RELATED PRODUCTS

- Oracle Database Vault
- Oracle Database Firewall
- Oracle Audit Vault
- Oracle Label Security
- Oracle Data Masking

accessed data blocks are cached in memory in the same manner as traditional non-encrypted data blocks. This efficient use of native database performance optimizations enables TDE to minimize overhead. TDE tablespace and column encryption also can be used in combination within the same database for hybrid encryption solutions.

Key Management

Oracle Advanced Security provides a built-in, two-tier key management architecture, consisting of a master encryption key and one or more data encryption keys. The TDE master encryption key is used to encrypt and protect the data encryption keys. The master encryption key resides outside of the database in the Oracle Wallet.

Strong Protection for Data In Transit

Oracle Advanced Security provides standards-based network encryption for protecting all communication to and from the Oracle Database. Connections can be rejected from clients that have encryption turned off. No changes to existing applications are required, allowing businesses to easily deploy network encryption.

65

Strong Authentication Replaces Password Based Authentication

Oracle Advanced Security provides strong authentication to the database using Kerberos, PKI or RADIUS. Oracle Advanced Security interoperates with the Microsoft Kerberos and MIT Kerberos v5. With Oracle Advanced Security, customers can require their users to plug-in a Smart Card (CAC, HSPD-12) as part of their SSL-based authentication to the Oracle Database.

Strong Protection for Database Backups

Data encrypted with TDE remains encrypted when the database files are backed-up to disk with Oracle RMAN. Oracle RMAN can also use TDE during the backup process to encrypt the entire database backup, including the SYSTEM and SYSAUX tablespaces. In addition, Oracle RMAN compression and TDE can be used together to generate backups that are both compact and secure.

Application Certification with Transparent Data Encryption

Oracle Advanced Security TDE is certified with many applications, including Oracle E-Business Suite, Oracle PeopleSoft Enterprise, Oracle Siebel CRM, Oracle JD Edwards EnterpriseOne and SAP.

Contact Us

For more information about Oracle Advanced Security, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

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

ORACLE

- Perform cryptographic operations to off load RSA operations from the server, freeing the CPU to respond to other transactions

Cryptographic information can be stored on two types of hardware devices:

- (Server-side) Hardware boxes where keys are stored in the box, but managed by using tokens.
- (Client-side) Smart card readers, which support storing private keys on tokens.

An Oracle environment supports hardware devices using APIs that conform to the RSA Security, Inc., Public-Key Cryptography Standards (PKCS) #11 specification.

Note: Currently only nCipher devices are certified with Oracle Advanced Security. Certificate with other vendors is in progress.

See Also: "Configuring Your System to Use Hardware Security Modules" on page 8-32 for details configuration details.

SSL Combined with Other Authentication Methods

You can configure Oracle Advanced Security to use SSL concurrently with database user names and passwords, RADIUS, and Kerberos, which are discussed in the following sections:

- Architecture: Oracle Advanced Security and SSL
- How SSL Works with Other Authentication Methods

See Also: Appendix A, "Data Encryption and Integrity Parameters" for information about how to configure SSL with other supported authentication methods, including an example of a `sqlnet.ora` file with multiple authentication methods specified.

65

Architecture: Oracle Advanced Security and SSL

Figure 1–4 on page 1-10, which displays the Oracle Advanced Security implementation architecture, shows that Oracle Advanced Security operates at the **session layer** on top of SSL and uses TCP/IP at the **transport layer**. This separation of functionality lets you employ SSL concurrently with other supported protocols.

See Also: *Oracle Database Net Services Administrator's Guide* for information about stack communications in an Oracle networking environment

How SSL Works with Other Authentication Methods

Figure 8–1 illustrates a configuration in which SSL is used in combination with another authentication method supported by Oracle Advanced Security.