Oracle® Communications

LSMS Security Guide

Release 13.5

F42044-02

April 2024

ORACLE

Oracle Communications LSMS Security Guide, Release 13.5

F42044-02

Contents

My Oracle Support (MOS)

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

Release 13.5 - F42044-02, April 2024

Updated steps 2b, 3, and 4c in Installing an SSL Certificate for LSMS from a Trusted Certificate Authority.

Release 13.5 - F42044-01, July 2021

There are no updates in this document in this release.

1 Introduction

This chapter contains general information such as an overview of the manual, how to get technical assistance, and where to find additional information.

1.1 Overview

This document provides guidelines and recommendations for configuring the Oracle Communications **LSMS** to enhance the security of the system. The recommendations herein are optional and should be considered along with the approved security strategies of your organization. Additional configuration changes that are not included herein are not recommended and may hinder the product's operation or Oracle's capability to provide appropriate support.

1.2 Scope and Audience

This manual is intended for system administrators that are installing and configuring **LSMS**.

1.3 Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

1.4 Manual Organization

This manual contains the following chapters:

- Introduction contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- LSMS Security Overview describes basic security considerations and provides an overview of **LSMS** security.
- Performing a Secure LSMS Installation describes the process to ensure a secure installation of **LSMS**.
- Implementing LSMS Security explains **LSMS** security features.
- Secure Turnover to Customer describes the secure password turnover process used to ensure security of systems delivered to our customers.

1.5 My Oracle Support (MOS)

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select 1
   - For Non-technical issues such as registration or assistance with MOS, Select 2

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

1.6 Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

1.7 Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

1.8 Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

1.9 Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

2
LSMS Security Overview

This chapter describes basic security considerations and provides an overview of **LSMS** security.

2.1 Basic Security Considerations

The following principles are fundamental to using any application securely:

- Keep software up to date
  This includes the latest product release and any patches that apply to it.
- Limit privileges as much as possible
  Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- Monitor system activity
  Establish who should access which system components, and how often, and monitor those components.
- Install software securely
  For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See Performing a Secure LSMS Installation for more information.
- Learn about and use the LSMS security features
  See Implementing LSMS Security for more information.
- Use secure development practices
  For example, take advantage of existing database security functionality instead of creating your own application security.
- Keep up to date on security information
  Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site:http://www.oracle.com/technetwork/topics/security/alerts-086861.html

When planning for security, consider the following questions:

- Which resources need to be protected?
  - You need to protect customer data, such as telephone number (TN) information and associated data.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?
  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your work flows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

- What happens if protections on strategic resources fail?
  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

2.2 Understanding the LSMS Environment

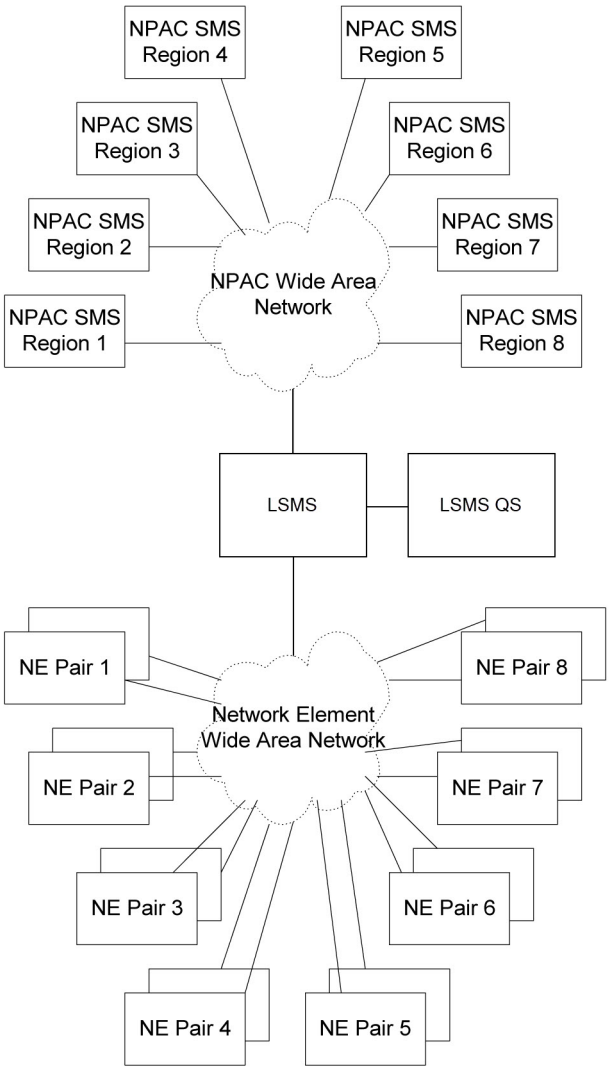
Local Number Portability (**LNP**) allows a subscriber to change location, service provider, or service while keeping the same directory number. Number portability ensures that subscribers receive the same freedom of choice for local service as they have with long-distance service providers.

These changes in telephone service enable **LNP**:

- When a subscriber is granted **LNP** service, the subscriber's telephone number is "ported" into various **LNP** databases that contain routing information. The official repository for **LNP** database information is contained in government-controlled Number Portability Administration Centers (**NPACs**). Currently, eight regional **NPACs** serve the United States and Canada.
- Central office and tandem switches no longer will use only a telephone number's **NPA**-**NXX** code (area code and local exchange code) to determine where a call should be delivered. Routing information is stored in **LNP** databases, which must be queried when any call is made to an **NPA**-**NXX** that contains one or more ported numbers.

LSMS Security Overview details how an **LSMS** serves as an interface between **NPAC** Service Management Systems (**SMSs**) and network elements (central office or tandem switches). The **LSMS** maintains a service provider's **LNP** data so that it is not necessary for each network element (**NE**) to have a direct connection with each **NPAC**. This figure shows the maximum number of **NPACs** and network elements supported by Oracle's **LSMS**.

Figure 2-1 LNP Configuration



The **LSMS** application receives **LNP** data from the **NPAC**, stores the data, and transfers the data to the correct **NE**. **LSMS** supports the following **NPACs**:

- Midwest
- MidAtlantic
- Northeast
- Southeast
- Southwest
- Western
- WestCoast
- Canada

When connected to multiple **NPACs**, **LSMS** keeps the data for each **NPAC** separate. Each **NPAC** can access data only in its corresponding regional database.

The **LSMS** is composed of hardware and software components that interact to create a secure and reliable **LNP** system.

2.3 Overview of LSMS Security

The LSMS is a secure and reliable Local Number Portability (LNP) system that enables customers to administer their LNP data in a central place.

Operating System Security

Oracle Communications Tekelec Platform (TPD) handles all operating system security for the LSMS application. Make sure you always have the latest TPD software/patches installed on your machines.

TMN Toolkit licenses and Marben OSI stack licenses must be installed for both LSMS servers. License files are obtained from NE Technologies, Inc. For information about how to obtain and install the TMN Toolkit licenses, refer to this release's *Incremental Upgrade/Installation Guide*.

GUI Security

By default, both Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS) are enabled for the GUI.

HTTPS supports encryption of data exchanged between the web server and the browser, thus facilitating data privacy. HTTP is not encrypted/secure and can be disabled. For more information, see Using Login Sessions.

Database Security

The following LSMS-specific security considerations apply to the MySQL database:

- Secure Database Access Credentials
  Only authorized personnel are allowed to access the database and a user ID and password are required.

  Provide minimum privileges to the user so that unauthorized modifications can be avoided. For more information, see Managing User Accounts.
- Use SSH/SSL Connections
  SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption. SSH/SSL provides secure data transmission through encryption keys.

  Encryption is required for the connection between the NPAC and the LSMS. The LSMS has a key for each NPAC that it services. For more information about using key lists, refer to *Configuration Guide*.
- Modify the MySQL Port for Query Servers
  Since the default MySQL port 3306 is a well-known port, to prevent eavesdropping use the LSMS GUI to change the MySQL port for query servers. For more information about modifying the MySQL port for query servers, see *Alarms and Maintenance Guide*.

SPID Security for Locally Provisioned Data

Without the optional Service Provider Identifier (SPID) Security feature, any user is able to log in using any SPID that is defined on the LSMS. The user is able to view any

data for any SPID, and depending on the user privileges that were assigned to the user, the user might even be able to change data associated with any SPID.

The SPID Security feature enables the LSMS administrator to control the users that can log on with a specified SPID. In addition, the LSMS administrator can assign special access to a user that provides access to all SPIDs; such a user is called a *golden user*.

The SPID Security feature is especially useful for LSMS customers that act as service bureaus, offering LSMS services to other service providers. The service bureau may administer locally provisioned data for a client and may choose to allow the client to administer or view its own data without allowing that client to view or change data belonging to other clients.

For more information, refer to Managing SPID Security.

Secure Network Management

LSMS can interact with Oracle Communications EAGLE Element Management System (OCEEMS) or other network management systems using secure SNMP v3 authentication and encryption. For more information, see *Alarms and Maintenance Guide*.

LSMS can interact with LSMS Query Server using TLS 1.2 encryption. For more information, see *LSMS Query Server on Linux Installation and Upgrade Guide*.

3
Performing a Secure LSMS Installation

This chapter describes the process to ensure a secure installation of LSMS.

3.1 Pre-Installation Configuration

All pre-installation configuration is set by TPD. No additional user configuration regarding security is required.

3.2 Installing LSMS Securely

The TPD Initial Product Manufacture *Software Installation Procedure* (Release 6.7.2+) ensures a secure installation of the LSMS application. All non-essential and non-secure services are removed or excluded from the default installation.

Oracle recommends using the default installation, unless there are specific customer needs for additional services.

3.3 Post-Installation Configuration

There are no required post-installation configuration changes pertaining to Security.

Establishing various network connections from the LSMS to other customer network elements is performed by using the LSMS **GUI** as documented in *Configuration Guide*.

You can disable HTTP and use only HTTPS for the GUI, so that data is encrypted when exchanged between the web server and the browser. For more information, see Using Login Sessions.

To install specific SSL certificates, including for LSMS with customized parameters and from a trusted Certificate Authority (CA) to replace a self-signed certificate, see Chapter 4, "Implementing LSMS Security."

4
Implementing LSMS Security

This chapter explains the **LSMS** security features.

4.1 Managing User Accounts

The system administrator assigns user names and passwords, and each user name is assigned to one of the following permission groups:

- lsmsall
- lsmsadm
- lsmsuser
- lsmsuext
- lsmsview

The permission groups govern which commands and which GUI functions the user is allowed to use.

> **Note:**
>
> It is possible for an individual user name to have the same value as a group name. For example, usually a user named lsmsadm is assigned to the lsmsadm permission group. Some LSMS commands require the user to be logged in with the lsmsadm user name.

For more information about managing user accounts, refer to the *Alarms and Maintenance Guide*.

4.2 Managing Password Security

By default, the LSMS does not provide any password expiration limit. The password expiration limit must be set by the system administrator using the LSMS GUI.

You can set the limit for password expiration from 1-180 days. After a password expires, the user cannot log in without changing the password.

For more information about setting password timeout values, refer to *Alarms and Maintenance Guide*.

4.3 Managing SPID Security

Association of a user name with a SPID enables the LSMS system administrator to restrict access to the following types of locally provisioned data:

- Default global title translation (GTT)

- Override GTT
- GTT groups
- Telephone number (TN) filters
- Assignment of GTT groups and TN filters to an element management system (EMS)

Accessibility to these types of data is protected by SPID Security for any access method (for example, through the GUI, or through input data by file, audit, and reconcile).

The optional SPID Security feature is activated by Oracle customer service using secure activation procedures. After the feature is activated, the LSMS system administrator is advised to immediately define associations between user names and SPIDs. For information about associating user names with SPIDs, refer to *Alarms and Maintenance Guide*.

4.4 Modifying the MySQL Port

This optional feature enhances the security of LSMS databases by enabling the system administrator to change the MySQL port. By default, MySQL uses port 3306, and because this is a well-known port you should change it.

Through the LSMS GUI, the MySQL port can be configured to ports 34000-34099. The port can be maintained through the GUI, and any changes to the port setting will raise an alarm on the LSMS. The MySQL port can also be changed back to the default port if necessary.

For information about how to modify the MySQL port, refer to *Alarms and Maintenance Guide*.

4.5 Using Login Sessions

You can log into the LSMS command line or the LSMS GUI to configure and maintain the LSMS system.

- You can access the command line from any terminal that has the Secure Shell (ssh) client installed.
  If your terminal does not already have ssh installed, PuTTY (Oracle does not make any representations or warranties about this product) is an open source ssh utility for Windows that you can download from the web.
- You can access the GUI through a web browser if you activate the optional IP User Interface feature.
  If you have not activated the IP User Interface feature, you can establish a login session first from an X-windows compatible terminal and then start a GUI session.

  By default, both HTTP and HTTPS are enabled for the GUI. The lsmsadm user can disable HTTP using the following command at the LSMS command line:

  ```
  lsmsadm@lsmspri bin]$ httpConfig.pl https
  ```

  The `httpConfig.pl` script is located in the `/usr/TKLC/lsms/bin` directory.

You must have a user ID and password before you can log in to LSMS.

For more information about using login sessions, refer to *Alarms and Maintenance Guide*.

4.6 Installing an SSL Certificate for LSMS With Customized Parameters

Perform the following steps to install a certificate with customized parameters:

1. Sign the certificates on the LSMS A server:
   a. Log in to the LSMS A server as admusr.
   The certificate files have been generated for the same IP.

   Sign both certificate files with the same IP using the following command:

   ```
   sudo /usr/bin/openssl req -x509 -sha<SHA Hash> -nodes -days <No of
   days to certify the certificate for, after which the certificate
   shall expire> -subj "/CN=<LSMS A GUI IP address >" -newkey rsa:<RSA
   Key Management> -keyout /usr/TKLC/plat/etc/ssl/server.key -out /usr/
   TKLC/plat/etc/ssl/server.crt
   ```

2. Sign the certificates on the LSMS B server.
   Execute the same scenario that is executed on the LSMS A server.
3. Restart the httpd service on both the LSMS A and B servers using the following command:

   ```
   [admus    r@mps-A ~]$ sudo service httpd restart
   [admusr@mps-B ~]$ sudo service httpd restart
   ```

4. Open the LSMS A and B GUI using https and Install the SSL Certificate.
   Use the following command to open LSMS GUI using Active server IP:

   ```
   https://<LSMS Active GUI IP>
   ```

5. Verify that the certificate is installed successfully and the LSMS A and B GUI is opened successfully.
6. Copy key and cert files for the `tpdProvd` process running on Port `20000`.

   ```
   cp /usr/TKLC/plat/etc/ssl/server.key /usr/TKLC/plat/etc/ssl/server.pem
   cp /usr/TKLC/plat/etc/ssl/server.crt /usr/TKLC/plat/etc/ssl/server.cert
   ```

7. Restart the `tpdProvd` process by killing the existing process and letting it restart.

   ```
   ps -eaf | grep tpdProvd
   Output:
   tpdProvd 13468     1  0 03:42 ?        00:00:04 /usr/TKLC/plat/bin/
   tpdProvd
   kill -9 <pid>
   Example: kill -9 13468
   Run ps again to check process is restarted
   ps -eaf | grep tpdProvd
   Output:
   ```

```
tpdProvd  9090     1  3 04:09 ?        00:00:00 /usr/TKLC/plat/bin/
tpdProvd
```

8. Repeat Steps 6 and 7 on LSMS B, as well.

4.7 Installing an SSL Certificate for LSMS from a Trusted Certificate Authority

Perform the following steps to install an SSL certificate from a trusted Certificate Authority (CA):

1. Log in as the root user on both the LSMS A and B servers, create a new directory in the root directory, and change to that new directory.
   In the following example, a `certificate` directory is created:

   ```
    [admusr@mps-A ~]$ pwd
   /home/admusr
   [admusr@mps-A ~]$ sudo mkdir /var/TKLC/lsms/free/certificate
   ```

   Give permissions to the new directory:

   ```
   [admusr@mps-A ~]$ sudo chmod 777 /var/TKLC/lsms/free/certificate
   ```

   Move to the new directory using the following command:

   ```
   [admusr@mps-A ~]$ cd /var/TKLC/lsms/free/certificate
   ```

2. Generate certificate signing request (CSR) and private key files for the LSMS A server using the following commands from within the `certificate` directory.

   a. Enter the following commands on the LSMS A server:

   ```
   sudo /usr/bin/openssl req -x509 -sha<SHA Hash> -nodes -days <No
   of days to certify the certificate for, after which the
   certificate shall expire > -newkey rsa:2048 -nodes -keyout
   server.key -out server.csr -subj "/C=US/ST=New York/L=Brooklyn/
   O=Example Brooklyn Company/OU=Example Org Unit/CN=<LSMS GUI IP
   address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
   ```

   > **Note:**
   >
   > The -subj option in the previous commands has example fields, which must be replaced with your organization-specific domain information.
   > /C = Country, /ST = State, /L = Location, /O = Oganization, /OU = Organizational Unit, /CN = Common Name Field which is the IP address or fully-qualified domain name that you want to use with your certificate.

These commands generate the following files on the LSMS A server:

```
[admusr@mps-A certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:08 server.key
-rw-r----- 1 root root 968 May 21 11:08 server.csr
```

b. Enter the following commands on the LSMS A server:

```
sudo /usr/bin/openssl req -x509 -sha -nodes -days -newkey rsa:2048 -
nodes
      -keyout server.key -out secserver.csr -subj "/C=US/ST=New York/
L=Brooklyn/ O=Example
      Brooklyn Company/OU=Example Org Unit/CN=/
emailAddress=xxx@yyy.com"
```

The following files will be generated on the LSMS B server:

```
[admusr@mps-B certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:02 server.key
-rw-r----- 1 root root 968 May 21 11:02 secserver.csr
```

3. Send the generated CSR files `server.csr` and `secserver.csr` to the CA. The CA will provide signed certificate files `server.crt` and `secserver.crt` in return.
4. Copy the appropriate files to the appropriate ssl directory, and rename (in the B server only) as needed:
   a. On the LSMS A server, copy the two files generated through the openssl commands (`server.key` and `server.csr`) and the files provided by the CA (`server.crt`) to the `/usr/TKLC/plat/etc/ssl` directory.
   b. On the LSMS B server, copy the two files generated through the openssl command (`server.key` and `secserver.csr`) and the file provided by the CA for the LSMS B server (`secserver.crt`) to the `/usr/TKLC/plat/etc/ssl` directory.
   c. After copying `secserver.crt` to the `/usr/TKLC/plat/etc/ssl` directory on the LSMS B server, rename it to `server.crt`.
5. Restart the httpd service on both the LSMS A and LSMS B servers using the following command:

```
[admusr@mps-A certificate]$ sudo service httpd restart
[admusr@mps-B certificate]$ sudo service httpd restart
```

6. Open the LSMS A and B GUI using https and install the SSL Certificate.
   Use the following command to open LSMS Active GUI:

```
https://<LSMS Active GUI IP>
```

7. Verify that the certificates installed successfully and the LSMS A and B GUI opened successfully.
8. If the LSMS GUI does not open, follow these steps on the LSMS A and B servers:

a. Open the `/etc/httpd/conf.d/ssl.conf` file:

```
[admusr@mps-A certificate]$ sudo vi /etc/httpd/conf.d/ssl.conf
```

b. Edit `/etc/httpd/conf.d/ssl.conf` and un-comment the appropriate code:

- If the CA provides `ca.crt` (CA intermediate certificate), change from:

```
#SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
to
SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
```

- If the CA provides CA certificate(s), change from:

```
#SSLCACertificatePath /etc/httpd/conf/ca-cert
#SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
to
SSLCACertificatePath /etc/httpd/conf/ca-cert
SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
```

c. Make sure that these files (CA certs) are copied to the right path on both servers, as mentioned in `/etc/httpd/conf.d/ssl.conf`.

d. Restart the httpd service using the following command on both servers:

```
[admusr@mps-A certificate]$ sudo service httpd restart
[admusr@mps-B certificate]$ sudo service httpd restart
```

e. Verify that the LSMS A GUI opens successfully.

9. Copy key and cert files for the `tpdProvd` process running on Port `20000`.

```
cp /usr/TKLC/plat/etc/ssl/server.key /usr/TKLC/plat/etc/ssl/
server.pem
cp /usr/TKLC/plat/etc/ssl/server.crt /usr/TKLC/plat/etc/ssl/
server.cert
```

10. Restart the `tpdProvd` process by killing the existing process and letting it restart.

```
ps -eaf | grep tpdProvd
Output:
tpdProvd 13468     1  0 03:42 ?        00:00:04 /usr/TKLC/plat/bin/
tpdProvd
kill -9 <pid>
Example: kill -9 13468
Run ps again to check process is restarted
ps -eaf | grep tpdProvd
Output:
tpdProvd  9090     1  3 04:09 ?        00:00:00 /usr/TKLC/plat/bin/
tpdProvd
```

11. Repeat Steps 9 and 10 on LSMS B, as well.

4.8 Installing an SSL Certificate for VIP With Customized Parameters

Perform the following steps to install the certificate for VIP with customized parameters.

1. Sign the certificate on the LSMS A server.
   Sign the certificate file using the following command:

   ```
   sudo /usr/bin/openssl req -x509 -sha<SHA Hash> -nodes -days <No of days
   to certify the certificate for, after which the certificate shall expire>
   -subj "/CN=<LSMS A VIP  address >" -newkey rsa:<RSA Key Management> -
   keyout /usr/TKLC/plat/etc/ssl/server_vip.key -out /usr/TKLC/plat/etc/ssl/
   server_vip.crt
   ```

2. Sign the certificates on the LSMS B server:
   Execute the same scenario that is executed on LSMS A.
3. Restart the httpd service on both the LSMS A and B servers using the following command:

   ```
   [admusr@mps-A ~]$ sudo service httpd restart
   [admusr@mps-B ~]$ sudo service httpd restart
   ```

4. Open the GUI using VIP IP using https and Install the SSL Certificate.
   Use the following command to open the GUI using VIP IP:

   ```
   https://<LSMS  VIP  IP>
   ```

5. Verify that the certificate is installed successfully and the GUI is opened successfully.

4.9 Installing an SSL Certificate for VIP from a Trusted Certificate Authority

Perform the following steps to install an SSL certificate from a trusted Certificate Authority (CA).

1. Log in as admusr on both LSMS A and B servers.
2. Generate certificate signing request (CSR) and private key files for the LSMS A server using the following commands from within the certificate directory.
   Enter the following commands on the LSMS A server:

   ```
   sudo /usr/bin/openssl req -x509 -sha<SHA Hash> -nodes -days <No of days
   to certify the certificate for, after which the certificate shall expire
   > -newkey rsa:2048 -nodes -keyout server_vip.key -out server_vip.csr -
   subj "/C=US/ST=New York/L=Brooklyn/O=Example Brooklyn Company/OU=Example
   Org Unit/CN=<LSMS VIP IP address>/emailAddress=xxx@yyy.com"
   ```

> **Note:**
>
> The -subj option in the previous commands has example fields, which must be replaced with your organization-specific domain information. /C = Country, /ST = State, /L = Location, /O = Oganization, /OU = Organizational Unit, /CN = Common Name Field which is the IP address or fully-qualified domain name that you want to use with your certificate.

These commands generate the following files on the LSMS A server:

```
These commands generate the following files on the LSMS A server:
[admusr@mps-A certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:08 server_vip.key
-rw-r----- 1 root root 968 May 21 11:08  server_vip.csr
```

3. Generate the CSR and private key files for the LSMS B server by executing steps 1 - 3. Execute the same scenario that is executed on the LSMS A server from step 2 on the LSMS B server. Use the `server_vip.csr` and `serverB_vip.csr` files for the LSMS B server.
   The following files will be generated on the LSMS B server:

   ```
   [admusr@mps-B certificate]$ ls -lrt
   -rw-r--r-- 1 root root 1679 May 21 11:02 server_vip_v4.key
   -rw-r--r-- 1 root root 968 May 21 11:02  serverB_vip_v4.csr
   ```

4. Send the generated CSR files (`server_vip.csr`, `serverB_vip.csr`) to the CA. The CA will provide signed certificate files (`server_vip.crt`, `serverB_vip.crt`) in return.
5. Copy the appropriate files to the appropriate ssl directory, and rename as needed:
   a. On the LSMS A server, copy the two files generated through the openssl commands (`server_vip.key` and `server_vip.csr`) and the files provided by the CA (`server_vip.crt`) to the `/usr/TKLC/plat/etc/ssl` directory.
   b. On the LSMS B server, copy the two files generated through the openssl command (`server_vip.key` and `secserverB_vip.csr`) and the file provided by the CA for the LSMS B server (`secserverB_vip.crt`) to the `/usr/TKLC/plat/etc/ssl` directory.
   c. After copying `secserverB_vip.crt` to the `/usr/TKLC/plat/etc/ssl` directory on the LSMS B server, rename it to `server_vip.crt`.
6. Restart the httpd service on both the LSMS A and LSMS B servers using the following command:

   ```
   [admusr@mps-A certificate]$ sudo service httpd restart
   [admusr@mps-B certificate]$ sudo service httpd restart
   ```

7. Open the LSMS GUI using VIP IP using https and install the SSL Certificate. Use the following command to open LSMS GUI using VIP IP:

   ```
   https://<LSMS VIP  IP>
   ```

8. Verify that the certificates installed successfully and the LSMS A and B GUI opened successfully.
9. If the LSMS GUI does not open, follow these steps on the LSMS A and B servers:
   a. Open the `/etc/httpd/conf.d/ssl.conf` file:

      ```
      [admusr@mps-A certificate]$ sudo vi /etc/httpd/conf.d/ssl.conf
      ```

   b. Edit `/etc/httpd/conf.d/ssl.conf` and un-comment the appropriate code:
      - If the CA provides `ca.crt` (CA intermediate certificate), change from:

        ```
        #SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
        to
        SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
        ```

      - If the CA provides CA certificate(s), change from:

        ```
        #SSLCACertificatePath /etc/httpd/conf/ca-cert
        #SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
        to
        SSLCACertificatePath /etc/httpd/conf/ca-cert
        SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
        ```

   c. Make sure that these files (CA certs) are copied to the right path on both servers, as mentioned in `/etc/httpd/conf.d/ssl.conf`.
   d. Restart the httpd service using the following command on both servers:

      ```
      [admusr@mps-A certificate]$ sudo service httpd restart
      [admusr@mps-B certificate]$ sudo service httpd restart
      ```

   e. Verify that the LSMS GUI opens successfully.

A

Secure Turnover to Customer

To ensure security of systems delivered to our customers and to satisfy Oracle policies, all passwords must be owned by the customer once transfer of ownership of systems has occurred.

A.1 Secure Turnover Process

Three key requirements address the fundamental principles of the secure turnover process:

- Oracle default passwords shall not remain on fielded systems.
- Oracle default passwords shall not be revealed to customers.
- Customer installed passwords shall not be known by Oracle.

Goals of the Secure Turnover Process

Following are the goals of the password handoff process:

1. Install the system securely with Oracle internal default passwords (passwords exclusively known and used by Oracle personnel).
2. Change the special account passwords during the installation process to a unique value (meeting password complexity rules required by the system).
3. Provide a non-repudiation process for the customer agent to set all special passwords.

Secure Turnover Procedure

Perform the following steps for secure system turnover:

1. System servers are installed by Oracle personnel using common ISO deliverables and installation procedures. The OS root password, OS admusr password, and the passwords for the default LSMS login accounts (lsmsadm, lsmsmgr, and platcfg) are from the build process, and are private and known only by Oracle.
2. Following installation, the Oracle installer performs a login to each server OS (real and virtual) as admusr and changes the password to a new unique secure password. The Oracle installer then switches user to root and changes the root password to a new unique password.
3. The Oracle installer uses a web browser to log in to the application on each relevant server using each default LSMS login name (such as lsmsadm) and changes the password to a new unique password.
4. As a precursor to the official handoff of the system (all servers) to the customer, the Oracle installer ensures that the new unique passwords for root, admusr, and default LSMS login accounts have been securely given to the authorized customer agent.
5. The authorized customer agent is instructed to log in to each OS account on each server (real and virtual) and change the password for accounts admusr and root to the authorized operational setting for the customer.

6. The customer agent is instructed to use a web browser to log in to each relevant application server and change the password for the default LSMS login accounts to the authorized operational password for the customer.
7. Following the entry of the new passwords by the customer agent, the Oracle installer or authorized Oracle agent attempts to log in to each server using the previously known password. This should result in a failed login attempt verifiable in the server logs.
8. The customer agent again logs in to each OS account and the default LSMS login accounts using the new customer passwords to verify success with the new customer passwords.