

Tru64 UNIX Best Practice

Obtaining Certificates from a Windows 2000 Certification Authority for IPsec Use

November 2002

Product Version: Tru64 UNIX

Operating System and Version: Version 5.1B

This Best Practice describes how obtain certificates from a Windows 2000 Certification Authority (CA) for IPsec use on a Tru64 UNIX system.

Contents

Obtaining Certificates from a Windows 2000 Certification Authority for IPsec Use

Is This Best Practice Right for You?	1
Before You Begin	2
A Sample Scenario	2
Applying the Best Practice	3
Configuring the Windows 2000 Certification Authority ...	3
Downloading the CA Certificate to the Tru64 UNIX System	6
Requesting a Host Certificate	7
Making the Certificates Available to IPsec on Tru64 UNIX	9
.....	10
Verifying Success	10
Troubleshooting	10
Alternative Practices	11
Comments and Questions	11
Legal Notice	11

Obtaining Certificates from a Windows 2000 Certification Authority for IPsec Use

This Best Practice describes how to obtain certificates from a Windows 2000 Certification Authority (CA) for IPsec use on a Tru64 UNIX system.

When you use Internet Protocol Security (IPsec) among many systems, it is convenient to authenticate the systems using public key certificates. Each system only needs to be configured with its own identity certificate and a Certificate Authority (CA) certificate.

In some cases, an enterprise might not have CA available to issue certificates. One choice is to use the Certificate Authority that is a part of the Windows 2000 operating system. You might already have a CA in an existing Windows environment, or you can configure a separate Windows 2000 system to act as the CA.

See the Tru64 UNIX Best Practices Web page for more information about Best Practices documentation:

http://www.tru64unix.compaq.com/docs/best_practices/

Is This Best Practice Right for You?

Not all Best Practices apply to all configurations, so you must be sure that this Best Practice is appropriate for your system and circumstances. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 5.1B
System Configuration	CDSA and IPsec
Need	To obtain certificates from a Windows 2000 CA

Requirement	Description
Impact on Availability	None
Skills	Knowledge of IPsec and Windows 2000 environments

If you do not meet the previous requirements, see *Alternative Practices* for information.

Before You Begin

Before you apply the Best Practice for obtaining certificates from a Windows 2000 system for IPsec use on a Tru64 UNIX system, you must understand some background information and perform some preliminary tasks.

- Understand Tru64 UNIX IPsec operation
You must know how to configure IPsec on a Tru64 UNIX system. See the *Network Administration: Connections* manual for more information.
- Understand Windows 2000 operation
You must have a thorough knowledge of Windows 2000 system administration; specifically, using the MMC Console. See the Windows 2000 documentation.
You should also know how IPsec operates on a Windows 2000 system. See the *Step-by-Step Guide to Internet Protocol Security (IPSec)* at the Microsoft Windows 2000 web site.
- Understand the interoperability scenario.

A Sample Scenario

The sample scenario in this document consists of the following systems at a minimum:

- A Windows 2000 system will be configured to act as a CA for one or more Tru64 UNIX systems. The host name is `test-ca.mycorp.com`. The certificate server web site will be set up to allow anonymous access. Alternatively, you can allow access to a specific user. However, the types of templates that you select are still the same.
- A Tru64 UNIX system with the IP address 10.140.0.1 will use a certificate issued by the CA for IPsec authentication. The host name is `myhost.mycorp.com`.

Applying the Best Practice

Before you obtain certificates from the Windows 2000 CA, be sure to follow the recommendations in *Before You Begin*.

This section describes the following steps:

1. Configuring the Windows 2000 certificate authority (CA)
2. Downloading the CA certificate to the Tru64 UNIX system
3. Requesting the host certificate
4. Making the certificates available to IPsec

Configuring the Windows 2000 Certification Authority

To configure a Windows 2000 system as a CA, do the following:

1. Install the High Encryption Pack for Windows 2000 or Windows 2000 Service Pack 2, if either is not already installed. You can obtain the pack from the following location:

`www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp`

After installing the pack, reboot your system.

2. If your system is already in a Windows 2000 Active Directory domain, go to step 3. Otherwise, install the Active Directory service. Do the following:
 - a. Select Active Directory from the Configure Your Server Wizard.
 - b. Click the Start the Active Directory wizard link and select the following options:
 - Domain controller for a new domain.
 - Create a new domain tree.
 - Create a new forest of domain trees.
 - Full DNS name for the new domain. For this scenario, enter `ipsec.mycorp.com`.
 - Domain: NETBIOS (the default).
 - Install and configure DNS on the system.
 - c. Reboot your system.

3. If Certificate Services is already installed, write down the CA name and go to step 4. Otherwise, install Certificate Services. Do the following:
 - a. Click Start, click Settings, click Control Panel, click Add-Remove Programs, then click the Add-Remove Windows Components tab.
 - b. Select Configure under the Certificate Services entry.
 - c. Modify the Enterprise root CA settings and the advanced options as follows:
 - CSP = Microsoft Enhanced Cryptographic Provider V1.0
 - Hash algorithm = SHA-1
 - Key length = 1024
 - d. Enter a CA name (for this scenario, enter `mycorp_ipsec_ca2`), Organization (O), Organizational Unit (OU), city, state, country, e-mail address, CA description, Validity, and so on.
4. If the Certification Authority snap-in is already installed, go to step 5. Otherwise, add a Certification Authority (local) snap-in. Do the following:
 - a. Enter `mmc` at the command prompt.
 - b. In the console window, enter `ctrl-m` to display the Add/Remove Snap-in dialog box.
 - c. Click Add to display the Add Standalone Snap-in dialog box.
 - d. Select Certification Authority and click Add.
 - e. In the Certification Authority dialog box, select Local Computer, then click Finish.
 - f. Close the Add Standalone Snap-in dialog box, then click OK in the Add/Remove Snap-in dialog box.

A Certification Authority entry now appears under the Console Root in the left pane.
5. Set the CA policy. Do the following:
 - a. Left click on the Certificate Authority entry in the left pane of the MMC Console, and select Properties.
 - b. Select the Policy Module tab and select Configure.

- c. Select “Always issue the certificate”. This allows certificates to be enrolled from a Tru64 UNIX system without requiring manual intervention on the Windows 2000 system.
6. Set up web site access. This can be either anonymous access (this scenario) or specific user access. Do the following:
 - a. Click Start, click Program, click Administrative Tools, then click the Internet Service Manager.
 - b. In the Internet Information Service window, expand the system name, expand the default web site, and right click `certsrv` to display the `certsrv` Properties dialog box.
 - c. Click the Directory Security tab. Then, click the Edit button of the “Anonymous access and authentication control” frame to display the Authentication Methods dialog box.
 - d. Click the Anonymous access check box. Then, click OK to close the Authentication Methods dialog box.
 - e. Click OK to close the `certsrv` Properties dialog box.
 - f. Close the Internet Information Service window.
7. Select the certificate template that will issue the host certificate. By default, a user can only access the USER and EFS certificate templates. These are certificates for users, not computer systems (hosts). As such they do not contain SubjectAltNames. You need to make a certificate template for computers accessible to the user. Do the following:
 - a. Click Start, click Programs, click Administrative Tools, then click the Certification Authority.
 - b. Expand the CA name, right click on the Policy Settings node in the left pane, point to New, and then click “Certificate to Issue”.
 - c. In the Select Certificate Template dialog box, click on either the IPSec (Offline request) certificate template or the Web Server certificate template. Either will issue a certificate for a computer. Then, Click OK.
 - d. Close the Certification Authority console.

8. Assign the certificate template to the default user account for anonymous access. Do the following:
 - a. Click Start, click Programs, click Administrative Tools, then click the Active Directory Sites and Services.
 - b. On the View menu, click Show Services Node.
In the console tree, click Certificate Templates.
 - c. Right click on the template you want to use, and select Properties to display the template's Properties dialog box.
 - d. Select the Security tab, then click Add and add the default user account (DOMAIN\IUSER_*systemname*) of the certsrv Web site.
 - e. Close the console window.

Downloading the CA Certificate to the Tru64 UNIX System

To download the CA certificate to the Tru64 UNIX system, do the following:

Note

We recommend that you perform this step from the root account so the CA certificate file is placed directly into a secure system directory. However, this is not a requirement.

1. Run the Netscape browser by entering the command:

```
# /usr/bin/x11/netscape
```
2. Enter the URL of the Windows 2000 Certificate Authority. For this scenario, enter the following:

```
http://test-ca.mycorp.com/certsrv
```
3. Enter a valid username and password for the Windows 2000 system, if a login request dialog box is displayed. Depending on the web server's configuration and security policy, a user name and password might not be required.
4. Select "Retrieve the CA certificate or certificate revocation list" and click on the Next> button.
5. If the Certificate Authority has multiple CA certificates, select the one you want to download. Then, select the format for the certificate — either DER encoded (BIN format) or Base 64 encoded (PEM format) — and click on "Download CA certificate". For this scenario, select PEM format.

6. Enter the destination for the downloaded CA certificate. For this scenario, enter the following:

```
/var/ipsec/w2k-ca-cert.pem
```

Requesting a Host Certificate

To request a host certificate from the Windows 2000 CA, do the following:

1. Using a text editor, create an X.509 certificate request file named `myhost-certreq.x509` with the following information:

```
%  
% Request to generate a certificate  
%  
CertificateRequest ::= {  
    OutputFile ::= ":p:/var/ipsec/myhost-certreq.pem" 1  
  
    SubjectName ::= <C=US, O=MyCorp Corporation, CN=myhost>  
  
    PublicKeyInfo ::= {  
        Size ::= 1024 2  
        Type ::= rsaEncryption  
        PrivateKeyFile ::= ":p:/var/ipsec/myhost-private.pem"  
    }  
    Signature ::= {  
        SignatureAlgorithm ::= sha1WithRSAEncryption  
    }  
  
    %  
    % Extensions  
    %  
    Extensions ::= {  
        SubjectAltNames ::= {  
            IP ::= 10.140.0.1 3  
        }  
        KeyUsage ::= {  
            DigitalSignature  
            KeyEncipherment  
        }  
    }  
}
```

- 1 The `OutputFile` field must specify PEM encoding.
- 2 The `PublicKeyInfo.Size` attribute must match the key length for the CA certificate.
- 3 You can specify additional subject alternative names (`SubjectAltNames`) by adding additional lines to that stanza. For example, you can add either or both of the following:

```
DNS ::= myhost.mycorp.com  
EMAIL ::= user@myhost.mycorp.com
```

2. Create a certificate request with the following command:

```
# /usr/sbin/ipsec_certmake myhost-certreq.x509
```

This creates the certificate request `/var/ipsec/myhost-certreq.pem` and the certificate's private key in `/var/ipsec/myhost-private.pem`. For security, you must place the private key file placed in a secure directory that has only root read access allowed. See `ipsec_certmake(8)` for more information.

3. Run the Netscape browser by entering the command:

```
# /usr/bin/X11/netscape
```

4. Enter the URL of the Windows 2000 Certificate Authority as follows:

```
http://test-ca.mycorp.com/certsrv
```

5. Enter a valid username and password for the Windows 2000 system, if a login request dialog box is displayed. Depending on the web server's configuration and security policy, a user name and password might not be required.
6. Select Request a certificate and click on the Next> button.
7. Select Advanced request and click on the Next> button.
8. Select "Submit a certificate request using a base64 encoded PKCS #10 file..." and click on the Next> button.
9. In a terminal window, display the contents of the certificate request that you created in step 2 as follows:

```
# cat /var/ipsec/myhost-certreq.pem
-----BEGIN X509 CERTIFICATE-----
MIIBqjCCARMCAQAwOzELMAkGA1UEBhMCVVMxGzAZBgNVBAoTEk15Q29ycCBDdb3Jw
b3JhdGlvbjEPMA0GA1UEAxMGbXlob3N0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDNoZiOt73HjO+gy0ELbFbBjSEzG1Tc179JcDiPUymCTHN2q2umvEJ7xO2X
/3btLa+09M5IWYCi+9QuoMezooUw489nu//eXEaiF0dERUjj0tK0Xud5rFMnwF66
nkTg6vdzMHhFkM9jP0UtIyt3emn+DH/A+ng+arV6QKzDUz10rQIDAQABOC8wLQYJ
KoZIHvcNAQkOMSAwHjALBgNVHQ8EBAMCBaAwDwYDVR0RBAGwBocEEIxAAjANBgkq
hkiG9w0BAQUFAAOBgQC4axz2QnmgwFdSVvINr9CQBzQixTVGuQ8pS9FHOva6+hm+
BPp11+TxOhWAC4Px78ShiUwV5azBiKA+symvxWfU3R+FCfAZG34kb8BX0r/3OzPj
hxukLKqJwRZ6BXQm395j4PkCRUYRDNQeJktx4N4k/lRZh7/KKUI29riDuesZ3w==
-----END X509 CERTIFICATE-----
```

10. Cut and paste this entire text into the Saved request box in the Web form. Then, select certificate template as "Web Server" or "IPSec Offline Request" and click on the Submit> button. The Certificate Issued page is displayed.

11. Select the format for the certificate, either DER encoded (BIN) or Base 64 encoded (PEM). Then, click on Download CA certificate. For this scenario, select PEM format.
12. Enter the destination for downloaded CA certificate. For this scenario, enter the following:

```
/var/ipsec/myhost-cert.pem
```

If the Certificate Issued page is not displayed, the Certificate Authority might be configured to require manual authorization of certificates. After the certificate has been authorized on the Windows 2000 system, return to the <http://test-ca.mycorp.com/certsrv> Web page, and use Check on a pending certificate to download the certificate.

Making the Certificates Available to IPsec on Tru64 UNIX

After the certificates have been downloaded, install them into the Tru64 UNIX IPsec subsystem. Do the following:

1. Run the SysMan IPsec application.
2. Add the public key certificate for the Certificate Authority with the following information:
 - Certificate Name: w2k-CA-certificate
 - Certificate Encoding: PEM
 - Certificate File: /var/ipsec/w2k-ca-cert.pem
 - CA Certificate: Selected
 - No Certificate Revocation List (CRL) available: Selected
3. Add the public key certificate for myhost with the following information:
 - Certificate Name: myhost-certificate
 - Certificate Encoding: PEM
 - Certificate File: /var/ipsec/myhost-cert.pem
 - Private Key Encoding: PEM
 - Private Key File: /var/ipsec/myhost-private.pem

Verifying Success

After you apply this Best Practice for obtaining certificates from a Windows 2000 CA, verify that the certificates were successfully created and installed by issuing the `ipsec_certview` command as follows:

```
% ipsec_certview /var/ipsec/myhost-certreq.pem
% ipsec_certview /var/ipsec/myhost-cert.pem
% ipsec_certview /var/ipsec/w2k-ca-cert.pem
% ipsec_certview -prv /var/ipsec/myhost-private.pem
```

When viewing the `myhost-cert.pem` certificate, make sure that the `SubjectAltNames` specified in the certificate request are included in the certificate. In cases where you choose the wrong template, a certificate is issued but the `SubjectAltNames` will not be included. The certificate is considered valid, but cannot be used for IPsec authentication.

See `ipsec_certview(8)` for more information.

Then, you can verify that the certificates correctly authenticate an IPsec connection by configuring an IPsec policy between `myhost` and another Tru64 UNIX or Windows 2000 system, and initiating the IPsec connection.

From `myhost`, issue the `ping` command to an IPsec peer. The two systems should perform IKE negotiation and eventually communicate with each other using an agreed upon IPsec protocol and mode. The successful display of the `ping` command output indicates this.

The peer system must authenticate itself using a certificate issued from the same Windows 2000 Certificate Authority. If that is not possible, you will need to configure the CA certificate for the peer's CA on `myhost`. Follow the steps in *Downloading the CA Certificate to the Tru64 UNIX System*.

You can then issue the `netstat -x` and `netstat -X` commands to display the negotiated Security Associations (SAs) to verify that the correct SAs have been created. Also, the `/var/adm/syslog.dated/current/auth.log` file shows the log messages that are generated by the IPsec subsystem.

If the Best Practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

Troubleshooting

If you determine that this Best Practice was not successful, as described in *Verifying Success*, see the problem solving section of the *Network Administration: Connections* manual for Tru64 UNIX IPsec problems

and the appropriate Microsoft Windows 2000 documentation for Windows 2000 problems.

Alternative Practices

Although this Best Practice is the recommended method for obtaining certificates from a Windows 2000 CA, if your system does not meet the requirements described in *Is This Best Practice Right for You?*, you can use alternative methods.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

`best_practices@zk3.dec.com`

Legal Notice

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation in the United States and/or other countries. UNIX® is a trademark of The Open Group in the United States and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq Computer Corporation, a wholly owned subsidiary of Hewlett-Packard Company, required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

None of Compaq, HP, or any of their subsidiaries shall be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP or Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.