Documentation for Digital Signature verify tool

Table of Contents

Table of Contents 2
Digital Signature verify tool 3
License 3
Digital Signature verify tool compatibility 3
Download 3
Requirements 4
Configuration 5
Configuration steps 5
Additional configuration 5
Changelog 6
Digital Signature verify tool 6
v1.0 6

Digital Signature verify tool

The Digital Signature verify tool is a REST service application to check the validation of the digital signature of the signed documents.

License

Digital Signature verify tool compatibility

App version	OpenKM Compatibility			Status
	Professional 7.1.x		Community	
1.0	Version 7.1.14 and upper.	Version 6.4.53 and upper	Not compatible.	Active.

Download

- OpenKM Digital Signature verify tool is available at OpenKM download center.

Requirements

The application is distributed as a war file.

- The application might be deployed in a tomcat version 8.5.40 or upper. In previous versions will be raised errors because of tomcat bugs.

The application has not been tested in tomcat versions upper than 8.5.x

Configuration

The Digital Signature verify tool is distributed as a war file into a zip file. You can download the tool from OpenKM donwload center.

Configuration steps

- Deploy the "**signatureVerify.war**" file into tomcat "**webapps**" folder (ensure you deploy into a tomcat version 8.5.40 or upper).
- Enable the extension named "**Digital Signature viewer**". Check the related documentation for version 7.1.X at Enable extensions or version 6.4.x at Enable extensions.
- Configure the parameter named "**extension.signature.validation.url**". The most common value is "**http://localhost:8080/signatureVerify.war**".

Remember the value of the parameter "**extension.signature.validation.url**" it depends on the tomcat where has been deployed.

Additional configuration

The application comes with an embedded root certificates storage what is able to check almost certificates but sometimes is not enough. If you are in this scenario you can create your own trust storage certificates files what will be used by the application. The trusted storage file must be named "**truststore.jks**" and set into the $TOMCAT_HOME folder.

You can find interesting information about JAVA KeyStore at:

- Creating a KeyStore in JKS Format
- How to install the trusted root into Java cacerts Keystore
- How to import a .cer certificate into a java keystore

Changelog

Digital Signature verify tool

v1.0

- Released 2020-07-05