracle Identity Management, included in Oracle Application Server Enterprise Edition or as an option with Oracle Application Server Standard Edition.

**Availability, Getting Started**

Oracle Advanced Security can be licensed with Oracle Database 10g Enterprise Edition. It is available on all Oracle Database 10g Enterprise Edition platforms. Not all third party authentication services are available on all platforms. Check with your Oracle Representative for detailed availability information.

Oracle Advanced Security installs automatically with a typical Oracle Database 10g Enterprise Edition install. It can also be selected for a custom install of the Oracle Database 10g Enterprise Edition.