FORUM SYSTEMS HANDS-ON TRAINING

LAB 7. PKI MANAGEMENT IN FORUM SENTRY

Published: September 2014
Forum Systems Hands-on Training – Lab 7. PKI Management in Forum Sentry
D-ASF-SE-010029

Contents

Introduction

Lab 7. PKI Management in Forum Sentry

Skill Level

This lab is beginner skill level. Little to no prior experience with Forum Sentry or SOAPSonar is required.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy of SOAPSonar Enterprise Edition.

Refer to the “FS_Training_Labs_v8-1_Introduction” document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

Lab Overview

This lab discusses the PKI (Public Key Infrastructure) Management features of Forum Sentry. The keys built in this lab will be utilized in later labs in this series.

The Sentry PKI infrastructure is a critical piece to the Sentry deployment. All of the crypto operations performed by Sentry (encryptions, signatures, SSL, OpenPGP encryptions, SFTP and SSH operations) will require keys.

Sentry provides a secure platform to build and manage the keys that will be used to secure your web services / APIs, web portals / web sites, and FTP / SFTP servers.

This lab will provide instructions for generating and importing PKCS keys and certificates with Forum Sentry. Topics will include:

1. PKCS Key Pairs
2. X.509 Public Certificates
3. Signer Groups

PKCS Keys

PKCS stands for “Public Key Cryptography Standards”. In Sentry, different types of PKCS keys and certs will be used for cryptographic operations such as SSL Termination/Initiation, XML Encryption/Decryption, and Digital Signatures/Verifications.

Important Concepts:

- In Sentry, a “key pair” indicates both a public and private key exist
- For security reasons, it is not possible to export a PKCS private key from the Sentry configuration
- X.509 public certificates can be exported from the Sentry configuration
- If a PKCS private key is to be used outside of Sentry, build the key outside of Sentry (so you have a copy of the private key outside of Sentry) and then import the PKCS#12 key pair into Sentry
- Sentry can generate self-signed keys as well as CSRs to provide to a Certificate Authority (CA)
- Sentry can also act as a CA and consume CSRs

PKCS key pairs can be built in Sentry or imported into Sentry. Sentry supports importing the following PKCS formats:

- PKCS#12 Key Pairs
- PKCS #1 Key Pairs
- PKCS #8 Key Pairs
- PKCS#7 Public Certs
- X.509 Public Certs

The most common PKI / PKCS operations Sentry admins will encounter are:

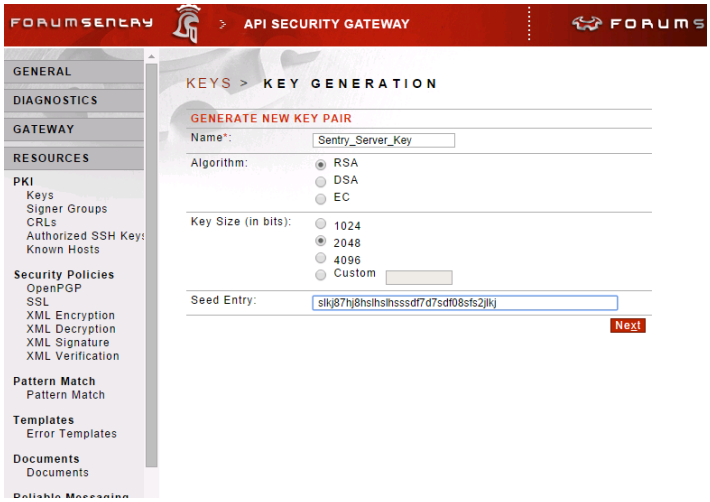
- Importing X.509 Certificates
- Importing PKCS#12 Key Pairs
- Generating PKCS Self Signed Key Pairs
- Generating PKCS non-Self Signed Key Pairs (generating a CSR)

Generate a New PKCS Key Pair

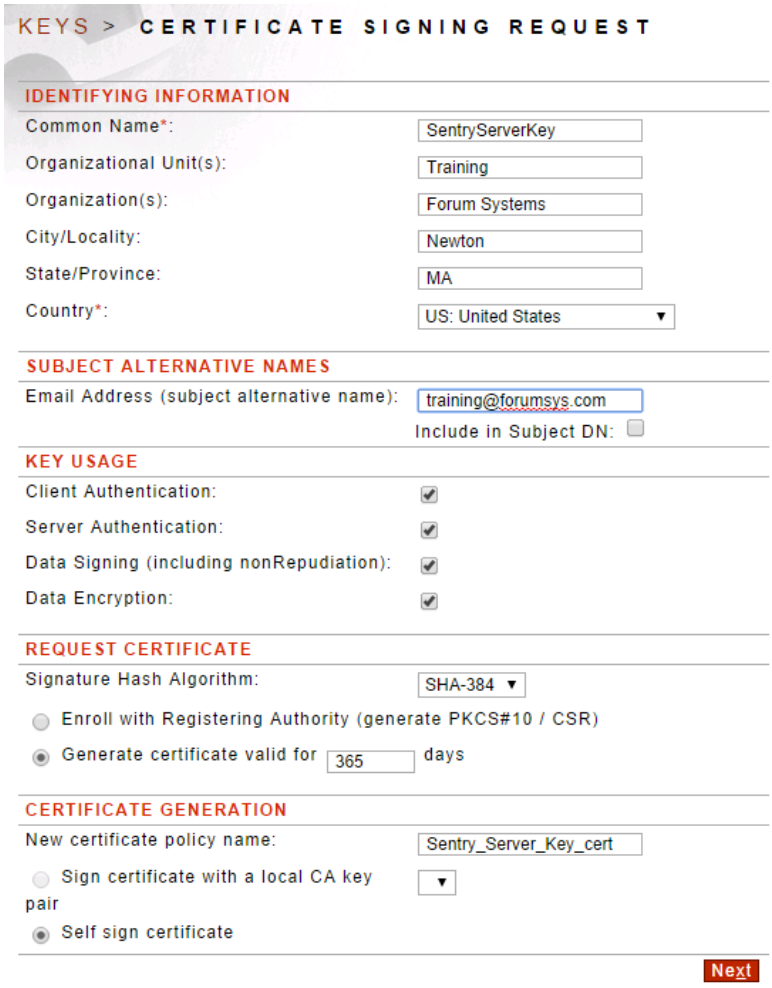
In this step we will generate a new PKCS key pair. This will generate both a private key (not exportable) and a pubic certificate. This will be a self-signed certificate that will later be used as the Sentry SSL Termination Key Pair.

Follow the steps below to generate a new PKCS #12 key pair in Sentry.

1. Navigate to the Resources→PKI→Keys screen
2. Click New (bottom right)
3. Choose PKCS Key Pair and click Next
4. Use the following information while generating the key pair
    a. Name: Sentry_Server_Key
    b. Algorithm: RSA
    c. Key Size: 2048
    d. Seed Entry: feel free to type a bunch of random characters



5. Click Next to open the Certificate Signing Request page. Enter the following options:
    a. Common Name: SentryServerKey
    b. Organization Unit: Training
    c. Organization: Forum Systems
    d. City/Locality: Newton
    e. State/Province: MA
    f. Country: US
    g. Email Address: training@forumsys.com
    h. Include in Subject DN: Not checked
    i. Key Usage: Check all options
    j. Signature Hash Algorithm: SHA-384
    k. Request Certificate: Select “Generate certificate valid for 365 days”



6. Click Next to generate the self-signed key and view the Key Details Page. Notice the following:
    a. The Subject and Issuer are the same which indicates this is a self-signed certificate
    b. You can view the PEM format (to copy/paste the public cert)
    c. You can download the public cert in PEM or DER formats

d. You can view the Key Usage and Extended Key Usages for the key pair

7. You have now built a PKCS#12 key pair in Sentry. If you click out to the PKI→Keys screen you will now see this key listed as both a key pair and a public certificate. This indicates that you can use this key anywhere in Sentry that calls for either a key pair (private key and public cert) or just a certificate.

Import a PKCS #12 Key Pair

In many circumstances Sentry administrators and/or developers may need to import a PKCS#12 key pair. This may be a .p12 file or sometimes a .pfx file. These will contain at least 1 private key and 1 public cert, but there may also be multiple public certificates - the intermediate and root CA certs.

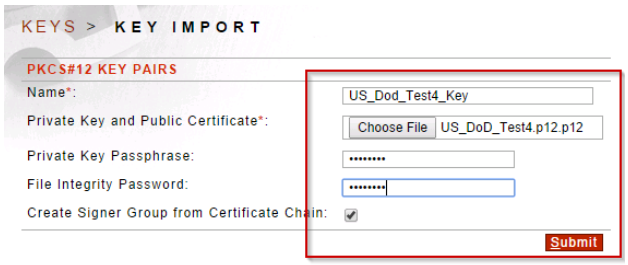
When you import a PKCS#12 key pair, there is an option to also generate a Signer Group from any intermediate and root certs included in the key pair. This is typically a good idea and the option is enabled by default. We will discuss Signer Groups later in this lab.

The key pair we use in this step will be used with encryption/decryption and signature/verification tasks built in later labs.

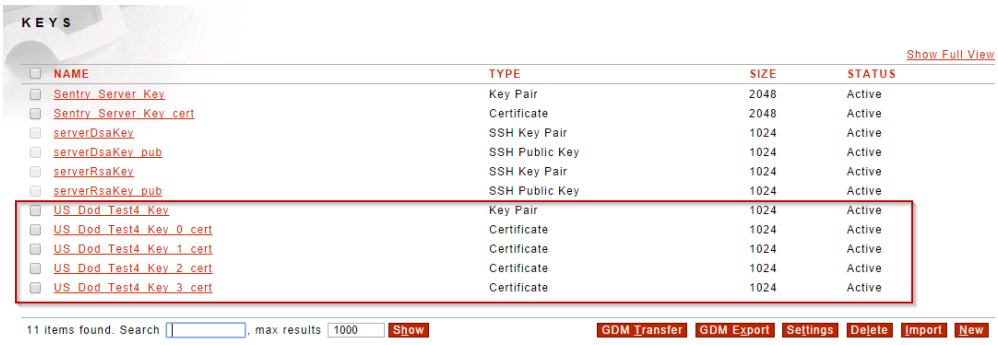
Follow the steps below to import a PKCS#12 key pair.

1. In the Samples folder on the Desktop of the Sentry Training Image, there is a US_DoD_Test4.p12 file - we will be importing this key pair into Sentry.
2. Navigate to the Resources→PKI→Keys screen and click Import.
3. On the Key Import screen, under PKCS, select PKCS#12 Key Pairs and click Next.

4. On the next screen, enter the following information:
    a. Name: US_Dod_Test4_Key
    b. Private and Public Certificate: browse to the US_DoD_Test4.p12 file
    c. Private Key Passphrase: password
    d. File Integrity Password: password
    e. Create Signer Group from Certificate Chain: checked



5. Click Submit to import the PKCS#12 key pair. You'll notice there is a new Key Pair as well as four new certificates in the Sentry key store. This process imported the private key and corresponding public certificate, along with two intermediate CA certs and one root CA cert.



Import an X.509 Certificate

Sentry administrators and developers may also need to import just a public certificate. The public certificate might be used to encrypt an XML payload for a trading partner, who will decrypt the XML payload using the corresponding private key.

When you import an X.509 certificate, you can use one of three import sources:

1. File Upload
2. Paste from Clipboard (PEM format)
3. LDAP request

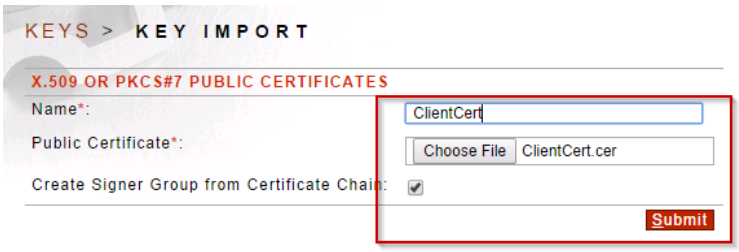
The most common options are File Upload and Paste from Clipboard. The X.509 certificate we import in this step will be used for XML payload encryption in a later task.

Follow the steps below to import an X.509 certificate.

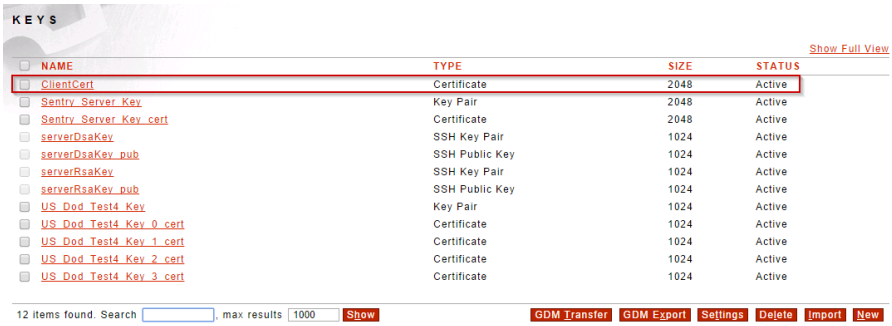
1. In the Samples folder on the Desktop of the Sentry Training Image, there is a ClientCert.cer file - we will be importing this X.509 certificate into Sentry.

2. Navigate to the Resources→PKI→Keys screen and click Import.
3. On the Key Import screen, under PKCS, choose: X.509 or PKCS#7 Public Certificates and click Next.

4. On the next page select the File Upload option.
5. On the next page use the following options:
    a. Name: ClientCert
    b. Public Certificate: Browse to the ClientCert.cer file in the Samples folder on the desktop
    c. Create Signer Group from Certificate Chain: Checked



6. Click Submit to import the X.509 certificate. You will notice a new certificate is listed in the Sentry key store.



Signer Groups in Forum Sentry

In Sentry a Signer Group contains the intermediate and root CA certificates that are used with the path validation of an end user certificate.

Other options within a Signer Group are certificate revocation (CRL Policies) and an option to send the client a "hint" or list of the CA certificates in the Signer Group during the SSL handshake (Send Accepted Issuers).

Signer Groups are used with SSL policies, signature verification policies, and encryption policies in Sentry.

There is one default Signer Group that ships with Sentry named “Default”. This Signer Group contains intermediate and root CA certs for many of the commonly used third party Certificate Authorities including:

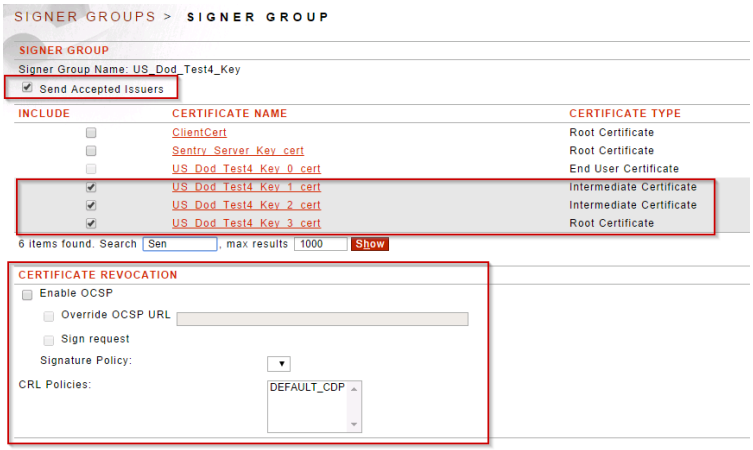
- VeriSign
- Thawte
- Entrust
- GeoTrust
- Equifax
- GoDaddy

When importing keys/certs into Sentry, there is an option to automatically create a Signer Group from any CA certs contained within the file being imported. Earlier in this lab we used this option when importing the PKCS12 key pair and the X.509 public cert. This process built two Signer Groups, so you should now have three in total.

Follow the steps below to verify there are three Signer Groups in your Sentry instance.

1. Navigate to the Resources→PKI→Signer Groups screen
2. Verify there are 3 Signer Groups listed:
    a. DEFAULT – the system default
    b. ClientCert – create when importing the X.509 certificate
    c. US_Dod_Test4_Key – created when importing the PKCS#12 key pair

3. Open the US_DoD_Test4_Key Signer Group and notice that only the intermediate and root cert are selected. End user certificates are not allowed in Signer Groups.
4. Within the Signer Group are the following options:
    a. Send Accepted Issuers – enabled by default, tells Sentry to provide the client a list of CA certs in the group during the SSL handshake
    b. Certificates to Include – Only Intermediate and Root Certificates
    c. Certificate Revocation – The ability to specify a CRL policy and/or enable OCSP



5. No further modifications are required for this step. The Signer Groups required for future labs have been built automatically.

END

Additional Testing and More Reading

BACK IT UP!

It is recommended that you export your full Sentry configuration after completing this lab.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

We recommend including the lab number in the name of the export files.

Additional Tests and Discussion Topics

1. Create different types of keys in Sentry. Sentry supports other types of keys in addition to PKCS. Specifically OpenPGP – used for OpenPGP security operations with FTP policies, and SSH keys – used for SFTP policies.
2. What crypto operations will you use that will require keys? Will the private keys need to be used outside of Sentry?
3. Create a self-signed CA cert in Sentry, then use it as a CA and consume a CSR.

For more information on PKI terms in Forum Sentry see:
https://helpdesk.forumss.com.com/entries/95096583-FAQ-Troubleshooting-SSL-Termination-Issues

For more information, review the following Forum Sentry Admin Guide:

1. Security Policies and PKI Guide

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum's patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.