Datalogics

Integration Guide: Using the SafeNet LunaSA HSM with Datalogics PDF Java Toolkit Applications

Matt Kuznicki, Ryan Swanson – Datalogics, Inc.

Introduction

The Datalogics PDF Java Toolkit™ is a Java language software development kit that allows software developers to add PDF file creation and processing to their Java applications. The PDF Java Toolkit interoperates with the SafeNet LunaSA hardware security module (HSM) for securely applying digital signatures to PDF files. This guide provides information on how to set up your PDF Java Toolkit to successfully work with the LunaSA HSM to securely add digital signature capabilities for PDF files to your Java application.

Digitally signed PDF documents provide a way for the recipient to ensure that the document comes from the place it claims to come from. Ensuring a document has not been altered since it was signed is important to developers and technology like the LunaSA HSM add reassurances by securely storing and protecting digital keys for authenticating and encrypting digital files. The LunaSA HSM is designed to keep private keys for digital signatures completely secure; an administrator can delete a private key on the HSM, but it is impossible to read or edit a private key stored on the HSM, or to copy the private key to another device. The private key never leaves the HSM, so it cannot be compromised. The HSM has a variety of security measures to block unauthorized access, including a feature that will automatically erase all content on the HSM if the HSM loses power.

Before starting, please ensure that your LunaSA HSM is set up properly and is accessible from the computer where your PDF Java Toolkit application will be run. The LunaSA HSM can be plugged into a local workstation or laptop using a USB connection, or it can be connected to a server and shared over a network. Every computer that accesses the HSM device must have the LunaSA HSM client software installed, provided with the hardware.

Using the LunaSA HSM with the PDF Java Toolkit

When the client is installed the process copies the LunaProvider.jar file to a local default directory. The PDF Java Toolkit uses the LunaSA client (LunaProvider.jar) to communicate with the HSM using Public Key Cryptography Standard (PKCS) #11 security protocol to sign and encrypt messages. While the specific technical parameters in use are up to the implementing developer, we will describe the example PDF Java Toolkit program *HSMCertifyDocument* for illustrative purposes.

After you register the LunaSA client on your development computer, you must add the name and path of the LunaProvider.jar file to your Java classpath for the sample program to build and run successfully.

The steps involved in using the LunaSA HSM to digitally sign a PDF file with the PDF Java Toolkit:

- Login to the LunaSA HSM using the SafeNet provided HSM_Manager class method hsmLogin
- Load the credentials into a KeyStore from the Luna keystore obtained from the LunaProvider security provider
- Retrieve a Java PrivateKey object from the LunaSA for the credentials obtained. NOTE: the PrivateKey object is not a copy of the private key; the private key never leaves the HSM. It is only an object that can be supplied for referencing the private key stored on the HSM
- Retrieve the X.509 certificate stored on the device for the obtained credentials
- Create a Credentials object to reference the PrivateKey holder and X.509 certificate
- Create the PDF digital signature structure, and visual appearance if a visual indicator for the digital signature is desired
- Call the PDF Java Toolkit SignatureManager API certify method with the credentials and digital signature structure
- Log out of the LunaSA HSM using the SafeNet provided HSM_Manager class method hsmLogout

By default, the HSMCertifyDocument example generates a SHA-256 PDF document hash, and the signature – which includes the time and date stamp, revocation information, public key, and signed hash – is stored in the PDF in PKCS#7 format. Even though the PDF Java Toolkit developer has great control over the format of the digital signature and hash used, the essential communication with the LunaSA HSM does not change significantly. That's how easy it is to add support for the LunaSA HSM and secure PDF digital signing to your PDF application.

For more information about the Datalogics PDF Java Toolkit, please visit http://www.datalogics.com/products/pdf/pdfjavatoolkit/.

PDF Java Toolkit is a trademark of Datalogics, Inc.