The purpose of this TechNote is how to install & configure Net Tools PKI 1.0. There is one important change necessary that PKI will handle Certificate Requests, which are by default set to none. This is described here as well.

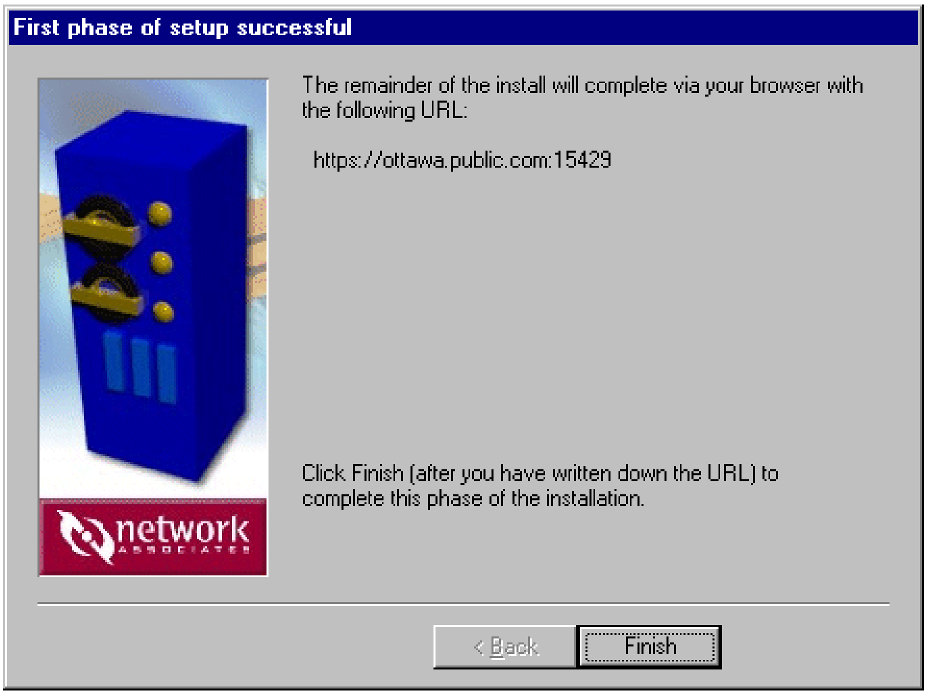
Because Net Tools PKI is an older product, you will have Windows NT4 with Service Pack 3 installed. I've tried to install this product on W2K with SP3 and on NT4 with SP 6a and the installation failed. Also, because Net Tools PKI Management is only supported by Netscape Communicator, you will have to install Netscape first, before starting with PKI Installation. I've used NetScape Communication 4.74.

The installation of Net Tools PKI requires a huge bunch of resources, because of all the certificate calculation and creating. Once PKI is installed it uses only a bit of all the resources.

When starting the installation PKI Install will try to find a high port available for https connection.

1. Stop all currently running applications
2. Double-click on setup.exe under 1.0 RSA
3. When getting the error code "GetFreePort() failed after 100 attempts, remove any NT Service Pack and make sure you have Service Pack 3 installed.
   PIX – netstat

4. When all files has been extracted and CA Setup finished the PHASE 1, you will be prompted with an administration URL, like https://ottawa.puplic.com:15429 (this is my PKI Server example)



First phase of setup successful

The remainder of the install will complete via your browser with the following URL:

https://ottawa.public.com:15429

Click Finish (after you have written down the URL) to complete this phase of the installation.

Rainer's Technical Tips

DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user

5. Netscape will start and connects to the administration port. Note, this port number is randomly choosen and may be different with your installation.

6. You will get a certificate warning, click on **NEXT**

7. A new site certificate is being presented. Click on **NEXT**

8. Accept this certificate forever (until is expires). Click on **NEXT**

9. Confirm the New Site Certificate and click **NEXT – FINISH**

10. You will be presented with the End User License Agreement

11. STEP1: General Configuration Information

WEBMASTER EMAIL ADDRESS:	webmaster@ottawa.public.com
NAME OF SERVER HOST (Internet FQDN):	ottawa.public.com
ADMINISTRATION SERVER PORT NUMBER:	443
ENROLLMENT SERVER PORT NUMBER:	444
DSS AUTHENTICATED ENROLLMENT SERVER PORT NUMBER:	4445
SECURE DIRECTORY (SSL-LDAP) SERVER PORT NUMBER:	636
DIRECTORY (LDAP) SERVER PORT NUMBER:	389
SMTP-SERVER HOST (DNS OR IP ADDRESS):	165.100.100.100
SMTP SERVER PORT:	25

12. STEP2: Root CA Creation

Common Name (used as CA nicknam):	Root CA
E-Mail Address:	rootca@public.com
Organization Name:	public
Organizational Unit:	testlab
Locality:	homeoffice
State or Province:	
2-letter Country Code:	DE
Validity Period:	11000 days
Signing Algorithm and Key Size:	RSA/MD5 – 1024
V3 Extensions for CA Certificate:	none

13. Proceed with Root CA Creation

14. You will be asked for a passphrase. As this is in a test environment only, better not to create a passphrase, unless you want to type every time you start the service, the passphrase

15. Click on **CONTINUE** – This will take a short while

16. You should get a confirmation, click on **CONTINUE**

17. STEP2b: Administrative CA Creation

Common Name (used as CA nickname):	Administrative CA
E-Mail Address:	adminca@public.com
Organization Name:	public
Organizational Unit:	testlab
Locality:	homeoffice
State or Province:	
2-letter Country Code:	DE
Validity Period:	11000 days
Signing Algorithm and Key Size:	RSA/MD5 – 1024
V3 Extensions for CA Certificate:	none

18. Proceed with Administrative CA Creation

19. You will be asked for a passphrase. As this is in a test environment only, better not to create a passphrase, unless you want to type every time you start the service, the passphrase

20. Click on **CONTINUE** – This will take a short while

21. You should get a confirmation, click on **CONTINUE**

22. STEP3: Web Server Information

ENROLLMENT SERVER

Common Name:	ottawa.public.com
E-Mail Address:	enrollserv@public.com
Organization Name:	public
Organizational Unit:	testlab
Locality:	homeoffice
State or Province:	
2-letter Country Code:	DE
Key Size:	1024

ADMINISTRATION SERVER

Common Name:	ottawa.public.com
E-Mail Address:	adminserv@public.com
Organization Name:	public
Organizational Unit:	testlab
Locality:	homeoffice
State or Province:	
2-letter Country Code:	DE
Key Size:	1024

23. You will be asked for a passphrase. As this is in a test environment only, better not to create a passphrase, unless you want to type every time you start the service, the passphrase

24. Next step will be Server Initiation. Click on **INITIATE NET TOOLS PKI SERVER CONFIGURATION**

25. This all will be now an automatic process, which can takes up to 20 minutes, depending on your system.

26. When this process has finished, you will get an error message regarding network problem. This is, because of initial port number has changed to 443.

27. Close the browser and restart.

28. type the new URL: **`https://ottawa.public.com:443`**

29. You will be prompted with a New Site Certificate Click **NEXT**

30. Click **NEXT**

31. Accept this certificate forever (until it expires)

32. Click **NEXT** – **NEXT** – **FINISH**

33. Create an Administrative Certificate for client authentication

Name:	Administrator
Email:	adminclient@public.com
Organization:	public
Organizational Unit:	testlab
Locality:	homeoffice
State/Province:	Bavaria
Country Code (2 Letter)	DE

34. Click on **CONTINUE**

35. Confirm the new Administrative Certificate by clicking on **CONTINUE**

36. You will be prompted to generate a private key, click on **OK**

37. Type in the password (password) and again to confirm. Click on **OK**

38. This was the final PKI Server installation. Now you will have to enable the administrative certificate access by clicking on **DOWNLOAD ADMINISTRATIVE CLIENT CERTIFICATE**

    After downloading the Administrative client certificate into your browser, please follow these steps to avoid a possible client authentication bug:

    1. Open the Security dialog box by clicking on the Show Security Information icon on your browser’s toolbar (next to stop icon)

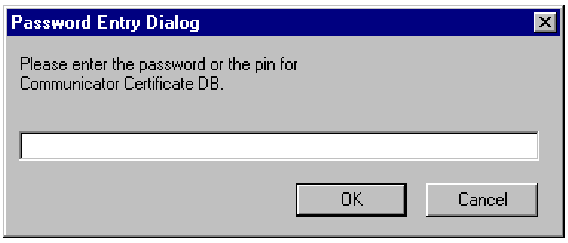
2. Click on the Navigator Link

3. Set the Certificate to identify you to a web site:" setting to the Administrative certificate you just downloaded. Selecting the "Ask every time" or "Select Automatically" options may cause some versions of Netscape to end abnormally

4. Click the "OK" Button and continue with step 39

39. Stop and restart your Net Tools PKI Web server

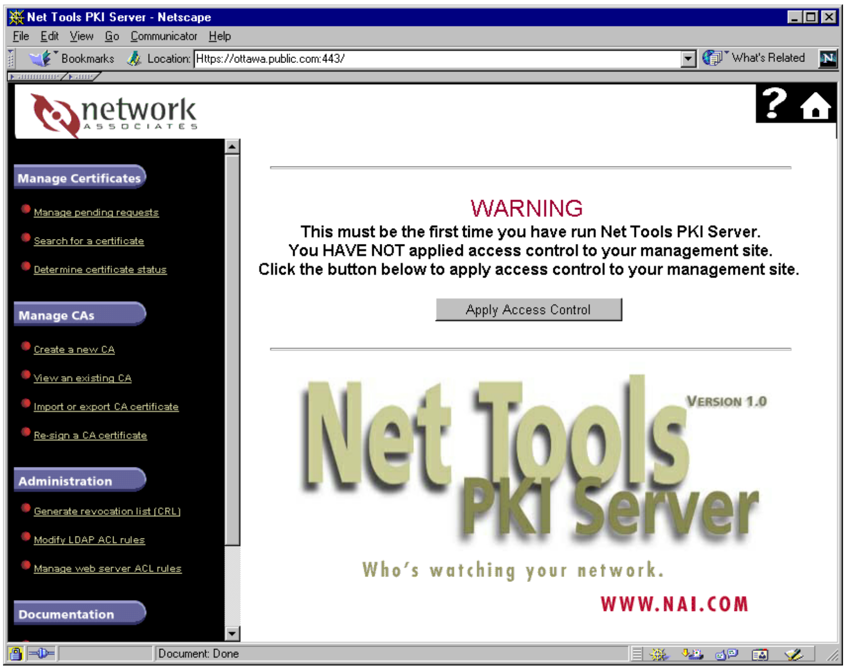
If you have completed all of the steps outlined above, your installation of Net Tools PKI Server is now fully operational. Please connect to https://ottawa.public.com:443 now to complete the secure installation by restriction access to the administrative portion of the server. Remember that up must present your newly acquired administrative certificate to properly identify yourself to the server.



Password Entry Dialog

Please enter the password or the pin for
Communicator Certificate DB.

40. You are now connected the first time on the Net Tools PKI Server



Net Tools PKI Server - Netscape

Location: Https://ottawa.public.com:443/

WARNING
This must be the first time you have run Net Tools PKI Server.
You HAVE NOT applied access control to your management site.
Click the button below to apply access control to your management site.

Document: Done

41. A warning message appears, telling you “This must be the firs time you have run Net Tools PKI Server. You have not applied access control to your management site.” Please **APPLY ACCESS CONTROL** – **there’s no way** to redo Access control, if you don’t do it now.

42. Choose Administrative CA from the pull down menu and click on **APPLY ACL**

43. Go to Administration – Modify LDAP ACL rules. Default is NONE. Scroll down to the rule that start with: access to dn=”request_queue”. This is the 9th rule from the top. The last line of the rule says:

```
by dn=*.* none
```

Change this to …

```
by dn=*.* write
```

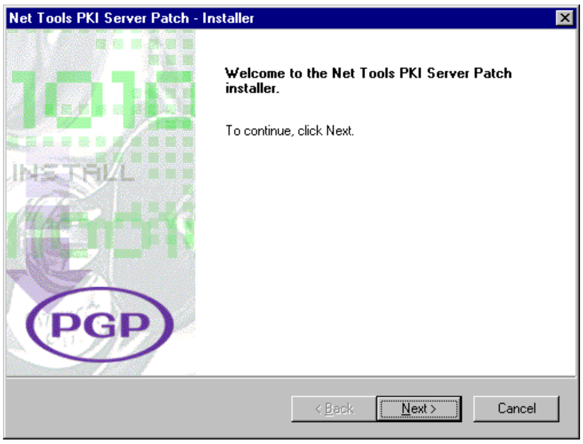
This allows ANY one to write to the request queue. This is harmless because certificates are issued only after the CA admin verifies that the request is a valid one. At the end of the Access Control List Editor click on ”**Press here to save ACL to DATABASE”**

44. Close the web browser, **Stop** following services:

☑ Net Tools PKI Directory Server
☑ Net Tools PKI Web Server

45. Run Service Pack 1 by executing **PKISERVER100-SP1-103-1.EXE**

46. The Installer prepares the execution

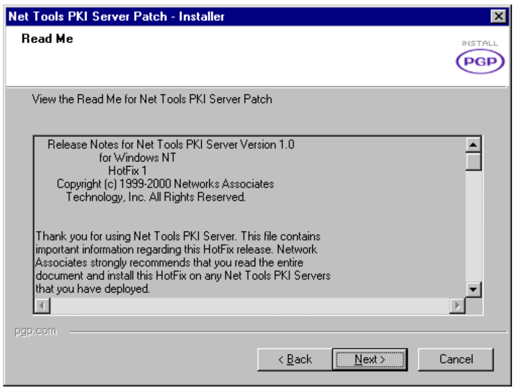

Net Tools PKI Server Patch - Installer

Welcome to the Net Tools PKI Server Patch installer.

To continue, click Next.

Click on **NEXT**

47. You will get the readme file – click on **NEXT**



Net Tools PKI Server Patch - Installer

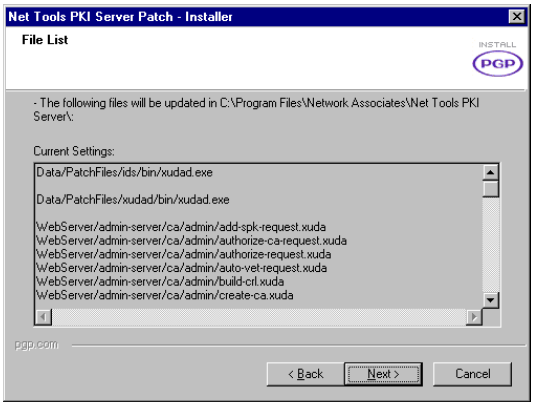
Read Me

View the Read Me for Net Tools PKI Server Patch

Release Notes for Net Tools PKI Server Version 1.0
for Windows NT
HotFix 1
Copyright (c) 1999-2000 Networks Associates
Technology, Inc. All Rights Reserved.

Thank you for using Net Tools PKI Server. This file contains important information regarding this HotFix release. Network Associates strongly recommends that you read the entire document and install this HotFix on any Net Tools PKI Servers that you have deployed.

48. On the next Window you'll see all the files, which will be updated. Click on **NEXT.**



Net Tools PKI Server Patch - Installer

File List

- The following files will be updated in C:\Program Files\Network Associates\Net Tools PKI Server\:

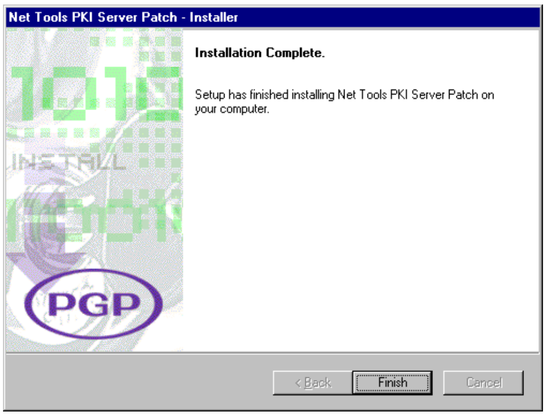
Current Settings:

```
Data/PatchFiles/ids/bin/xudad.exe

Data/PatchFiles/xudad/bin/xudad.exe

WebServer/admin-server/ca/admin/add-spk-request.xuda
WebServer/admin-server/ca/admin/authorize-ca-request.xuda
WebServer/admin-server/ca/admin/authorize-request.xuda
WebServer/admin-server/ca/admin/auto-vet-request.xuda
WebServer/admin-server/ca/admin/build-crl.xuda
WebServer/admin-server/ca/admin/create-ca.xuda
```

49. The Patch will be applied



Net Tools PKI Server Patch - Installer

Installation Complete.

Setup has finished installing Net Tools PKI Server Patch on your computer.

You are done – Please allow a final reboot. Remember, you had stopped the Directory Server and Web Server