Instructions for installing a Certifying Authority for Ingate VPN with Ingate System’s OpenSSL pack for Windows

1. Introduction

This document describes how to use Ingate System’s OpenSSL pack for Windows for installing a Certifying Authority, CA, to create and sign X.509 certificates for Road Warrior VPN clients with Ingate VPN.

Before starting, we suggest that you read the ’Instructions for installing a Certifying Authority for Ingate Firewall’ (can be found at http://www.ingate.com/vpn/ca.html). It contains an overview of the CA and X.509 certificate concepts, and some useful tips about security routines for these.

OpenSSL is a free software program for the use of SSL. Our OpenSSL pack contains a binary of the program, compiled for Windows 98, Windows NT and Windows 2000. It also contains some command line scripts to simplify the handling of OpenSSL. The original pack, and its documentation, can be downloaded from http://www.openssl.org/ .

2. Install OpenSSL on a Windows computer

- Download the pack from Ingate’s web site, http://www.ingate.com/ .
- Unpack the file. It is compressed using Zip, which means that you have to have some Zip software. Such software could be the unzip.exe program, which can be found at the same place as Ingate’s OpenSSL archive. Another zip program is WinZip, which can be downloaded from http://www.winzip.com/ .
- Install the pack by double clicking on SETUP.EXE from the archive and follow the instructions.
- Now, the pack has been installed.

3. Set up a CA

This is automatically done by the NewCA.bat script. You only have to run this once after installation.

- Change directory to where OpenSSL was installed. This directory will be referred to as CA-DIR in the rest of this instruction. Run NewCA.bat.
- Now OpenSSL will create a new key, which will take some time. When finished doing this, it will ask for a password for the CA. This is the password that later will be used when signing certificates.
- OpenSSL will ask for information for the fields in the CA certificate. Fill in the fields Country code and Common name (being the CA’s name) and leave the other fields empty.
- When NewCA.bat has created a certificate, the screen will say "Press any key to continue". When you have pressed a key, the script is finished and you can close the window.
- Now a CA has been created, and you can start signing certificates. The files for the CA are stored in CA-DIR\CA.
- The client will need the public CA certificate, which is called cacert.pem and is stored in CA-DIR\CA .

4. Do this to sign a certificate request

This description is valid for VPN clients who can create their own keys and certificate requests, such as the SafeNet client.

- Create a certificate request on the client and move it to CA-DIR.
- Rename the certificate request into CertReq.req.
- Sign it by changing directory to CA-DIR and run Sign.bat. OpenSSL will ask for the password you entered when you installed the CA. Answer ’y’ to other questions.

- When Sign.bat has created a certificate, the screen will say "Press any key to continue". When you have pressed a key, the script is finished and you can close the window.
- The new certificate, named newcert.pem, is stored in CA-DIR.
- Move the new certificate to the client.
- The client will also need the public CA certificate, which is called cacert.pem and is stored in CA-DIR\CA .

5. Do this to create a new certificate

This description is valid for VPN clients who can't create their own keys and certificate requests, such as the PGPNet client.

- Change directory to CA-DIR and run NewCert.bat.
- OpenSSL will create a new key, which will take some time. When finished doing this, it will ask for a password for the certificate. This password will be used when signing the certificate later.
- OpenSSL will ask for information for the fields in the certificate. Fill in the fields Country code and Common name (being the computer's name) and leave the other fields empty.
- Now OpenSSL will convert the key and the certificate to the pkcs12 format, which many clients understand. When doing this, it will ask for the password again.
- After this, a new password for the file is requested. You can use the same password as when the key was created.
- The new file is called newcert.p12 and is stored in CA-DIR. N.B. The file contains not only the certificate, but the secret key as well. Hence, handle this file with great care, so that no unauthorized people can read it.
- Move newcert.12 to the client.
- The client will also need the public CA certificate, which is called cacert.pem and is stored in CA-DIR\CA .