

Key and Certificate Generation

Contents

- 1 Overview
- 2 Prerequisites
- 3 Create private keys and certificates
 - ◆ 3.1 Creating DSA Private Key
 - ◆ 3.2 Creating a Certificate
- 4 Example output
- 5 Testing
- 6 Known Issues
- 7 Troubleshooting

Overview

Communication between the Application and the IDP is encrypted using a certificate, this document outlines how to create keys and a certificate on a Swivel hardware or Virtual Appliance.

Prerequisites

Swivel IDP

Swivel hardware or Virtual appliance 2.x

Create private keys and certificates

Communication between the SAML application and the Swivel instance is secure through the use of certificates.

Creating DSA Private Key

DSA key generation involves two steps, and can be done through the command line on a Swivel virtual or hardware appliance, usually accessed through the [CMI](#). Change directory to the key location, this can usually be found from the settings file.

Swivel Authentication Manager: keys/pinsafe/ssl

Backp the existing keys and certificates to a new location, then run the following commands:

1.

```
openssl dsaparam -out dsaparam.pem 2048
```

2.

```
openssl gendsa -out dsaprivkey.pem dsaparam.pem
```

The first step creates a DSA parameter file, dsaparam.pem, which in this case instructs OpenSSL to create a 2048-bit key in Step 2. The dsaparam.pem file is not itself a key, and can be discarded after the public and private keys are created. The second step actually creates the private key in the file dsaprivkey.pem which should be kept secret.

Export the key into a DER (binary) format. You can do so with the following steps:

1.

```
openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
```

2.

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
```

Step 1 extracts the public key into a DER format. Step 2 converts the private key into the pkcs8 and DER format. Once you've done this, you can use this public (dsapubkey.der) and private (dsaprivkey.der) key pair.

Creating a Certificate

Once you have your key pair, it's easy to create an X.509 certificate. The certificate holds the corresponding public key, along with some metadata relating to the organization that created the certificate. Follow this step to create a self-signed certificate from either an RSA or DSA private key:

```
openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
```

After you answer a number of questions, the certificate will be created and saved as dsacert.pem.

The created keys, dsapubkey.der and dsaprivkey.der need to be copied to the keys folder or wherever specified within settings.xml

The **dsacert.pem** certificate needs to be uploaded to the Application server, using a program such as WinSCP, see the [WinSCP How To Guide](#).

