

Working with the AS/400 Digital Certificate Manager

**Craig Pelkie
Bits & Bytes Programming, Inc.
craig@web400.com**

Working with the AS/400 Digital Certificate Manager

Edition AS400DCM_20020219

Published by

Bits & Bytes Programming, Inc.
Valley Center, CA 92082
craig@web400.com

Copyright © 2002, Craig Pelkie. All Rights Reserved

You are allowed to print copies of this document for your own personal use and for the use of others in your company or organization. Otherwise, no part of this document or any accompanying computer source code may be reproduced or distributed in any form or by any means, or stored in a database or data retrieval system, without the prior written permission of Craig Pelkie, who is the author of the document and the computer source code.

All computer source code distributed with this document, either on diskettes, CD-ROM, or available for downloading from sources such as the Internet is Copyright © 2002 Craig Pelkie, All Rights Reserved. The source code is for use in computer programs that you develop for internal use within your company, or for use within programs that you develop for the use of your clients. No part of the computer source code distributed with this document shall be reproduced in source code format, either printed or in electronic format, by you or by others who you allow to have access to the source code. You shall not cause the source code to be stored on any information retrieval system, such as the Internet. You shall not develop any written articles, books, seminar materials, or other presentations that include the source code provided on the diskettes accompanying this document or within the document itself.

For any questions regarding your rights and responsibilities using the computer source code distributed with this document, contact Craig Pelkie, Bits & Bytes Programming, Inc., who is the owner of the source code.

LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTY

No representation is made that any of the techniques, programs, computer source code, commands, or configurations described and depicted in this document and on the computer source code accompanying this document are error-free and suitable for any application that you may develop. Craig Pelkie makes no warranty of any kind, expressed or implied, including the warranties of merchantability or fitness for a particular purpose, with regard to the information, examples, and computer source code presented in this document and on the accompanying diskettes. Everything provided in this document and on the accompanying computer source code, if any, is provided "as is". Craig Pelkie shall not be liable in any event for incidental or consequential damages or any other claims, pursuant to your use of any of the techniques presented in this document, or your use of the computer source code, even if Craig Pelkie has been advised of the possibility of such damages.

You are responsible for testing any and all programs, configurations, commands, and procedures described in this document prior to using the programs, configurations, commands, and procedures with important user data. You must ensure that adequate and sufficient backup of important user data is available, in the event that recovery of the important user data is required.

Working with the AS/400 Digital Certificate Manager

The AS/400 system is rapidly evolving as an e-business server. In addition to embracing the TCP/IP protocol and application suite, IBM is adopting other standards for working in an Internet environment. One of the important features on the AS/400 system is the Digital Certificate Manager (DCM), to help you create and manage server and client certificates. Those certificates are required to provide authentication and encryption capabilities for applications such as Web browsing and for secure Client Access Express connections over the Internet.

In this article, I review how you can use the DCM that is provided with OS/400 V4R3 and above to create your own certifying authority certificate and a server certificate for your AS/400 system. For background information about certificates and encryption, see the article *An Overview of Certificates and Encryption*.

History of Certificates on the AS/400

Starting with OS/400 V4R1, IBM introduced the Internet Connection Secure Server (ICSS) product (5769-NC1 for U.S. and Canada, 5769-NCE for other countries). The two versions of the product provided support for encryption keys of different lengths, to comply with U.S. government export regulations. This chargeable Licensed Program Product (LPP) contained the support required to generate and work with server certificates on the AS/400 system and to work with encrypted transmissions.

Beginning with OS/400 V4R3, IBM created new LPPs and options and dropped the charge for encryption support. The products that you must install on an AS/400 system at OS/400 V4R3 and above to support encryption include:

- 5769-SS1 Option 34 – Digital Certificate Manager (provided as part of OS/400)
- 5769-ACx – Cryptographic Access Provider. There are three versions (AC1, AC2 and AC3), depending upon the encryption strength allowed in your country (AC1=40 bit, AC2=56 bit, AC3=128 bit). You can only order and install one of these LPPs on your AS/400 system.
- 5769-DG1 – IBM HTTP Server for AS/400, includes the browser-based configuration program used to work with digital certificates.

Although the Cryptographic Access Provider is a no-charge LPP, you must explicitly order it if you did not previously have ICSS (5769-NC1 or –NCE) installed on your AS/400 system.

A Plan for Certificates

Once you have the required software on your AS/400 software, you can create a server certificate for your AS/400 system. You need a server certificate so that your AS/400 system can provide encrypted SSL sessions between itself and client applications that support SSL. Some of the client applications that support SSL include Web browsers, IBM Personal Communications (PCOMM) version 4.3 and above, IBM Host on Demand version 3, and IBM Client Access Express (OS/400 V4R4 and above).

There are two ways to create a server certificate:

- Use DCM to generate a request to a Certifying Authority (such as VeriSign, Inc.). The request contains information about your company and about the server that the certificate will be installed on. You send the request via e-mail to the certifying authority. In turn, they send you a server certificate via e-mail, which you copy and paste into DCM.
- Use DCM to create a certifying authority on your AS/400 system. You can then use that certifying authority to self-certify your AS/400 server certificate.

This article describes the second technique. You will create a certifying authority on your AS/400 system and use it to create a server certificate. With the server certificate, you can establish SSL sessions between your AS/400 and client applications.

Get to the DCM

You work with the Digital Certificate Manager in the browser-based administration and configuration program. You can get to that program in two ways:

- In Operations Navigator, go to the Network branch, then the Internet branch. Double-click the Digital ID selection.
- Enter the URL `http://myas400:2001` in your browser (where myas400 is the TCP/IP name of your system). On the AS/400 Tasks page, click the link for Digital Certificate Manager.

Either technique takes you to the Digital Certificate Manager page, shown in Figure 1.



Figure 1: The Digital Certificate Manager page.

CERT01

Create a Certificate Authority

The left frame on the Digital Certificate Manager page is the *navigation frame*. In that frame, click the link for Certificate Authority. If you have not previously created a certificate authority on your AS/400 system, the frame expands to show the Create a Certificate Authority option, as shown in Figure 1. You can only have one certificate authority on your AS/400 system. If you had previously created the certificate authority, you would see options to maintain that certificate authority.

The Create a Certificate Authority page shown in Figure 2 prompts you to select a key size, specify a password for your key ring (where the public and private keys are stored), and specify certificate information. The key size is used to encrypt the public and private keys. You should select the largest size available to you (selections include 512, 1024 and 2048, depending upon the 5769-ACx LPP you have installed).

Figure 2: The Create a Certificate Authority page.

CERT02

The key ring password is used to protect the key ring files. Although you should enter a password that complies with AS/400 user profile naming standards, the password is not related to any AS/400 user profile. You should choose a difficult to guess password, since if anybody is able to freely access the key ring files, they can compromise the integrity of your digital certificates. Be sure to keep a secured copy of the password, as there is no way to recover it if you forget it.

You can enter as much of the certificate information as you want, or just the fields marked as required. The information you enter is typically shown when the certificate is displayed. For example, if you transmit a server certificate that you create based on this certificate authority, the information you enter is displayed to the browser user.

Finally, you specify the number of days that the certificate authority will be valid. The default is 1095 days (3 years). The certificate authority must be recreated after it expires and issue new certificates.

Click OK after entering your data for the certificate authority. The CA Certificate Created Successfully page shown in Figure 3 is displayed. You may want to print a copy of the page for reference. Also, you may want to make a backup of the key ring file. If the file is deleted or damaged, you will need to create a new certificate authority and reissue all of the certificates you previously issued.



Figure 3: The CA Certificate Completed Successfully page.

CERT03

Receiving the Certificate

Because you are working in a browser, you can optionally receive the newly created certificate authority certificate in your browser. By receiving the certificate, you indicate that you trust any server certificates that your browser encounters in the future that are created by the certificate authority you just created.

Click the Receive Certificate link shown in Figure 3. The browser responds by letting you enable the certificate and select the types of services that you will accept using the certificate. Figure 4 shows the Microsoft Internet Explorer version 4.01 dialog for accepting the new certificate. The View Certificate option displays the data that you entered when you created the certificate authority (Figure 5).

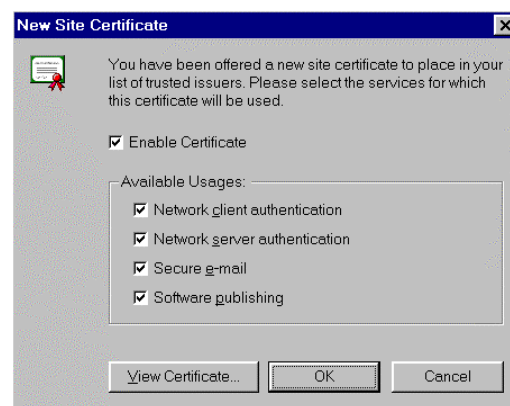
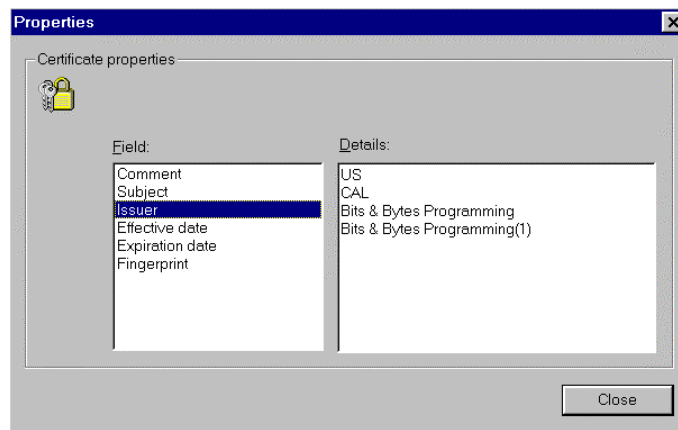


Figure 4: Your browser prompts you to accept the newly created certifying authority certificate.

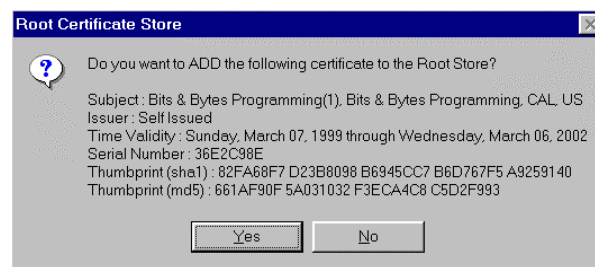
CERT04



CERT05

Figure 5: The Properties dialog shows information about the certificate.

When you click OK on the New Site Certificate dialog (Figure 4), the confirmation message shown in Figure 6 is displayed. You normally want to be extremely cautious about adding certificates to the root certificate store, since you are in effect saying that in the future, you will accept any server certificates that are signed by the certificate authority that you are adding to the root store. Since you are adding the certificate authority certificate that you just created, it is safe to accept this certificate into your browser root certificate store. You should regard it as an unusual event to add certificates to the root certificate store, and caution your users that they should never accept such certificates unless they are advised that the certificate is valid.



CERT06

Figure 6: The confirmation message for accepting the new root certificate.

You can view certificate authorities in your browser by working with your browser options. For example, Figure 7 shows the Microsoft Internet Explorer version 4.01 Certificate Authorities dialog. You can see that the new certificate for the certificate authority is now considered by the browser to be a valid certificate authority.

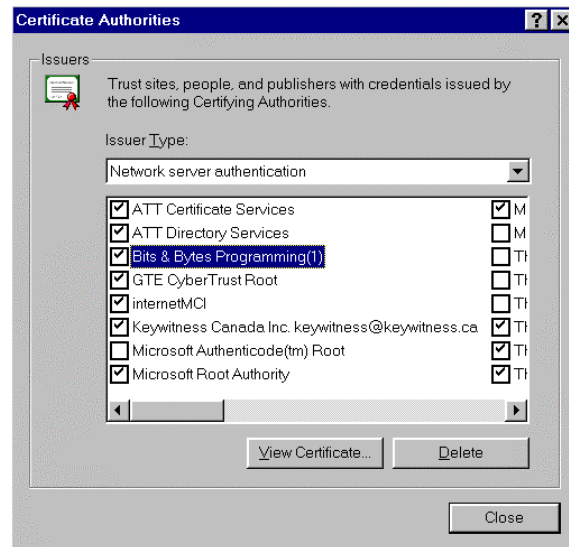


Figure 7: The Certificate Authorities dialog shows the list of authorities that are trusted by the browser.

CERT07

Completing the Certificate Authority

After receiving the certificate in your browser, DCM presents one more page where you set policy information (Figure 8). By default, the certificate authority that you just created can only be used to create server certificates. If you want to create client certificates, select the Yes option. Client certificates are used by the server so that it can verify that it is connecting to a known client. You can also change the validity period of certificates that you create with the certificate authority, from 1 to 2000 days.



Figure 8: The Certificate Authority Policy Data page.

CERT08

When you click OK on the Certificate Authority Policy Data page, the Policy Data Changed page is displayed (Figure 9). Click OK on that page to go directly to the Create a Server Certificate page shown in Figure 10. Because you have just configured your AS/400 system to act as a certificate authority, you can now issue server and client certificates. Those certificates are only useful in your intranet and possibly extranet (your business partners who agree to accept your certificates). There is little reason to expect that anyone else will trust your self-approved server certificates.

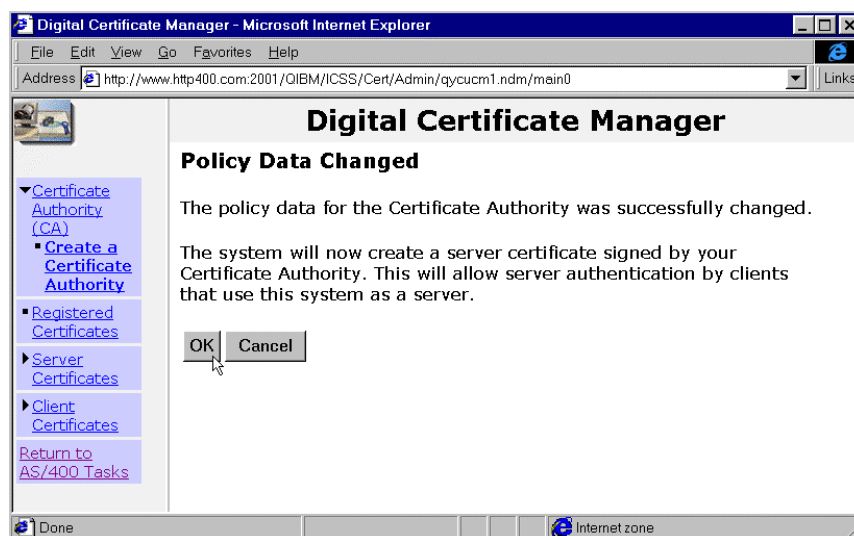


Figure 9: The Policy Data Changed page leads to server certificate creation.

CERT09

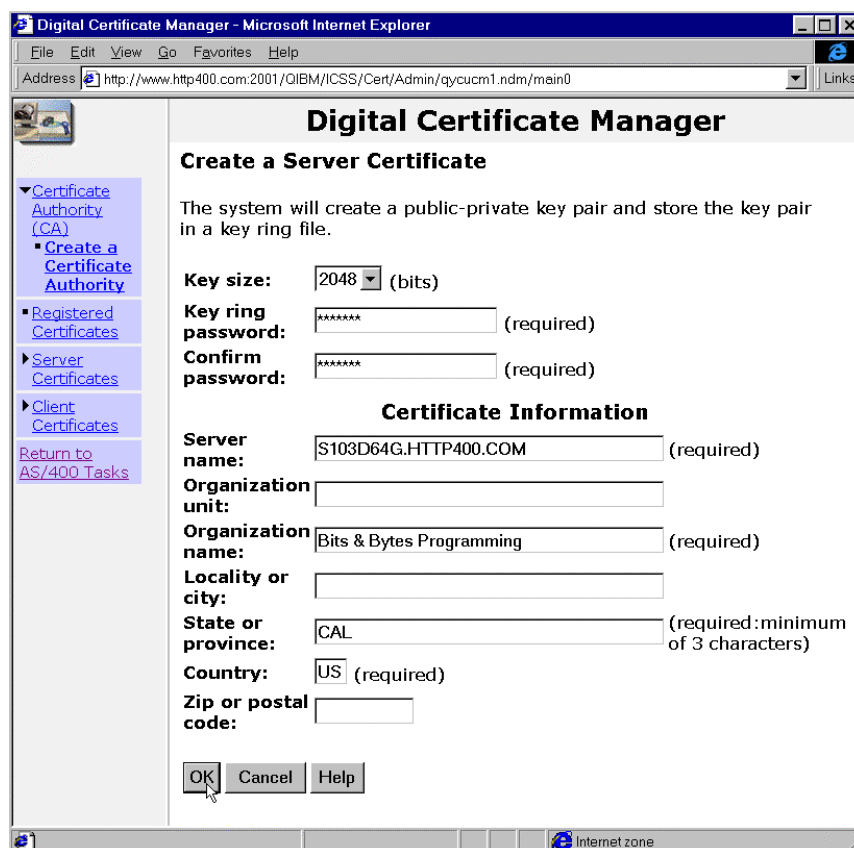


Figure 10: The Create a Server Certificate page.

CERT10

Create a Server Certificate

The Create a Server Certificate page shown in Figure 10 is almost identical to the Create a Certificate Authority page (Figure 2). The only difference is that instead of the certificate authority name, you enter the name of the server. You can enter any name you want for the server, but it is usually best to enter the name of the server as known on your network.

After completing the Create a Server Certificate form and clicking OK, the Server Certificate Created Successfully page is displayed (Figure 11). This page displays the path to the key ring file where the server certificate is stored on your AS/400 system. You can select servers on your AS/400 system that will use the certificate. Click OK to go to the last page.

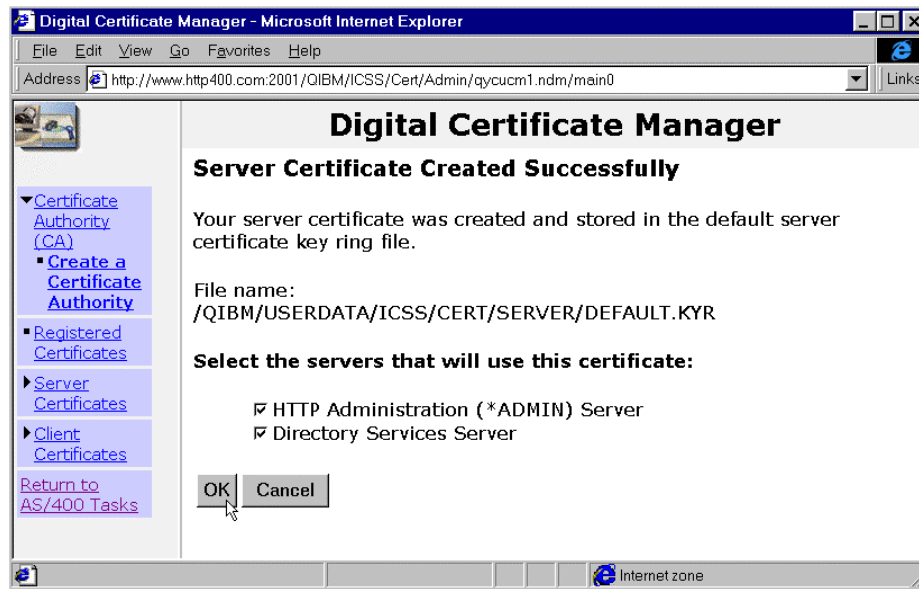


Figure 11: The Server Certificate Create Successfully page.

CERT11

The Server Configuration Status page is the last page in the series (Figure 12). This page summarizes the servers that use the newly created server certificate.

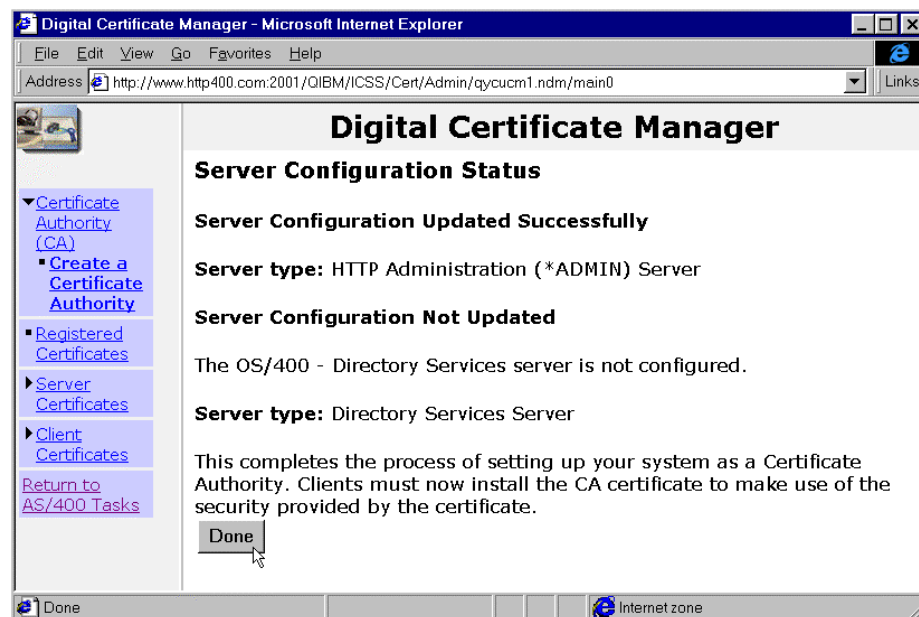


Figure 12: The Server Configuration Status page.

CERT12

Summary

As Internet applications become more widely used on the AS/400, it will be important to know how to use certificates with the applications. You should make it a point to get and install the required LPPs and walk through the process of creating a certificate authority and a server certificate. If you later decide to install a server certificate from a well known certificate authority, you will find the application and install processes much easier to understand if you have gone through these initial steps.

