Creating a Certificate-Enabled Public Web Site With Windows 2000

Michael Reiter

The Scenario

A system administrator is told by his boss, "Change our Web site. I want selected outsiders to have access to special information. Make sure it's secure – I want the users to authenticate their identity with digital certificates." The sysadmin, a Windows NT guru not yet fully introduced to the world of Windows 2000, has heard good things and decides to press ahead with a Win2K Public Key Infrastructure (PKI). He creates a test home page for a secured site he will call "ironclaw". It's now time to configure the Win2K box. Hardening of the Certificate Authority (CA) and web server boxes is assumed to be done in general accordance with the procedures outlined in *A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server*[1]; however, the sysadmin knows from hard experience that checklists like this frequently break vital services, and he will test each step on a pilot box before going live. The actual testing is beyond the scope of this paper.

Note: For the purposes of this paper, not to mention economy and space restrictions, a single PC was used for both the web server and the CA server. In reality, these would be separate machines, for security and for load distribution.

Creating the Certificate Authority

Our sysadmin decides to create a self-signed CA. He does this primarily for cost reasons (and because it is more illustrative for this paper). The relatively low per-unit costs associated with self-issued certificates is attractive; however, he does not consider the longer term cost of ownership. When purchasing a managed CA service from an outside source, licensing is often done on a per-certificate basis. A typical cost for a population of 100,000 users might be $5.00 each per year. According to a paper published on the VeriSign website[2], three-year cost of ownership for three different public key infrastructures ranged from $256,894 to $993,602 for 5000 seats, and $1,276,904 to $11,093,098 for 500,000 seats. Even for a very large company, this is a substantial cost. With a self-signed, self-managed CA, there is no additional cost per certificate. However, there are also no support services, and the cost of support staff might well rival the cost of managed services. Windows 2000 allows you to create the following types of CA's[3]:

Enterprise Root CA	Enterprise Subordinate CA
Stand-Alone Root CA	Stand-Alone Subordinate CA

[1] "A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server"; David S. Courington, March 29, 2001; http://www.sans.org/infosecFAQ/win2000/win2000_list.htm

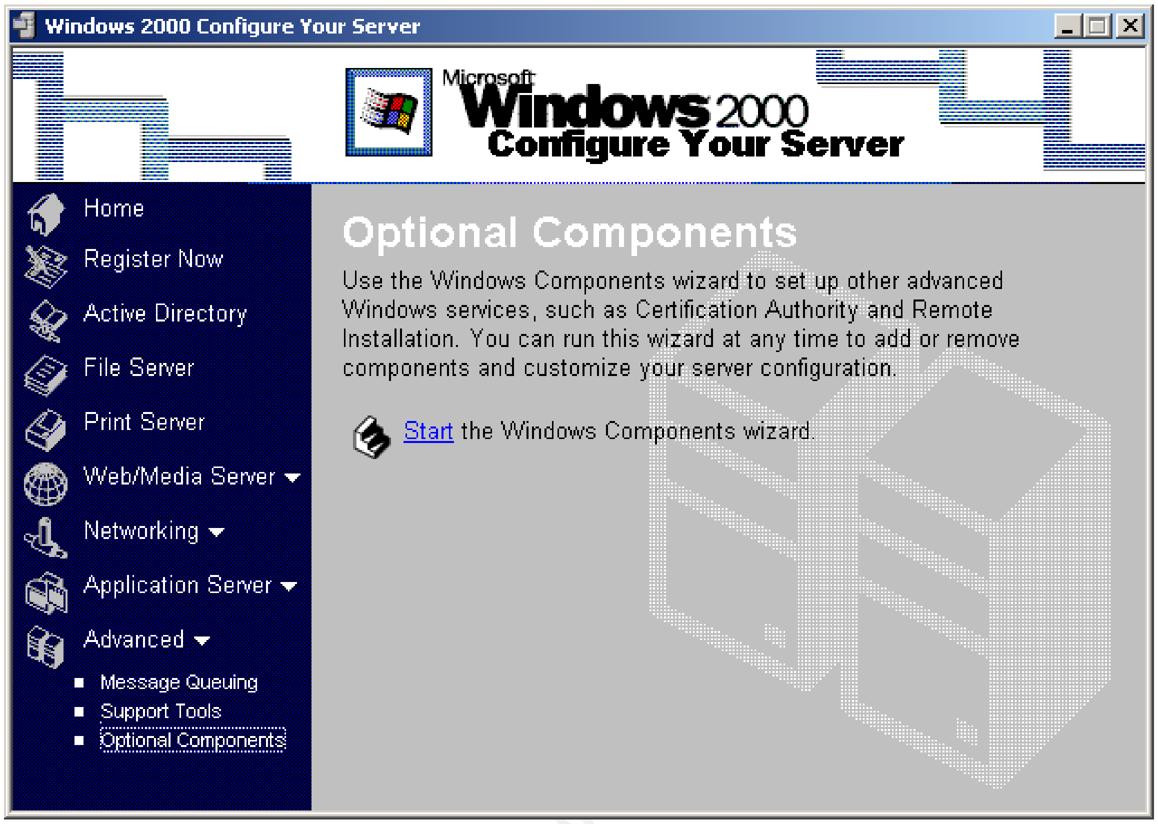
[2] "Evaluating the Cost of Ownership for Digital Certificate Projects"; The Aberdeen Group; July, 1998; http://www.verisign.com/library/reports/aberdeen/cost/index.html

[3] "Step-by-Step Guide to Setting up a Certification Authority"; Microsoft Corporation; February 16, 2000

An Enterprise CA would normally be installed as part of a corporate CA hierarchy, issuing certificates to subordinate CA's which in turn would issue certificates either to end-users or to further subordinate CA's. Enterprise root and subordinate CA's need Active Directory and DNS installed as well. Typically, you would use this when you expect that all of your PKI users will also be registered in the Active Directory of your Windows 2000 domain – as employees, for instance. In this case, an employee who registered would provide a shared secret – for instance, a Social Security Number – which would be compared to data in the Active Directory, and a certificate issued automatically. The shared secret is important – the certificate issued represents identity, and there must be some way to reasonably establish the identity of the certificate applicant. With any system that automatically issues a certificate, this will be problematic.

A stand-alone CA is typically used when certificates will be issued outside the enterprise. In this case, you would not expect to give each certificate holder an account in the Active Directory. However, if Active Directory is available, the stand-alone CA will make use of it. Since our sysadmin envisions issuing certificates outside the enterprise, and because this is still an NT shop with no Active Directory structure, he decides to go with the stand-alone CA.

Should the sysadmin create a root CA only, or subordinate CA's as well? This depends on the vision of the future the sysadmin maintains. If substantial growth is in the picture, a single CA will not scale. Multiple subordinate CA's must be used to segment the population, and each of these CA's must trust the others' certificates (in most scenarios). In this case, a root CA would be created and used to issue certificates for a number of subordinate CA's. These, in turn, might issue certificates for another layer of subordinate CA's, if the enterprise was very large; alternatively, they could begin issuing end-user certificates. As a general rule, one should assume growth, and create a root CA and a subordinate CA. In this way, additional subordinate CA's could be created as needed, without disrupting the existing infrastructure. The root CA would be taken offline and stored somewhere very secure in the interim. Again, for the purposes of this paper, in reality only a single root CA was created.



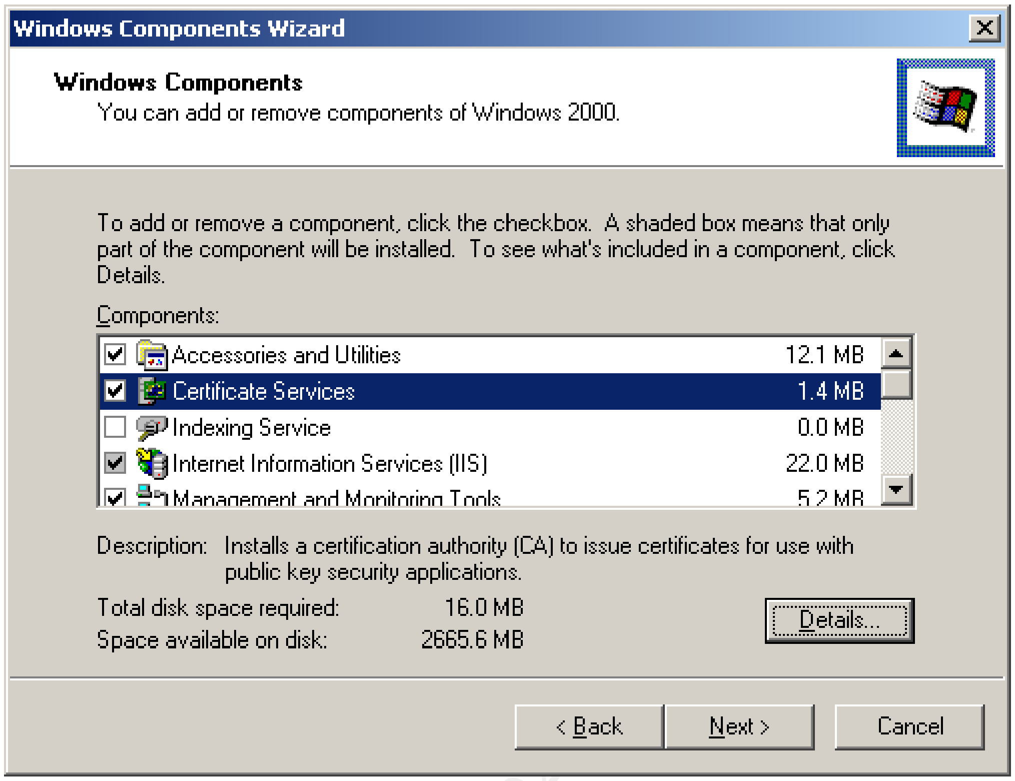
Optional Components

Use the Windows Components wizard to set up other advanced Windows services, such as Certification Authority and Remote Installation. You can run this wizard at any time to add or remove components and customize your server configuration.

Start the Windows Components wizard.

Figure 1: The Windows 2000 Component Wizard Splash Page

Windows 2000 offers a convenient way to add services to a new server. In this case, we are interested in turning this box into a Certification Authority.



Windows Components Wizard

Windows Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

✓	Accessories and Utilities	12.1 MB
✓	Certificate Services	1.4 MB
	Indexing Service	0.0 MB
✓	Internet Information Services (IIS)	22.0 MB
✓	Management and Monitoring Tools	5.2 MB

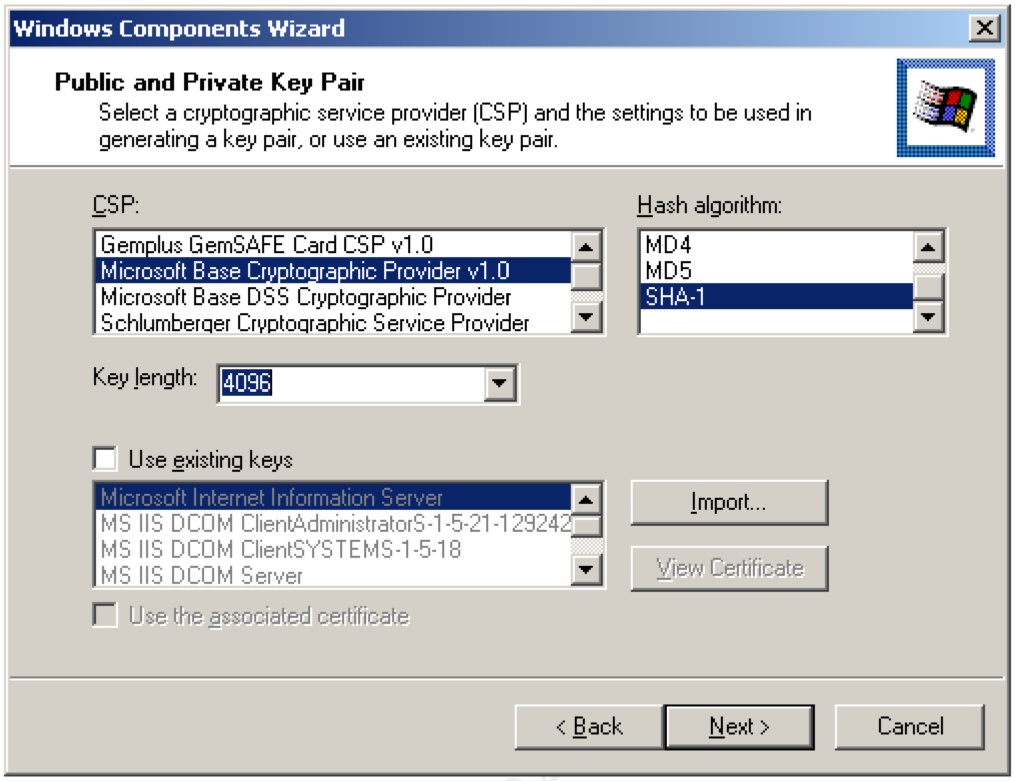
Description: Installs a certification authority (CA) to issue certificates for use with public key security applications.

Total disk space required: 16.0 MB

Space available on disk: 2665.6 MB

Figure 2: Adding Certificate Services

Adding Certificate Services is simply a matter of checking the appropriate box in the Component Wizard. However, failing to do your homework in advance will probably mean starting from scratch – possibly a disaster if you have already issued many certificates. Among the many pitfalls – after installing Certificate Services, you cannot change the domain or computer name without first uninstalling Certificate Services.


Windows Components Wizard

Public and Private Key Pair

Select a cryptographic service provider (CSP) and the settings to be used in generating a key pair, or use an existing key pair.

CSP:
Gemplus GemSAFE Card CSP v1.0
Microsoft Base Cryptographic Provider v1.0
Microsoft Base DSS Cryptographic Provider
Schlumberger Cryptographic Service Provider

Hash algorithm:
MD4
MD5
SHA-1

Key length: 4096

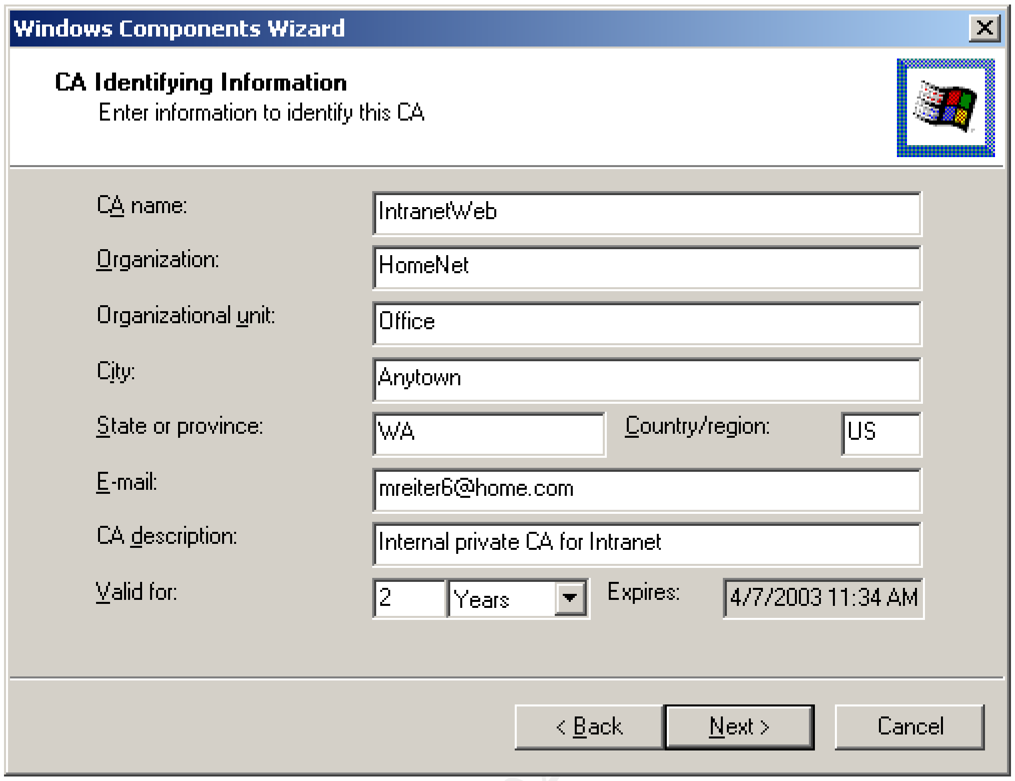
Use existing keys
Microsoft Internet Information Server
MS IIS DCOM ClientAdministratorS-1-5-21-129242
MS IIS DCOM ClientSYSTEMS-1-5-18
MS IIS DCOM Server

Use the associated certificate

Figure 3: Choosing the CSP

Unless there is a pressing reason to do otherwise, most sysadmins will want to choose the default Microsoft Cryptographic Service Provider (CSP). This is the component that does the actual encryption/decryption. This will provide the greatest interoperability and is not subject to government export restricitions[4].

[4] Windows 2000 Security, by Roberta Bragg; pp 448-450. 2001, New Riders Publishing


Windows Components Wizard

CA Identifying Information

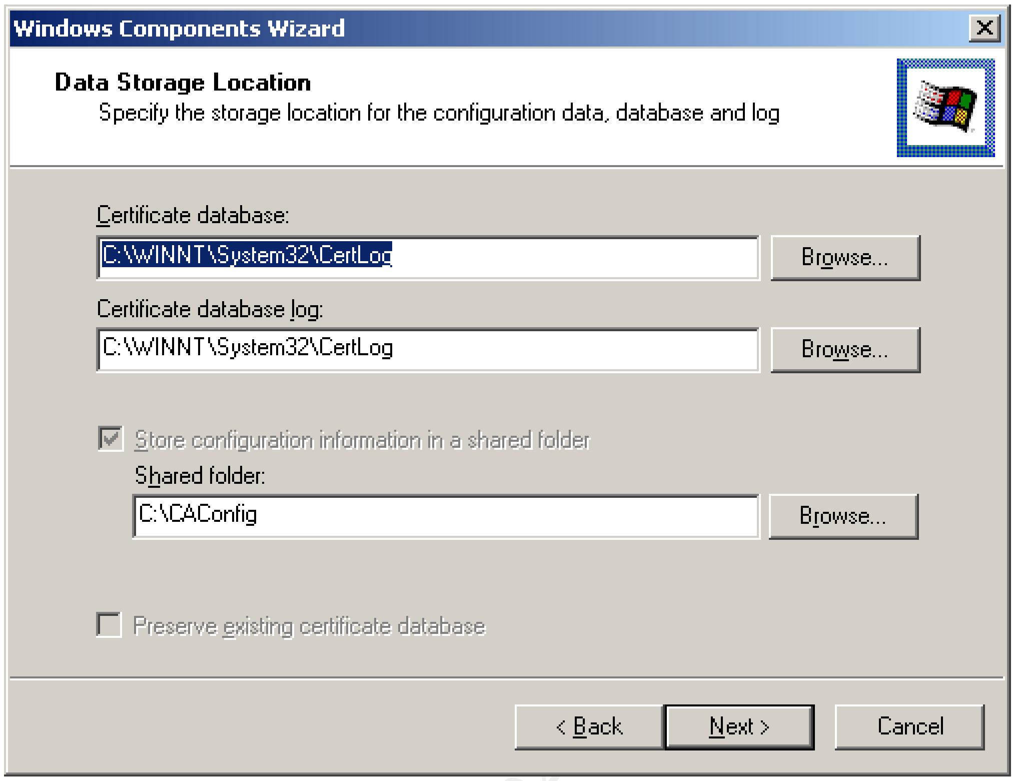
Enter information to identify this CA

CA name:	IntranetWeb
Organization:	HomeNet
Organizational unit:	Office
City:	Anytown
State or province:	WA
Country/region:	US
E-mail:	mreiter6@home.com
CA description:	Internal private CA for Intranet
Valid for:	2 Years
Expires:	4/7/2003 11:34 AM

Figure 4: CA Data

This data should be given careful thought – more careful, in fact, than was given to the window shown above. The categories listed above actually form X.509 fields in the root certificate and every certificate it issues. One thing that every sysadmin may take for granted is that most if not all of the original assumptions made at the beginning of the planning process will change at some point. Therefore, the fields – which are modeled after and designed to fit into an LDAP schema – should be as broad and generic as possible, without being completely meaningless. This way, when those assumptions change, the certificate fields will still be valid. Changing these fields after issuing certificates is impractical at best. In this case, the initial assumption was that this site was going to be solely an intranet sute; hence the CA name and description above.

At this point the CA's public/private key pair was generated.



Data Storage Location
Specify the storage location for the configuration data, database and log

Certificate database: C:\WINNT\System32\CertLog

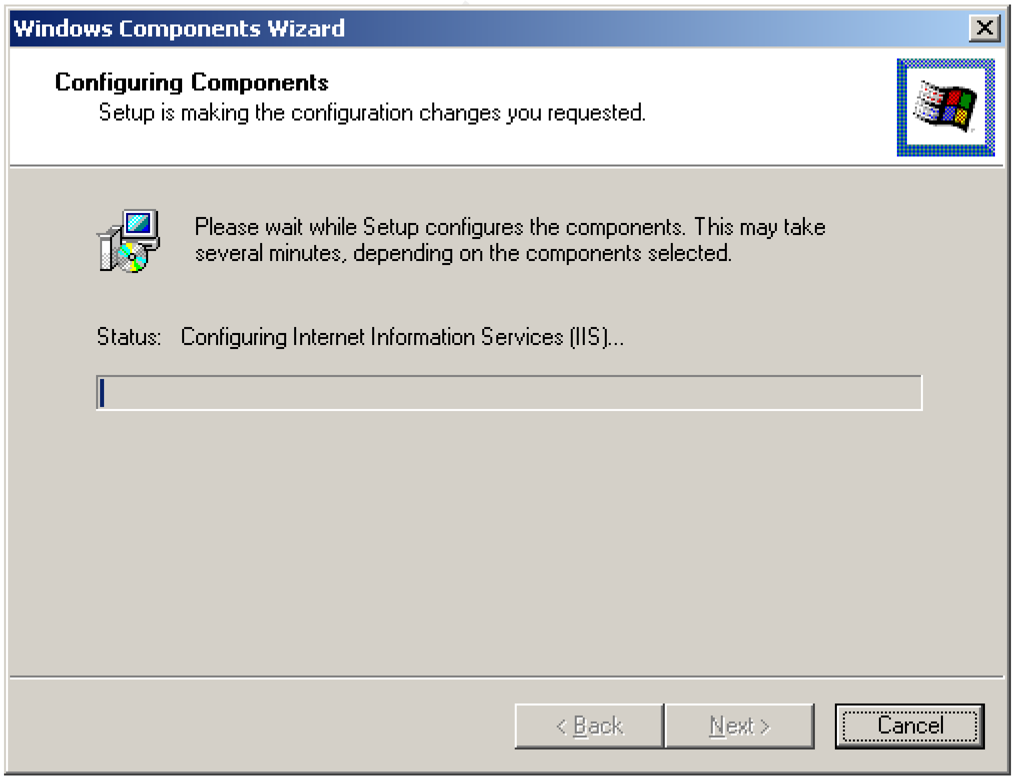
Certificate database log: C:\WINNT\System32\CertLog

[✓] Store configuration information in a shared folder

Shared folder: C:\CAConfig

[ ] Preserve existing certificate database

Figure 5: Default Data Storage Location

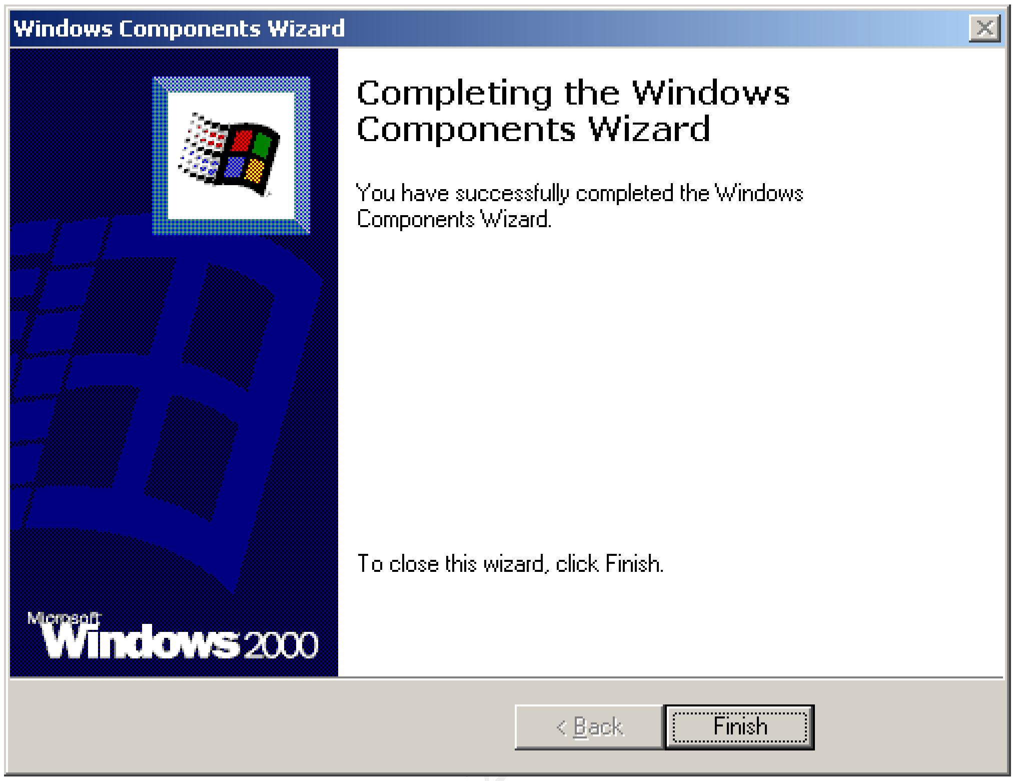


Configuring Components
Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Configuring Internet Information Services (IIS)...

Figure 6: Windows Does Its Thing



Windows Components Wizard

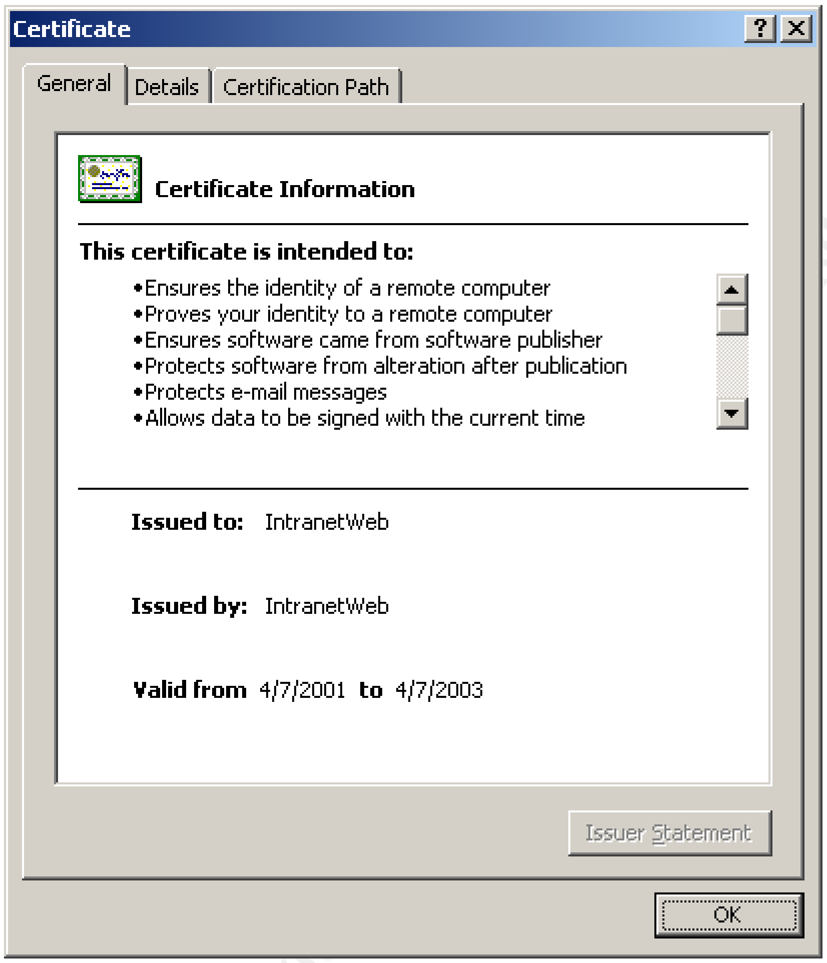
Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

Figure 7: Success!

Certificate Services is now installed, as well as a root CA certificate. The next step is to take a look at that certificate.



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

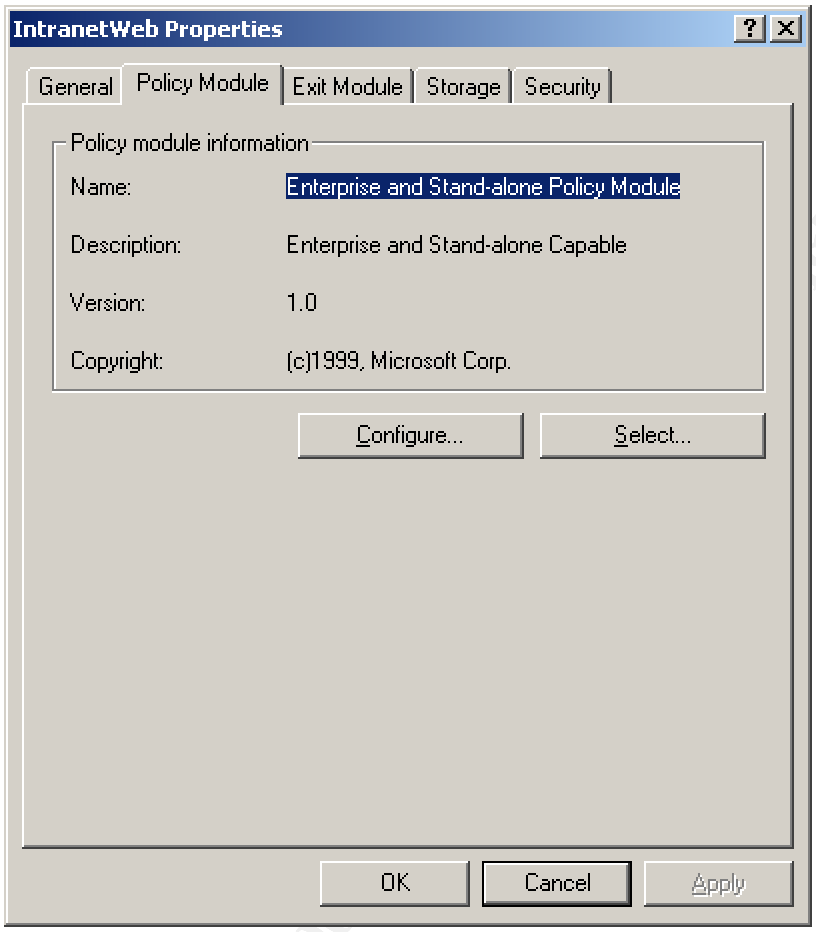
Issued to: IntranetWeb

Issued by: IntranetWeb

Valid from 4/7/2001 **to** 4/7/2003

Figure 8: The Certificate Information

This window tells us what the new certificate can do. Essentially, any function a certificate can do, this one can do. As a root CA, it would make no sense to limit the capabilities. New possibilities may arise overnight, causing major shifts in direction that require new functions. Best to have all possible capabilities.



IntranetWeb Properties

Policy module information

Name: Enterprise and Stand-alone Policy Module

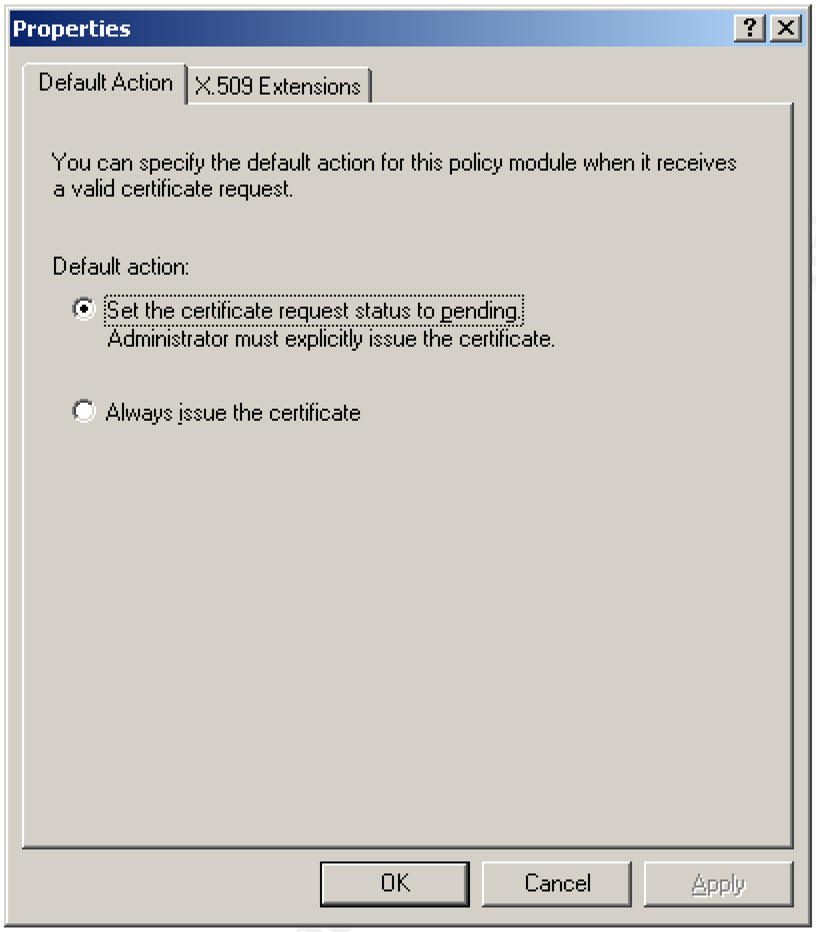
Description: Enterprise and Stand-alone Capable

Version: 1.0

Copyright: (c)1999, Microsoft Corp.

Figure 9: The Policy Module

Here, the sysadmin has to make a major decision: does the newly created CA issue a certificate automatically to all comers, or should it wait for manual approval?



You can specify the default action for this policy module when it receives a valid certificate request.

Default action:

(●) Set the certificate request status to pending. Administrator must explicitly issue the certificate.

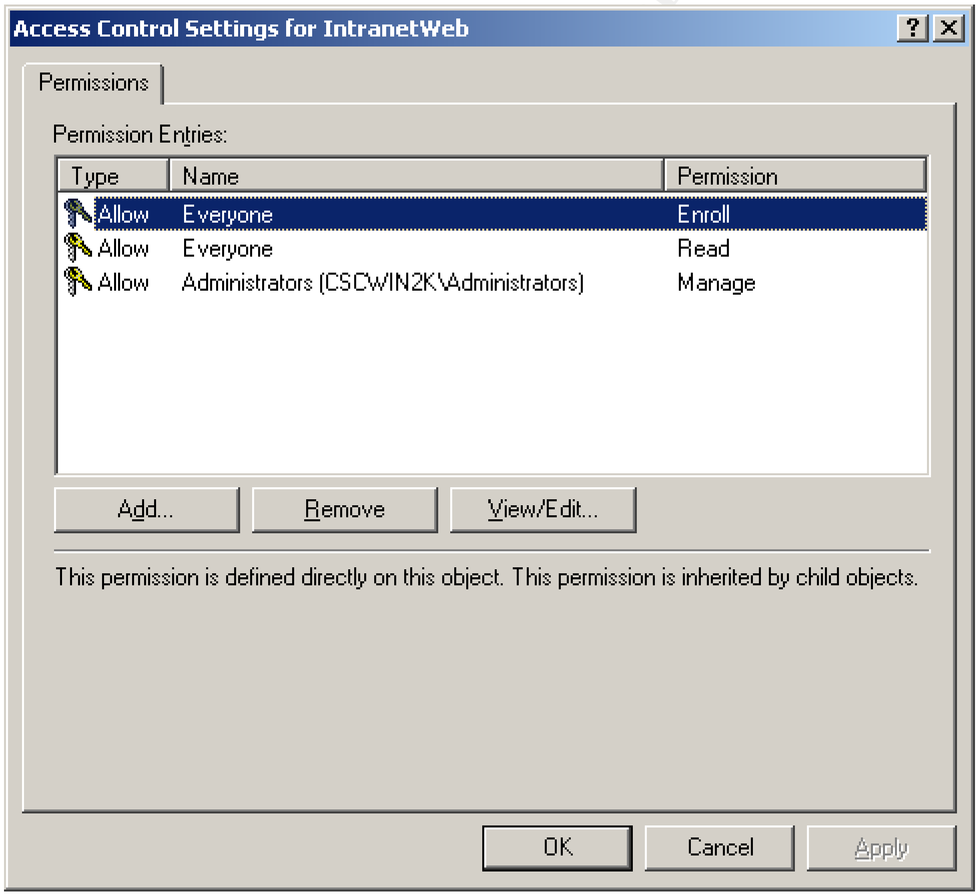
( ) Always issue the certificate

Figure 10: Certificate Request Status

The sysadmin makes the decision to set the certificate request to "pending", requiring the administrator to manually issue the certificate. This is a decision with far-reaching consequences. Manual issuance does not scale. If this site became popular on the scale of something like Amazon.com or Ebay, the number of certificate requests would quickly overwhelm the sysadmin's capability to verify the identity of the applicant and issue the certificate. And yet, if the option "Always issue the certificate" is set, there is no identity verification at all. In other words, the certificate provides no effective client authentication. Therefore, why have it?

All vendors of PKI's face this issue. There must be a scalable way for an individual to prove his or her identity prior to receiving a certificate. Ultimately, the only way for someone to truly prove identity is to physically go to another, trusted person who verifies identity based on driver's license, military ID, or some other document that provides reasonable assurance. Many other schemes have been devised to automate the process, usually involving a shared secret such as a Social Security Number or mother's maiden name. This data is now obtainable by anyone with a bit of savvy and perseverance. Therefore, a criminal could spoof another person's identity to get a certificate. Dumpster divers could easily gain the personal, confidential data most online identity verifiers require. Further, the online identity verifiers may access databases not generally

available to the public, such as credit bureaus. How many people want to provide increasingly private and sensitive information to a web site – even a trusted web site – to prove their identity?
An alternative is a service bureau that manually calls the applicant and verifies identity based on other data. In the case of a physician, this might be data such as medical license number, year of graduation, or other data.
Biometrics also provide an alternative, one that can provide high assurance of an individual's identity (although not yet absolute). However, this would require that the CA has a copy of the identifying characteristic in some form (usually a hash). How does it get there? We are back at the beginning of the problem.
This is not a Windows 2000 problem, but a PKI problem. We can issue certificates, but it is difficult to truly prove the identity of the end user. Since digital signatures are now legal signatures, the risks to an individual may actually rise substantially in the event of a compromise. These risks are discussed in some detail in *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*, By Carl Ellison and Bruce Schneier[5].



Type	Name	Permission
Allow	Everyone	Enroll
Allow	Everyone	Read
Allow	Administrators (CSCWIN2K\Administrators)	Manage

This permission is defined directly on this object. This permission is inherited by child objects.

Figure 11: Permissions

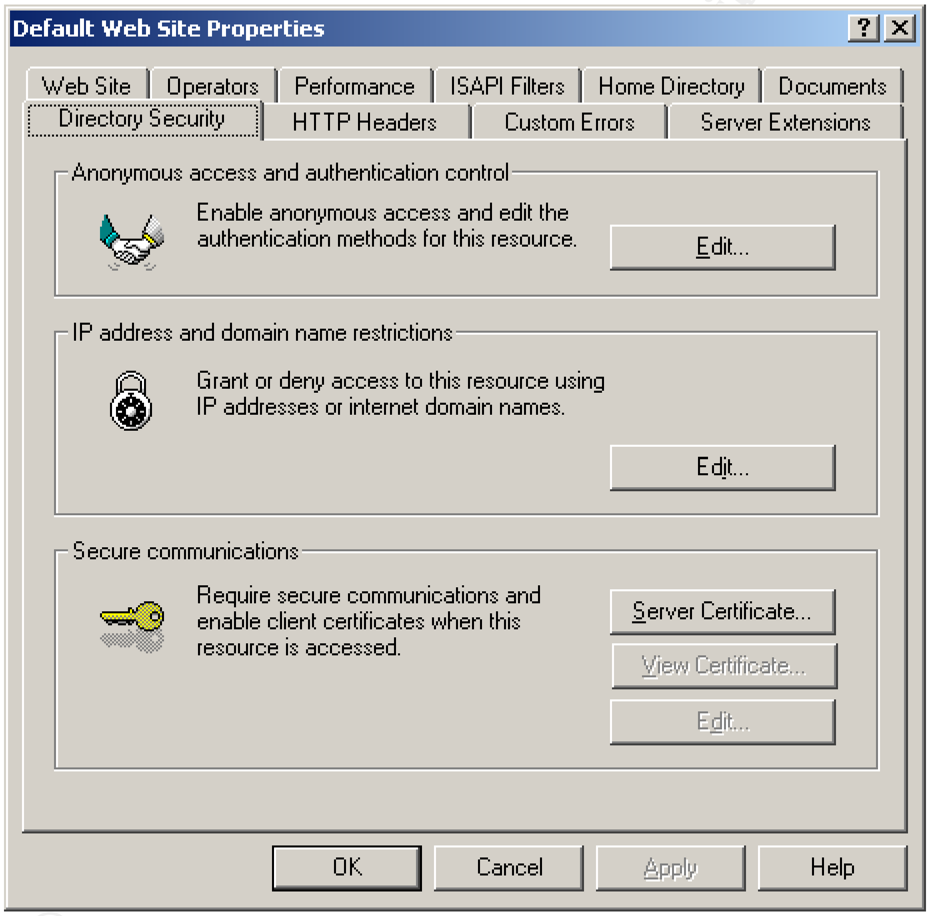
These are the defaults; they are reasonable, and the sysadmin (and most others) should

[5] "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure"; Computer Security Journal, Volume XVI, Number 1, 2000; Carl Ellison and Bruce Schneier

have no reason to change them.

Internet Information Server

A certificate authority may issue unlimited numbers of certificates, but there must be an application to take advantage of their capabilities. In this case, the certificate-aware application is Internet Information Server 5. IIS 5 is integrated into Windows 2000, but only if it is installed in the Windows Configuration tool. IIS appears as a Microsoft Management Console (MMC) snap-in or as a stand-alone. IIS 5 security is assumed to be configured in accordance with the procedures detailed in *Securing IIS on Windows 2000*[6] and *Securing Windows 2000 running IIS5*[7]; the actual details are beyond the scope of this paper, and it is assumed to be configured correctly.


Default Web Site Properties

Web Site | Operators | Performance | ISAPI Filters | Home Directory | Documents
Directory Security | HTTP Headers | Custom Errors | Server Extensions

Anonymous access and authentication control
Enable anonymous access and edit the authentication methods for this resource. [Edit...]

IP address and domain name restrictions
Grant or deny access to this resource using IP addresses or internet domain names. [Edit...]

Secure communications
Require secure communications and enable client certificates when this resource is accessed. [Server Certificate...] [View Certificate...] [Edit...]

[OK] [Cancel] [Apply] [Help]

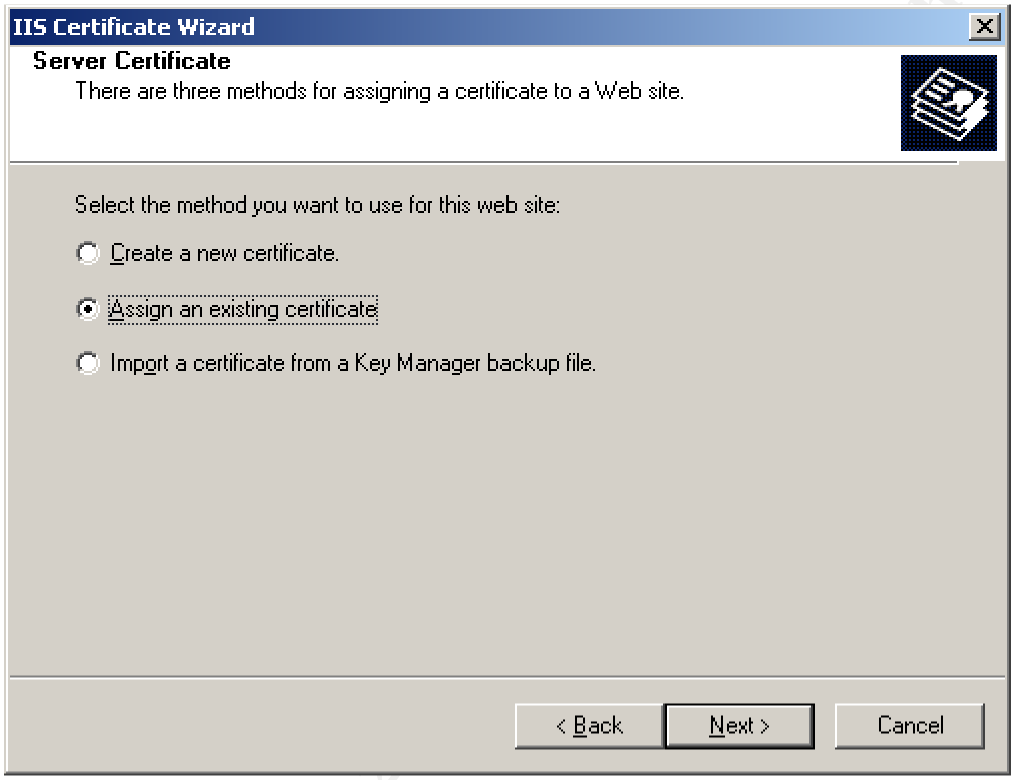
Figure 12: Internet Information Server Web Site Properties

The Directory Security tab holds most of the configurable parameters for a certificate

[6] Securing IIS on Windows 2000**;** Carl Denowh; March 6, 2001; http://www.sans.org/infosecFAQ/win2000/win2000_list.htm

[7] Securing Windows 2000 running IIS5; Alan McClelland; http://www.sans.org/y2k/practical/Alan_McClelland_GCNT.doc

authenticated web site. The sysadmin wants to create a certificate enrollment page that anyone can reach, and a protected page or set of pages that can only be accessed with a client certificate. So, under "Secure Communications" he clicks on "Server Certificate" to associate his web server with a CA.



IIS Certificate Wizard

Server Certificate

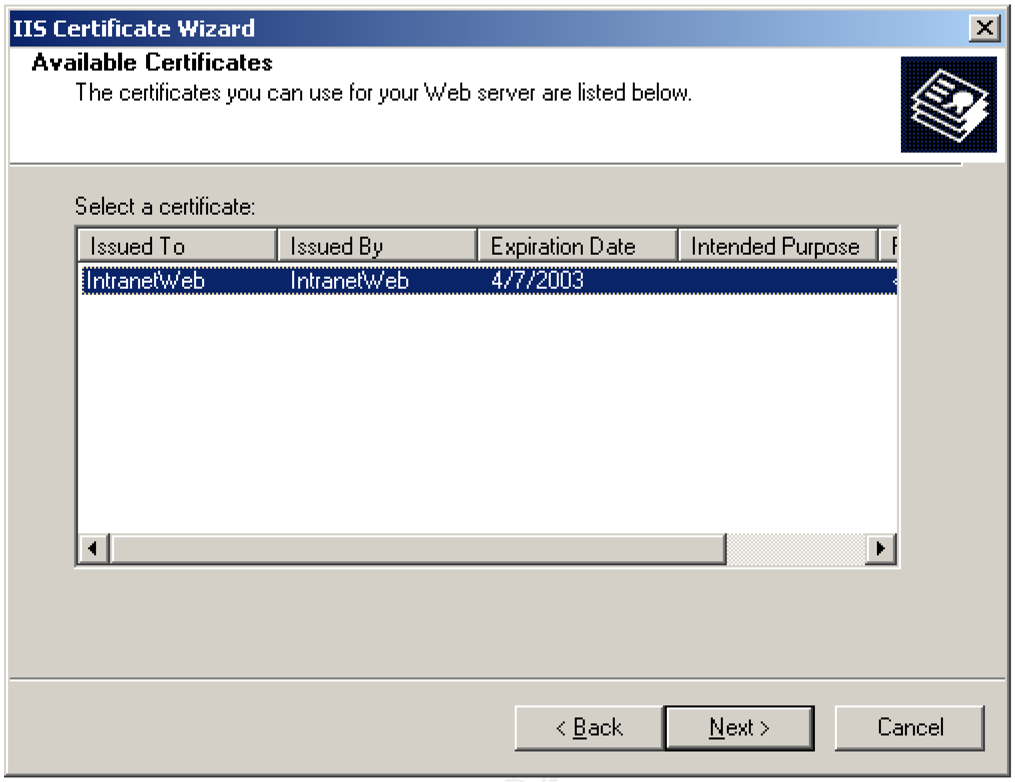
There are three methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

- ( ) Create a new certificate.
- [✓ Assign an existing certificate]
- ( ) Import a certificate from a Key Manager backup file.

Figure 13: The IIS Certificate Wizard

The sysadmin decides to assign the certificate he just created to his new web site.



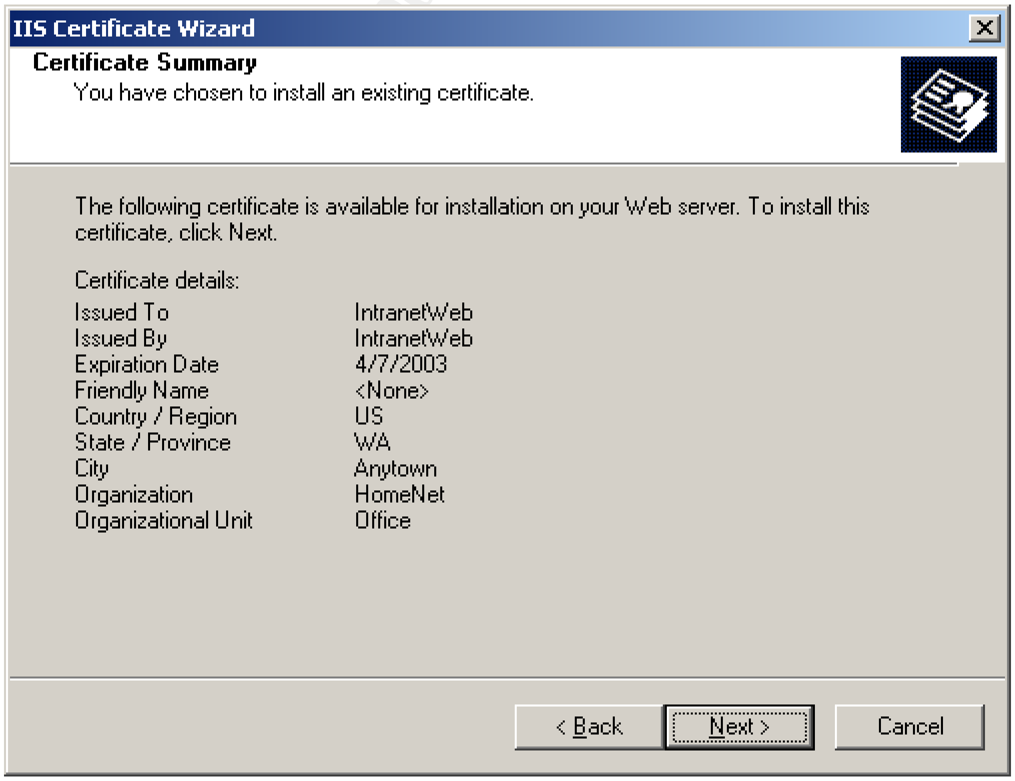
The certificates you can use for your Web server are listed below.

Select a certificate:

Issued To	Issued By	Expiration Date	Intended Purpose
IntranetWeb	IntranetWeb	4/7/2003	

Figure 14: The Store of Certificates

He has only one to choose.



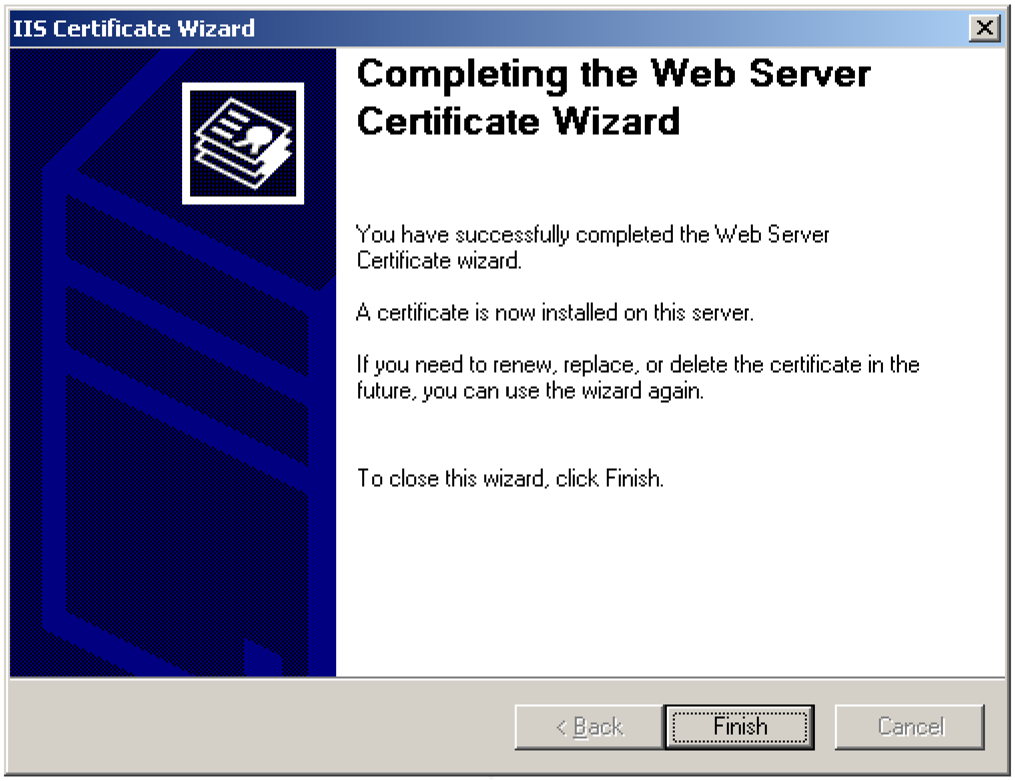
You have chosen to install an existing certificate.

The following certificate is available for installation on your Web server. To install this certificate, click Next.

Certificate details:

Issued To	IntranetWeb
Issued By	IntranetWeb
Expiration Date	4/7/2003
Friendly Name	<None>
Country / Region	US
State / Province	WA
City	Anytown
Organization	HomeNet
Organizational Unit	Office

Figure 15: Certificate Summary



Completing the Web Server Certificate Wizard

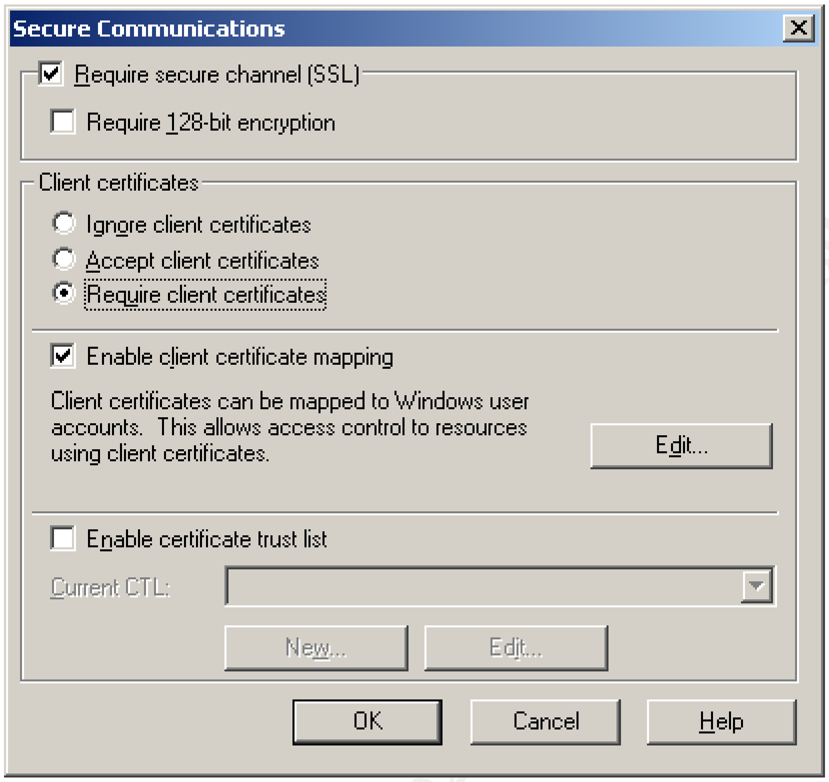
You have successfully completed the Web Server Certificate wizard.

A certificate is now installed on this server.

If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.

To close this wizard, click Finish.

Figure 16: Web Server Certificate Complete


Secure Communications

[✓] Require secure channel (SSL)

[ ] Require 128-bit encryption

Client certificates

○ Ignore client certificates

○ Accept client certificates

● Require client certificates

[✓] Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

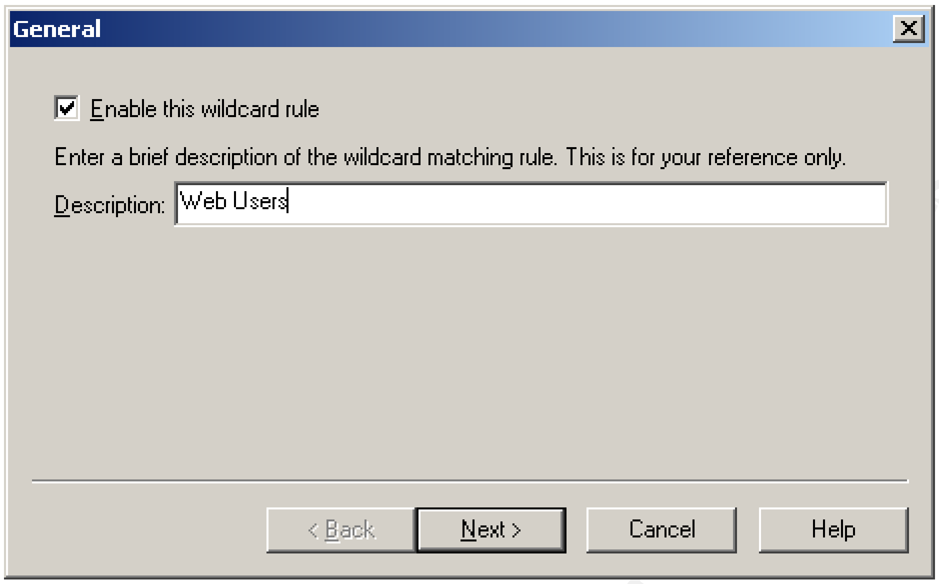
[ ] Enable certificate trust list

Current CTL:

Figure 17: Setting Up the Secure, Authenticated Connection

Here the sysadmin gets into the meat of the matter. Who actually gets into the site, and how? With the Configuration above, he expects to get an encrypted, authenticated connection. Note that this is still for the entire web site – the certificate enrollment pages will have to be reconfigured later to allow regular access to new users. He is not requiring 128 bit encryption because he does not yet plan to carry truly sensitive data, and many browsers still do not support 128 bit SSL out of the box. In fact, much to his surprise, he found that even after loading Service Pack 1 onto his Windows 2000 Server, he still had to go to the Microsoft site to download the High Encryption Pack separately. While 40 bit encrption has proven vulnerable to cracking, he does not consider this a significant issue. To require 128 bit SSL later would be relatively easy.

He also decides to enable client certificate mapping. This allows him to add an additional layer of security to the system. He clicks on the "Edit" button.


General

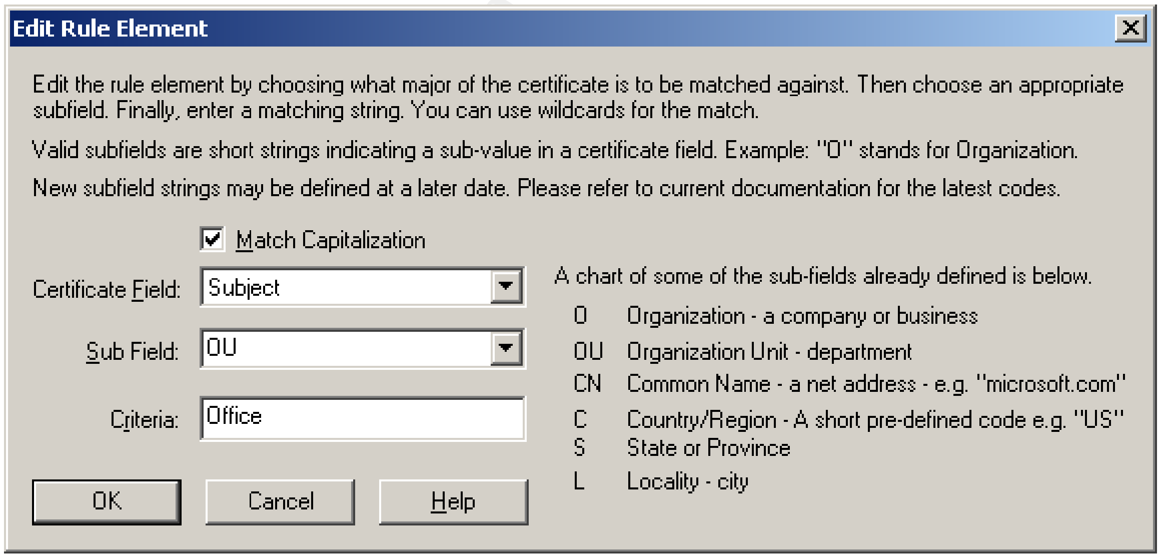
☑ Enable this wildcard rule

Enter a brief description of the wildcard matching rule. This is for your reference only.

Description: Web Users

Figure 18: Building a Mapping Rule

The sysadmin elects to use many-to-one mapping, which will allow him to assign multiple end users to a small number of accounts based on data contained in their certificates. For instance, he can break users down by their organizational unit (OU), which equates to their company department. Different departments might have differing levels of access.


Edit Rule Element

Edit the rule element by choosing what major of the certificate is to be matched against. Then choose an appropriate subfield. Finally, enter a matching string. You can use wildcards for the match.

Valid subfields are short strings indicating a sub-value in a certificate field. Example: "O" stands for Organization.

New subfield strings may be defined at a later date. Please refer to current documentation for the latest codes.

☑ Match Capitalization

Certificate Field: Subject

Sub Field: OU

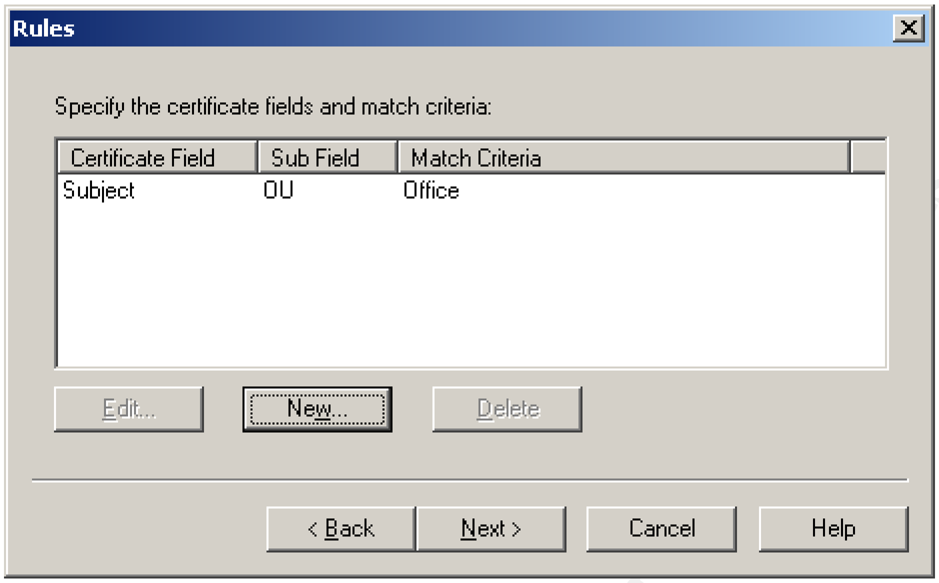
Criteria: Office

A chart of some of the sub-fields already defined is below.

O	Organization - a company or business
OU	Organization Unit - department
CN	Common Name - a net address - e.g. "microsoft.com"
C	Country/Region - A short pre-defined code e.g. "US"
S	State or Province
L	Locality - city

Figure 19: Setting the Rule Parameters

The Office department or OU will be the initial criterion. Others can be defined at later dates. Further, additional fields (extensions) can be added to the certificates later if required; older users would simply exchange their existing certificates for the new ones.

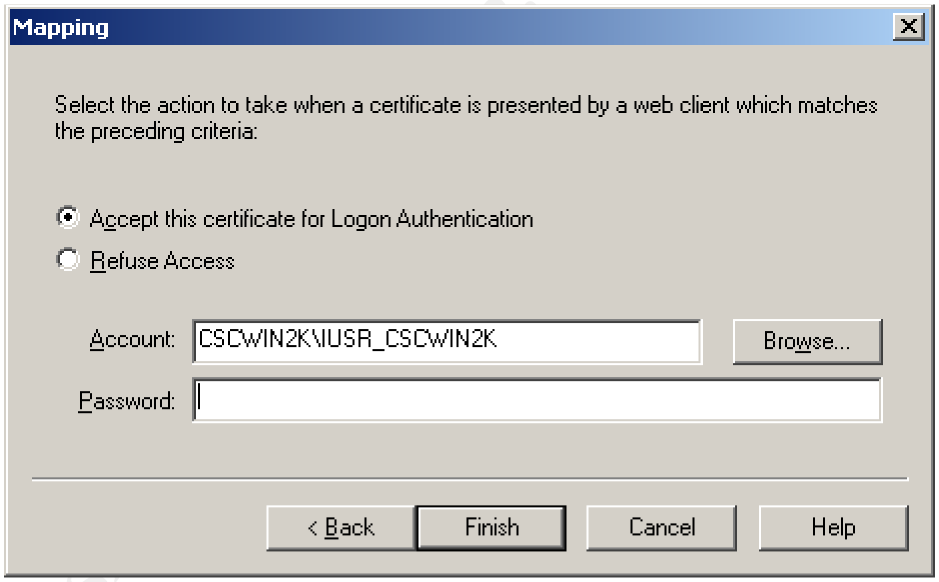


Rules

Specify the certificate fields and match criteria:

Certificate Field	Sub Field	Match Criteria
Subject	OU	Office

Figure 20: Setting the Rule



Mapping

Select the action to take when a certificate is presented by a web client which matches the preceding criteria:

[✓ Accept this certificate for Logon Authentication]

Refuse Access

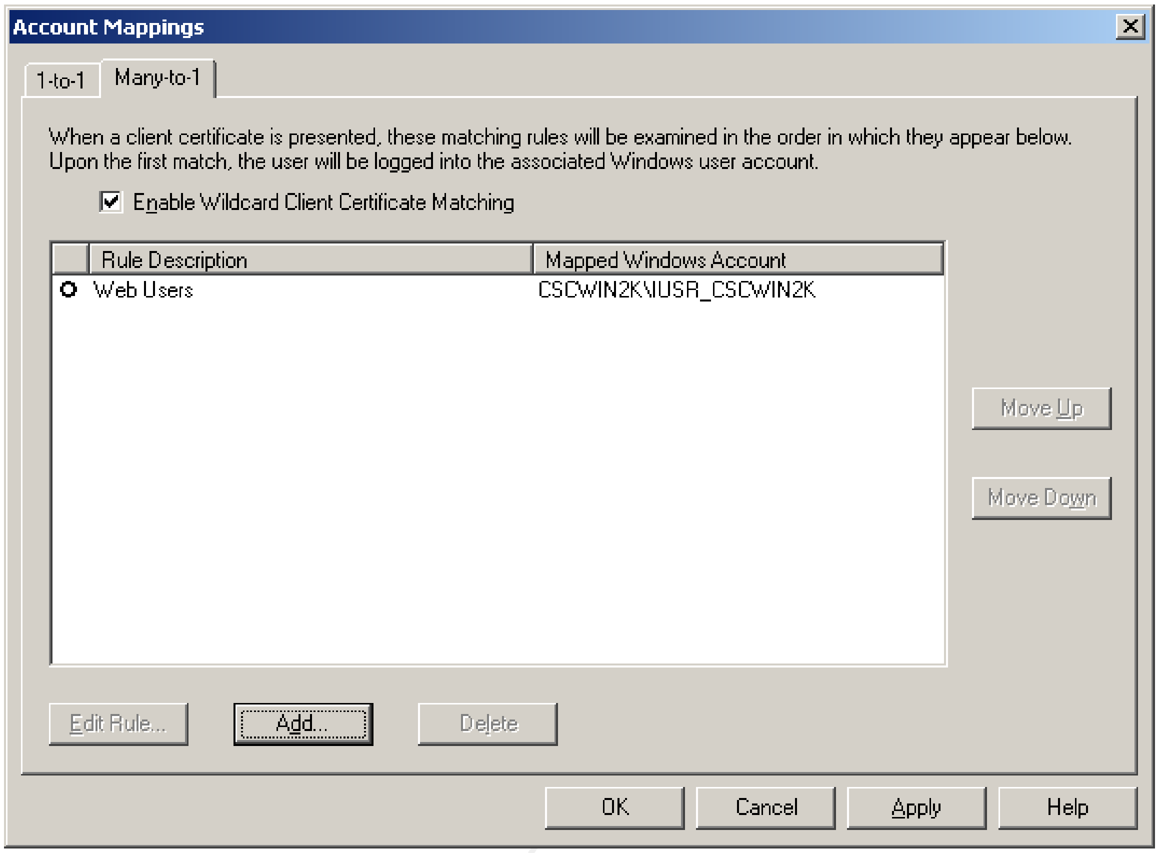
Account: CSCWIN2K\IUSR_CSCWIN2K

Password:

Figure 21: Mapping the Rule to an Account and an Action

The sysadmin selects the default anonymous IIS user account for now. Again, the mapping can be changed later. If the Windows 2000 environment expands, he may add Active Directory to the mix. After migrating his existing users and certificates to the Active Directory, he can take advantage of Group Policies and Group Policy Objects, thus implementing a form of Role-Based Access Control[8].

[8] Implementing Password Controls and Account Policies Using Windows 2000 Group Policy; Carlo Scannella; February 15, 2001; http://www.sans.org/infosecFAQ/win2000/win2000_list.htm



When a client certificate is presented, these matching rules will be examined in the order in which they appear below. Upon the first match, the user will be logged into the associated Windows user account.

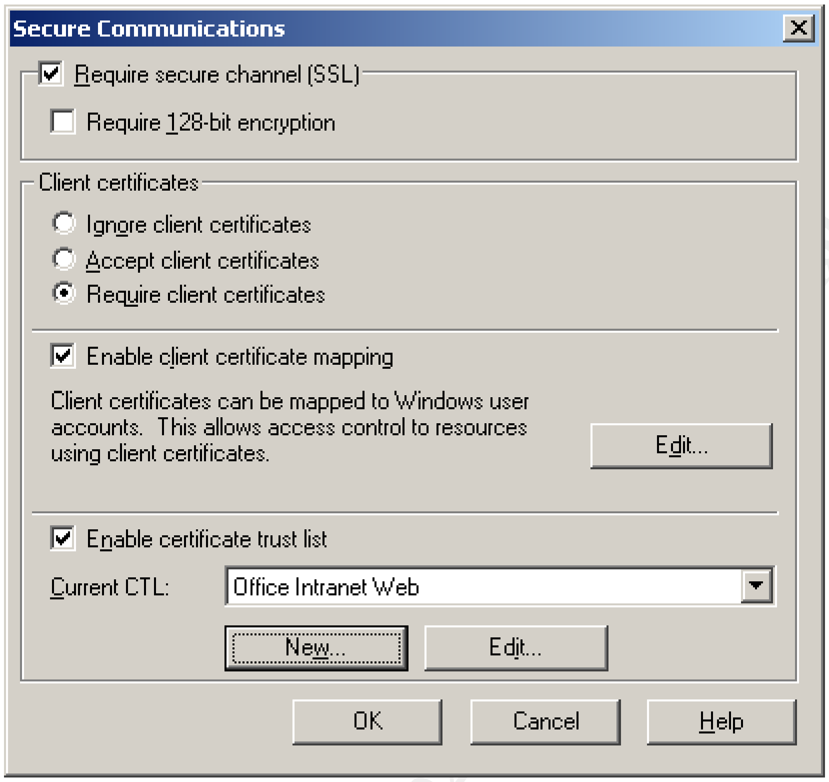
[✓] Enable Wildcard Client Certificate Matching

	Rule Description	Mapped Windows Account
○	Web Users	CSCWIN2K\IUSR_CSCWIN2K

Figure 22: Apply the Rule

There is a potentially huge security hole here. As it is currently configured, <u>any</u> certificate presented to server with a subject OU of "Office" may be granted access[9]. This is regardless of the originating CA. Now, there is no way for an intruder to find this out from an external probe; however, an administrator-level compromise of the web server would reveal it. Alternatively, someone might discover this by accident or industrial espionage. In any case, the sysadmin wants to close this hole. Fortunately, this is almost as easily said as done.

[9] "So You Want to Build a Win2K PKI", by Curtis Dalton; Information Security Magazine, May 2000; http://infosecuritymag.com/articles/may00/cover_a.shtml



Secure Communications

- [✓] Require secure channel (SSL)
  - [ ] Require 128-bit encryption

Client certificates

- ○ Ignore client certificates
- ○ Accept client certificates
- ● Require client certificates

- [✓] Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

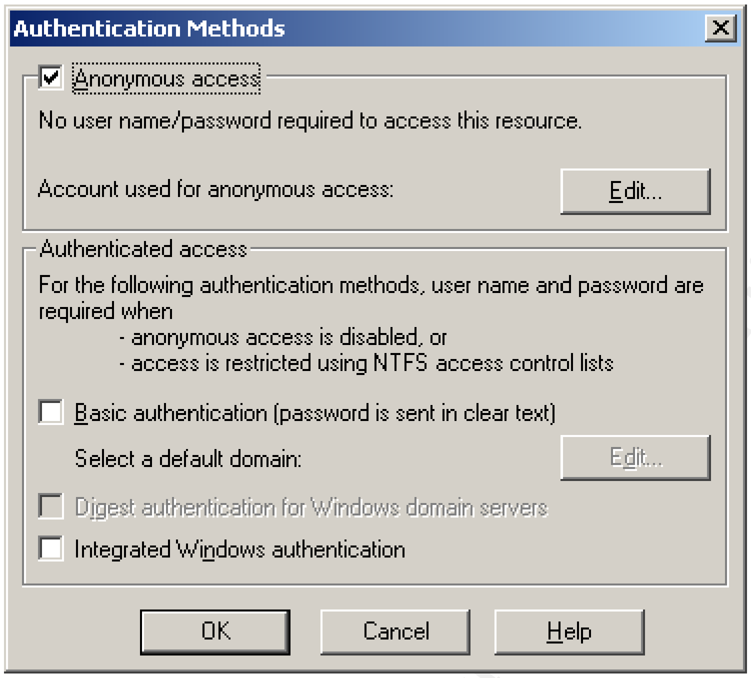
- [✓] Enable certificate trust list

Current CTL: Office Intranet Web

Figure 23: The Certificate Trust List

Going back to the Secure Communications window, the sysadmin enables the Certificate Trust List, and specifies his CA. Now, only certificates that he issues – regardless of the OU – will have access to the secured site. Should the shop ever go to a Windows 2000 native environment and build an internal PKI integrated with Active Directory, he could simply create a certificate trust list that included both his internet users and his internal users. This would have the same effect as cross-certifying multiple CA's[10]

[10] Windows 2000 PKI, Smart Cards, and the Encrypting File System, by Jason Fossen; sans.org, 2001


Authentication Methods

[✓] Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

[ ] Basic authentication (password is sent in clear text)

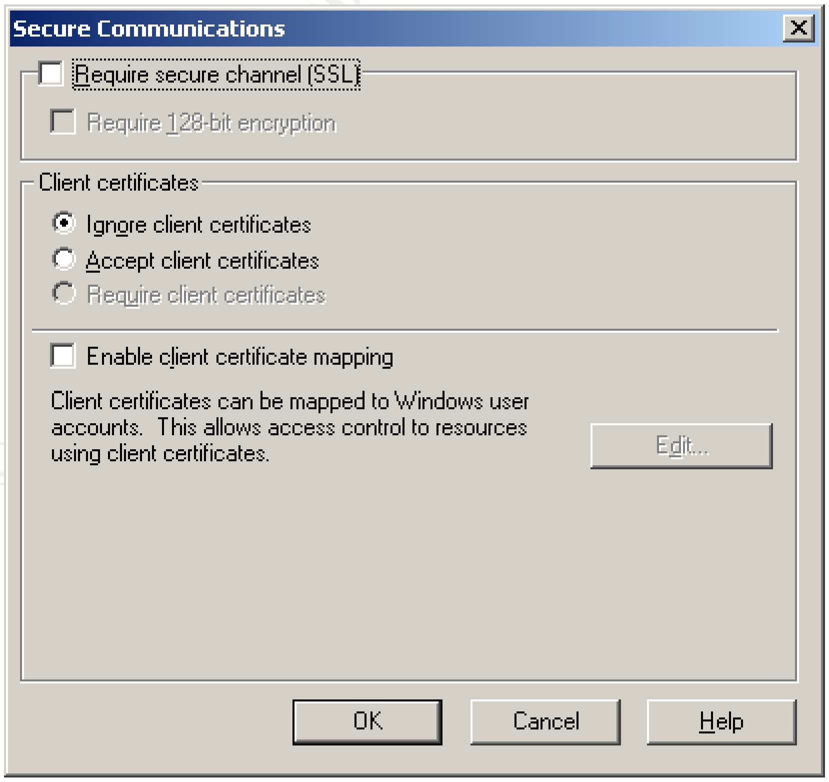
Select a default domain:

[ ] Digest authentication for Windows domain servers

[ ] Integrated Windows authentication

Figure 24: Altering the Access Rules for Certificate Enrollment

The certificate authority now protects the entire web site. So, how does a user get to the enrollment pages? These pages, which are found in the CertSrv virtual directory, must be removed from certificate-based authentication so that unregistered users can access them. The first step is to check and ensure that anonymous access is enabled.


Secure Communications

[ ] Require secure channel (SSL)

[ ] Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

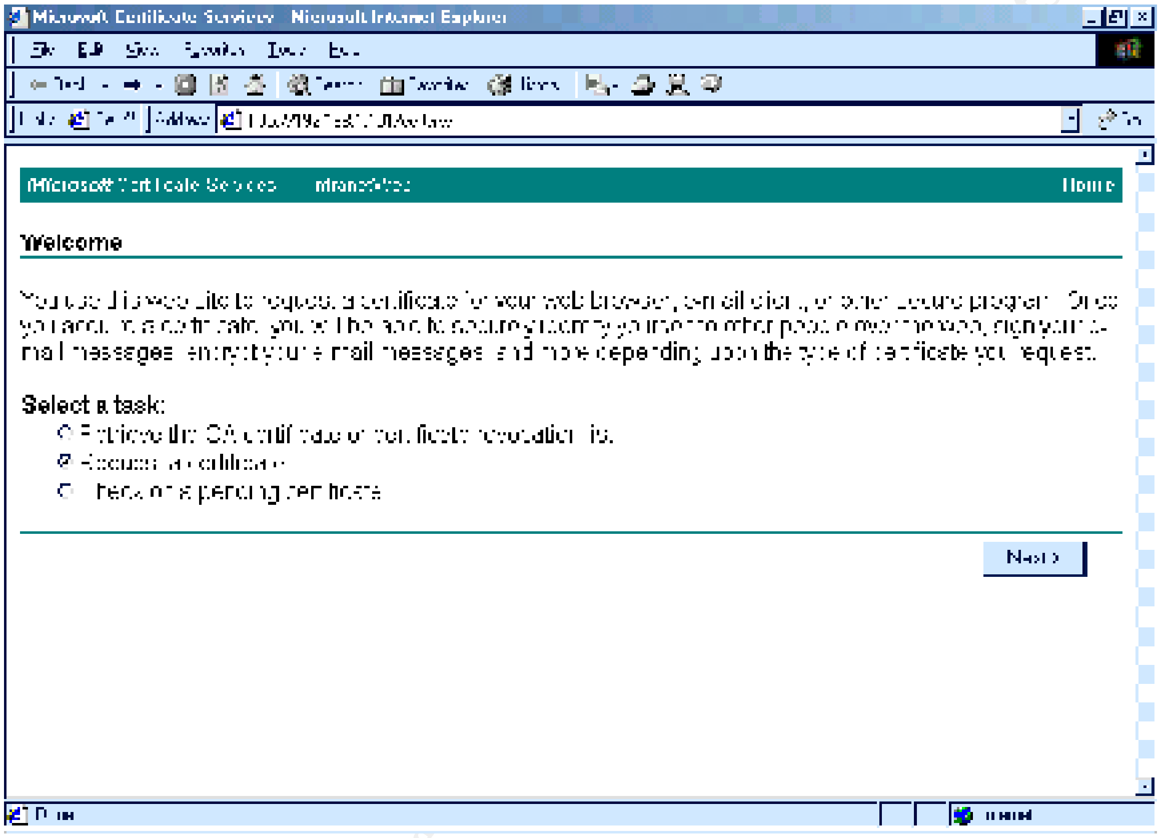
[ ] Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

Figure 25: Accessing the CertSrv Virtual Directory

Going into the "Secure Communications…Edit" function for the CertSrv virtual directory, the sysadmin selects "Ignore Client Certificates". This makes them ordinary web pages. Contrary to the illustration above, the sysadmin should also have chosen "Require secure channel (SSL)" and (in some cases) "Require 128-bit encryption", so that the data used to fill the X.509 fields is transmitted encrypted.

Enrolling for a Certificate



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Links Address
Go
Done
Internet

Microsoft Certificate Services -- [illegible] Home

Welcome

You use this Web site to request a certificate for your Web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the Web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

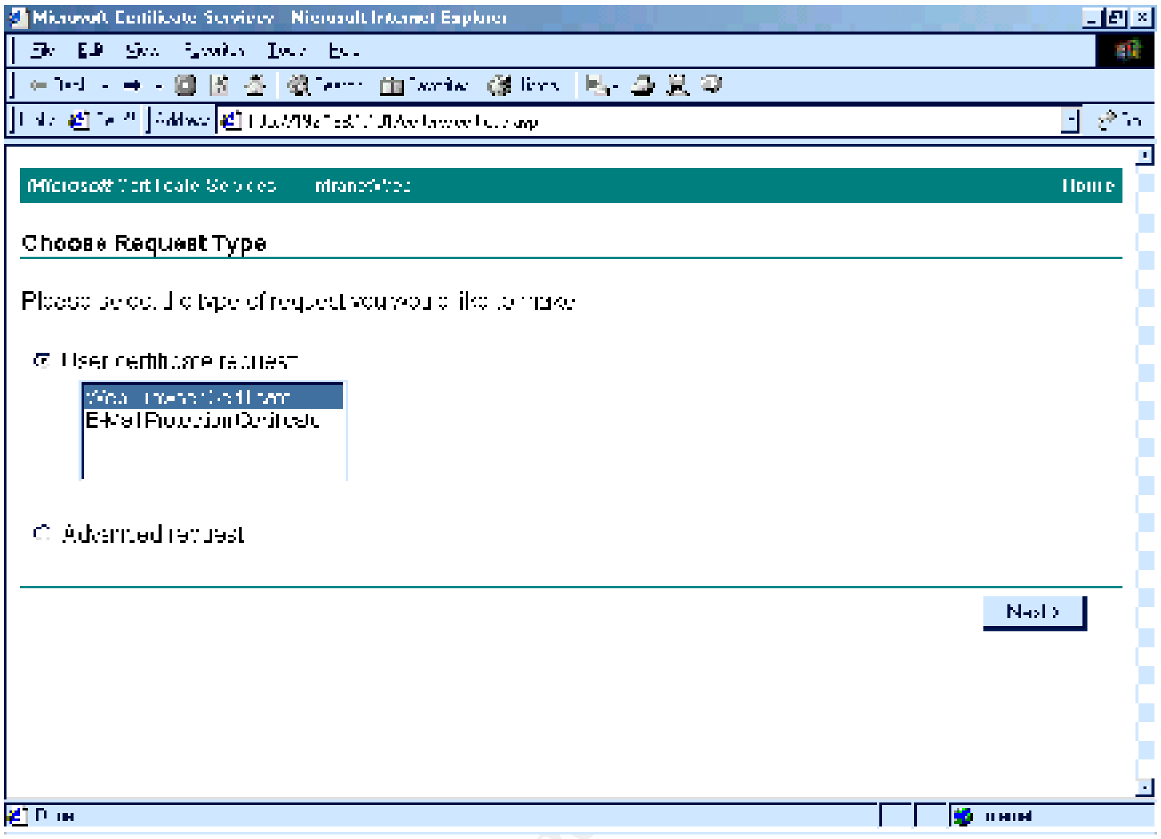
Select a task:

- ○ Retrieve the CA certificate or certificate revocation list
- [✓ Request a certificate]
- ○ Check on a pending certificate

Next >

Figure 26: The Certificate Enrollment Page

Using the IP address of the site (he has not registered the domain with DNS yet; obviously, in this example, we are using a non-routable IP due to the real-world limitations of building this system on a home network), the sysadmin goes to the CertSrv virtual directory to begin the enrollment process. These pages are created by default in IIS. A company that wanted more personalized pages could easily go in and alter the HTML to customize them as desired.


Microsoft Certificate Services - Microsoft Internet Explorer
Microsoft Certificate Services
Home
Next >

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

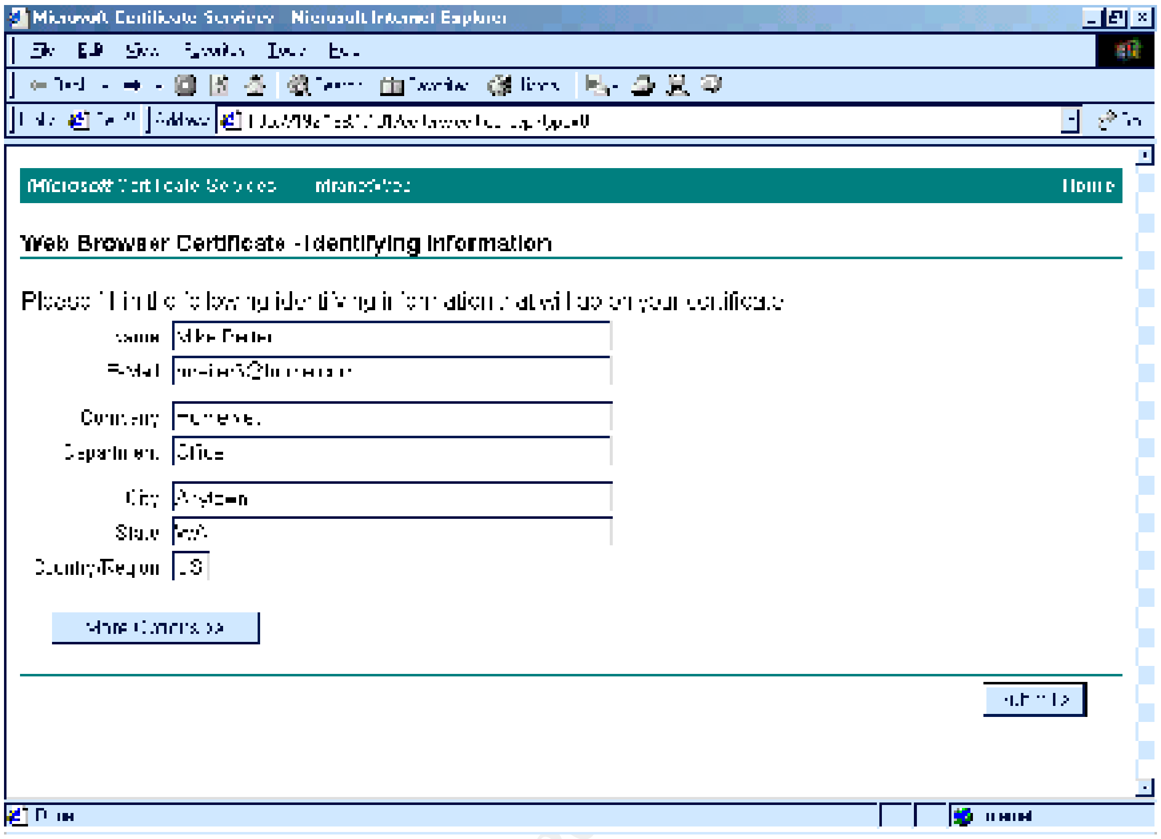
Web Browser Certificate

E-Mail Protection Certificate

Advanced request

Figure 27: Requesting a Browser Certificate

The end user also has the option to get a certificate for e-mail; e-mail encryption and signing is outside the scope of this paper. Assuming a compatible browser, the configuration process is reasonably simple, and encryption/decryption of email is simple, if not quite transparent.


Microsoft Certificate Services

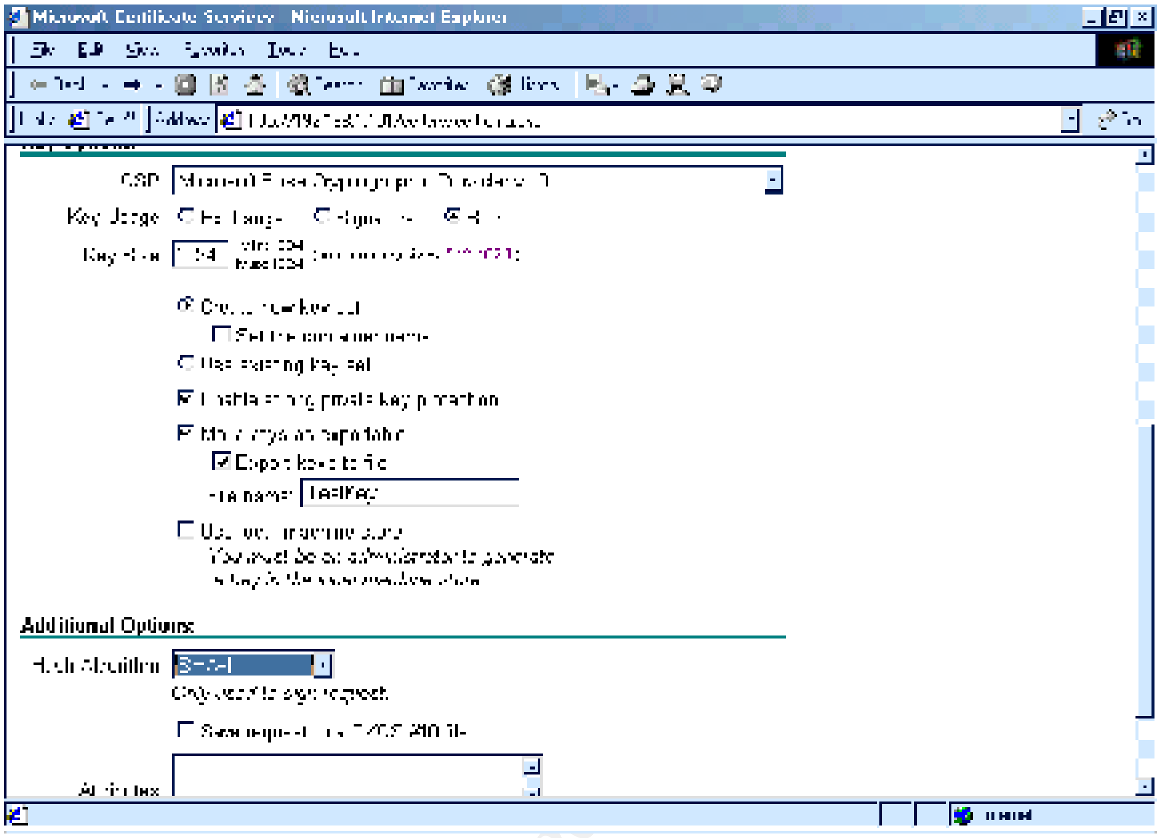
Web Browser Certificate - Identifying Information

Please fill in the following identifying information to be used on your certificate

Name	Mike Pelter
E-Mail	[illegible]
Company	[illegible]
Department	Office
City	Anytown
State	WA
Country/Region	US

Figure 28: Certificate Data

In this default form there is nothing to restrict the end user from inserting illegal or unusable data. Again, the page is configurable. For the production system, the sysadmin would alter the Department field to be a pull-down menu with choices limited to actual departments; an error checking script would prevent other data from being uploaded.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: ○ Exchange ○ Signature ● Both

Key Size: 1024 Min: 384 Max: 1024 (common key sizes: 512 1024)

● Create new key set

☐ Set the container name

○ Use existing key set

☑ Enable strong private key protection

☑ Mark keys as exportable

☑ Export keys to file

File name: TestKey

☐ Use local machine store
You must be an administrator to generate a key in the local machine store.

Additional Options

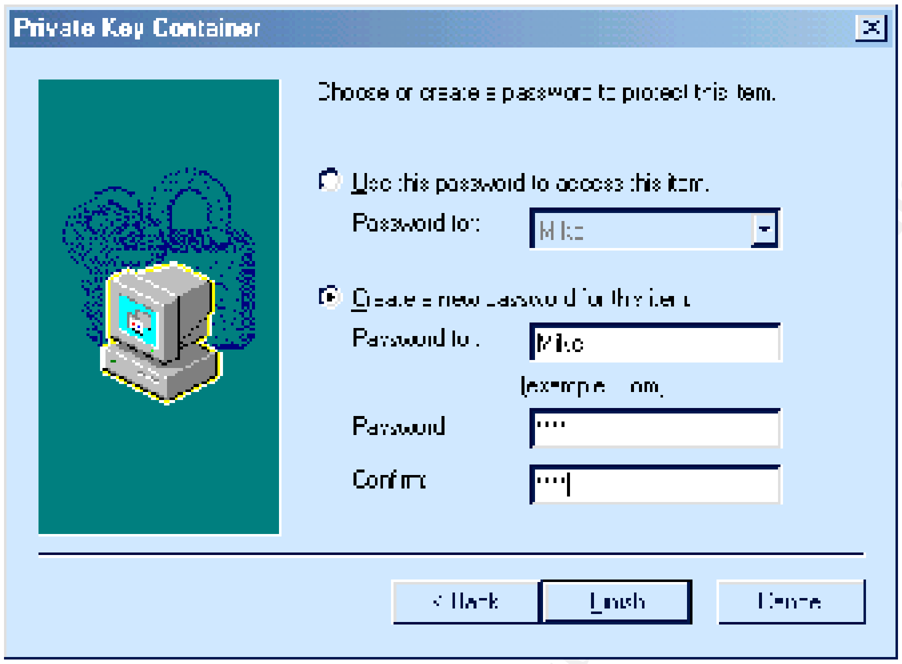
Hash Algorithm: SHA-1
Only used to sign request.

☐ Save request to a PKCS #10 file

Attributes:

Figure 29: Advanced Options

These options are accessible via the “More Options” button. In most cases, it would be advisable to disable this function, as the majority of users will use these options to misconfigure their certificate, causing additional admin overhead. Set the defaults, and remove these pages for production.


Private Key Container

Choose or create a password to protect this item.

Use this password to access this item.

Password for: Mike

Create a new password for this item. [✓]

Password for: Mike

(example: ... com)

Password: ****

Confirm: ****

Figure 30: Generating the Public-Private Key Pair

This function is handled by the browser. A Netscape browser goes through an analagous process. Microsoft gives the end user a choice of three security levels: High, Medium, and Low, with Medium the default. In Low security, the browser selects whatever certificate has the highest priority when challenged by the web server. This is transparent to the user. Medium security presents the end user with a popup window with a list of the available certificates and allows the user to pick one, without supplying a password. In a Windows NT or 2000 environment, where each person has an account and the individual's certificate only shows up when the end user is logged in, this does not present a problem. However, in a less secure environment – one where multiple users are on one machine, and there is no individual logon – this provides no security at all. Only the High security option, which prompts the user for a Private Key Container password each time the key is accessed, gives this environment any security. There are still many facilities where the desktops are primarily Windows 9x. There is a hitch here, however. An undocumented "feature" found in Windows 9x and Windows NT is that the password popup window will show and require a password each time the key is accessed within a single session – depending on the type of session, potentially dozens or even hundreds of times. The average end user will balk at this. End user acceptance is critical to many applications, and certainly a web site that requires unending passwords will quickly be abandoned. The author contacted Microsoft about this issue (in relation to another PKI implementation) and was told that this was not a bug but a security feature, and that they had fixed it in Windows Millennium and Windows 2000, which cache the password during the session. Their response is below:

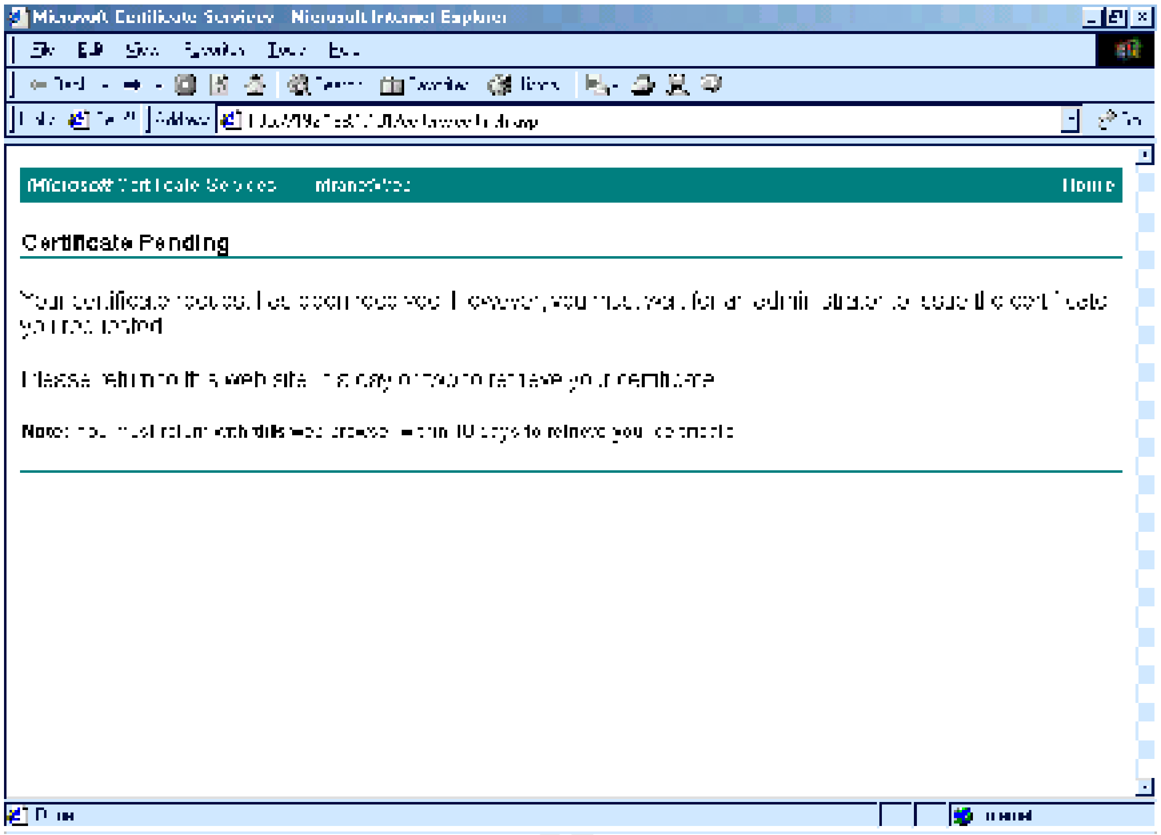
```
It is not possible to configure your clients so that the
password would only prompt once. The option "strong private
key protection" selection prompts for a password
continuously.  Your only other option would be to upgrade
```

```
the clients to Windows 2000.

This behavior you describe is actually by design. When the
feature to password encrypt the certificate locally was
implemented, it was done so that each request would require
the password to be retyped. In Windows 2000 the
implementation was changed.

The reason it is saved in Windows 2000 is because
subsequent calls (calls after the first request for the
cert password) to CryptSignHash use a cached private key in
Windows 2000 and does not in the down-level clients.

Your only options are to disable the "strong private key
encryption" or upgrade the clients to Windows 2000[11].
```

Netscape, on the other hand, allows the end user to decide how often to be prompted for the private key password: once per session, once per transaction, or once every *x* minutes.

Screen captures of key generation pages were skipped due to problems with interruptions during public/private key generation

[11] Personal Communication with Microsoft Support, March, 2001


Microsoft Certificate Services - Microsoft Internet Explorer
Home

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

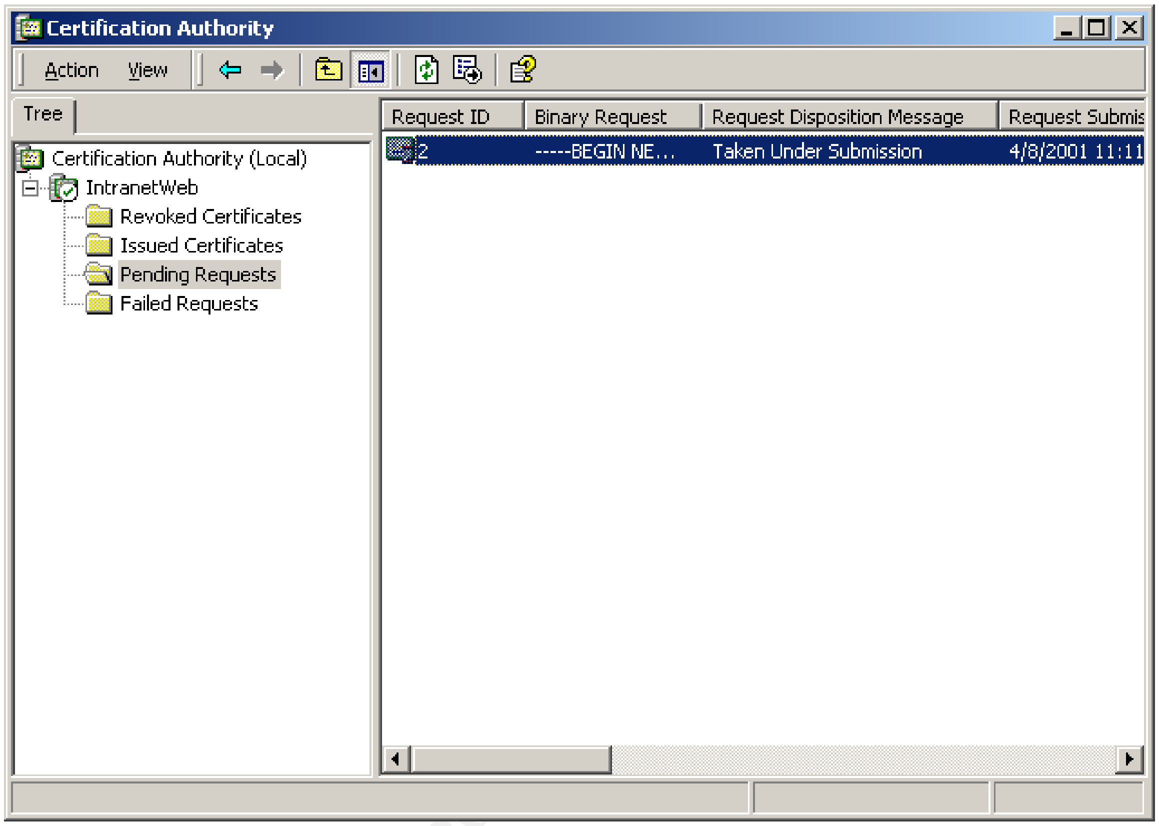
Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

Figure 31: Pending Certificate

Now it is time to wait. We are doing manual administration here, so the admin has to see the request, verify the identity of the requestor, and the approve the request. This is cumbersome on a small scale and potentially impossible on a large scale, as discussed above. The sysadmin must look into authentication service bureaus if he expects to do anything else when this site becomes popular.

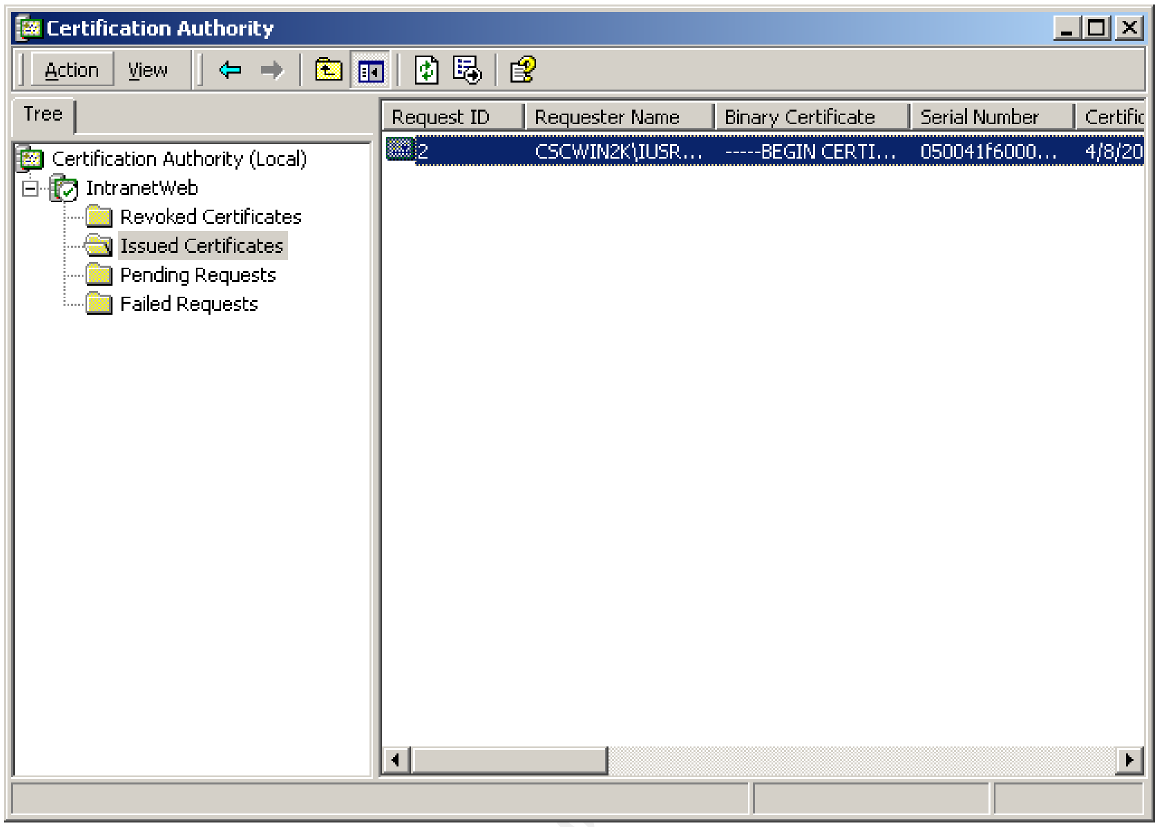
Approving the Certificate Request



Request ID	Binary Request	Request Disposition Message	Request Submis
2	-----BEGIN NE...	Taken Under Submission	4/8/2001 11:11

Figure 32: The Certification Authority Window

Checking the Pending Certificates folder, the sysadmin sees his certificate request. He approves his request – identity verification is not an issue here.

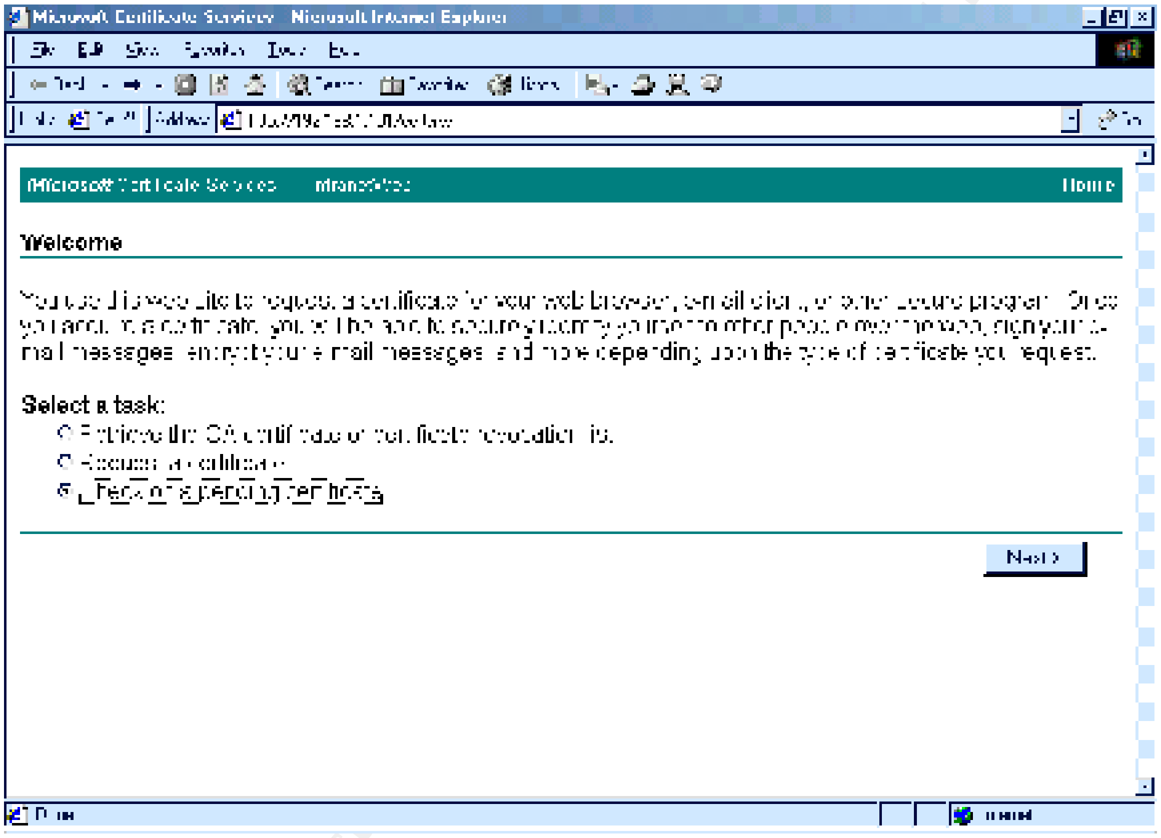


Request ID	Requester Name	Binary Certificate	Serial Number	Certific
2	CSCWIN2K\IUSR...	-----BEGIN CERTI...	050041f6000...	4/8/20

Figure 33: Approved

The certificate now moves to the Issued Certificates folder.

Downloading the Certificate to a Browser


Microsoft Certificate Services - Microsoft Internet Explorer
Microsoft Certificate Services
Home
Next >

Welcome

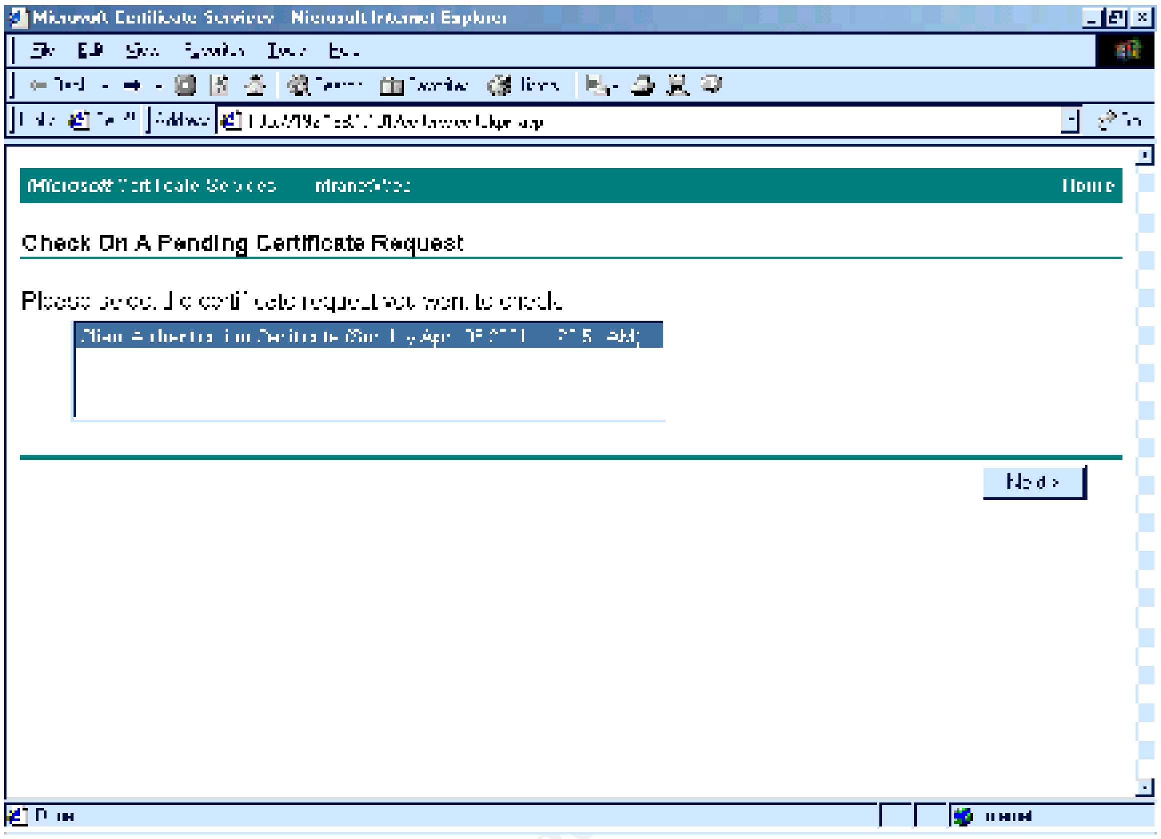
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- [✓ Check on a pending certificate]

Figure 34: Checking Pending Requests

The end user (here, the sysadmin) begins the process of downloading a certificate to his browser. Again, there is a usability issue here. How does the end user know when to check back? Presumably, there is a script triggered by approval that sends an email to the end user notifying him or her to come to this URL and begin the process. This script must be custom written to suit the site.


Microsoft Certificate Services - Microsoft Internet Explorer
Microsoft Certificate Services
Home
Next >

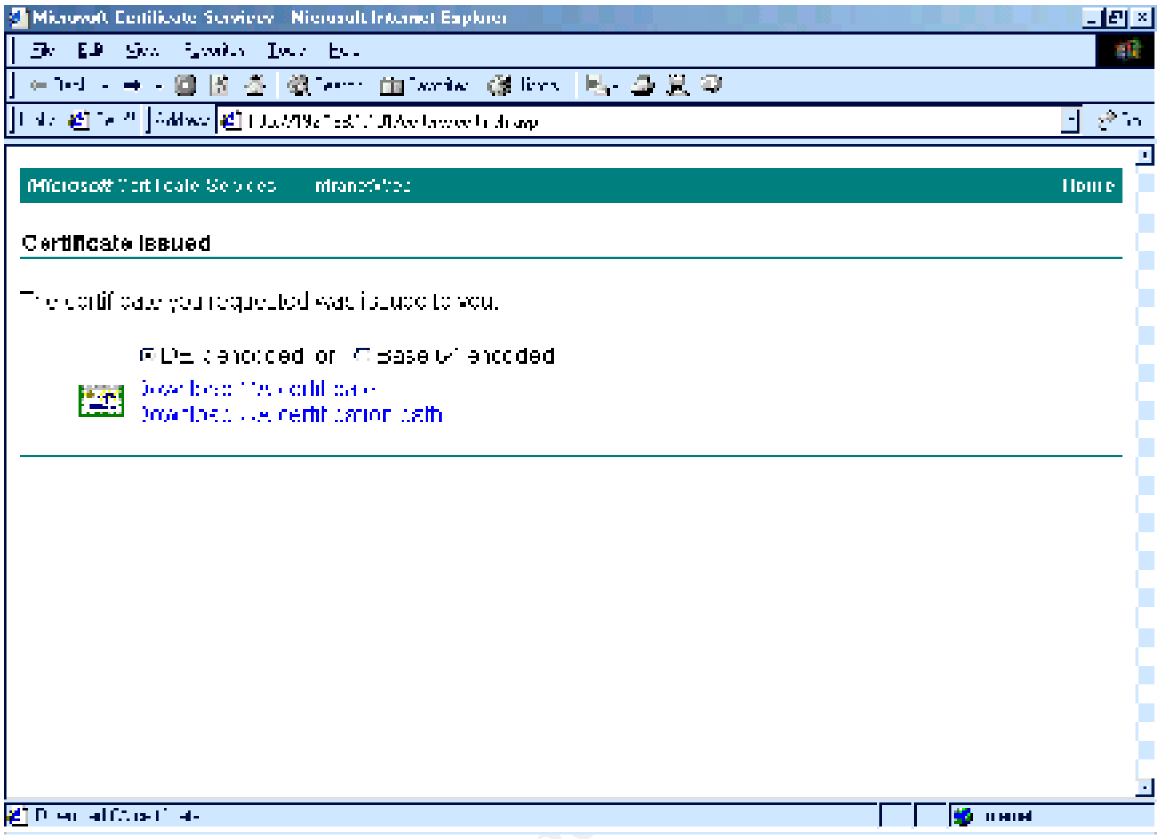
Check On A Pending Certificate Request

Please select the certificate request you want to check:

Client Authentication Certificate (Saturday, April 28, 2001 [illegible] AM)

Figure 35: The Request

It is possible for one individual to have more than one ceertificate; in fact, in many environments it would be unusual to have only one certificate. Each certificate might cover a different aspect of the user's identity. Of course, having too many certificates would quickly become cumbersome. In this case, the use of tokens or smart cards might become necessary.



Microsoft Certificate Services -- [illegible] Home

Certificate Issued

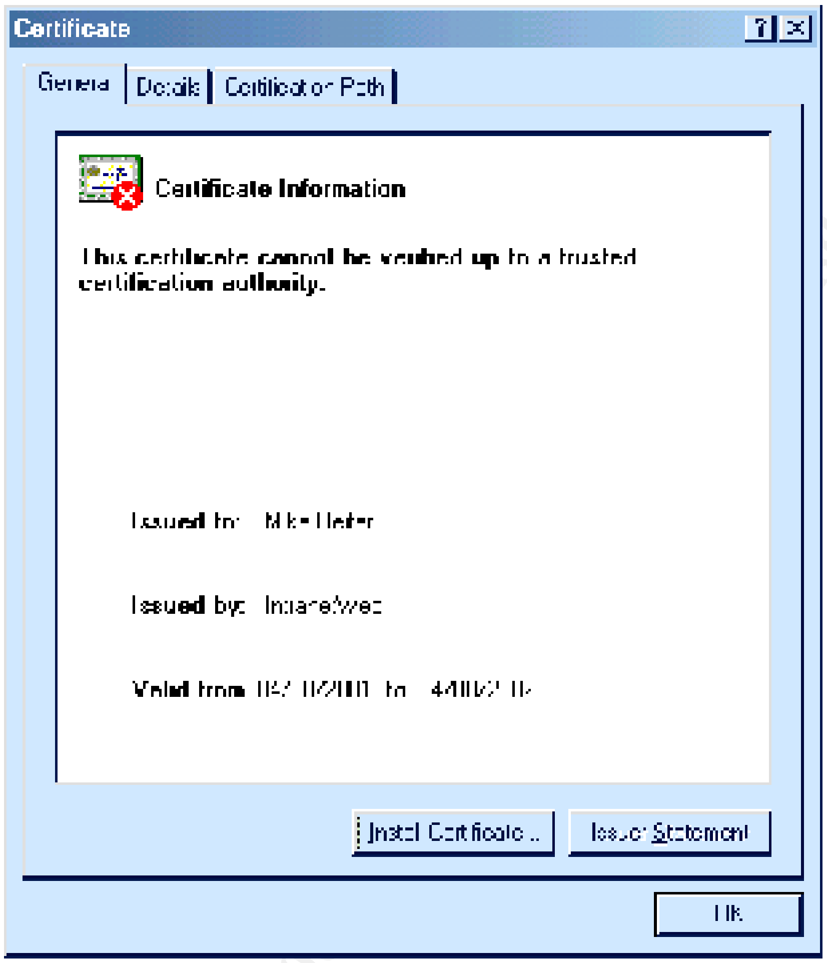
The certificate you requested was issued to you.

[✓ DER encoded] or Base 64 encoded

Download CA certificate
Download CA certification path

Figure 36: Downloading the Certificate

The end user must install the certificate, and the root CA as well, since this is self-signed. The browser will guide the user through this process.



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

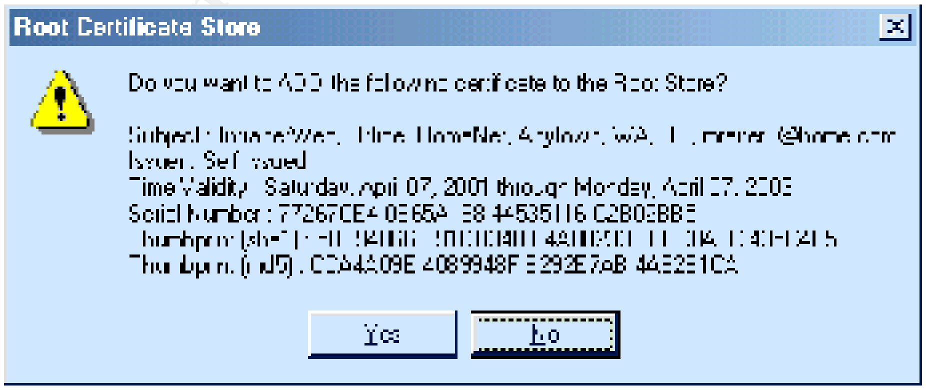
Issued to: Mike Heter

Issued by: InsaneWeb

Valid from 04/07/2001 to 4/[illegible]

Figure 37: The Unverified Certificate

Because the root CA has not yet been designated as trusted, we must install the certificate in the browser's root store.

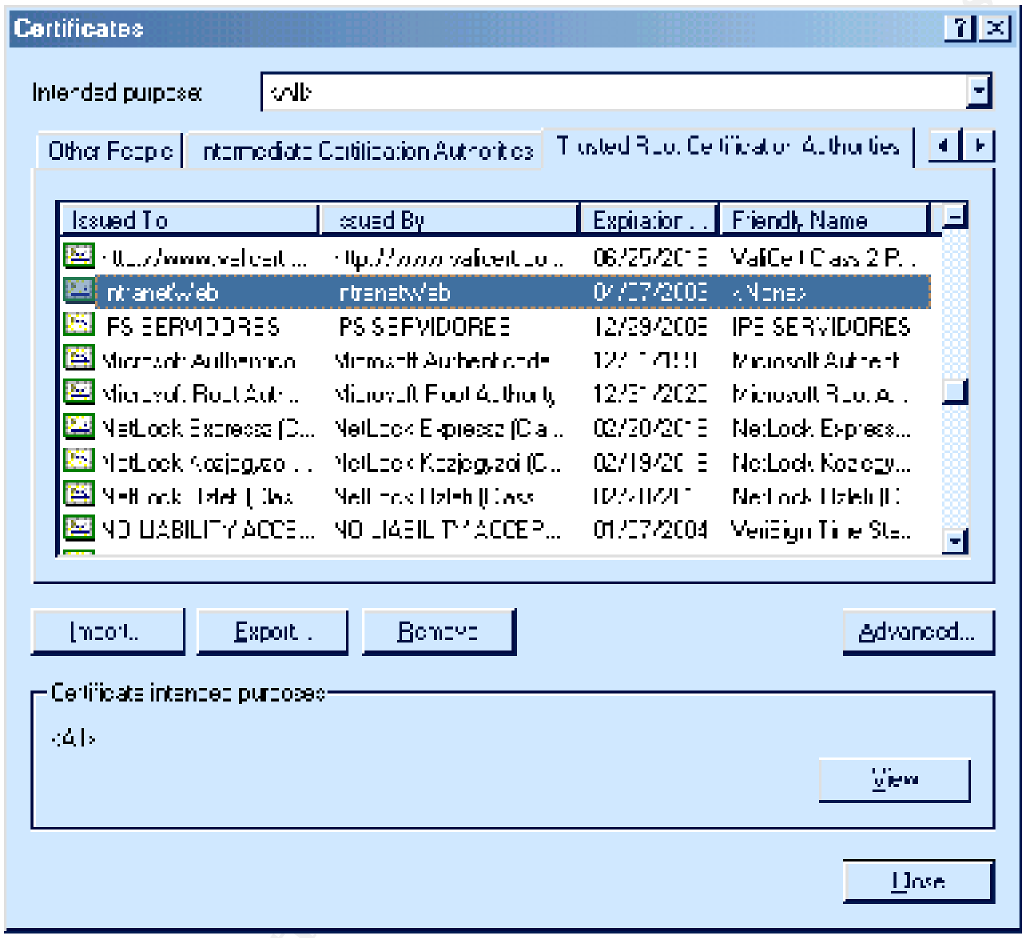


Do you want to ADD the following certificate to the Root Store?

Subject : InsaneWeb, [illegible], HomeNet, Anytown, WA, [illegible], [illegible]@home.com
Issuer : Self Issued
Time Validity : Saturday, April 07, 2001 through Monday, April 27, 2003
Serial Number : 77267CE4 03654 38 44535116 C2B03BB3
Thumbprint (sha1) : [illegible]
Thumbprint (md5) : C2A4A09E 4089948F 3292E7AB 4A3251CA

Figure 38: Installing the Root CA

The browser presents the user with all the public certificate information. It is up to the user to decide to accept or reject the certificate. Most users will not have the necessary information to make an informed decision; they will either accept or decline it blindly, or call the help desk to ask what they should do. The sysadmin should add explicit instructions to the certificate download page explaining exactly what to do, and why.


Certificates
Other People
Intermediate Certification Authorities
Trusted Root Certification Authorities
Import...
Export...
Remove
Advanced...
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiration ...	Friendly Name
http://www.valicert...	http://www.valicert.co...	06/25/2019	ValiCert Class 2 P...
IntranetWeb	IntranetWeb	07/27/2003	<None>
IPS SERVIDORES	IPS SERVIDORES	12/29/2009	IPS SERVIDORES
Microsoft Authenticode	Microsoft Authenticode	12/31/1999	Microsoft Authenti...
Microsoft Root Auth...	Microsoft Root Authority	12/31/2020	Microsoft Root Au...
NetLock Expressz (C...	NetLock Expressz (Cla...	02/20/2019	NetLock Expressz...
NetLock Kozjegyzo...	NetLock Kozjegyzoi (C...	02/19/2019	NetLock Kozjegy...
NetLock Uzleti (Cla...	NetLock Uzleti (Class...	02/20/2019	NetLock Uzleti (C...
NO LIABILITY ACCE...	NO LIABILITY ACCEP...	01/07/2004	VeriSign Time Sta...

Certificate intended purposes

<All>

Figure 39: Checking the Root Store

Here we see that the end user has successfully installed the CA certificate as a root CA. At this point, it is as trusted as any other root CA.

Accessing the Secured Web Page

So, now it's time for all this hard work to pay off. The sysadmin confidently types the web site IP into the address line of his browser and gets…….Page Not Found. Why? He trouble shoots, turning services on and off, reconfiguring, and finally discovers that SSL is the cause of the issue. No SSL connection is established, and since he has required SSL, there is no web site access. Unchecking the "Require SSL" box brings back access to the site. After a great deal of soul searching, web browsing, and hair pulling, the sysadmin finds that many people have had a similar problem, but that there is no single answer – and none of the answers he found were solutions to his problem. In other words, there are many places to make a mistake that will have the same result. A scan of the web server reveals that it is listening on port 443, the default SSL port, so that is not the problem. Days of troubleshooting do not bring resolution; however, he believes he has discovered the problem – although he has enabled the root CA to carry out all of the available functions, it is not, in fact, acting as an SSL server certificate. So, he stops the default web site, which he had been working with, and copies all of his HTML files and his scripts to another web site which he has just created with IIS. Using the Certificate Wizard accessed through IIS, he goes through a slightly different process. This time, he creates a request for a new certificate. This results in a simple text file, labeled cert.cer, as below:

```
-----BEGIN CERTIFICATE-----
MIICWTCCAgMCEA7xjOHaVxZ009CQO6TTaKowDQYJKoZIhvcNAQEEBQAwgakxFjAU
BgNVBAoTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20v
cmVwb3NpdG9yeS9UZXN0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYw
RAYDVQQLEz1Gb3IgVmVyaVNpZ24gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5v
IGFzc3VyYW5jZXMgKEMpVlMxOTk3MB4XDTAxMDQxMzAwMDAwMFoXDTAxMDQyNzIz
NTk1OVowcjELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNV
BAcUB0FueXRvd24xGDAWBgNVBAoUD0lyb25jbGF3SG9tZU5ldDEPMA0GA1UECxQG
T2ZmaWNlMREwDwYDVQQDFAhjc2N3aW4yazCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEApNnimyQ8kPCAuhZvcPIUDoqsRKFSMhf0iPCdkDI+oYSu/9tsypnOOo1X
OosixZ3MSDuHmhCf2BtowNU7nDk+lGjvLyMwE+T2aNvmbvS1+P79oTsNZRl6ePSB
CnzFh3wR3i05QDv+2YHkLRnwUi4ODmvlae1mmxjhP5n7QdfGtQ8CAwEAATANBgkq
hkiG9w0BAQQFAANBAH3OLzhC9cVRNoQjsnChUPeFWzK63EcRblZc8y8ReWLji9Ln
zSUKtJc3LR7jtzere82/mzqSL5TqdxIWKV/b3hw=
-----END CERTIFICATE-----
```

This is uploaded to the VeriSign site, which conveniently contains a function to create SSL server certificates. The cost of a VeriSign SSL certificate is nominal, and has the added benefit of being recognized by all standard browsers. The VeriSign SSL certificate arrives via a URL in an e-mail, and he goes through the installation function on their web site. With the new SSL certificate installed, he again tries to access his web site.

Success

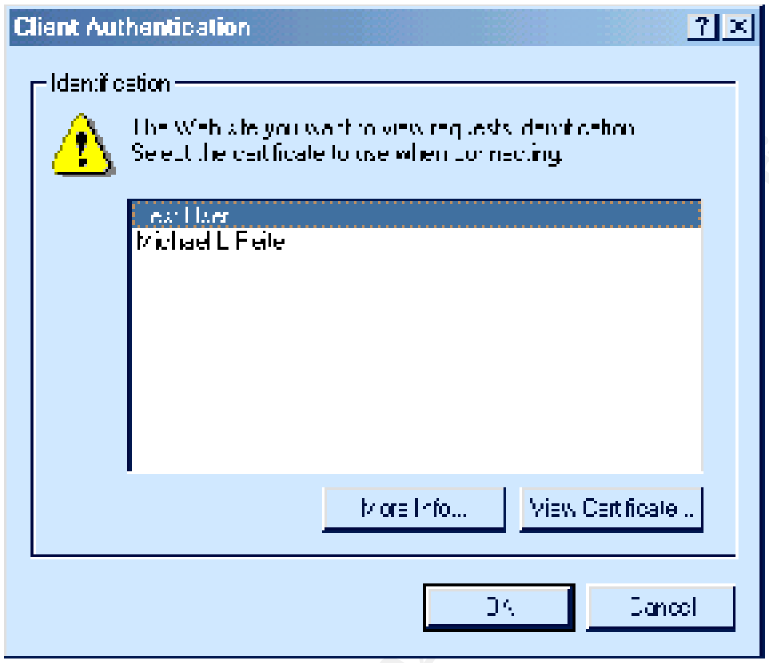

Client Authentication
Identification
The Web site you want to view requests identification. Select the certificate to use when connecting.
Test User
Michael L Feile
More Info...
View Certificate...
OK
Cancel

Figure 40: Challenged for a Valid Certificate;

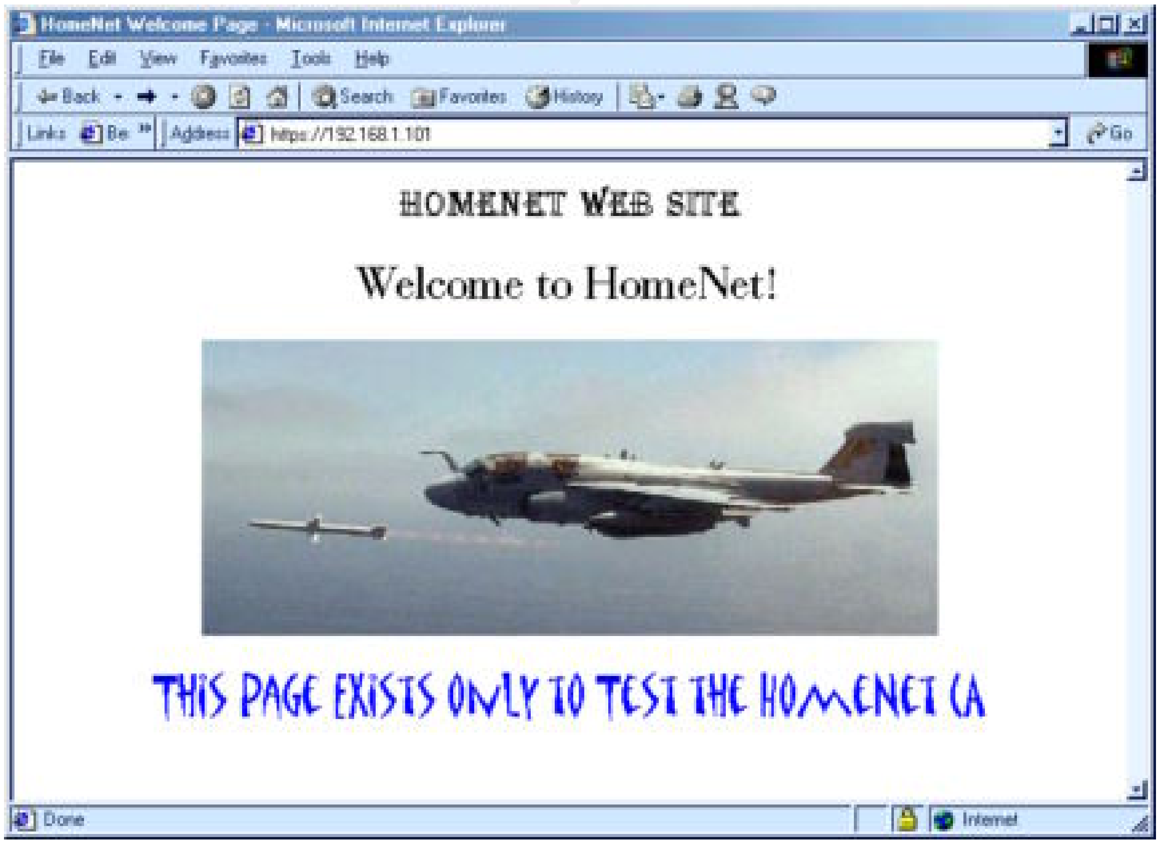

HomeNet Welcome Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Links Address https://192.168.1.101 Go
HOMENET WEB SITE
Welcome to HomeNet!
THIS PAGE EXISTS ONLY TO TEST THE HOMENET CA
Done
Internet

Figure 41 The Secure, Encrypted, Certificate Protected Web Page

It is important to note that the client certificate comes from the original root CA generated by the sysadmin with the Windows 2000 Certificate Authority, not from the VeriSign SSL certificate. These are two separate entities.

Conclusion

Creating a certificate enabled web site with a self-signed Certificate Authority under Windows 2000 is not exactly straightforward, but is not overly complicated either. Building the site itself is only part of the work – there must be security policies to go along with it, especially a Certificate Practice Statement (CPS) which documents the responsibilities associated with issuing and having certificates. There are step-by-step guides available from Microsoft for individual procedures, but they generally focus on the trees, not the forest. In other words, I have a CA to accomplish a certain task, not to brag to my buddies. I run SSL to secure data, not because I am enamored of encryption. I want to accomplish certain business objectives, and these are tools to reach a goal, not ends in themselves. Further, the variety of answers found to a given CA or SSL question on the newsgroups indicates that there is still a fair amount of confusion out there. This tends to point out the importance of piloting any project before production. This is complicated somewhat by the nature of PKI; without careful planning, the pilot and production networks may be cryptographically incompatible. Public key cryptography has been around since the 1970's[12]; however, the implementing technology is more recent, and in many cases may charitably be described as "immature". Undoubtedly the leading companies in the field will continue to improve the technology; ultimately, from the end user perspective, it should become almost completely transparent. There is some distance to go before this goal is reached.

[12] Diffie-Hellman Public Key Distribution Scheme: A Complete Overview; Hamid Pirooz; December 4, 2000; http://www.sans.org/infosecFAQ/encryption/diffie.htm