# Key and Certificate Generation

## Contents

# 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 dsapubkey.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.

## Example output

```
[admin@pinsafe-wby-01 ssl]# openssl dsaparam -out dsaparam.pem 2048
Generating DSA parameters, 2048 bit long prime
This could take some time
..............+.......+...................+...+..++++++++++++++++++++++++++++++++++++++++++++++++++*.................+.+.+........+.+......
[admin@pinsafe-wby-01 ssl]# openssl gendsa -out dsaprivkey.pem dsaparam.pem
Generating DSA key, 2048 bits
[admin@pinsafe-wby-01 ssl]# openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
read DSA key
writing DSA key
[admin@pinsafe-wby-01 ssl]# openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
[admin@pinsafe-wby-01 ssl]# openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name (full name) [Berkshire]:West Yorkshire
Locality Name (eg, city) [Newbury]:Wetherby
Organization Name (eg, company) [My Company Ltd]:Swivel Secure Ltd
Organizational Unit Name (eg, section) []:Dev
Common Name (eg, your name or your server's hostname) []:pinsafe-wby-01
Email Address []:
[admin@pinsafe-wby-01 ssl]# ls -la
total 32
drwxrwxr-x  3 swivel swivel 4096 Aug 28 14:52 .
drwxrwxr-x  3 swivel swivel 4096 Aug 28 14:35 ..
-rw-r--r--  1 root   root   1980 Aug 28 14:52 dsacert.pem
-rw-r--r--  1 root   root    804 Aug 28 14:50 dsaparam.pem
-rw-r--r--  1 root   root    592 Aug 28 14:50 dsaprivkey.der
-rw-r--r--  1 root   root   1192 Aug 28 14:50 dsaprivkey.pem
-rw-r--r--  1 root   root    830 Aug 28 14:50 dsapubkey.der
drwxr-xr-x  2 root   root   4096 Aug 28 14:49 orig
```

## Testing

## Known Issues

## Troubleshooting