Tomcat server certificate change

<?xml version="1.0"?><DocumentFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"> <GraphicCharterDefinitionId>0</GraphicCharterDefinitionId> <TemplateBaseTypeId>0</TemplateBaseTypeId> <CompanyId>2</CompanyId> <ConfidentialId>0</ConfidentialId> <ConfidentialDescription /> <CountryId>0</CountryId> <PageSizeId>1</PageSizeId> <PageOrientationId>1</PageOrientationId> <PrePrintedStationary>false</PrePrintedStationary> <Project>&lt;Project&gt;</Project> <Reference>20141020-121035-SQ</Reference> <TemplateType>3</TemplateType> <CultureId>en-US</CultureId> <LanguageId>8</LanguageId> <Customer>&lt;Customer&gt;</Customer> <DocumentDate>2014-10-20T12:37:48.2086419+02:00</DocumentDate> <Saved>false</Saved> <IsValid>true</IsValid> <FirstPageCover>false</FirstPageCover> <IsNew>false</IsNew> <CurrentVersion>1.00</CurrentVersion> <DocumentType>&lt;Document Type&gt;</DocumentType> <DocumentTypeId>0</DocumentTypeId> <Entity>&lt;Entity&gt;</Entity> <HasDistributionList>true</HasDistributionList> <HasForeword>true</HasForeword> <Title>&lt;Document Name&gt;</Title> <Status>1</Status> <StatusDescription>Preliminary Draft</StatusDescription> <SetEdition>false</SetEdition> <SetVersion>false</SetVersion> <setCreationMode>false</setCreationMode></DocumentFile>

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  | All Customers |
|  |  | Accounting Suite |
|  |  | Tomcat server certificate change |
|  |  | Version 4.0 of Tuesday, March 21, 2017 |
|  |  | Status: Preliminary Draft  |
|  |  |  |  |

To

|  |
| --- |
|  |

Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Update Origin** | **Written by** | **Verified By** |
| 1.0 | 03/08/2018 |  | Marcel Oaida |  |
| 2.0 | 03/15/2018 | Monica Anghel | Marcel Oaida |  |
| 3.0 | 03/19/2018 | Thibaud Kahn | Marcel Oaida |  |
| 4.0 | 03/21/2018 | Thibaud Kahn, Laurentiu Dimana | Marcel Oaida |  |

Foreword

Starting with 31th of May 2018, the Tomcat server certificate delivered with Axway Installer will expire. Although Axway is strongly advising against the usage of sample certificate (at least for production purposes) we’re going, nevertheless, to present a procedure for changing this certificate since there are multiple entities (Support, PSO, etc) that are using sample certificates for testing purposes.

Table of Contents

[1 Introduction 5](#_Toc508877045)

[2. Changing the certificate with a new one with SHA-1 algorithm 6](#_Toc508877046)

[3. Changing the certificate with a new one using SHA-256 algorithm 7](#_Toc508877047)

# Introduction

As specified in the Foreword, the clients are strongly advised to use custom certificates. For specific information regarding the usage/replacement of custom certificates please refer to **InterPlay\_2.3.0\_AdministratorsGuide\_SecurityGuide\_allOS\_en, Change the HTTPS server certificate** section.

The purpose of this document is to treat the case when the actual Axway Tomcat certificate is to be replaced by another Axway Tomcat certificate with modified expiration date. The following products are impacted:

Interplay 2.2.1/2.3, Designer 2.2.1/2.3, AdministrationUI 2.2.1/2.3, DatastoreClient 2.2.1/2.3.

We are going to treat also the specific situation of changing the certificate with another that has a more powerful signature algorithm. The actual certificate is using SHA-1 algorithm. We’re going to provide a replacement with SHA-1 algorithm and/or one with SHA-256 algorithm (for the clients that will request this type of security).

The procedure for both replacements is slightly different and it will be treated separately.

We consider that PassPort is used for authentication by the Axway products.

This procedure must be implemented on each Axway tomcat with Axway product installed. So if you have separate installation for Interplay, Datastore, Designer, Report etc… you need to upgrade each one separately with the same procedure.

To confirm the hashing mechanism in use (SHA-1 or both SHA-1 and SHA-256), you can check the "Signature Algorithm", by clicking on the certificate in PassPort: Security > Entities > Intermediate CA Certificates > CN=PassPort SSO CA, O=Axway, C=FR

# 2. Changing the certificate with a new one with SHA-1 algorithm

Obtain a new Tomcat server certificate (normally, this should be delivered by Axway Support in a keystore form)

1. Stop the Tomcat server.
2. Replace completely the keystore from here: *AIS\_Install\_folder\AIS\Tools\config\certs*
3. If you are using (or plan to use ) the newSSO feature, request (if not received) and replace the **ssofilter.jks** file from *AIS\_Install\_folder* \*InterPlay\war\WEB-INF.* (Reason: the certificate inside ssofilter.jks have expired on our side. On PassPort side was replaced in 4.6 SP15 version).
4. Start Tomcat
5. Nothing to do on PassPort.
6. Validate that you can connect to the different UI as before, If not please contact Axway Support.

# Changing the certificate with a new one using SHA-256 algorithm

Obtain a new SHA-256 Tomcat server certificate/SHA-256 intermediate PassPort SSO CA + ssofilter.jks (normally, these should be delivered by Axway Support).

**On application side – Case 1 – the client has both SHA-1 and SHA-256 intermediate CA’s in PassPort**

**Comment:** We suppose that all AISuite web components (Interplay, Designer, AdminUI, Datastore Client) are using the same Tomcat. If not the case, repeat the procedure for each Tomcat used.

1. Stop the Tomcat server.
2. Replace completely the keystore from : *AIS\_Install\_folder\AIS\Tools\config\certs with* the certificates delivered by support
3. If you are using (or plan to use ) the newSSO feature, request (if not received) and replace the **ssofilter.jks** file from *AIS\_Install\_folder* \*InterPlay\war\WEB-INF.* (Reason: the certificate inside ssofilter.jks have expired on our side. On PassPort side was replaced in 4.6 SP15 version).

**On application side – Case 2 – the client has only SHA-256 intermediate CA in PassPort**

1. With the new PassPortCA.crt and PassPort\_SSO\_CA\_1.crt (the ones signed with SHA-256) already in the keystore provided by support, **truststorePassPort.jks** and **truststoreSSO.jks** from *AIS\_Install\_folder\AIS\Tools\config\certs* must be updated accordingly.

Use keytool (importcert option) to insert these CA certificates in the above files:

* 1. PassPortCA.crt goes inside **truststorePassPort.jks** (use alias **passportca**)

keytool -importcert -v -alias passportca -file ~/PassPortCAs.zip\_FILES/PassPortCA.crt -keystore truststorePassPort.jks

* 1. PassPort\_SSO\_CA\_1.crt goes inside **truststoreSSO.jks** (use alias **passportssoca**)

keytool -importcert -v -alias passportssoca -file ~/PassPortCAs.zip\_FILES/PassPort\_SSO\_CA\_1.crt -keystore truststoreSSO.jks

1. Check that the truststore from registry contains the correct PassPortCA certificate:
	1. Go to *AIS\_Install\_folder\AIS\Repository\* and open a registry console
	2. Export the registry and go to the *export/registry/truststore* folder
	3. Using keytool -list on **truststore.jks** compare the certificate with alias **passportca** with the one delivered by support (PassPortCA.crt) and with the one from PassPort (see screenshot below). Everything should match (by default, the PassPortCA.crt delivered by support is matching the one from PassPort).



* 1. If not, unregisterPassPort for all applications that are using PassPort (default, designer, admin)
	2. Go to the *export/registry/truststore* folder and add (using keytool -imporcert) in the truststore.jks the CA certificates delivered by support (use **passportca** alias).
	3. importRegistry

**On PassPort side**

1. Connect to PassPort UI with a user that has rights on the Entity and certificates management
2. Open **SECURITY > Entities** page
3. Open the **Intermediate CA Certificates** entity
4. Identify the certificate with Alias **CN=PassPort SSO CA, O=Axway, C=FR**
5. Click on **Import a Version** (replacing completely the actual SHA-1 CA certificate has a greater impact and complexifies the process somehow unnecessarily).

**

1. Select the received certificate (the PassPort SSO CA signed with SHA-256: PassPort\_SSO\_CA\_1.crt )
2. Enter the entity password: “intermediate” and click OK
3. Click on the Show Versions and mark the newly imported CA as “Active”

**

1. Close the entity window
2. Optionally, if you are using newSSO, check if **ssofilter.jks** (from *PassPort\webapps\WEB-INF*) contains the new certificate (the one with alias *passportssofilter)* that was signed with the new SHA-256 PassPort SSO CA. If not, you either request one from support either inject the certificate in the file using keytool.
3. Restart PassPort