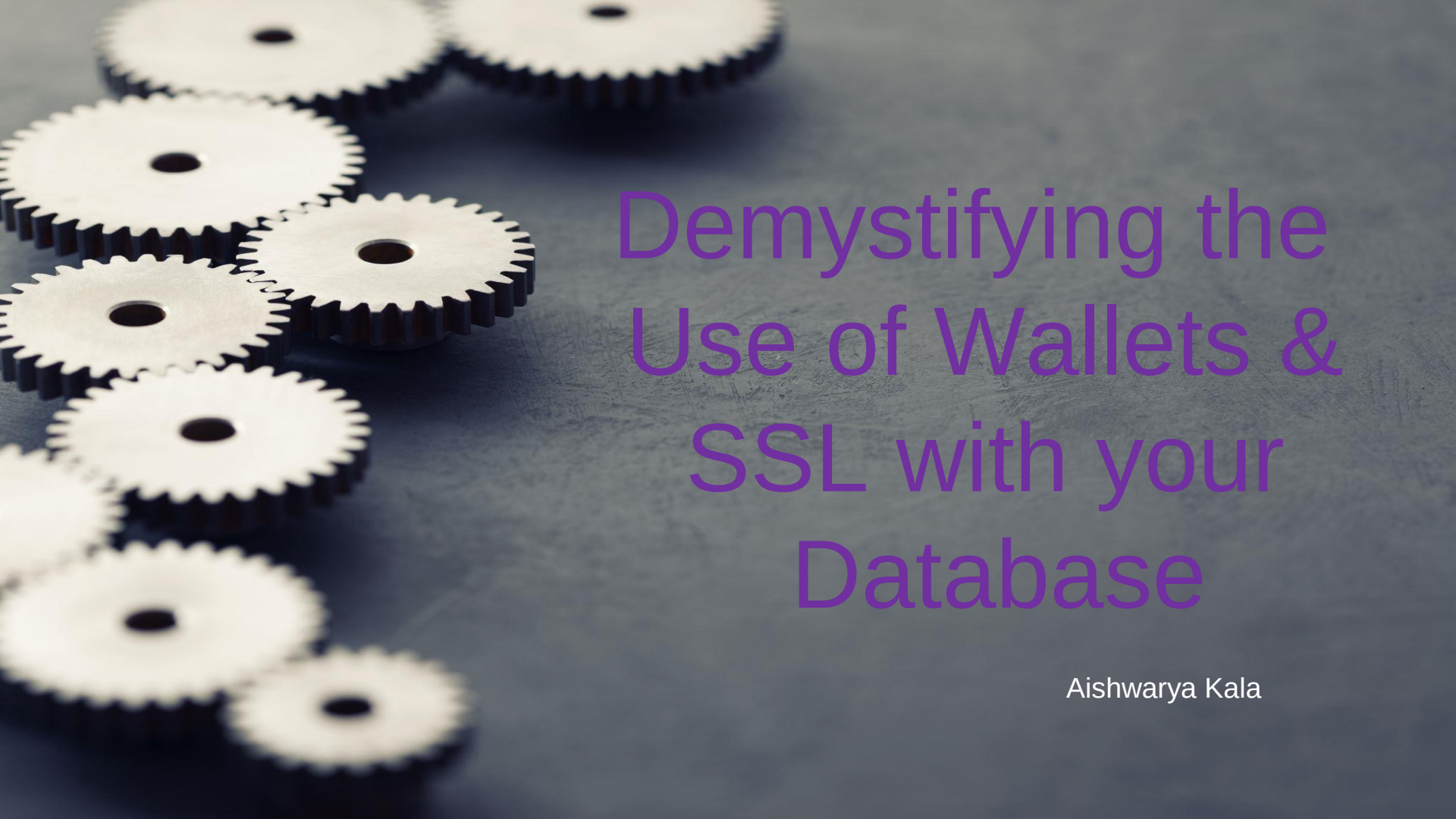


Demystifying the Use of Wallets & SSL with your Database

Aishwarya Kala

AGENDA

- ✓ Wallets
- ✓ Encryption Essentials
- ✓ Database Network Encryption
- ✓ Native Network Encryption
- ✓ Network Data Integrity
- ✓ TLS / SSL
- ✓ Appendix

Wallets

What are wallets ?

*“**Oracle Wallet** is a container that stores **authentication** and **signing credentials**.”*

Wallets can be

- ✓ Password Protected
- ✓ Autologin
  - ✓ Auto_login
  - ✓ auto_login_local

Filesystem permissions

Server Name - /etc/hosts

Owner

Why Should I Use One ?

Passwords stored in config files

```
-bash-4.2$ ls -ltrh
total 4.0K
-rw-r--r--. 1 oracle oinstall 25 Jul  5 19:09 some-script.sh
-bash-4.2$
-bash-4.2$ ls -ltrh
total 4.0K
-rw-r--r--. 1 oracle oinstall 25 Jul  5 19:09 some-script.sh
-bash-4.2$
-bash-4.2$
-bash-4.2$ grep -i config some-script.sh
. ./.some-script.config
-bash-4.2$
-bash-4.2$
-bash-4.2$ cat ./.some-script.config
PASSWORD=critical_password
-bash-4.2$
```

Why Should I Use One ?

Passwords in config files

- Did you check your umask ?

```
-bash-4.2$ umask
0022
-bash-4.2$
-bash-4.2$
```

- Is this access truly restricted ?

```
-bash-4.2$ pwd
/home/oracle/nfs-share
-bash-4.2$
-bash-4.2$
```

Why Should I Use One ?

- Protect Sensitive Passwords
  - Review your code

```
[akala@lab1~]$ ps -ef | grep rman
oracle    4669 26916  1 00:22 pts/1    00:00:01 rman target / catalog rman/rman_password@catalog_db
akala    20213 11800  0 00:23 pts/0    00:00:00 grep --color=auto rman
```

Why Should I Use One ?

- ✓ Surely No-one can see the password now..

```
[oracle@labwork1 wallet]$ rman

Recovery Manager: Release 19.0.0.0.0 - Production on Tue Jul 7 05:47:10 2020
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

RMAN> connect target $RMAN_USER/$RMAN_PASSWORD

connected to target database: TESTDB (DBID=2821646721)
```

```
-bash-4.2$ strings /proc/841/environ | grep -i rman
RMAN_PASSWORD=mypassword
RMAN_USER=c##rman
```

Why Should I Use One ?

- ✓ We use OS Authentication for backups. (rman target /)
- ✓ Have you offloaded backups offloaded to Standby ?

```
RMAN-06820: WARNING: failed to archive current log at primary database
ORACLE error from target database:
ORA-17629: Cannot connect to the remote database server
ORA-17627: ORA-01031: insufficient privileges
```

RMAN-06820 ORA-17629 During Backup at Standby Site (Doc ID 1616074.1)

Have you wondered ?

What happens now ??

```
-bash-4.2$ sqlplus sys/mypassword@testdb as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Jul 7 04:28:09 2020
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.
```

Have you wondered ?

- ✓ What happens now ??

```
[oracle@labwork1 ~]$ ps -ef | grep sqlplus
oracle   27343 27236  0 04:28 pts/1    00:00:00 sqlplus                    as sysdba
oracle   27426 27387  0 04:28 pts/1    00:00:00 grep --color=auto sqlplus
[oracle@labwork1 ~]$
```

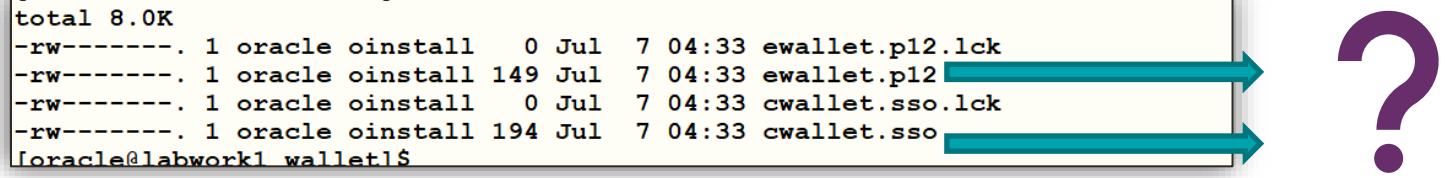
How to create

- ✓ Create a wallet

```
[oracle@labwork1 testdb]$ mkstore  -wrl /opt/oracle/admin/testdb/wallet  -create
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Enter password:
PKI-01002: Invalid password. Passwords must have a minimum length of eight characters and contain alphabetic characters combined with numbers or s
pecial characters.
Enter password:
Enter password again:
```

- ✓ Files Created

```
total 8.0K
-rw-------. 1 oracle oinstall   0 Jul  7 04:33 ewallet.p12.lck
-rw-------. 1 oracle oinstall 149 Jul  7 04:33 ewallet.p12
-rw-------. 1 oracle oinstall   0 Jul  7 04:33 cwallet.sso.lck
-rw-------. 1 oracle oinstall 194 Jul  7 04:33 cwallet.sso
[oracle@labwork1 wallet]$
```



How to create

- ✓ Create a wallet

```
[oracle@labwork1 testdb]$ mkstore  -wrl /opt/oracle/admin/testdb/wallet  -create
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Enter password:
PKI-01002: Invalid password. Passwords must have a minimum length of eight characters and contain alphabetic characters combined with numbers or s
pecial characters.
Enter password:
Enter password again:
```

- ✓ Files Created

Public Key Cryptography Standards

```
total 8.0K
-rw-------. 1 oracle oinstall   0 Jul  7 04:33 ewallet.p12.lck
-rw-------. 1 oracle oinstall 149 Jul  7 04:33 ewallet.p12
-rw-------. 1 oracle oinstall   0 Jul  7 04:33 cwallet.sso.lck
-rw-------. 1 oracle oinstall 194 Jul  7 04:33 cwallet.sso
[oracle@labwork1 wallet]$
```

PKCS#12 Wallet

Autologin Wallet

Creating Credentials

- Create a credential

```
$  mkstore -wrl "/opt/oracle/admin/testdb/wallet" -createCredential testdb_bkp sys
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Your secret/Password is missing in the command line
Enter your secret/Password:
Re-enter your secret/Password:
Enter wallet password:
```

```
$mkstore  -wrl /opt/oracle/admin/testdb/wallet  -listCredential
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Enter wallet password:
List credential (index: connect_string username)
1: testdb_bkp sys
```

Using Wallets

- SQLNET.ORA
  - WALLET_LOCATION
  - WALLET_OVERRIDE

```
DIRECTORY = /opt/oracle/admin/testdb/wallet
```

```
TRUE
```

Using Wallets

- ✓ sqlnet.ora
  - ✓ WALLET_LOCATION — DIRECTORY = /opt/oracle/admin/testdb/wallet
  - ✓ WALLET_OVERRIDE — TRUE

Use a custom SQLNET & set TNS_ADMIN appropriately

Maintenance

- ✓ Backup Your Wallet !!
  - ✓ How ??

The way you backup sqlnet.ora !!

- ✓ Rotation of master keys
  - ✓ Extremely important to secure your master key
  - ✓ Keepass, Last pass or password manager used by your organization

Tools to Manage Your Wallet

- ✓ mkstore
- ✓ Oracle Wallet Manager (GUI)
- ✓ orapki

Tools to Manage Your Wallet

```
-bash-4.2$ mkstore help
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

No wallet location specified.
mkstore [-wrl wrl] [-create] [-createSSO] [-createLSSO] [-createALO] [-delete] [
-deleteSSO] [-list] [-createEntry alias secret] [-viewEntry alias] [-modifyEntry
 alias secret] [-deleteEntry alias] [-createCredential connect_string username p
assword] [-listCredential] [-modifyCredential connect_string username password]
[-deleteCredential connect_string]  [-createUserCredential map key  <username> p
assword]  [-modifyUserCredential map key username password]  [-deleteUserCredent
ial map key] [-help] [-nologo]
```

Tools to Manage Your Wallet

```
-bash-4.2$ orapki help
Oracle PKI Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

orapki [crl|wallet|cert|help] <-nologo> <-jsafe> <-use_jce> <-use_jce_only> <-fi
ps140_mode>
Syntax :
[-option [value]]      : mandatory, for example [-wallet [wallet]]
[-option <value>]      : optional, but when option is used its value is mandatory
.
<option>               : optional, for example <-summary>, <-complete>
[option1] | [option2] : option1 'or' option2
```

Contents of Wallet

- ✓ mkstore

```
$mkstore  -wrl /opt/oracle/admin/testdb/wallet  -listCredential
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Enter wallet password:
List credential (index: connect_string username)
1: testdb_bkp sys
```

Contents of Wallet

- ✓ orapki

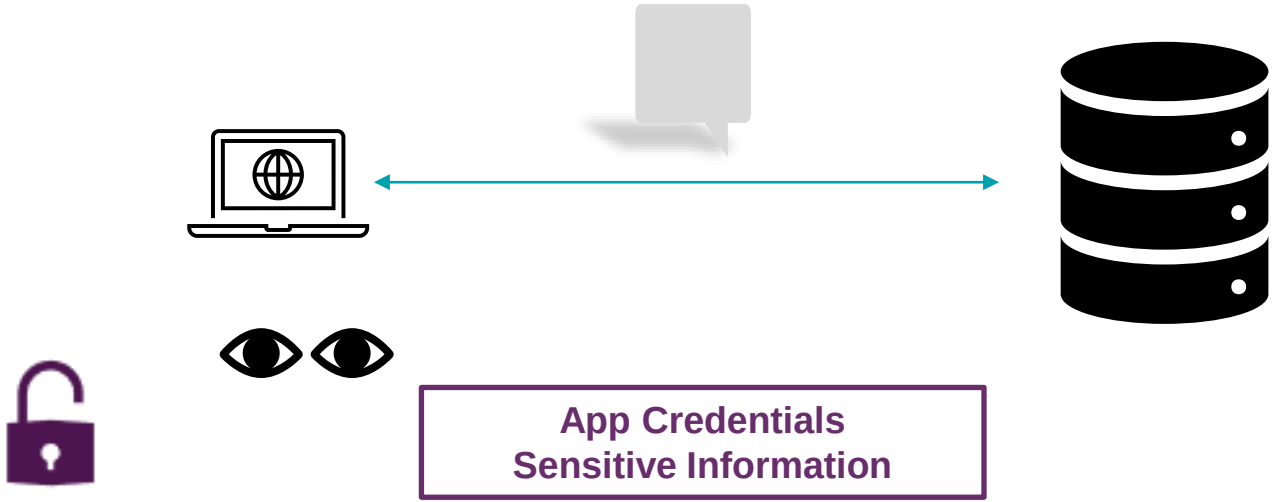
```
[oracle@labwork1 wallet]$ orapki wallet display -wallet /opt/oracle/admin/testdb/wallet
Oracle PKI Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:
User Certificates:
Trusted Certificates:
[oracle@labwork1 wallet]$
```

Wallet contents

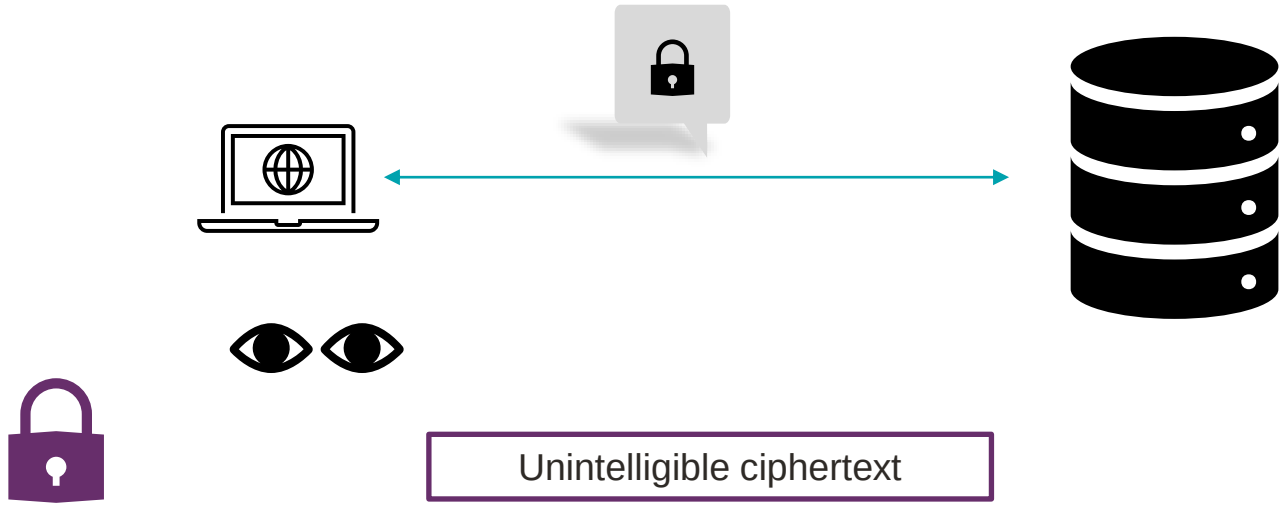
- ✓ mkstore
  - ✓ Credentials
- ✓ orapki
  - ✓ PKI Signed Digital Certificates
  - ✓ Keys
  - ✓ Certificate Revocation list
  - ✓ Java Key Store

Encryption Essentials

No Encryption



Encryption

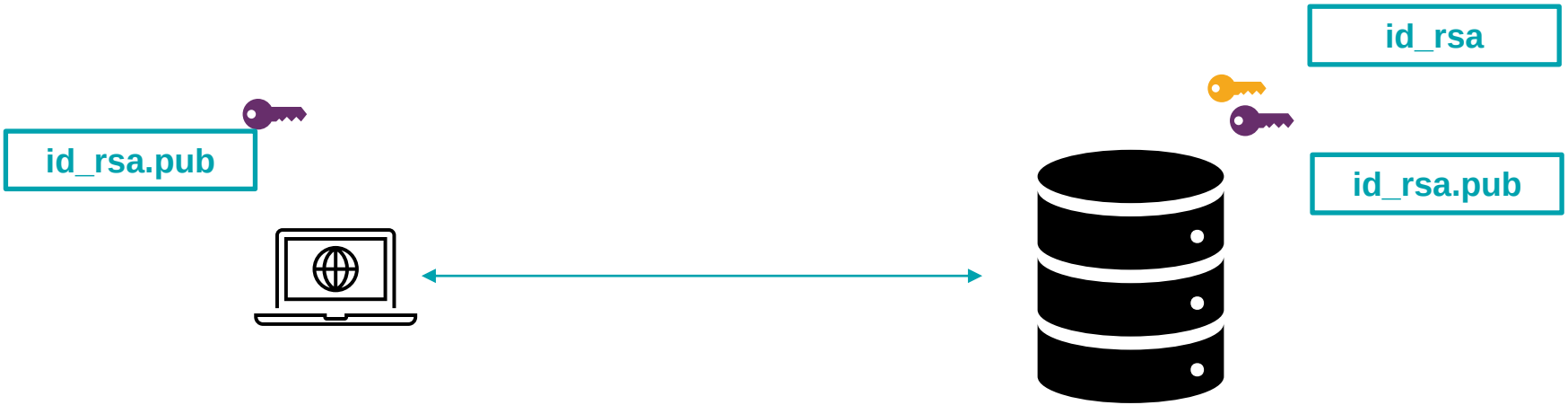


Encryption

Symmetric Encryption

Same Key used to encrypt as well as decrypt

Asymmetric Encryption



Key Pair , Public & Private Key

A Comparison

- ✓ Symmetric
  - ✓ Better Performance
  - ✓ Risk in transferring the key
  - ✓ AES, DES, and 3DES.

- ✓ Asymmetric Encryption
  - ✓ Compared to symmetric, slower
  - ✓ Safer as private key is never transmitted
  - ✓ RSA, DSA, and Diffie-Hellman.

Database Network Encryption

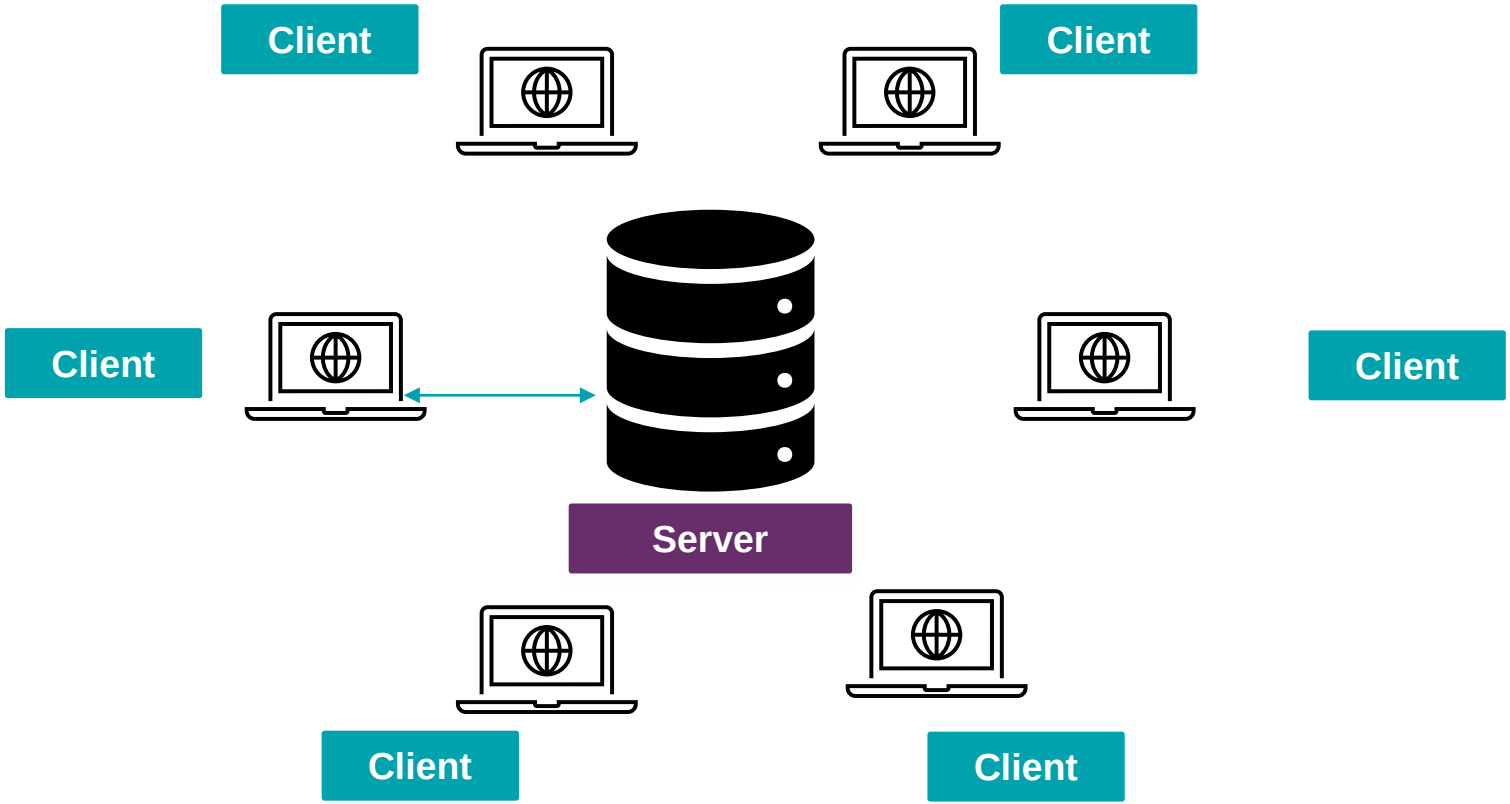
Database Network Encryption

- ✓ Native Network Encryption
- ✓ Network Data Integrity
- ✓ SSL/TLS

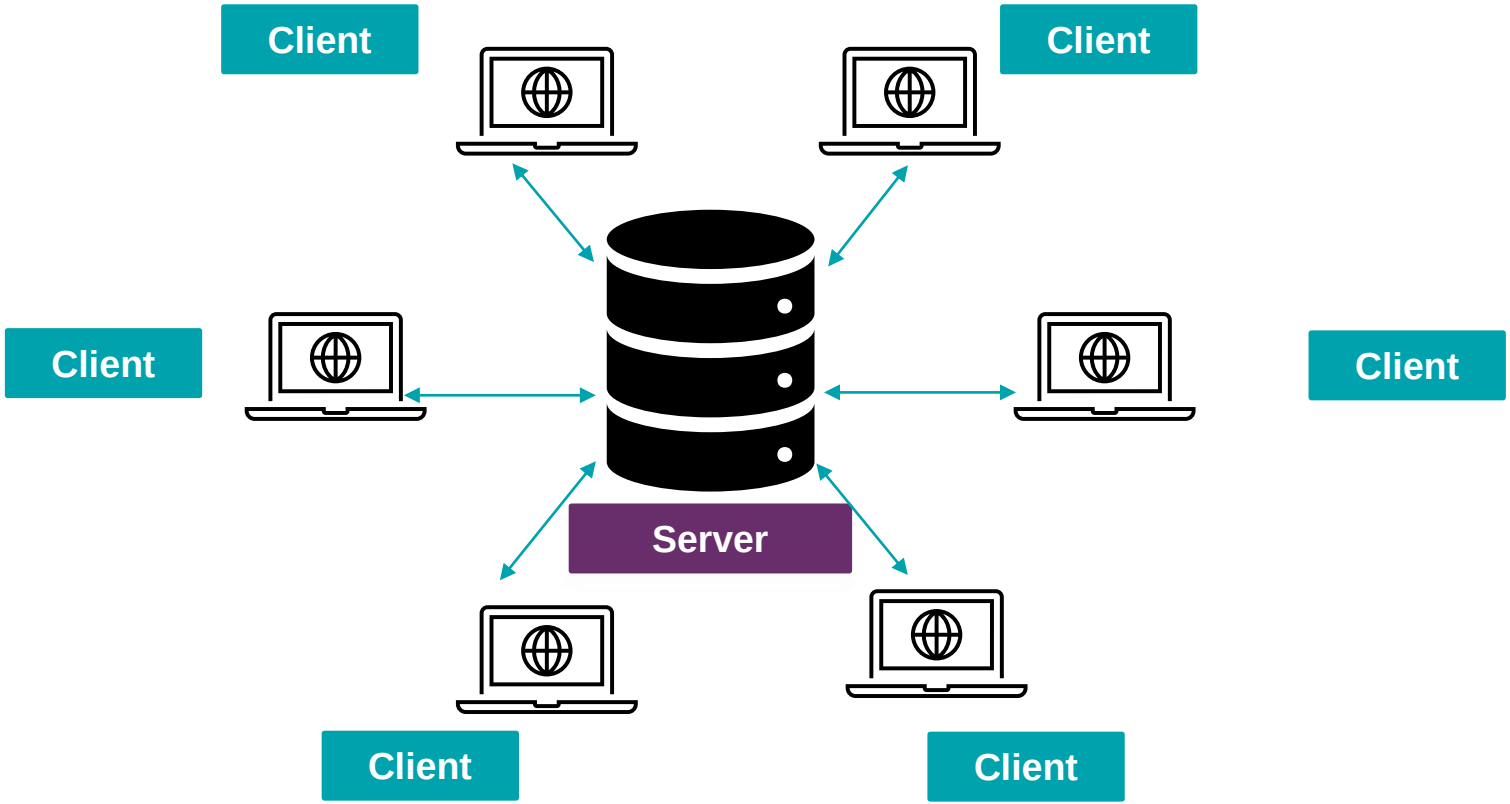
Not a part of Oracle Advanced Security Option

"Network encryption (native network encryption, network data integrity, and SSL/TLS) and strong authentication services (Kerberos, PKI, and RADIUS) are no longer part of Oracle Advanced Security and are available in all licensed editions of all supported releases of Oracle Database"

Configurable at Client Side



Configurable at Server Side



Native Network Encryption

Encryption

Session specific Key based on algorithm chosen

Enabling Native Network Encryption

1

Enabling Native Network Encryption

REQUIRED

Requires or Forces native encryption

- ✓ **ALL Connections will be Encrypted .**
- ✓ **No unencrypted Connections Allowed to the database**

Enabling Native Network Encryption

REQUESTED

Requests native encryption

- ✓ **Attempts to encrypt the traffic, if client allows**
- ✓ **If not, then will continue to ALLOW unencrypted connections**

Enabling Native Network Encryption

ACCEPTED

Accepts native encryption

- ✓ **Allows Encryption if the other side requests or requires it.**
- ✓ **Does not initiate encryption, how-ever will allow it .**

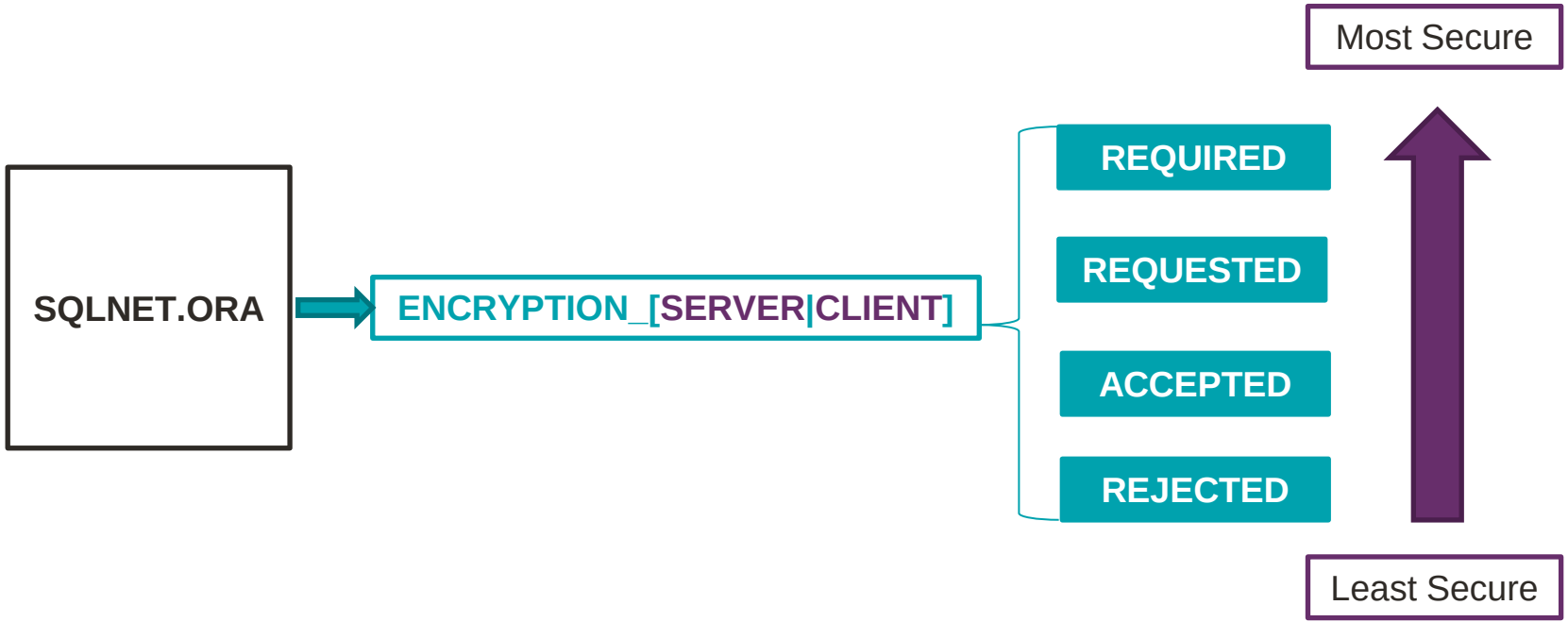
Enabling Native Network Encryption

REJECTED

Rejects native encryption

✓ **Disables Native Encryption**

Enabling Native Network Encryption



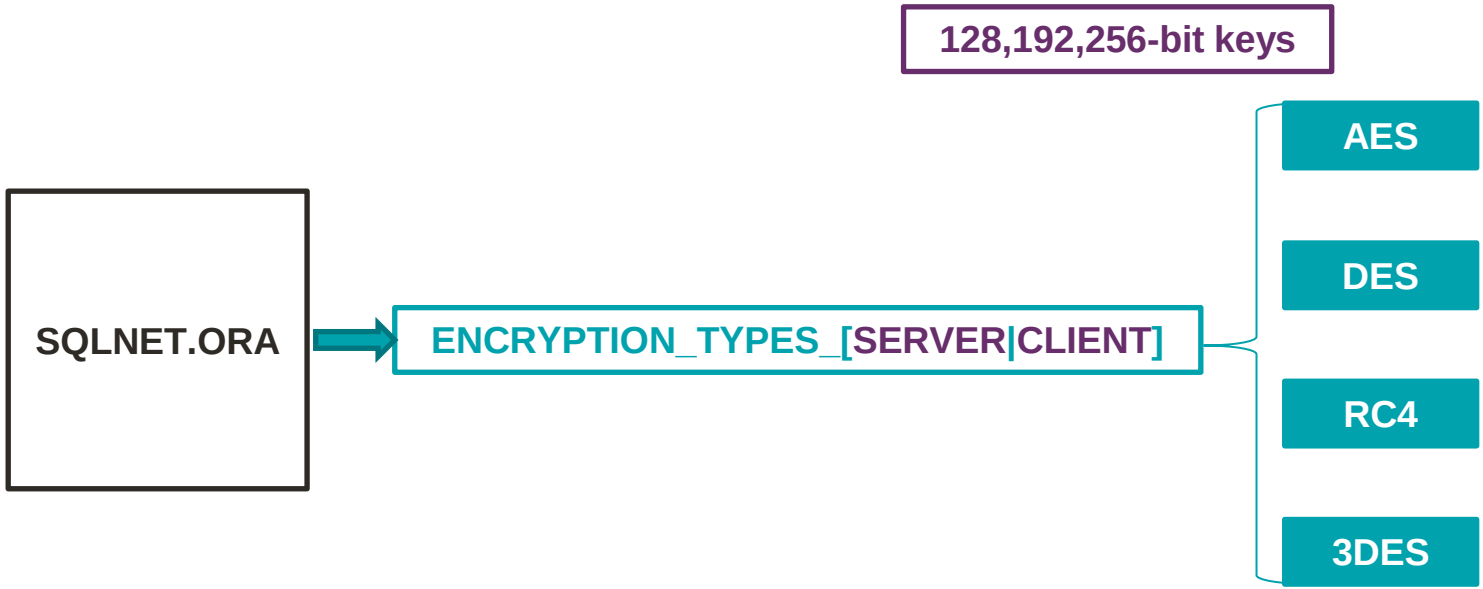
Enabling Native Network Encryption

SERVER

CLIENT

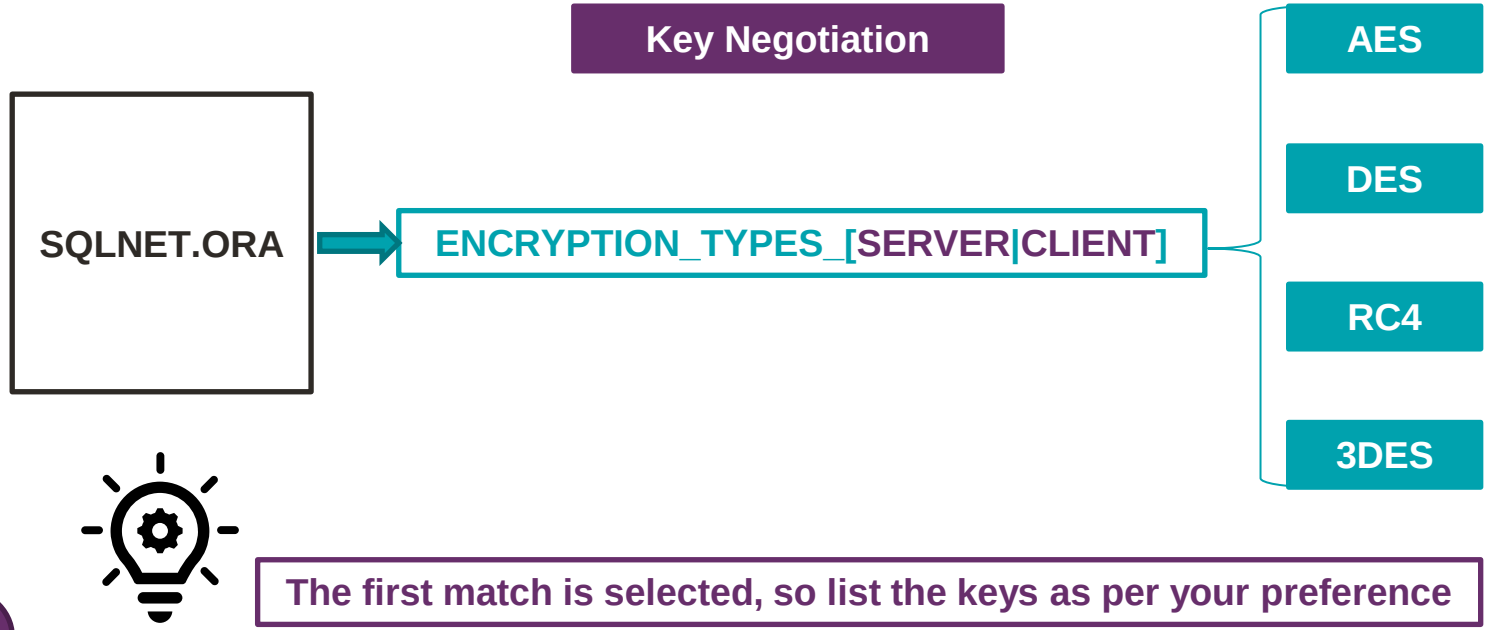
	REJECTED	ACCEPTED	REQUESTED	REQUIRED *
REJECTED	Disabled	Disabled	Disabled	Error in connection (ORA-12650)
ACCEPTED	Disabled	Disabled	Enabled	Enabled
REQUESTED	Disabled	Enabled	Enabled	Enabled
REQUIRED *	Error in connection (ORA-12650)	Enabled	Enabled	Enabled

Selecting Algorithms for Native Network Encryption



2

Selecting Algorithms for Native Network Encryption



2

Enabling Native Network Encryption

SERVER

CLIENT

	REJECTED	ACCEPTED	REQUESTED	REQUIRED *
REJECTED	Disabled	Disabled	Disabled	Error in connection (ORA-12650)
ACCEPTED	Disabled	Disabled	Enabled	Enabled
REQUESTED	Disabled	Enabled	Enabled	Enabled
REQUIRED *	Error in connection (ORA-12650)	Enabled	Enabled	Enabled

* If no matching algorithm + encryption is required = ORA-12650

Network Data Integrity

Network Data Integrity

Set of Integrity Algorithms that create a checksum

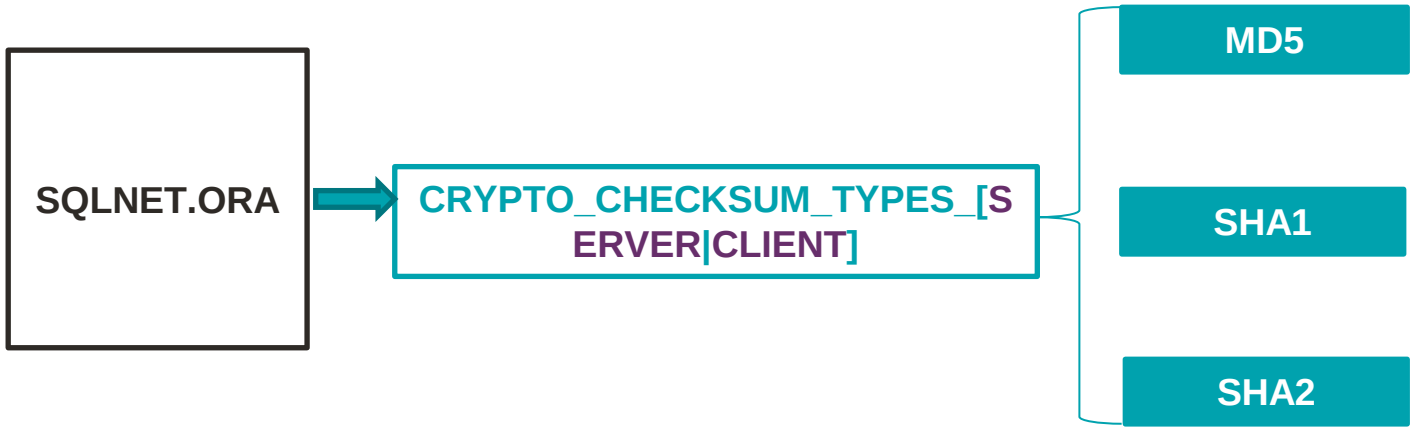
- ✓ Changes if data is altered
- ✓ Protection against attacks (Data Modification, Replay Attack)
- ✓ Support for multiple algorithms

Enabling Network Data Integrity

1

Enabling Network Data Integrity

- ✓ Selecting Algorithms for Data Integrity

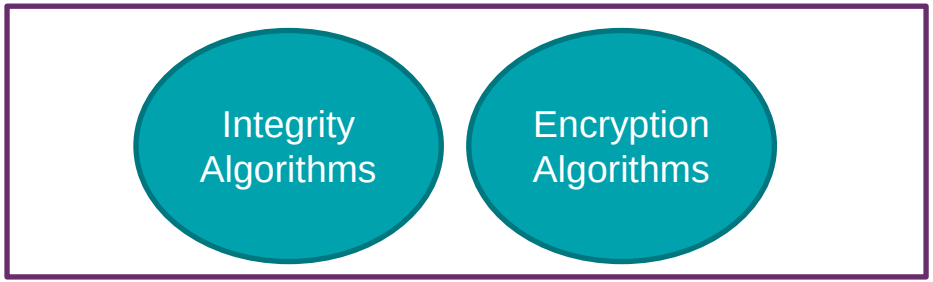


2

Native Network Encryption

To summarize

- ✓ Configured via SQLNET.ORA
- ✓ Support for multiple Integrity & Encryption Algorithms
- ✓ Symmetric cryptosystem
- ✓ Keys Valid Only for a session



Native Network Encryption

Implementation

```
-bash-4.2$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Jul 7 17:06:45 2020
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0


Session altered.

SYS@testdb:SQL> @/home/oracle/ssl-demo/demo-native-encryption.sql
Connected as sysdba
====================
SYS@testdb:SQL> select   NETWORK_SERVICE_BANNER from    v$session_connect_info where    SID = sys_context('USERENV','SID');

NETWORK_SERVICE_BANNER
----------------------------------------------------------------------------------------------------
Oracle Bequeath NT Protocol Adapter for Linux: Version 19.0.0.0.0 - Production
Authentication service for Linux: Version 19.0.0.0.0 - Production
Encryption service for Linux: Version 19.0.0.0.0 - Production
Crypto-checksumming service for Linux: Version 19.0.0.0.0 - Production
SYS@testdb:SQL> set echo off
```

Implementation – No Encryption

```
USER is "C##DEMO"
Connected as demo@testdb
==========================



View Contents of sqlnet.ora
==========================

# sqlnet.ora Network Configuration File: /opt/oracle/product/19c/dbhome_1/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.

NAMES.DIRECTORY_PATH= (TNSNAMES, ONAMES, HOSTNAME)



Check network Banner
==========

NETWORK_SERVICE_BANNER
----------------------------------------------------------------------------------------------------
TCP/IP NT Protocol Adapter for Linux: Version 19.0.0.0.0 - Production
Encryption service for Linux: Version 19.0.0.0.0 - Production
Crypto-checksumming service for Linux: Version 19.0.0.0.0 - Production
```

Implementation – Default Algorithms

```
Enable Native Encryption
========================

Reconnect
Connected.
Check network Banner
============================

NETWORK_SERVICE_BANNER
----------------------------------------------------------------------
TCP/IP NT Protocol Adapter for Linux: Version 19.0.0.0.0 - Production
Encryption service for Linux: Version 19.0.0.0.0 - Production
AES256 Encryption service adapter for Linux: Version 19.0.0.0.0 - Production
Crypto-checksumming service for Linux: Version 19.0.0.0.0 - Production
SHA1 Crypto-checksumming service adapter for Linux: Version 19.0.0.0.0 - Production
```

ENCRYPTION_SERVER
CRYPTO_CHECKSUM_SERVER

Implementation – With Custom Algorithms

```
Enable Custom Encryption
====================================


Connected.


Reconnect
=========


NETWORK_SERVICE_BANNER
----------------------------------------------------------------------------
TCP/IP NT Protocol Adapter for Linux: Version 19.0.0.0.0 - Production
Encryption service for Linux: Version 19.0.0.0.0 - Production
AES128 Encryption service adapter for Linux: Version 19.0.0.0.0 - Production
Crypto-checksumming service for Linux: Version 19.0.0.0.0 - Production
MD5 Crypto-checksumming service adapter for Linux: Version 19.0.0.0.0 - Production
```

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
SQLNET.ENCRYPTION_TYPES_SERVER

Native Encryption & Integrity

Encryption

Data Integrity

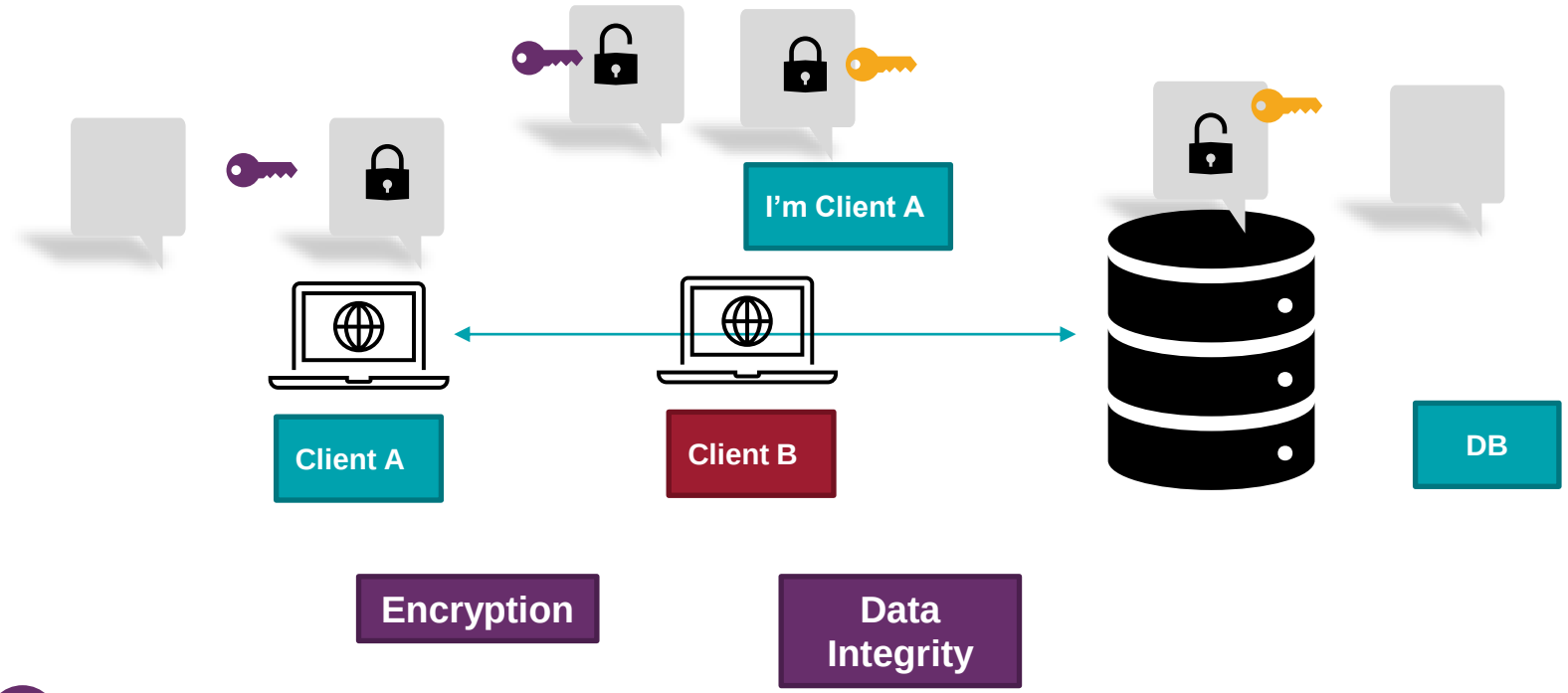
TLS / SSL

TLS / SSL – Why do we Need It ?

Encryption

Data Integrity

TLS / SSL – Why do we Need It ?



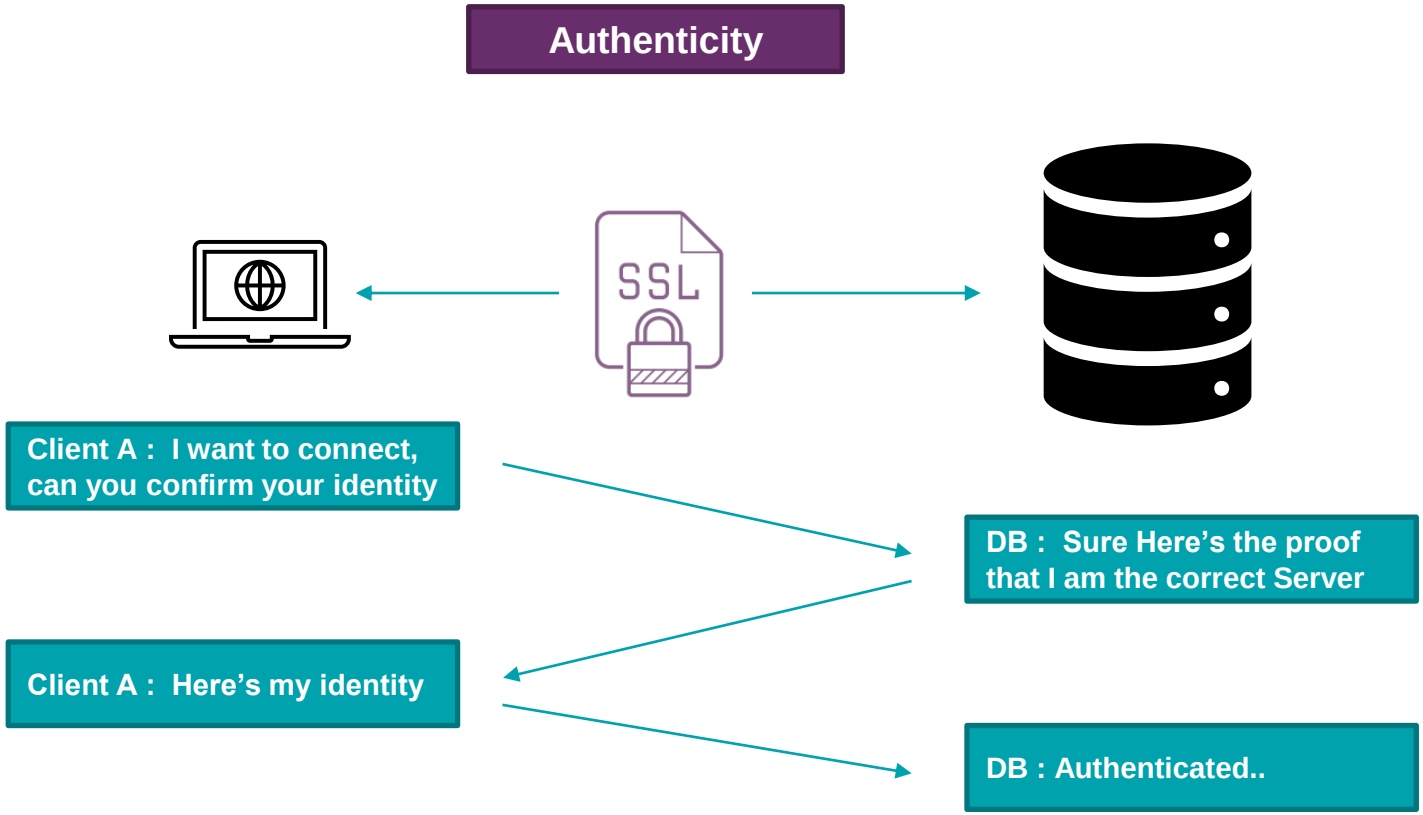
TLS / SSL

Encryption

Data Integrity

Authentication

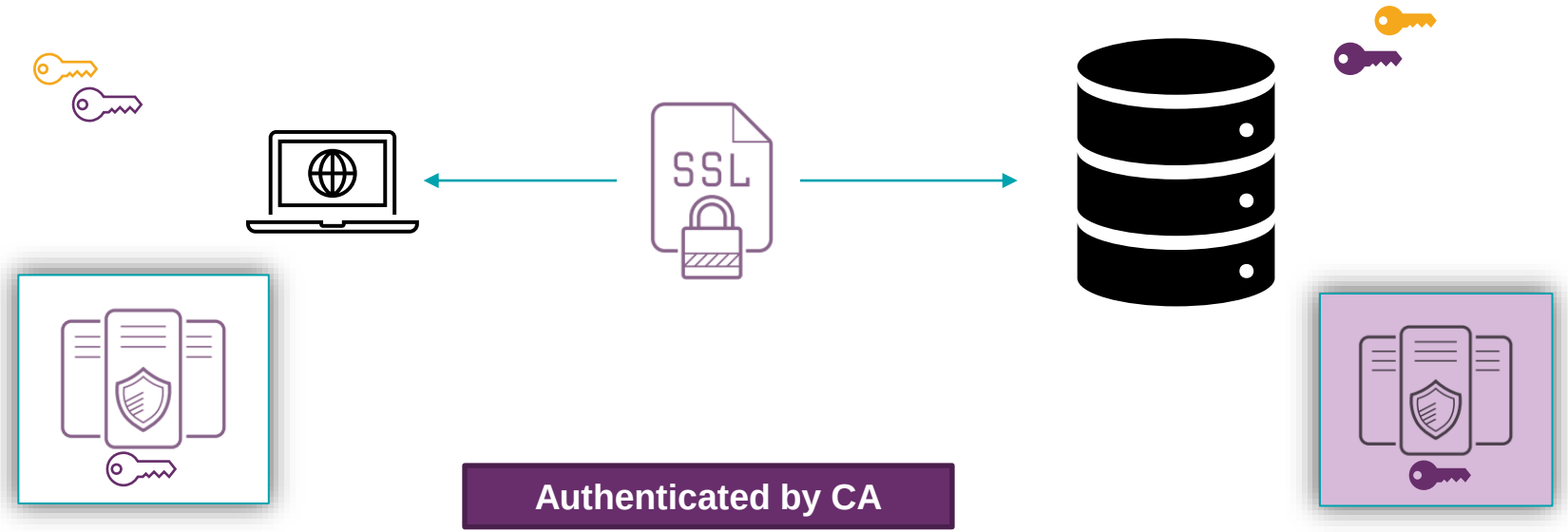
TLS / SSL


Authenticity
SSL
Client A : I want to connect, can you confirm your identity
DB : Sure Here's the proof that I am the correct Server
Client A : Here's my identity
DB : Authenticated..

TLS / SSL – Proof ?

Proof = Certificates

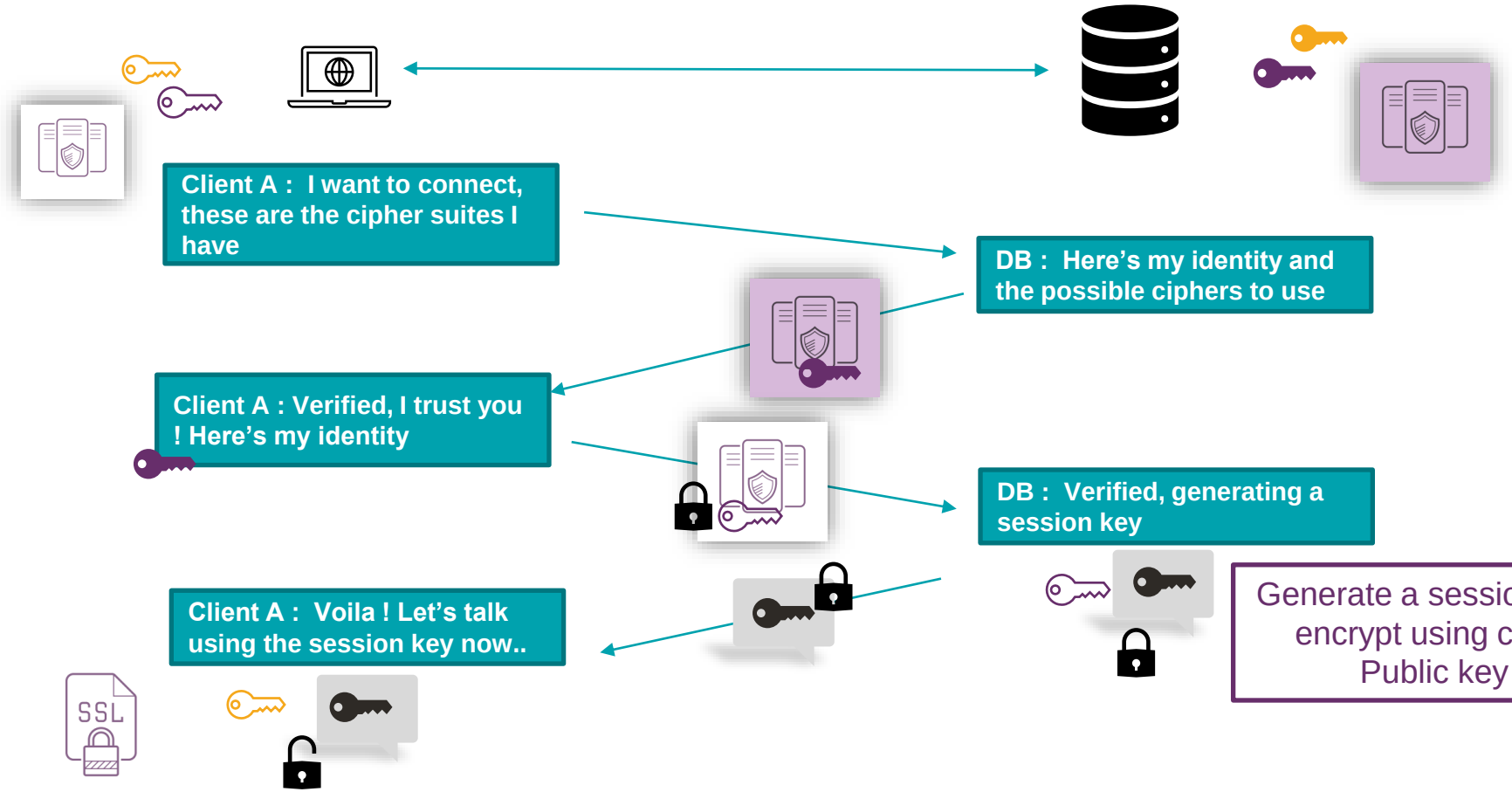
TLS / SSL



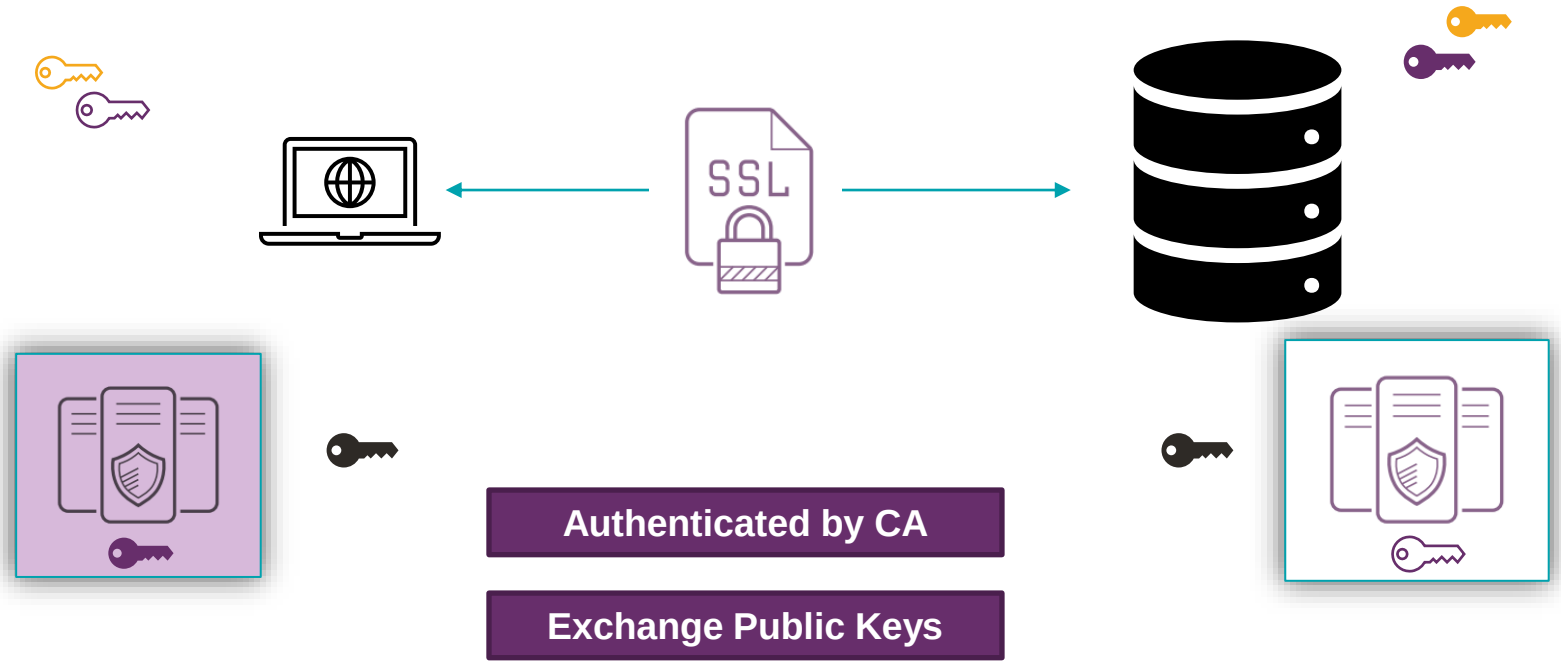
Authenticated by CA

Exchange Public Keys

SSL Handshake



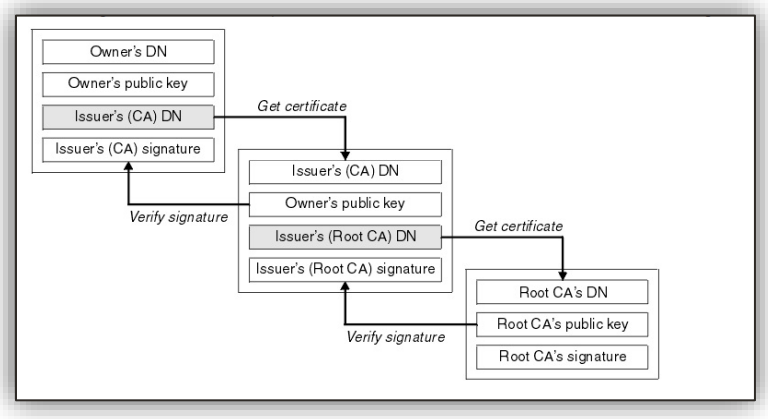
TLS / SSL



Certificates Authority

- ✓ A Root CA is a **Certificate Authority that owns one or more trusted roots**.

  - Trusted by both the parties
  - Responsible for verifying the identities, issuing & revoking certificates
  - Can form a chain



https://knowledge.digicert.com/solution/SO16297

Implementation

- ✓ Step 1: Get Signed Certificates
  - ✓ Stored in Wallets

```
[oracle@labwork1 wallet]$ orapki wallet display -wallet /opt/oracle/admin/testdb/wallet
Oracle PKI Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:
User Certificates:
Trusted Certificates:
[oracle@labwork1 wallet]$
```

Implementation

- ✓ Create a Certificate Signing Request (CSR)

```
$ orapki wallet add -wallet "/opt/oracle/admin/testdb/wallet" -dn "CN=labwork1.subnet.vcn.oraclevcn.com" -keysize 2048 -sign_alg sha256

$ orapki wallet display -wallet /opt/oracle/admin/testdb/wallet

Enter wallet password:
Requested Certificates:
Subject:        CN=labwork1.subnet.vcn.oraclevcn.com
User Certificates:
Trusted Certificates:
```

Implementation

- ✓ Create a Certificate Signing Request (CSR)

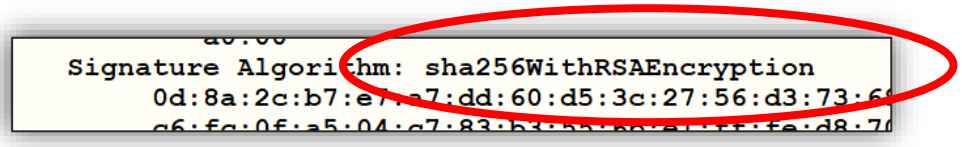
Send this to CA

```
$ openssl pkcs12 -in ewallet.p12 -nodes -out oracle_wallet.pem
Enter Import Password:
Can't read Password



$ openssl req -new -key oracle_wallet.pem -sha256 -out labwork1_certificate.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Uttarakhand
Locality Name (eg, city) [Default City]:Dehradun
Organization Name (eg, company) [Default Company Ltd]:labwork
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:labwork1.subnet.vcn.oraclevcn.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Implementation

- ✓ Verify your Signing Algorithms

```
$ openssl req -text -noout -verify -in labwork1_certificate.csr
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=IN, ST=Uttarakhand, L=Dehradun, O=labwork, CN=labwork1.subnet.vcn.oraclevcn.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```



ORAPKI Tool Not Generating Certificate Request With Sha256 (Doc ID 2216288.1)

Receiving Signed Certificates

- ✓ After receiving the signed Certificates from CA
  - ✓ Review both the server as well as the interim certificates (expiry dates, validity)
  - ✓ Separate out interim certificates (using OS utilities like vi)

```
$ openssl x509 -in labwork1_certificate_interm.cer -text | head -15
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services
Validity
Not Before: Jan 1 00:00:00 2004 GMT
Not After : Dec 31 23:59:59 2028 GMT
Subject: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:be:40:9d:f4:6e:e1:ea:76:87:1c:4d:45:44:8e:
```

Certificate Chain

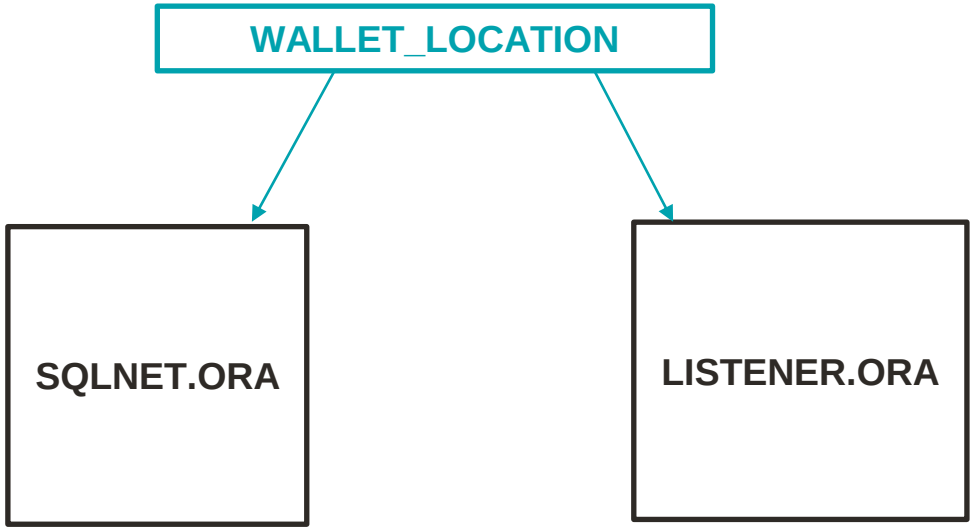
Import the Certificates back into the wallet

- ✓ Import the Interim Certificates
- ✓ Import the User Certificates

```
orapki wallet add -wallet /opt/oracle/admin/testdb/wallet -trusted_cert -cert ./labwork1_certificate_interm1.cer -pwd ******
orapki wallet add -wallet /opt/oracle/admin/testdb/wallet -trusted_cert -cert ./labwork1_certificate_interm2.cer -pwd ******
orapki wallet add -wallet /opt/oracle/admin/testdb/wallet -user_cert -cert labwork1_certificate.cer -pwd *****



$ orapki wallet display -wallet /opt/oracle/admin/testdb/wallet

Enter wallet password:
Requested Certificates:
User Certificates:
Subject:        CN=labwork1.subnet.vcn.oraclevcn.com
Trusted Certificates:
 Subject: CN=InCommon RSA Server CA,OU=InCommon,O=Internet2,L=Ann Arbor,ST=MI,C=US
 Subject: CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB
```

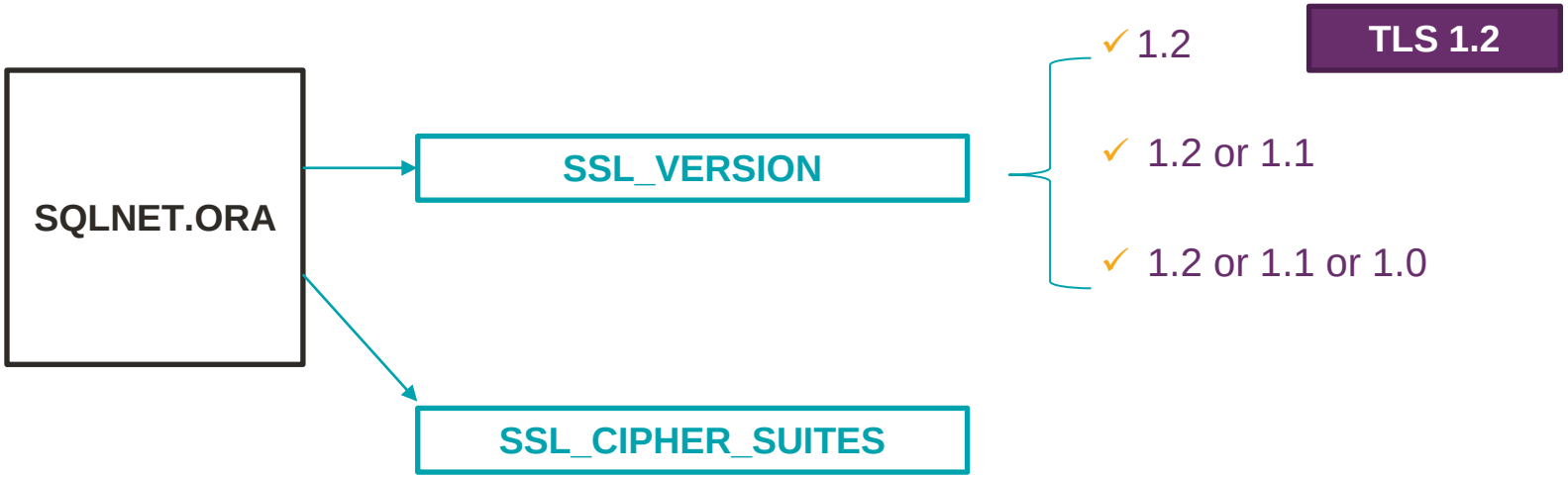
Implementation

- ✓ Step 2: Server Side Changes



Implementation

- ✓ Step 2: Server Side Changes



TLS 1.2

SSL_CIPHER_SUITES

Table 21-1 Secure Sockets Layer Cipher Suites

Cipher Suites	Authentication	Encryption	Data Integrity	TLS Compatibility
SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE_ECDSA	AES 128 GCM	SHA256 (SHA-2)	TLS 1.2 only
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA	AES 128 CBC	SHA-1	TLS 1.0 and later
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE_ECDSA	AES 128 CBC	SHA256 (SHA-2)	TLS 1.2 only
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA	AES 256 CBC	SHA-1	TLS 1.0 and later
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE_ECDSA	AES 256 CBC	SHA384 (SHA-2)	TLS 1.2 only
SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE_ECDSA	AES 256 GCM	SHA384 (SHA-2)	TLS 1.2 only
SSL_RSA_WITH_AES_128_CBC_SHA256	RSA	AES 128 CBC	SHA256 (SHA-2)	TLS 1.2 only
SSL_RSA_WITH_AES_128_GCM_SHA256	RSA	AES 128 GCM	SHA256 (SHA-2)	TLS 1.2 only
SSL_RSA_WITH_AES_128_CBC_SHA	RSA	AES 128 CBC	SHA-1	TLS 1.0 only
SSL_RSA_WITH_AES_256_CBC_SHA	RSA	AES 256 CBC	SHA-1	TLS 1.0 and later
SSL_RSA_WITH_AES_256_CBC_SHA256	RSA	AES 256 CBC	SHA256 (SHA-2)	TLS 1.2 only
SSL_RSA_WITH_AES_256_GCM_SHA384	RSA	AES 256 GCM	SHA384 (SHA-2)	TLS 1.2 only

Implementation

- ✓ Add TCPS Listener Endpoints

```
$ srvctl modify listener -p "TCP:1521/TCPS:2484"
$ srvctl modify scan_listener -p "TCP:1521/TCPS:2484"


$ srvctl stop scan_listener
$ srvctl start scan_listener

$ srvctl stop listener
$ srvctl start listener
```

- ✓ Update local_listener to use TCPS & Secure port

Implementation

- ✓ Client Certificates (If Used)
  - ✓ Export/Import of Certificates
- ✓ Verify Protocol

```
select instance_name, sys_context('userenv','network_protocol') from v$instance;

INSTANCE_NAME
----------------
SYS_CONTEXT('USERENV','NETWORK_PROTOCOL')
--------------------------------------------------------------------------------
testdb
tcps
```

Implementation

- ✓ Verify Ciphers

```
openssl s_client  -connect testdb:2484
CONNECTED(00000003)
depth=3 C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = AAA Certificate Services
verify return:1
depth=2 C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust RSA Certification Authority
verify return:1
depth=1 C = IN, ST = UT, L = Dehradun, O = labwork, OU = labwork, CN=labwork1.subnet.vcn.oraclevcn.com
verify return:1


Certificate chain
 0 s:/C=US/postalCode=248006/SC=IN/ST=Uttarakhand/O=Dehradun/OU=labwork/CN=labwork1.subnet.vcn.oraclevcn.com
   i:/C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA
 1 s:/C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA
   i:/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority
 2 s:/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority
   i:/C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services

---
Acceptable client certificate CA names

---
SSL handshake has read 6611 bytes and written 138 bytes
---

SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 93F224CE577385ABA3316829F22F4E358CEE7B1BCC[illegible]C4BE1AB0A5C9F6DE7A575
    Session-ID-ctx:
    Master-Key: 29CFD5A6658ECA7420085F72F4EC4D248AD[illegible]BFA5AC6EDDDCD43E0A48C6DEA0B1727B8AA67540E1C7DE89EDFA080D92
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
```

Other Use Cases

- ✓ utl_smtp for PL/SQL Packages that send email
  - ✓ Authenticate with mail server
- ✓ Oracle Enterprise Manager

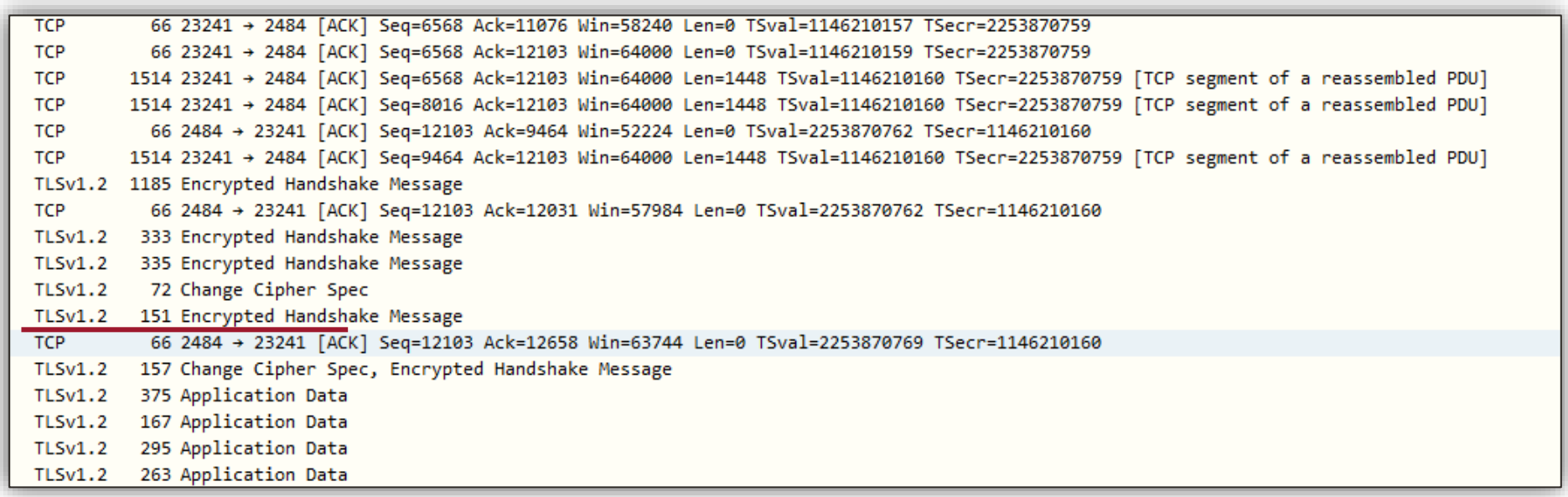
Maintenance

- ✓ Certificate Expiry & Renewal

```
$ openssl s_client -connect labwork1.subnet.vcn.oraclevcn.com :2484 2> /dev/null | openssl x509 -noout -dates
notBefore=May 18 00:00:00 2020 GMT
notAfter=May 18 23:59:59 2021 GMT
```

- ✓ For Troubleshooting
  - ✓ Enable Tracing (TRACE_LEVEL_CLIENT, TRACE_FILE_CLIENT)
  - ✓ Identify the NIC associated with the IP of the TCPS Port & create a session
  - ✓ Tcpdump
    - ✓ tcpdump -nnvvXSs0 -i eth0 host labwork1 -w /tmp/tcp_out.trc
  - ✓ Wireshark

Wireshark



```
TCP         66 23241 → 2484 [ACK] Seq=6568 Ack=11076 Win=58240 Len=0 TSval=1146210157 TSecr=2253870759
TCP         66 23241 → 2484 [ACK] Seq=6568 Ack=12103 Win=64000 Len=0 TSval=1146210159 TSecr=2253870759
TCP       1514 23241 → 2484 [ACK] Seq=6568 Ack=12103 Win=64000 Len=1448 TSval=1146210160 TSecr=2253870759 [TCP segment of a reassembled PDU]
TCP       1514 23241 → 2484 [ACK] Seq=8016 Ack=12103 Win=64000 Len=1448 TSval=1146210160 TSecr=2253870759 [TCP segment of a reassembled PDU]
TCP         66 2484 → 23241 [ACK] Seq=12103 Ack=9464 Win=52224 Len=0 TSval=2253870762 TSecr=1146210160
TCP       1514 23241 → 2484 [ACK] Seq=9464 Ack=12103 Win=64000 Len=1448 TSval=1146210160 TSecr=2253870759 [TCP segment of a reassembled PDU]
TLSv1.2   1185 Encrypted Handshake Message
TCP         66 2484 → 23241 [ACK] Seq=12103 Ack=12031 Win=57984 Len=0 TSval=2253870762 TSecr=1146210160
TLSv1.2    333 Encrypted Handshake Message
TLSv1.2    335 Encrypted Handshake Message
TLSv1.2     72 Change Cipher Spec
TLSv1.2    151 Encrypted Handshake Message
TCP         66 2484 → 23241 [ACK] Seq=12103 Ack=12658 Win=63744 Len=0 TSval=2253870769 TSecr=1146210160
TLSv1.2    157 Change Cipher Spec, Encrypted Handshake Message
TLSv1.2    375 Application Data
TLSv1.2    167 Application Data
TLSv1.2    295 Application Data
TLSv1.2    263 Application Data
```

Comparsion

- ✓ Native
  - ✓ Ease of Implementation
  - ✓ No maintenance overhead
  - ✓ Less Secure

ENCRYPTION_SEED

- ✓ TLS
  - ✓ Configuration is tricky
  - ✓ Need to be careful about certificate expiry
  - ✓ Possible Performance Overhead
  - ✓ Most Secure
  - ✓ Meets Industry Standards

Can I use both together ??

- ✓ Prior to 19c
  - ✓ ORA-12696 Double Encryption Turned On

Double Encryption

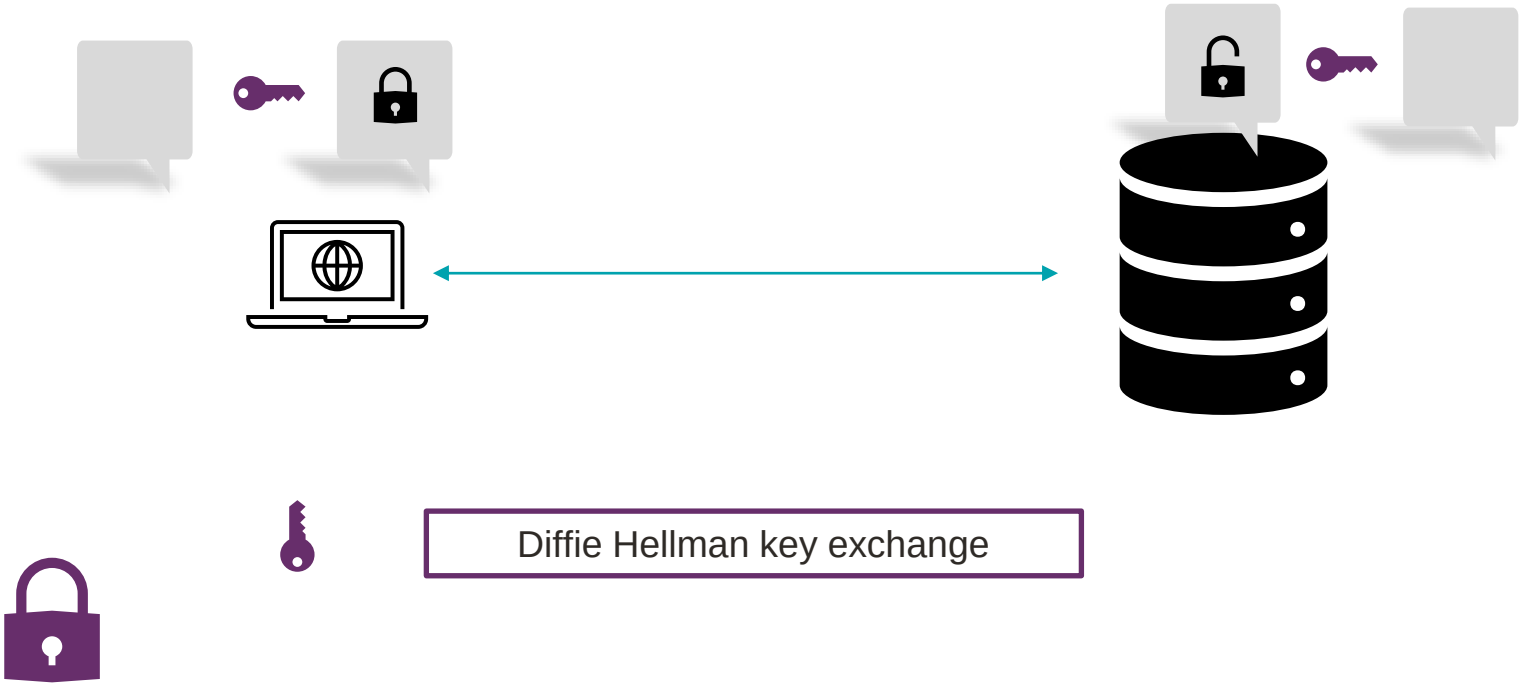
- ✓ Prior to 19c
  - ✓ ORA-12696 Double Encryption Turned On
- ✓ By default disallowed for different users
  - ✓ IGNORE_ANO_ENCRYPTION_FOR_TCPS=TRUE

Advanced Networking Option (Native Encryption)

APPENDIX

How is the session key transmitted??

How is the session key transmitted??



Appendix

- https://blog.pythian.com/oracle-secure-external-password-stores/
- How To Prevent The Secure Password Store Wallet From Being Moved to Another Host (Doc ID 1114599.1)
- RMAN-06820 ORA-17629 During Backup at Standby Site (Doc ID 1616074.1)
- https://www.slideshare.net/ncalero/ssl-certificates-in-the-oracle-database-without-surprises
- Step by Step Guide: How to Configure SSL/TLS on ORACLE RAC (with SCAN) (Doc ID 1448841.1)
- How To Investigate And Troubleshoot SSL/TLS Issues on the Database And Client SQL*Net Layer (Doc ID 2238096.1)
- https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-9EB5CE4D-AEDD-438F-A08B-60F7FC276BA0

THANK YOU !!

You can reach me

- @aishwaryakala13
- aishwarya-kala-471b3616
- oratrails.wordpress.com