- 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.

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.