

VPSX<sup>®</sup>

## VPSX Best Practices

### CERTIFICATES FOR HA

Version: 1.0



**Enterprise  
Output Management**




## **Abstract**


This document is a general discussion on the Best Practices in implementing the VPSX output management server component of the LRS Enterprise Output Server in a Highly Available environment.

Copyright 2019 Levi, Ray & Shoup, Inc.

Creation Date: 05/20/2019

Author: JKW

LRS, , VPS, VPSX, VPSX/OutputManager, and PageCenterX are registered trademarks of Levi, Ray & Shoup, Inc.

LRS and  are service marks of Levi, Ray & Shoup, Inc.

All other brand and product names are trademarks or service marks of their respective holders

## Revisions

---

<b>Date:</b>	<b>Version:</b>	<b>Revised By:</b>
05/20/2019	0.0	JKW
05/21/2019	1.0	JKW

## **Executive Summary**

---

This Systems Engineering Techtip discusses “Best Practices” in the installation, configuration, and use of LRS Enterprise Output Management (EOM) products. Specifically, this document addresses the use, configuration, and placement of Certificates in a High Availability environment with VPSX and MFPsecure.

This is considered a “living document” and will be updated periodically as new information arises and new lessons are learned.

## Table of Contents

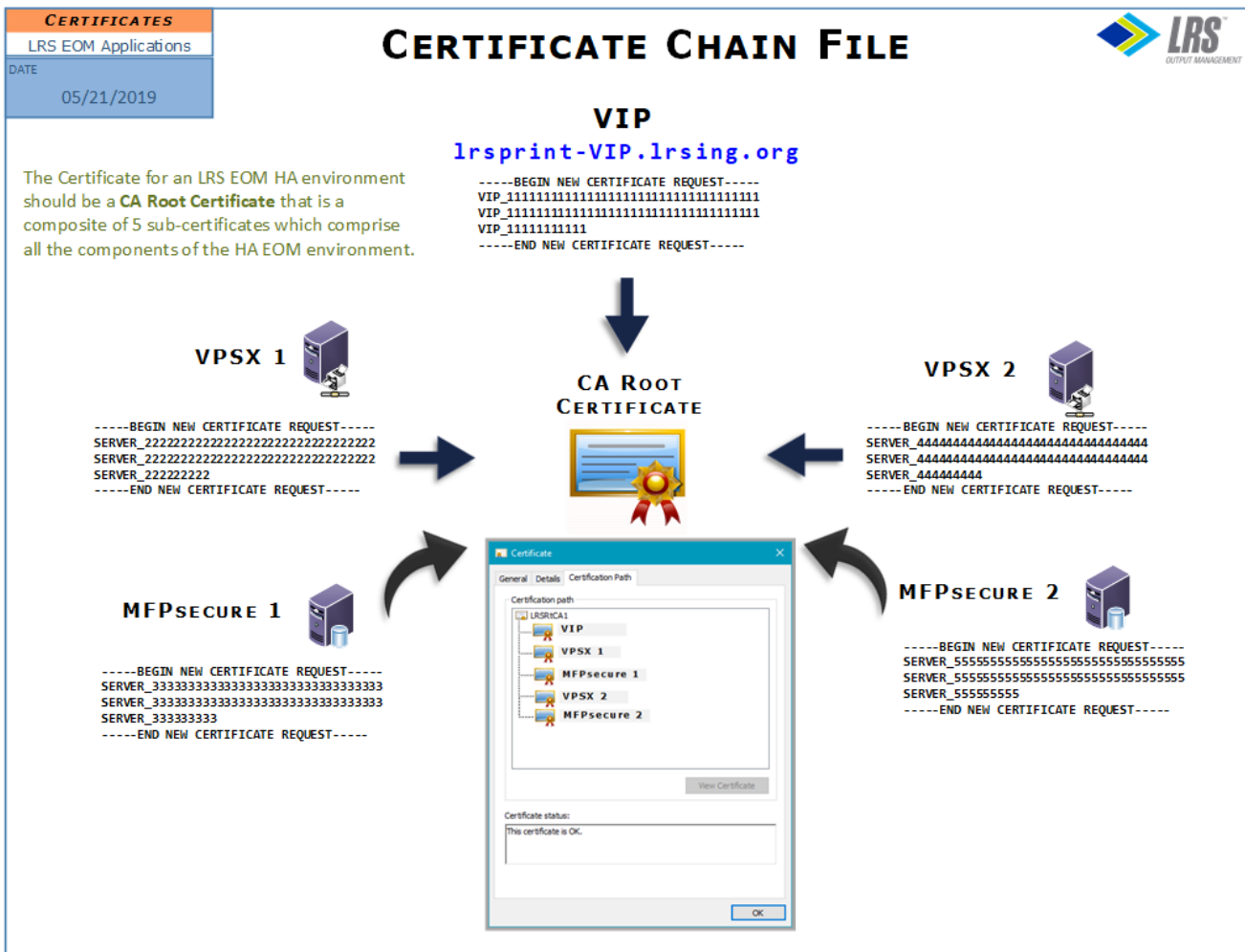
Revisions.....	1
Executive Summary.....	2
<b>VPSX – Certificate Chain File .....</b>	<b>4</b>
Create a Certificate Chain File .....	4
Configuration Options .....	4
<b>VPSX – Subject Alternate Name.....</b>	<b>5</b>
Recommendation for Subject Alternate Name Field Content.....	5
Configuration Options .....	5
<b>VPSX – Certificate Placement for HA.....</b>	<b>6</b>
Certificate Placement .....	6
Configuration Options .....	7
MFPsecure Certificate Naming Convention.....	7

**VPSX – CERTIFICATE CHAIN FILE**

**CREATE A CERTIFICATE CHAIN FILE**

A Certificate Chain File contains a concatenation of all the Certificate Signing Requests (CSRs) for all the individual servers in the EOM HA Group. The concatenated CSR Chain File is added to the Root Certificate as depicted below.

The individual servers are displayed on the Certification Path Tab of the resulting Root Certificate (.cer file) and this .cer file is now used for all the servers within the group.



**CONFIGURATION OPTIONS**

In this example, we assume that MFPsecure is part of the EOM configuration and that MFPsecure resides on separate servers. If MFPsecure resides on the same server as VPSX, then it is only necessary to add the VPSX servers to the Certificate Chain File.

# VPSX – SUBJECT ALTERNATE NAME

## RECOMMENDATION FOR SUBJECT ALTERNATE NAME FIELD CONTENT

It is strongly recommended that the Root Certificate used for the LRS EOM HA environment should utilize the Subject Alternate Name rather than simply using the Common Name (CN = ) field as is standard practice by many organizations.

The Subject Alternate Name field should include (depicted in the graphic below):

- The VIP name – Fully qualified.
- The individual EOM Server names – Fully qualified.
- The VIP IP address.
- The individual EOM Server IP addresses.


**CERTIFICATES**

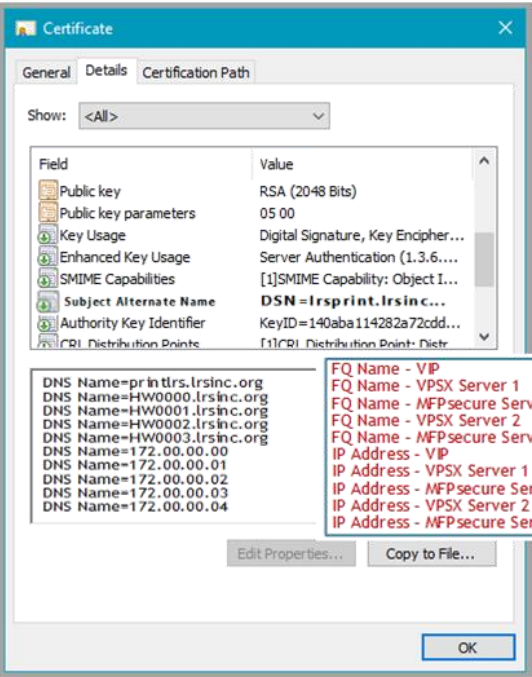
LRS EOM Applications

DATE

05/21/2019

## SUBJECT ALTERNATE NAME PROPERTIES





**Subject Alternate Name (SAN) Field**

**NOTE:**

All the entries in the SAN Field begin with "DNS Name=" regardless of type of entry. Fully Qualified DNS Names and Server IP Addresses both begin with "DNS Name=".

## CONFIGURATION OPTIONS

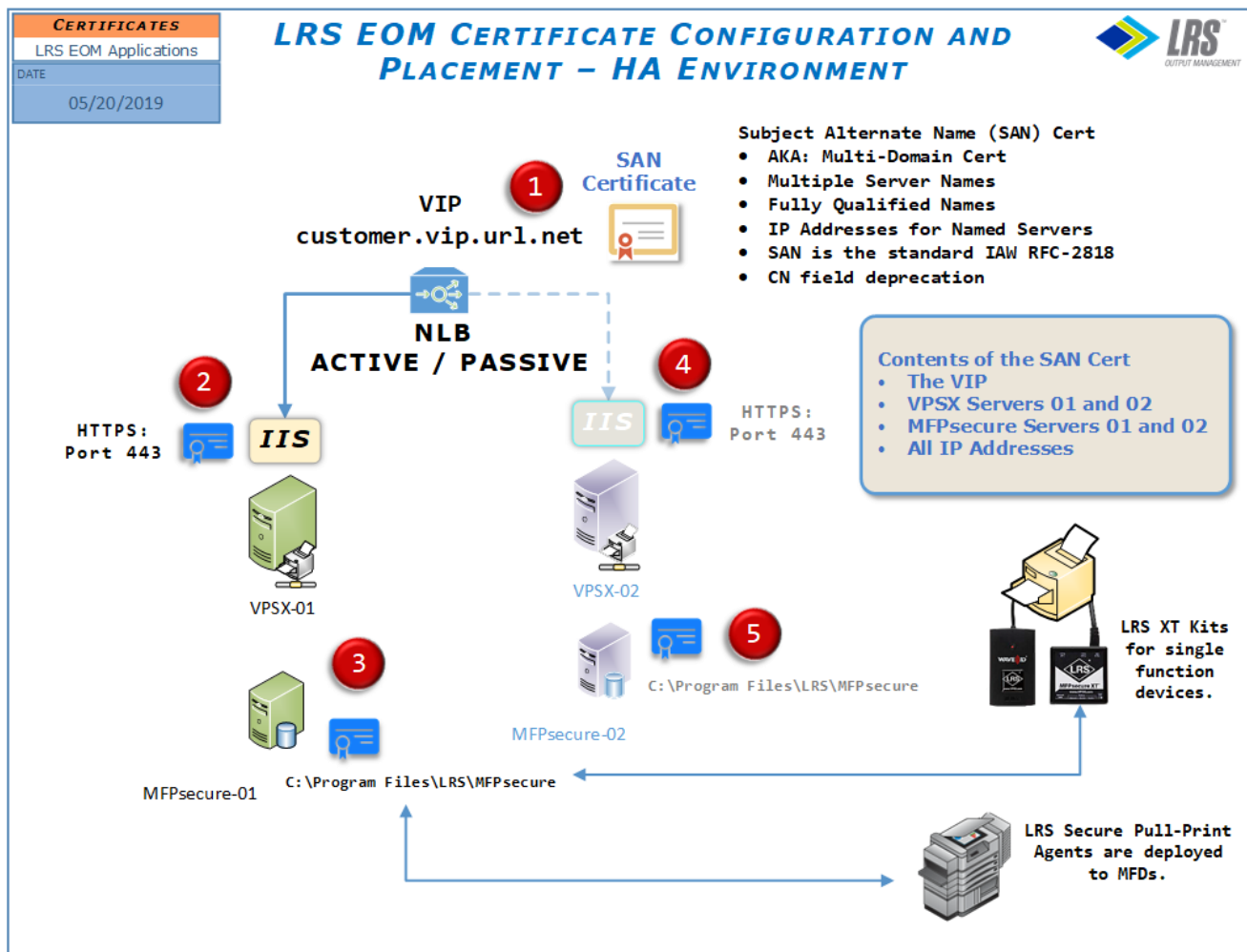
If VPSX and MFPsecure reside on the same server, it is only necessary to add the VPSX server information to the SAN field.

# VPSX – CERTIFICATE PLACEMENT FOR HA

## CERTIFICATE PLACEMENT

Once the new Root SAN Certificate has been created, it should be distributed to the following locations:

- On the NLB servicing the EOM HA environment. The exact location of the certificate will be determined by the type of NLB in use.
- Bound to IIS for each of the VPSX nodes in the HA configuration (nominally two servers).
- Assuming that MFPsecure is part of the HA environment, two copies of the .cer file should be placed in the following directory:
  - ♦ C:\Program Files\LRS\MFPsecure\
- The copies of the Certificate should be Re-Named according to the following guidance:
  - ♦ One copy named according to the Fully Qualified Domain name of the MFPsecure server.
  - ♦ One copy named according to the IP Address of the MFPsecure server.





**CONFIGURATION OPTIONS**

If VPSX and MFPsecure reside on the same server, the SAN Certificate must still be placed in two locations on the VPSX servers:

- 1.) Bound to IIS.
- 2.) Two copies of the certificate deposited in the **\Program Files\** directory referenced above, using the naming convention, also referenced above.

**MFPSECURE CERTIFICATE NAMING CONVENTION EXAMPLE**

The content of the Root CA SAN Certificate files in the examples below should be the same as those placed in other EOM locations. Simply change the names of the certificate files to reflect the Fully Qualified Name and IP Address of the MFPsecure servers where they reside.

<b>Primary HA MFPsecure Server</b>	
<b>Location:</b>	<b>C:\Program Files\LRS\MFPsecure\</b>
<b>File 1</b>	<b>IIS Mfpsecure-01.lrsinc.org.cer</b>
<b>File 2</b>	<b>IIS 172.0.0.02.cer</b>
<b>Secondary HA MFPsecure Server</b>	
<b>Location:</b>	<b>C:\Program Files\LRS\MFPsecure\</b>
<b>File 1</b>	<b>IIS Mfpsecure-02.lrsinc.org.cer</b>
<b>File 2</b>	<b>IIS 172.0.0.04.cer</b>