Innovapptive - SMP Certificate Renewal Procedure

Doc. Version: 1.0

Table of Contents

Product Information 3
Prerequisites 3
Overview 3
Procedure 3
  Backing up existing keystore file 4
  Deleting the existing certificate 4
  Creation of new self-signed Certificate 5
  Importing the new certificate to Keystore 5
  Validating renewal of Certificate. 5
Results 7
Document Revision History 7

Product Information

This document covers the information on how to renew SMP server certificate.

Pre-requisites

For SMP Certificate renewal, the following prerequisites and components should be installed.

Please validate before we start:

- **System and Software**
    - SAP Mobile Platform
    - SAP Gateway System
- **Access**
    - Access to SMP system as an administrator
- **Assumptions**
    - You have access to SMP Admin portal
    - Keystore Password

Overview

During installation of the SMP 3.0 server, it will automatically generate a self-signed certificate that will be used for mutual authentication between SMP and Gateway system. This certificate will be based on the fully qualified domain name at the time of the installation and tend to expire in few years.

This document outlines the steps needed to renew the certificate using the Java keytool utility. For the process mentioned in this document we need Keystore password you specified during the installation of the SMP 3.0 server to perform these steps. The commands in this document assume the SMP JAVA directory is in your path and that you are executing the commands from the \sap\MobilePlatform3\Server\configuration

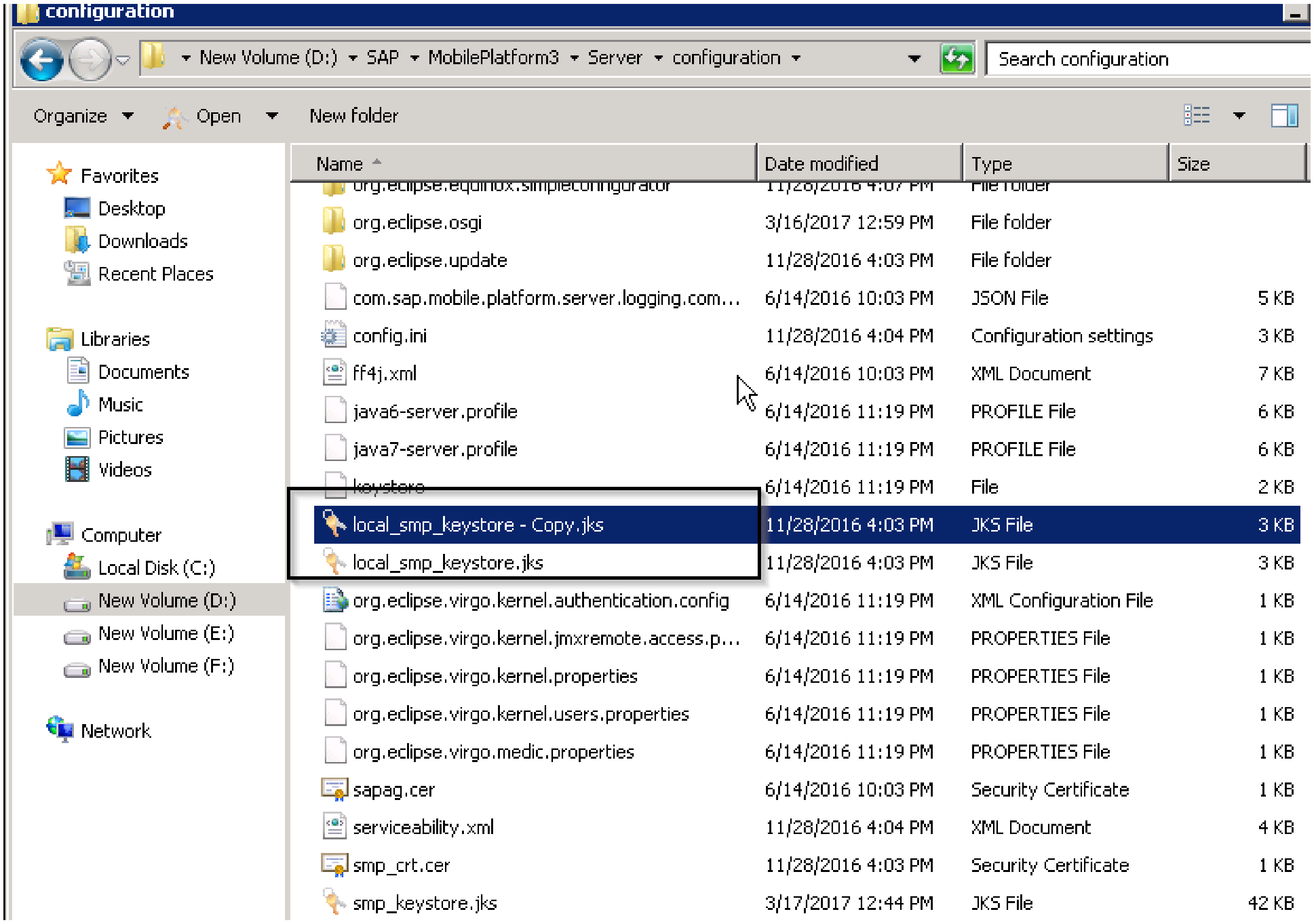
Procedure

In the commands you should mention the keystore filename and with the release of SP 08 the keystore filename where the certificate is stored has changed.

Keystore filename with less than SP 08 is smpkeystore.jks
keystore filename with SP 08 or higher is local_smpkeystore.jks

Backing up existing keystore file

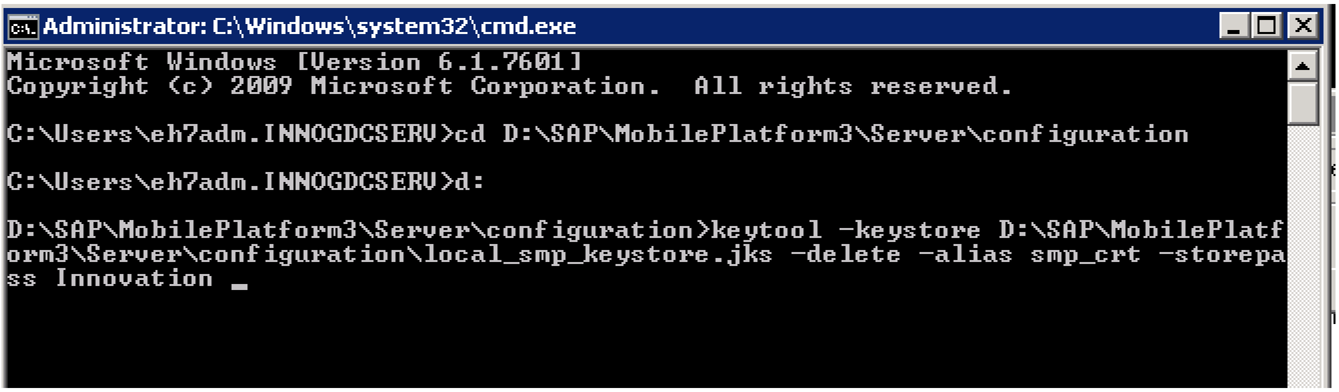
→ In the SMP server goto \sap\MobilePlatform3\Server\configuration
→ Backup the keytore file.



Name	Date modified	Type	Size
org.eclipse.equinox.simpleconfigurator	11/28/2016 4:07 PM	File folder	
org.eclipse.osgi	3/16/2017 12:59 PM	File folder	
org.eclipse.update	11/28/2016 4:03 PM	File folder	
com.sap.mobile.platform.server.logging.com...	6/14/2016 10:03 PM	JSON File	5 KB
config.ini	11/28/2016 4:04 PM	Configuration settings	3 KB
ff4j.xml	6/14/2016 10:03 PM	XML Document	7 KB
java6-server.profile	6/14/2016 11:19 PM	PROFILE File	6 KB
java7-server.profile	6/14/2016 11:19 PM	PROFILE File	6 KB
keystore	6/14/2016 11:19 PM	File	2 KB
local_smp_keystore - Copy.jks	11/28/2016 4:03 PM	JKS File	3 KB
local_smp_keystore.jks	11/28/2016 4:03 PM	JKS File	3 KB
org.eclipse.virgo.kernel.authentication.config	6/14/2016 11:19 PM	XML Configuration File	1 KB
org.eclipse.virgo.kernel.jmxremote.access.p...	6/14/2016 11:19 PM	PROPERTIES File	1 KB
org.eclipse.virgo.kernel.properties	6/14/2016 11:19 PM	PROPERTIES File	1 KB
org.eclipse.virgo.kernel.users.properties	6/14/2016 11:19 PM	PROPERTIES File	1 KB
org.eclipse.virgo.medic.properties	6/14/2016 11:19 PM	PROPERTIES File	1 KB
sapag.cer	6/14/2016 10:03 PM	Security Certificate	1 KB
serviceability.xml	11/28/2016 4:04 PM	XML Document	4 KB
smp_crt.cer	11/28/2016 4:03 PM	Security Certificate	1 KB
smp_keystore.jks	3/17/2017 12:44 PM	JKS File	42 KB

Deleting the existing certificate

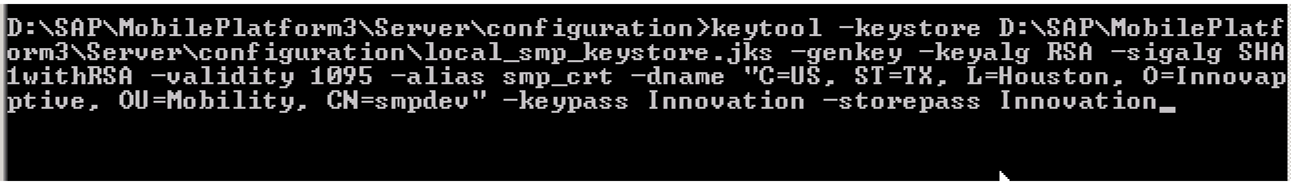
➔ keytool -keystore <location and keystore filename.jks> -delete -alias smp_crt -storepass <keystore password>



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\eh7adm.INNOGDCSERV>cd D:\SAP\MobilePlatform3\Server\configuration

C:\Users\eh7adm.INNOGDCSERV>d:

D:\SAP\MobilePlatform3\Server\configuration>keytool -keystore D:\SAP\MobilePlatf
orm3\Server\configuration\local_smp_keystore.jks -delete -alias smp_crt -storepa
ss Innovation _
```

Creation of new self-signed Certificate

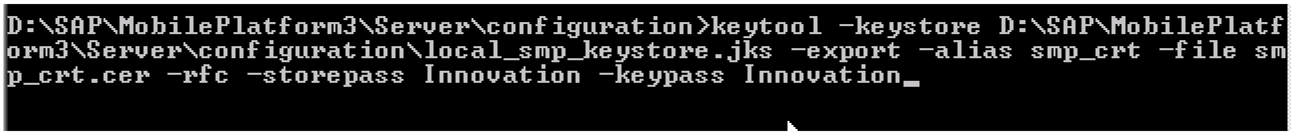
- ➔ keytool -keystore <location and keystore filename.jks> -genkey -keyalg RSA -sigalg SHA1withRSA -validity 1095 -alias smp_crt -dname “<C=country, ST=state, L=city, O=org, OU=orgunit, CN=SMPDomainName>” -keypass <keystore password> -storepass <keystore password>



```
D:\SAP\MobilePlatform3\Server\configuration>keytool -keystore D:\SAP\MobilePlatf
orm3\Server\configuration\local_smp_keystore.jks -genkey -keyalg RSA -sigalg SHA
1withRSA -validity 1095 -alias smp_crt -dname "C=US, ST=TX, L=Houston, O=Innovap
ptive, OU=Mobility, CN=smpdev" -keypass Innovation -storepass Innovation_
```

Importing the new certificate to Keystore

- ➔ keytool -keystore <location and keystore filename.jks> -export -alias smp_crt -file smp_crt.cer -rfc -storepass <keystore password> -keypass <keystore password>

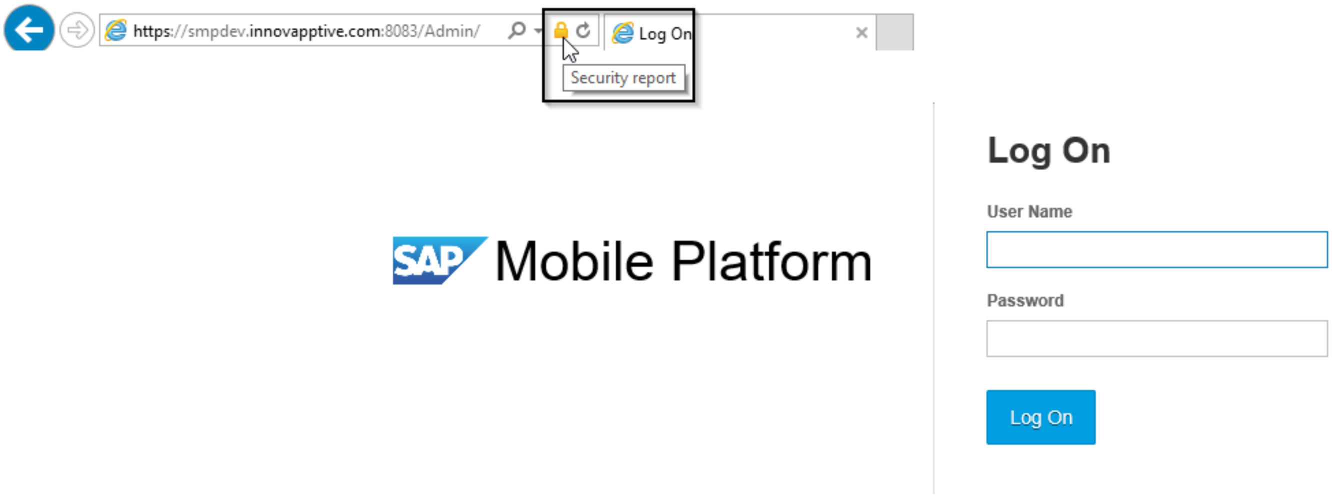


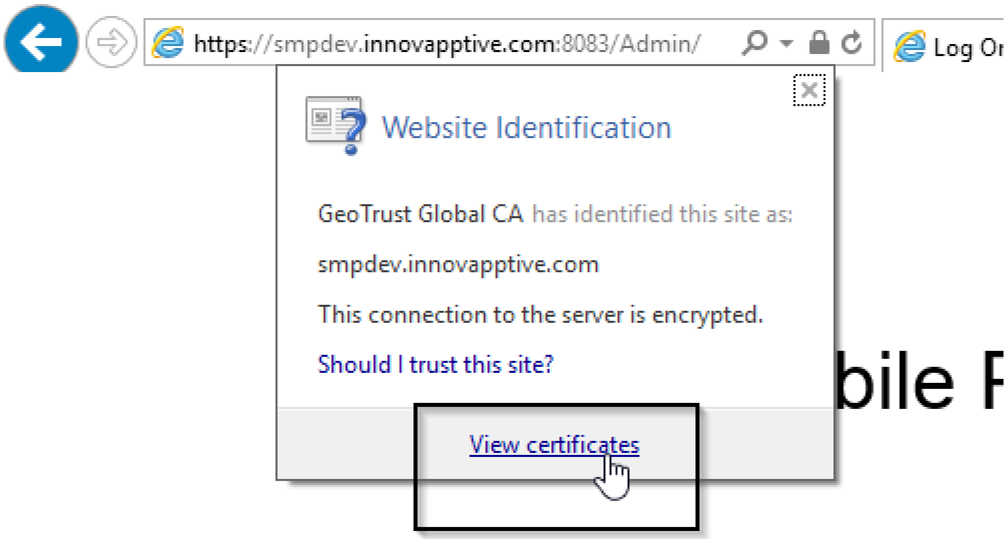
```
D:\SAP\MobilePlatform3\Server\configuration>keytool -keystore D:\SAP\MobilePlatf
orm3\Server\configuration\local_smp_keystore.jks -export -alias smp_crt -file sm
p_crt.cer -rfc -storepass Innovation -keypass Innovation_
```

After the new certificate is imported in the keystore restart the SMP server.

Validating renewal of Certificate.

- ➔ Use Internet explorer and open SMP Admin console.
  https://< hostname >:8083/Admin/
- ➔ Click on the security report as shown in below image
- ➔ View certificates to see the validity of new SMP certificate.





Website Identification

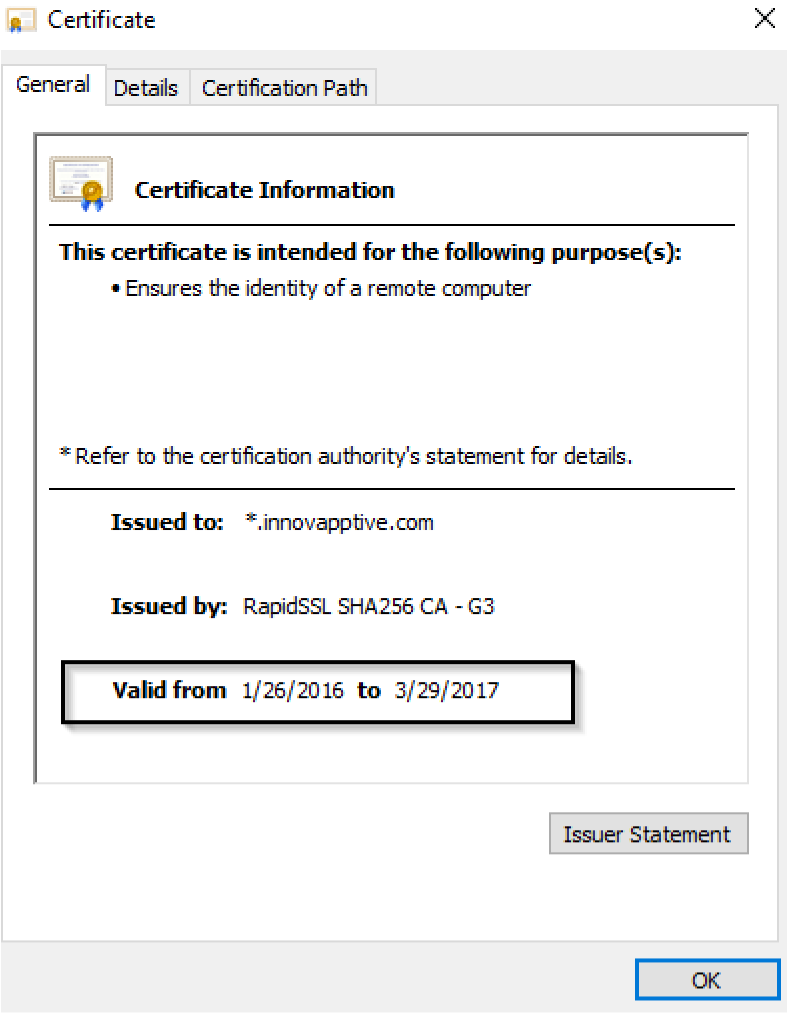
GeoTrust Global CA has identified this site as:

smpdev.innovapptive.com

This connection to the server is encrypted.

Should I trust this site?

View certificates


Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.innovapptive.com

Issued by: RapidSSL SHA256 CA - G3

Valid from 1/26/2016 **to** 3/29/2017

End of Procedure

Results

SAP Mobile Platform System default certificate validity is extended and can be used for mutual authentication with the SAP Gateway system.

Document Revision History

S.No	Document version	Date Modified	Change History
1.	**1.0**		

If you have questions about Innovapptive products, please visit the Innovapptive Support Portal at **http://helpdesk.innovapptive.com/**

Updates to this document are made on a continuous basis based on Product releases, support pack and hotfixes. We recommend that you check this Web site periodically for updated documentation.

If you have questions or need additional information about this document, please send an email to documentation@innovapptive.com

END OF DOCUMENT

SAP Pinnacle Awards 2016 Winner

SAP Pinnacle Awards 2015 Winner

SAP Pinnacle Awards 2014 Finalist

SAP Silver Partner

SAP® Certified
Mobile App