# 19

# Securing Data for Oracle Database Connections

You can configure the industry standard Transport Layer Security (TLS) or Oracle proprietary Native Network Encryption (NNE) to secure your connection to the Oracle Database.

Data in transit runs into unique risks that are not quite the same as those related to data at rest. Some of these risks stem from unsecure public networks, the dynamic nature of the network traffic, and the fuzzy lines of ownership between the client and the server.

To safeguard data while it is in transit, the following security mechanisms are relevant to the discussion:

- Confidentiality through encryption: The process of encryption converts data into an unreadable format that can only be deciphered with a decryption key.
- Authentication through certificate signature verification: Authentication verifies the sender's and recipient's identities.
- Integrity through checksum validation: Checksum validation is the process of verifying the integrity to ensure that there has been no tampering or modification in any way.

Network encryption protects data moving over communications networks. Oracle database provides two choices for network encryption:

- Native Network Encryption (NNE): Configuring Oracle Database Native Network Encryption and Data Integrity
- Transport Layer Security (TLS) Encryption: Configuring Transport Layer Security Encryption
  TLS (transport layer security) is the default form of network data protection for Internet communications. Security-savvy organizations go a step beyond their Internet traffic and also protect their internal networks, corporate network infrastructure, and virtual private networks with network-level encryption.

The transition from NNE to TLS is a critical initiative to support the contemporary network landscape's heterogeneous ecosystem. In addition to TLS having a stronger security posture and the ability to go undetected by port scanner tools, TLS also supports PKI certificate-based authentication.

TLS is a standard that is omnipresent in global deployments.

**Tip:**

Oracle's recommendation is for customers to adopt TLS.

**Table 19-1 Native Network Encryption vs. Transport Layer Security**

| Security mechanism | Native Network Encryption | Transparent Layer Security |
|---|---|---|
| Confidentiality through encryption | Yes | Yes |

**Table 19-1 (Cont.) Native Network Encryption vs. Transport Layer Security**

| Security mechanism | Native Network Encryption | Transparent Layer Security |
|---|---|---|
| Authentication through certificate signature verification | No | Yes |
| Integrity through checksum validation | Yes | Yes |