

# Glossary

## **access control**

The ability of a system to grant or limit access to specific data for specific clients or groups of clients.

## **Access Control Lists (ACLs)**

The group of access directives that you define. The directives grant levels of access to specific data for specific clients, or groups of clients, or both.

## **Advanced Encryption Standard**

Advanced Encryption Standard (AES) is a new cryptographic algorithm that has been approved by the National Institute of Standards and Technology as a replacement for DES. (DES is deprecated in this release. To transition your Oracle Database environment to use stronger algorithms, download and install the patch described in My Oracle Support note [2118136.2](#).) The AES standard is available in Federal Information Processing Standards Publication 197. The AES algorithm is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.

## **AES**

See [Advanced Encryption Standard](#)

## **application context**

A name-value pair that enables an application to access session information about a user, such as the user ID or other user-specific information, and then securely pass this data to the database.

See also [global application context](#).

## **attribute**

An item of information that describes some aspect of an entry in an LDAP directory. An entry comprises a set of attributes, each of which belongs to an [object class](#). Moreover, each attribute has both a *type*, which describes the kind of information in the attribute, and a *value*, which contains the actual data.

**application role**

A database role that is granted to application users and that is secured by embedding passwords inside the application.

See also [secure application role](#).

**authentication**

The process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to granting access to resources in a system. A recipient of an authenticated message can be certain of the message's origin (its sender). Authentication is presumed to preclude the possibility that another party has impersonated the sender.

**authentication method**

A security method that verifies a user's, client's, or server's identity in distributed environments. Network authentication methods can also provide the benefit of [single sign-on \(SSO\)](#) for users. The following authentication methods are supported:

- [Kerberos](#)
- [RADIUS](#)
- [Transport Layer Security \(TLS\)](#)
- [Windows native authentication](#)

**authorization**

Permission given to a user, program, or process to access an object or set of objects. In Oracle, authorization is done through the role mechanism. A single person or a group of people can be granted a role or a group of roles. A role, in turn, can be granted other roles. The set of privileges available to an authenticated entity.

**auto-login wallet**

Password-based access to services without providing credentials at the time of access. This auto-login access stays in effect until the auto-login feature is disabled for that wallet. File system permissions provide the necessary security for auto-login wallet. When auto-login is enabled for a wallet, it is only available to the operating system user who created that wallet. Sometimes these are called "SSO wallets" because they provide single sign-on capability.

**CDB**

Multitenant container database. An Oracle Database installation contains one [root](#) and zero or more pluggable databases ([PDBs](#)). Every Oracle database is a CDB.

**base**

The root of a subtree search in an [LDAP](#)-compliant directory.

**CA**

See [certificate authority](#)

**certificate**

An ITU x.509 v3 standard data structure that securely binds an identify to a public key.

A certificate is created when an entity's public key is signed by a trusted identity, a certificate authority. The certificate ensures that the entity's information is correct, and that the public key belongs to that entity.

A certificate contains the entity's name, identifying information, and public key. It is also likely to contain a serial number, expiration date, and information about the rights, uses, and privileges associated with the certificate. Finally, it contains information about the certificate authority that issued it.

**certificate authority**

A trusted third party that certifies that other entities—users, databases, administrators, clients, servers—are who they say they are. When it certifies a user, the certificate authority first seeks verification that the user is not on the certificate revocation list (CRL), then verifies the user's identity and grants a certificate, signing it with the certificate authority's private key. The certificate authority has its own certificate and public key which it publishes. Servers and clients use these to verify signatures the certificate authority has made. A certificate authority might be an external company that offers certificate services, or an internal organization such as a corporate MIS department.

**certificate chain**

An ordered list of certificates containing an end-user or subscriber certificate and its certificate authority certificates.

**certificate request**

A certificate request, which consists of three parts: certification request information, a signature algorithm identifier, and a digital signature on the certification request information. The certification request information consists of the subject's distinguished name, public key, and an optional set of attributes. The attributes may provide additional information about the subject identity, such as postal address, or a challenge password by which the subject entity may later request certificate revocation. See [PKCS #10](#).

**certificate revocation list (CRL)**

(CRLs) Signed data structures that contain a list of revoked [certificate s](#). The authenticity and integrity of the CRL is provided by a digital signature appended to it. Usually, the CRL signer is the same entity that signed the issued certificate.

**checksumming**

A mechanism that computes a value for a message packet, based on the data it contains, and passes it along with the data to authenticate that the data has not been tampered with. The recipient of the data recomputes the cryptographic checksum and compares it with the cryptographic checksum passed with the data; if they match, it is "probabilistic" proof the data was not tampered with during transmission.

**cleartext**

Unencrypted plain text.

**Cipher Block Chaining (CBC)**

An encryption method that protects against block replay attacks by making the encryption of a cipher block dependent on all blocks that precede it; it is designed to make unauthorized decryption incrementally more difficult. Oracle Database employs *outer* cipher block chaining because it is more secure than *inner* cipher block chaining, with no material performance penalty.

**CIDR**

The standard notation used for IP addresses. In CIDR notation, an IPv6 subnet is denoted by the subnet prefix and the size in bits of the prefix (in decimal), separated by the slash (/) character. For example, `fe80:0000:0217:f2ff::/64` denotes a subnet with addresses `fe80:0000:0217:f2ff:0000:0000:0000:0000` through `fe80:0000:0217:f2ff:ffff:ffff:ffff:ffff`. The CIDR notation includes support for IPv4 addresses. For example, `192.0.2.1/24` denotes the subnet with addresses `192.0.2.1` through `192.0.2.255`.

**cipher suite**

A set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During a TLS handshake, for example, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth.

**cipher suite name**

Cipher suites describe the kind of cryptographics protection that is used by connections in a particular session.

**ciphertext**

Message text that has been encrypted.

**Classless Inter-Domain Routing**

See [CIDR](#) .

**client**

A client relies on a service. A client can sometimes be a user, sometimes a process acting on behalf of the user during a database link (sometimes called a proxy).

**common privilege grant**

A privilege that a [common user](#) grants to another common user or to a [common role](#). Common privilege grants can be either system privileges or object privileges, and they apply across all [PDBs](#) in a [CDB](#).

See also [local privilege grant](#).

**common role**

A role that exists in all containers in a [CDB](#).

**common user**

In a [CDB](#), a database user that exists with the same identity in every existing and future [PDB](#).

**confidentiality**

A function of cryptography. Confidentiality guarantees that only the intended recipient(s) of a message can view the message (decrypt the ciphertext).

**connect descriptor**

A specially formatted description of the destination for a network connection. A connect descriptor contains destination [service](#) and network route information. The destination service is indicated by using its service name for Oracle9i or Oracle8i databases or its Oracle [system identifier \(SID\)](#) for Oracle databases version 8.0. The network route provides, at a minimum, the location of the [listener](#) through use of a network address. See [connect identifier](#)

**connect identifier**

A name, net service name, or service name that resolves to a [connect descriptor](#). Users initiate a connect request by passing a user name and password along with a connect identifier in a connect string for the service to which they want to connect.

For example:

```
CONNECT username@connect_identifier  
Enter password: password
```

**connect string**

Information the user passes to a [service](#) to connect, such as [user name](#), password and [net service name](#). For example:

```
CONNECT username@net_service_name  
Enter password: password
```

**container**

In a [CDB](#) either, a [root](#) or a [PDB](#).

**container data object**

In a CDB, a table or view containing data pertaining to multiple containers and possibly the CDB as a whole, along with mechanisms to restrict data visible to specific common users through such objects to one or more containers. Examples of container data objects are Oracle-supplied views whose names begin with `V$` and `CDB_`.

**credentials**

A [user name](#), password, or certificate used to gain access to the database.

**CRL**

See [certificate revocation list \(CRL\)](#)

**CRL Distribution Point**

(CRL DP) An optional extension specified by the X.509 version 3 certificate standard, which indicates the location of the Partitioned CRL where revocation information for a certificate is stored. Typically, the value in this extension is in the form of a URL. CRL DPs allow revocation information within a single [certificate authority](#) domain to be posted in multiple CRLs. CRL DPs subdivide revocation information into more manageable pieces to avoid proliferating voluminous CRLs, thereby providing performance benefits. For example, a CRL DP is specified in the certificate and can point to a file on a Web server from which that certificate's revocation information can be downloaded.

**CRL DP**

See [CRL Distribution Point](#)

**cryptography**

The practice of encoding and decoding data, resulting in secure messages.

**data dictionary**

A set of read-only tables that provide information about a database.

**Data Encryption Standard (DES)**

An older Federal Information Processing Standards encryption algorithm superseded by the Advanced Encryption Standard (AES). The DES, DES40, 3DES112, and 3DES168 algorithms are deprecated in this release. To transition your Oracle Database environment to use stronger algorithms, download and install the patch described in My Oracle Support note [2118136.2](#).

**database administrator**

(1) A person responsible for operating and maintaining an Oracle Server or a database application. (2) An Oracle user name that has been given DBA privileges and can perform database administration functions. Usually the two meanings coincide. Many sites have multiple DBAs.

**database alias**

See [net service name](#)

**Database Installation Administrator**

Also called a database creator. This administrator is in charge of creating new databases. This includes registering each database in the directory using the Database Configuration Assistant. This administrator has create and modify access to database service objects and attributes. This administrator can also modify the Default [domain](#).

**database link**

A network object stored in the local database or in the network definition that identifies a remote database, a communication path to that database, and optionally, a user name and password. Once defined, the database link is used to access the remote database.

A public or private database link from one database to another is created on the local database by a DBA or user.

A global database link is created automatically from each database to every other database in a network with Oracle Names. Global database links are stored in the network definition.

**database password version**

An irreversible value that is derived from the user's database password. It is also called a password verifier. This value is used during password authentication to the database to prove the identity of the connecting user.

**Database Security Administrator**

The highest level administrator for database enterprise user security. This administrator has permissions on all of the enterprise domains and is responsible for:

- Administering the Oracle `DBSecurityAdmins` and `OracleDBCreators` groups.

Creating new [enterprise domains](#).

- Moving databases from one [domain](#) to another within the enterprise.

### decryption

The process of converting the contents of an encrypted message (ciphertext) back into its original readable format ([plaintext](#)).

### definer's rights procedure

A procedure (or program unit) that runs with the privileges of its owner, not its current user. Definer's rights subprograms are bound to the schema in which they are located.

For example, assume that user `blake` and user `scott` each have a table called `dept` in their respective user schemas. If user `blake` calls a definer's rights procedure, which is owned by user `scott`, to update the `dept` table, then this procedure will update the `dept` table in the `scott` schema. This is because the procedure runs with the privileges of the user who owns (defined) the procedure (that is, `scott`).

See also [invoker's rights procedure](#).

### denial-of-service (DoS) attack

An attack that renders a Web site inaccessible or unusable. The denial-of-service attack can occur in many different ways but frequently includes attacks that cause the site to crash, reject connections, or perform too slowly to be usable. DoS attacks come in two forms:

- Basic denial-of-service attacks, which require only one or a few computers
- Distributed DoS attacks, which require many computers to run

### DES

See [Data Encryption Standard \(DES\)](#)

### dictionary attack

A common attack on passwords. The attacker creates a list of many common passwords and encrypts them. Then the attacker steals a file containing encrypted passwords and compares it to their list of encrypted common passwords. If any of the encrypted password values (called verifiers) match, then the attacker can steal the corresponding password. Dictionary attacks can be avoided by using "salt" on the password before encryption. See [salt](#).

### Diffie-Hellman key negotiation algorithm

This is a method that lets two parties communicating over an insecure channel to agree upon a random number known only to them. Though the parties exchange information over the insecure channel during execution of the Diffie-Hellman key negotiation algorithm, it is



computationally infeasible for an attacker to deduce the random number they agree upon by analyzing their network communications. Oracle Database uses the Diffie-Hellman key negotiation algorithm to generate session keys.

**digital signature**

A digital signature is created when a public key algorithm is used to sign the sender's message with the sender's private key. The digital signature assures that the document is authentic, has not been forged by another entity, has not been altered, and cannot be repudiated by the sender.

**directory information tree (DIT)**

A hierarchical tree-like structure consisting of the DNs of the entries in an LDAP directory. See [distinguished name \(DN\)](#)

**directory naming**

A [naming method](#) that resolves a database service, [net service name](#), or [net service alias](#) to a [connect descriptor](#) stored in a central directory server. A

**directory naming context**

A subtree which is of significance within a directory server. It is usually the top of some organizational subtree. Some directories only permit one such context which is fixed; others permit none to many to be configured by the directory administrator.

**distinguished name (DN)**

The unique name of a directory entry. It is comprised of all of the individual names of the parent entries back to the root entry of the directory information tree. See [directory information tree \(DIT\)](#)

**domain**

Any tree or subtree within the [Domain Name System \(DNS\)](#) namespace. Domain most commonly refers to a group of computers whose host names share a common suffix, the domain name.

**Domain Name System (DNS)**

A system for naming computers and network services that is organized into a hierarchy of [domains](#). DNS is used in TCP/IP networks to locate computers through user-friendly names. DNS resolves a friendly name into an IP address, which is understood by computers.

In [Oracle Net Services](#), DNS translates the host name in a TCP/IP address into an IP address.

**directly granted role**

A [role](#) that has been granted directly to the user, as opposed to an [indirectly granted role](#).

**encrypted text**

Text that has been encrypted, using an encryption algorithm; the output stream of an encryption process. On its face, it is not readable or decipherable, without first being subject to [decryption](#). Also called [ciphertext](#). Encrypted text ultimately originates as [plaintext](#).

**encryption**

Disguising a message, rendering it unreadable to all but the intended recipient.

**enterprise domain**

A directory construct that consists of a group of databases and [enterprise roles](#). A database should only exist in one enterprise domain at any time. Enterprise domains are different from Windows 2000 domains, which are collections of computers that share a common directory database.

**Enterprise Domain Administrator**

User authorized to manage a specific [enterprise domain](#), including the authority to add new enterprise domain administrators.

**enterprise role**

Access privileges assigned to [enterprise users](#). A set of Oracle role-based [authorizations](#) across one or more databases in an [enterprise domain](#). Enterprise roles are stored in the directory and contain one or more [global roles](#).

**enterprise user**

A user defined and managed in a directory. Each enterprise user has a unique identify across an enterprise.

**entry**

The building block of a directory, it contains information about an object of interest to directory users.

**external authentication**

Verification of a user identity by a third party authentication service, such as Kerberos or RADIUS.

**Federal Information Processing Standard (FIPS)**

A U.S. government standard that defines security requirements for cryptographic modules—employed within a security system protecting unclassified information within computer and

telecommunication systems. Published by the National Institute of Standards and Technology (NIST).

**FIPS**

See [Federal Information Processing Standard \(FIPS\)](#).

**forced cleanup**

The ability to forcibly cleanup (that is, remove) all audit records from the database. To accomplish this, you set the `USE_LAST_ARCH_TIMESTAMP` argument of the `DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL` procedure to `FALSE`.

See also [purge job](#).

**forest**

A group of one or more Active Directory trees that trust each other. All trees in a forest share a common [schema](#), configuration, and global catalog. When a forest contains multiple trees, the trees do not form a contiguous namespace. All trees in a given forest trust each other through transitive bidirectional trust relationships.

**Forwardable Ticket Granting Ticket**

A special Kerberos ticket that can be forwarded to proxies, permitting the proxy to obtain additional Kerberos tickets on behalf of the client for proxy authentication.

See also [Kerberos ticket](#).

**global role**

A role managed in a directory, but its privileges are contained within a single database. A global role is created in a database by using the following syntax:

```
CREATE ROLE role_name IDENTIFIED GLOBALLY;
```

**global application context**

A name-value pair that enables application context values to be accessible across database sessions.

See also [application context](#).

**grid computing**

A computing architecture that coordinates large numbers of servers and storage to act as a single large computer. Oracle Grid Computing creates a flexible, on-demand computing resource for all enterprise computing needs. Applications running on the Oracle Database grid computing infrastructure can take advantage of common infrastructure services for failover,

software provisioning, and management. Oracle Grid Computing analyzes demand for resources and adjusts supply accordingly.

## HTTP

Hypertext Transfer Protocol: The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

## HTTPS

The use of Transport Layer Security (TLS) as a sublayer under the regular HTTP application layer.

## indirectly granted role

A [role](#) granted to a user through another role that has already been granted to this user. Then you grant the `role2` and `role3` roles to the `role1` role. Roles `role2` and `role3` are now under `role1`. This means `psmith` has been indirectly granted the roles `role2` and `role3`, in addition to the direct grant of `role1`. Enabling the direct `role1` for `psmith` enables the indirect roles `role2` and `role3` for this user as well.

## identity

The combination of the public key and any other public information for an entity. The public information may include user identification data such as, for example, an e-mail address. A user certified as being the entity it claims to be.

## identity management

The creation, management, and use of online, or digital, entities. Identity management involves securely managing the full life cycle of a digital identity from creation (provisioning of digital identities) to maintenance (enforcing organizational policies regarding access to electronic resources), and, finally, to termination.

## identity management realm

A subtree in Oracle Internet Directory, including not only an [Oracle Context](#), but also additional subtrees for users and groups, each of which are protected with access control lists.

## initial ticket

In Kerberos authentication, an initial ticket or ticket granting ticket (TGT) identifies the user as having the right to ask for additional service tickets. No tickets can be obtained without an initial ticket. An initial ticket is retrieved by running the `okinit` program and providing a password.

**instance**

Every running Oracle database is associated with an Oracle instance. When a database is started on a database server (regardless of the type of computer), Oracle allocates a memory area called the [System Global Area \(SGA\)](#) and starts an Oracle process. This combination of the SGA and an Oracle process is called an instance. The memory and the process of an instance manage the associated database's data efficiently and serve the one or more users of the database.

**integrity**

A guarantee that the contents of a message received were not altered from the contents of the original message sent.

**invoker's rights procedure**

A procedure (or program unit) that runs with the privileges of the current user, that is, the user who invokes the procedure. These procedures are not bound to a particular schema. They can be run by a variety of users and allow multiple users to manage their own data by using centralized application logic. Invoker's rights procedures are created with the `AUTHID` clause in the declaration section of the procedure code.

For example, assume that user `blake` and user `scott` each have a table called `dept` in their respective user schemas. If user `blake` calls an invoker's rights procedure, which is owned by user `scott`, to update the `dept` table, then this procedure will update the `dept` table in the `blake` schema. This is because the procedure runs with the privileges of the user who invoked the procedure (that is, `blake`).

See also [definer's rights procedure](#).

**java code obfuscation**

Java code [obfuscation](#) is used to protect Java programs from reverse engineering. A special program (an obfuscator) is used to scramble Java symbols found in the code. The process leaves the original program structure intact, letting the program run correctly while changing the names of the classes, methods, and variables in order to hide the intended behavior. Although it is possible to decompile and read non-obfuscated Java code, the obfuscated Java code is sufficiently difficult to decompile to satisfy U.S. government export controls.

**Java Database Connectivity (JDBC)**

An industry-standard Java interface for connecting to a relational database from a Java program, defined by Sun Microsystems.

**JDBC**

See [Java Database Connectivity \(JDBC\)](#)

**KDC**

See [Key Distribution Center \(KDC\)](#).

**Kerberos**

A network authentication service developed under Massachusetts Institute of Technology's Project Athena that strengthens security in distributed environments. Kerberos is a trusted third-party authentication system that relies on shared secrets and assumes that the third party is secure. It provides single sign-on capabilities and database link authentication (MIT Kerberos only) for users, provides centralized password storage, and enhances PC security.

**Kerberos ticket**

A temporary set of electronic credentials that verify the identity of a client for a particular service. Also referred to as a service ticket.

**Key Distribution Center (KDC)**

In Kerberos authentication, the KDC maintains a list of user principals and is contacted through the `kinit` (`okinit` is the Oracle version) program for the user's [initial ticket](#). Frequently, the KDC and the Ticket Granting Service are combined into the same entity and are simply referred to as the KDC. The Ticket Granting Service maintains a list of service principals and is contacted when a user wants to authenticate to a server providing such a service. The KDC is a trusted third party that must run on a secure host. It creates ticket-granting tickets and service tickets.

See also [Kerberos ticket](#).

**key pair**

A [public key](#) and its associated [private key](#). See [public and private key pair](#).

**keytab file**

A Kerberos key table file containing one or more service keys. Hosts or services use *keytab* files in the same way as users use their passwords.

**kinstance**

An instantiation or location of a Kerberos authenticated service. This is an arbitrary string, but the host Computer name for a service is typically specified.

**kservice**

An arbitrary name of a Kerberos service object.

**last archive timestamp**

A timestamp that indicates the timestamp of the last archived audit record. For the database audit trail, this timestamp indicates the last audit record archived. For operating system audit

files, it indicates the highest last modified timestamp property of the audit file that was archived. To set this timestamp, you use the `DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP` PL/SQL procedure.

See also [purge job](#).

## LDAP

See [Lightweight Directory Access Protocol \(LDAP\)](#)

### ldap.ora file

A file created by Oracle Net Configuration Assistant that contains the following directory server access information:

- Type of directory server
- Location of the directory server
- Default identity management realm or Oracle Context (including ports) that the client or server will use

### Lightweight Directory Access Protocol (LDAP)

A standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. The framework of design conventions supporting industry-standard directory products, such as the Oracle Internet Directory.

### listener

A process that resides on the server whose responsibility is to listen for incoming client connection requests and manage the traffic to the server.

Every time a client requests a network session with a server, a listener receives the actual request. If the client information matches the listener information, then the listener grants a connection to the server.

### listener.ora file

A configuration file for the listener that identifies the:

- Listener name
- Protocol addresses that it is accepting connection requests on
- Services it is listening for

The `listener.ora` file typically resides in `$ORACLE_HOME/network/admin` on UNIX platforms and `ORACLE_BASE\ORACLE_HOME\network\admin` on Windows.

### lightweight user session

A user session that contains only information pertinent to the application that the user is logging onto. The lightweight user session does not hold its own database resources, such as

transactions and cursors; hence it is considered "lightweight." Lightweight user sessions consume far less system resources than traditional database session. Because lightweight user sessions consume much fewer server resources, a lightweight user session can be dedicated to each end user and can persist for as long as the application deems necessary.

**local privilege grant**

A privilege that applies only to the [PDB](#) in which it was granted.

See also [common privilege grant](#).

**local role**

A role that exists only in a single [PDB](#). Unlike a [common role](#), a local role can only contain roles and privileges that apply within the container in which the role exists.

**local user**

In a [CDB](#), any user that is not a [common user](#).

**MD5**

Message Digest 5. An algorithm that assures data integrity by generating a 128-bit cryptographic message digest value from given data. If as little as a single bit value in the data is modified, the MD5 checksum for the data changes. Forgery of data in a way that will cause MD5 to generate the same result as that for the original data is considered computationally infeasible.

MD5 is deprecated in this release. To transition your Oracle Database environment to use stronger algorithms, download and install the patch described in My Oracle Support note [2118136.2](#).

**mandatory auditing**

Activities that are audited by default. Examples are modifications to unified audit trail policies (such as `ALTER AUDIT POLICY` statements) and top level statements by the administrative users `SYS`, `SYSDBA`, `SYSOPER`, `SYSASM`, `SYSBACKUP`, `SYSDBG`, and `SYSKM`, until the database opens. See "[Activities That Are Mandatorily Audited](#)" for more information.

**message authentication code**

Also known as data authentication code (DAC). A [checksumming](#) with the addition of a secret key. Only someone with the key can verify the cryptographic checksum.

**message digest**

See [checksumming](#)



**CDB**

See [CDB](#).

**namespace**

In Oracle Database security, the name of an application context. You create this name in a `CREATE CONTEXT` statement.

**naming method**

The resolution method used by a client application to resolve a [connect identifier](#) to a [connect descriptor](#) when attempting to connect to a database service.

**National Institute of Standards and Technology (NIST)**

An agency within the U.S. Department of Commerce responsible for the development of security standards related to the design, acquisition, and implementation of cryptographic-based security systems within computer and telecommunication systems, operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function.

**net service alias**

An alternative name for a [directory naming](#) object in a directory server. A directory server stores net service aliases for any defined [net service name](#) or database service. A net service alias entry does not have connect descriptor information. Instead, it only references the location of the object for which it is an alias. When a client requests a directory lookup of a net service alias, the directory determines that the entry is a net service alias and completes the lookup as if it was actually the entry it is referencing.

**net service name**

A simple name for a service that resolves to a connect descriptor. Users initiate a connect request by passing a user name and password along with a net service name in a connect string for the service to which they want to connect:

```
CONNECT username@net_service_name  
Enter password: password
```

Depending on your needs, net service names can be stored in a variety of places, including:

- Local configuration file, `tnsnames.ora`, on each client
- Directory server
- External naming service, such as NIS

**network authentication service**

A means for authenticating clients to servers, servers to servers, and users to both clients and servers in distributed environments. A network authentication service is a repository for storing

information about users and the services on different servers to which they have access, as well as information about clients and servers on the network. An authentication server can be a physically separate computer, or it can be a facility co-located on another server within the system. To ensure availability, some authentication services may be replicated to avoid a single point of failure.

**network listener**

A listener on a server that listens for connection requests for one or more databases on one or more protocols. See [listener](#).

**NIST**

See [National Institute of Standards and Technology \(NIST\)](#).

**non-repudiation**

Incontestable proof of the origin, delivery, submission, or transmission of a message.

**obfuscation**

A process by which information is scrambled into a non-readable form, such that it is extremely difficult to de-scramble if the algorithm used for scrambling is not known.

**obfuscator**

A special program used to obfuscate Java source code. See [obfuscation](#).

**object class**

A named group of [attributes](#). When you want to assign attributes to an entry, you do so by assigning to that entry the object classes that hold those attributes. All objects associated with the same object class share the same attributes.

**Oracle Context**

1. An entry in an LDAP-compliant internet directory called `cn=OracleContext`, under which all Oracle software relevant information is kept, including entries for [Oracle Net Services](#) directory naming and [checksumming](#) security.

There can be one or more Oracle Contexts in a directory. An Oracle Context is usually located in an [identity management realm](#).

**Oracle Virtual Private Database**

A set of features that enables you to create security policies to control database access at the row and column level. Essentially, Oracle Virtual Private Database adds a dynamic `WHERE`

clause to a SQL statement that is issued against the table, view, or synonym to which an Oracle Virtual Private Database security policy was applied.

**Oracle Net Services**

An Oracle product that enables two or more computers that run the Oracle server or Oracle tools such as Designer/2000 to exchange data through a third-party network. Oracle Net Services support distributed processing and distributed database capability. Oracle Net Services is an open system because it is independent of the communication protocol, and users can interface Oracle Net to many network environments.

**Oracle PKI certificate usages**

Defines Oracle application types that a [certificate](#) supports.

**Password-Accessible Domains List**

A group of [enterprise domains](#) configured to accept connections from password-authenticated users.

**PCMCIA cards**

Small credit card-sized computing devices that comply with the Personal Computer Memory Card International Association (PCMCIA) standard. These devices, also called PC cards, are used for adding memory, modems, or as hardware security modules. PCMCIA cards that are used as hardware security modules securely store the private key component of a [public and private key pair](#) and some also perform the cryptographic operations as well.

**PDB**

An individual database that is part of a [CDB](#).

See also [root](#).

**peer identity**

SSL connect sessions are between a particular client and a particular server. The identity of the peer may have been established as part of session setup. Peers are identified by [X.509 certificate chains](#).

**PEM**

The Internet Privacy-Enhanced Mail protocols standard, adopted by the Internet Architecture Board to provide secure electronic mail over the Internet. The PEM protocols provide for encryption, authentication, message integrity, and key management. PEM is an inclusive standard, intended to be compatible with a wide range of key-management approaches, including both symmetric and public-key schemes to encrypt data-encrypting keys. The

specifications for PEM come from four Internet Engineering Task Force (IETF) documents: RFCs 1421, 1422, 1423, and 1424.

**PKCS #10**

An RSA Security, Inc., Public-Key Cryptography Standards (PKCS) specification that describes a syntax for certification requests. A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are referred to as certificate requests in this manual. See [certificate request](#)

**PKCS #11**

An RSA Security, Inc., Public-Key Cryptography Standards (PKCS) specification that defines an application programming interface (API), called Cryptoki, to devices which hold cryptographic information and perform cryptographic operations. See [PCMCIA cards](#)

**PKCS #12**

An RSA Security, Inc., Public-Key Cryptography Standards (PKCS) specification that describes a transfer syntax for storing and transferring personal authentication credentials—typically in a format called a [wallet](#).

**PKI**

See [public key infrastructure \(PKI\)](#)

**plaintext**

Message text that has not been encrypted.

**pluggable database**

See [PDB](#).

**principal**

A string that uniquely identifies a client or server to which a set of Kerberos credentials is assigned. It generally has three parts: `kservice/kinstance@REALM`. In the case of a user, `kservice` is the user name. See also [kservice](#), [kinstance](#), and [realm](#)

**private key**

In public-key cryptography, this key is the secret key. It is primarily used for decryption but is also used for encryption with digital signatures. See [public and private key pair](#).

**proxy authentication**

A process typically employed in an environment with a middle tier such as a firewall, wherein the end user authenticates to the middle tier, which thence authenticates to the directory on the

user's behalf—as its *proxy*. The middle tier logs into the directory as a *proxy user*. A proxy user can switch identities and, once logged into the directory, switch to the end user's identity. It can perform operations on the end user's behalf, using the authorization appropriate to that particular end user.

**public key**

In public-key cryptography, this key is made public to all. It is primarily used for encryption but can be used for verifying signatures. See [public and private key pair](#).

**public and private key pair**

A set of two numbers used for [encryption](#) and [decryption](#), where one is called the [private key](#) and the other is called the [public key](#). Public keys are typically made widely available, while private keys are held by their respective owners. Though mathematically related, it is generally viewed as computationally infeasible to derive the private key from the public key. Public and private keys are used only with asymmetric encryption algorithms, also called public-key encryption algorithms, or public-key cryptosystems. Data encrypted with either a public key or a private key from a [key pair](#) can be decrypted with its associated key from the key-pair. However, data encrypted with a public key cannot be decrypted with the same public key, and data enwrapped with a private key cannot be decrypted with the same private key.

**public key infrastructure (PKI)**

Information security technology utilizing the principles of public key cryptography. Public key cryptography involves encrypting and decrypting information using a shared public and private key pair. Provides for secure, private communications within a public network.

**PUBLIC role**

A special role that every database account automatically has. By default, it has no privileges assigned to it, but it does have grants to many Java objects. You cannot drop the `PUBLIC` role, and a manual grant or revoke of this role has no meaning, because the user account will always assume this role. Because all database user accounts assume the `PUBLIC` role, it does not appear in the `DBA_ROLES` and `SESSION_ROLES` data dictionary views.

**purge job**

A database job created by the `DBMS_AUDIT_MGMT.CREATE_PURGE_JOB` procedure, which manages the deletion of the audit trail. A database administrator schedules, enables, and disables the purge job. When the purge job becomes active, it deletes audit records from the database audit tables, or it deletes Oracle Database operating system audit files.

See also [forced cleanup](#), [last archive timestamp](#).

**RADIUS**

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

**realm**

1. Short for [identity management realm](#). 2. A Kerberos object. A set of clients and servers operating under a single key distribution center/ticket-granting service (KDC/TGS). Services (see [kservice](#)) in different realms that share the same name are unique.

**realm Oracle Context**

An [Oracle Context](#) that is part of an [identity management realm](#) in Oracle Internet Directory.

**registry**

A Windows repository that stores configuration information for a computer.

**remote computer**

A computer on a network other than the local computer.

**role**

A named group of related privileges that you grant as a group to users or other roles.

See also [indirectly granted role](#).

**root**

A collection of Oracle-supplied and user-created schemas to which all PDBs belong. The container database has only one root. Each PDB is considered to be a child of this root. Root has an entry in its data dictionary that indicates the existence of each PDB.

See also [container](#), [CDB](#), [PDB](#).

**root key certificate**

See [trusted certificate](#)

**salt**

In cryptography, a way to strengthen the security of encrypted data. Salt is a random string that is added to the data before it is encrypted, making it more difficult for attackers to steal the data by matching patterns of ciphertext to known ciphertext samples. Salt is often also added to passwords, before the passwords are encrypted, to avoid dictionary attacks, a method that unethical hackers (attackers) use to steal passwords. The encrypted salted values make it

difficult for attackers to match the hash value of encrypted passwords (sometimes called verifiers) with their dictionary lists of common password hash values.

#### **schema**

1. Database schema: A named collection of objects, such as tables, [views](#), clusters, procedures, packages, [attributes](#), [object classes](#), and their corresponding matching rules, which are associated with a particular user. 2. LDAP directory schema: The collection of attributes, object classes, and their corresponding matching rules.

#### **schema mapping**

See [user-schema mapping](#)

#### **secure application role**

A database role that is granted to application users, but secured by using an invoker's right stored procedure to retrieve the role password from a database table. A secure application role password is not embedded in the application.

See also [application role](#).

#### **Secure Hash Algorithm (SHA)**

An algorithm that assures data integrity by generating a 160-bit cryptographic message digest value from given data. If as little as a single bit in the data is modified, the Secure Hash Algorithm checksum for the data changes. Forgery of a given data set in a way that will cause the Secure Hash Algorithm to generate the same result as that for the original data is considered computationally infeasible.

An algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5 (which Oracle Database no longer supports), but the larger message digest makes it more secure against brute-force collision and inversion attacks.

#### **Secure Sockets Layer (SSL)**

An industry standard protocol designed by Netscape Communications Corporation for securing network connections. SSL provides authentication, encryption, and data integrity using public key infrastructure (PKI).

The [Transport Layer Security \(TLS\)](#) protocol is the successor to the SSL protocol.

#### **separation of duty**

Restricting activities only to those users who must perform them. For example, you should not grant the SYSDBA administrative privilege to any user. Only grant this privilege to administrative users. Separation of duty is required by many compliance policies. See "[Guidelines for](#)

[Securing User Accounts and Privileges](#)" for guidelines on granting privileges to the correct users.

**server**

A provider of a service.

**service**

1. A network resource used by clients; for example, an Oracle database server.
2. An executable process installed in the Windows [registry](#) and administered by Windows. Once a service is created and started, it can run even when no user is logged on to the computer.

**service name**

For Kerberos-based authentication, the [kservice](#) portion of a service principal.

**service principal**

See [principal](#)

**service key table**

In Kerberos authentication, a service key table is a list of service principals that exist on a [kinstance](#). This information must be extracted from Kerberos and copied to the Oracle server computer before Kerberos can be used by Oracle.

**service ticket**

A service ticket is trusted information used to authenticate the client, to a specific service or server, for a predetermined period of time. It is obtained from the [KDC](#) using the [initial ticket](#). See also [Kerberos ticket](#).

**session key**

A key shared by at least two parties (usually a client and a server) that is used for data encryption for the duration of a single communication session. Session keys are typically used to encrypt network traffic; a client and a server can negotiate a session key at the beginning of a session, and that key is used to encrypt all network traffic between the parties for that session. If the client and server communicate again in a new session, they negotiate a new session key.

**session layer**

A network layer that provides the services needed by the presentation layer entities that enable them to organize and synchronize their dialogue and manage their data exchange. This layer



establishes, manages, and terminates network sessions between the client and server. An example of a session layer is Network Session.

#### SHA

See [Secure Hash Algorithm \(SHA\)](#).

#### shared schema

A database or application schema that can be used by multiple enterprise users. Oracle Database supports the mapping of multiple enterprise users to the same shared schema on a database, which lets an administrator avoid creating an account for each user in every database. Instead, the administrator can create a user in one location, the enterprise directory, and map the user to a shared schema that other enterprise users can also map to. Sometimes called [user/schema separation](#).

#### single key-pair wallet

A [PKCS #12](#)-format [wallet](#) that contains a single user [certificate](#) and its associated [private key](#). The [public key](#) is imbedded in the certificate.

#### single password authentication

The ability of a user to authenticate with multiple databases by using a single password. In the Oracle Database implementation, the password is stored in an LDAP-compliant directory and protected with encryption and Access Control Lists.

#### single sign-on (SSO)

The ability of a user to *authenticate once*, combined with strong authentication occurring transparently in subsequent connections to other databases or applications. Single sign-on lets a user access multiple accounts and applications with a single password, entered during a single connection. *Single password, single authentication*. Oracle Database supports Kerberos and SSL-based single sign-on.

#### smart card

A plastic card (like a credit card) with an embedded integrated circuit for storing information, including such information as user names and passwords, and also for performing computations associated with authentication exchanges. A smart card is read by a hardware device at any client or server.

A smartcard can generate random numbers which can be used as one-time use passwords. In this case, smartcards are synchronized with a service on the server so that the server expects the same password generated by the smart card.

**sniffer**

Device used to surreptitiously listen to or capture private data traffic from a network.

**SSO**

See [single sign-on \(SSO\)](#)

**System Global Area (SGA)**

A group of shared memory structures that contain data and control information for an Oracle [instance](#).

**system identifier (SID)**

A unique name for an Oracle [instance](#). To switch between Oracle databases, users must specify the desired SID. The SID is included in the `CONNECT DATA` parts of the [connect descriptor](#) in a [tnsnames.ora](#) file, and in the definition of the [network listener](#) in a [listener.ora](#) file.

**third-party attack**

A security attack characterized by the third-party, surreptitious interception of a message, wherein the third-party decrypts the message, re-encrypts it (with or without alteration of the original message), and re-transmits it to the originally-intended recipient—all without the knowledge of the legitimate sender and receiver. This type of security attack works only in the absence of [authentication](#). Formerly called man-in-the-middle attack.

**ticket**

A piece of information that helps identify who the owner is. See [initial ticket](#) and [service ticket](#).

**tnsnames.ora**

A file that contains connect descriptors; each [connect descriptor](#) is mapped to a [net service name](#). The file may be maintained centrally or locally, for use by all or individual clients. This file typically resides in the following locations depending on your platform:

- (UNIX) `ORACLE_HOME/network/admin`
- (Windows) `ORACLE_BASE\ORACLE_HOME\network\admin`

**token card**

A device for providing improved ease-of-use for users through several different mechanisms. Some token cards offer one-time passwords that are synchronized with an authentication service. The server can verify the password provided by the token card at any given time by contacting the authentication service. Other token cards operate on a challenge-response basis. In this case, the server offers a challenge (a number) which the user types into the token

card. The token card then provides another number (cryptographically-derived from the challenge), which the user then offers to the server.

**transport layer**

A networking layer that maintains end-to-end reliability through data flow control and error recovery methods. [Oracle Net Services](#) uses *Oracle protocol supports* for the transport layer.

**Transport Layer Security (TLS)**

An industry standard protocol for securing network connections. The TLS protocol is a successor to the SSL protocol. It provides authentication, encryption, and data integrity using public key infrastructure (PKI). The TLS protocol is developed by the Internet Engineering Task Force (IETF).

**trusted certificate**

A trusted certificate, sometimes called a root key certificate, is a third party identity that is qualified with a level of trust. The trusted certificate is used when an identity is being validated as the entity it claims to be. Typically, the certificate authorities you trust are called trusted certificates. If there are several levels of trusted certificates, a trusted certificate at a lower level in the certificate chain does not need to have all its higher level certificates reverified.

**trusted certificate authority**

See [certificate authority](#).

**trust point**

See [trusted certificate](#).

**user name**

A name that can connect to and access objects in a database.

**user-schema mapping**

An [LDAP](#) directory entry that contains a pair of values: the [base](#) in the directory at which users exist, and the name of the database schema to which they are mapped. The users referenced in the mapping are connected to the specified schema when they connect to the database. User-schema mapping entries can apply only to one database or they can apply to all databases in a domain. See [shared schema](#).

**user/schema separation**

See [shared schema](#).

**user search base**

The node in the LDAP directory under which the user resides.

**views**

Selective presentations of one or more tables (or other views), showing both their structure and their data.

**wallet**

A data structure used to store and manage security credentials for an individual entity.

**Windows native authentication**

An [authentication method](#) that enables a client single login access to a Windows server and a database running on that server.

**X.509**

An industry-standard specification for digital [certificate s](#).