



Web Security with Kx509 [Windows]

Kx509 merges two highly respected security standards: Kerberos and x509. Kerberos authentication (proving you are who you say you are) has been successfully used at the University of Michigan for many electronic services including e-mail. It cannot, however, be used with web browsers such as Netscape Navigator and Internet Explorer.

Kx509 enhances Kerberos with x509 digital certification so that you can now use one tool to protect your electronic security at U-M including when using your web browser. Refer to Section I, “Kx509 Benefits,” to better understand Kx509’s advantages and—for your protection—please read Section D, “What You Must Know About Kx509.”

Table of Contents

A. Accessing the Internet through U-M	1
B. System Requirements.....	1
C. Obtaining Kx509.....	1
D. What You Must Know About Kx509	2
E. Installing Kx509.....	2
F. Creating a Kerberos Ticket and Kx509 Certificate.....	3
G. Time Limits for Your Kerberos Ticket and Kx509 Certificate	4
H. Ending Your Kx509 Session.....	4
I. Kx509 Benefits.....	5
J. Verifying Your Kerberos and Kx509 Security.....	6
K. Additional Resources.....	7

A. Accessing the Internet through U-M

We highly recommend you install the **Windows Internet Access Kit (WIAK)** from the current **Blue Disc** [www.itd.umich.edu/kits/]. With the exception of Kx509, the WIAK automatically installs and configures all the files you need to access the Internet via the U-M computing environment.

B. System Requirements

Kx509 can be used on any computer running:

- Windows 95 or later
- version 4 or later of either Netscape Navigator (Communicator) or Internet Explorer
- a Kerberos program such as Kerberos 95 which is automatically installed when you use the WIAK but is also available free from the ITCS Software Distribution Directory (swdist) at <https://itd.www.umich.edu/software/download/kerberos/windows/Kerberos95/Kerb95.exe>

NOTE: If you are typing the URL, you must enter it with the exact upper and lower case characters.

C. Obtaining Kx509

Kx509 is free. You can download the installer from the ITCS Software Distribution Directory (swdist) at

<https://itd.www.umich.edu/software/download/k/kx509/windows/KX509Setup.exe>

NOTE: If you are typing the URL, you must enter it with the exact upper and lower case characters.

Select the Desktop as the download (“Save in”) location.

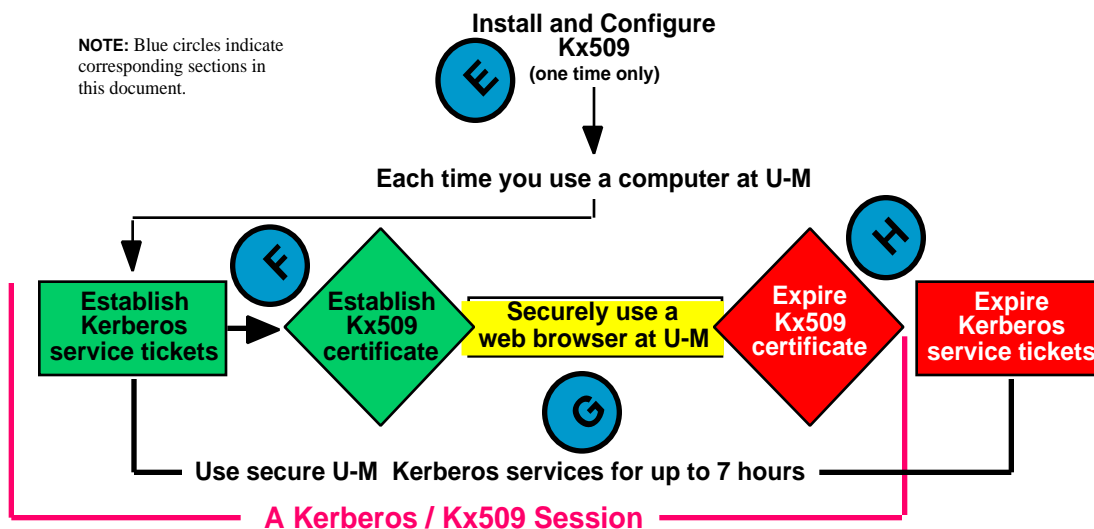
D. What You Must Know About Kx509

Kx509 works in conjunction with Kerberos—the security system you use whenever you’re asked to enter your unqname and UMICH password. Kerberos generates **tickets** for your computer, while Kx509 generates a **certificate** that works only within your web browser. When you run Kx509, Kerberos generates a **ticket** called cert.x509@UMICH.EDU, but this is not the same as the Kx509 **certificate** installed within your web browser.

A Kerberos ticket lasts for seven (7) hours. When your Kerberos tickets expire due to time limits, your Kx509 certificate also automatically expires. However, you can manually expire your Kerberos tickets (such as logging out of a service) but doing so does not expire your web browser’s Kx509 certificate. That means someone could still pretend to be you using your web browser. It’s confusing, but...

Why should you care? **IMPORTANT WARNING!** To protect yourself, you must expire *both* the Kerberos tickets on your computer and the Kx509 certificate in your web browser when you leave a computer. If you do not, someone else can sit down at the computer you were using and do things like printing on your student account and sending e-mail in your name. **Protect Yourself**; always close both the **Kerberos tickets** and the **Kx509 certificate** before you leave a computer.

Here’s a graphic representation of how it all works.

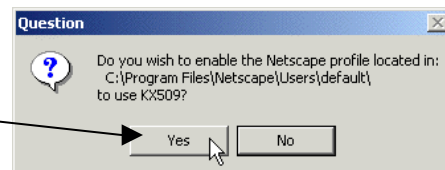


E. Installing Kx509

1. Double-click the **KX509Setup** icon you downloaded to your computer under “Obtaining Kx509.”
2. At the “Welcome to InstallShield Wizard for KX509” window, click **Next**.



NETSCAPE USERS NOTE: KX509Setup will prompt you to allow Netscape to use Kx509. Click the **Yes** button.



3. In the “Install Shield Wizard Complete” window, click **Finish**.

- Configure your web browser to automatically accept Kx509 certificates:

NETSCAPE 4 or later

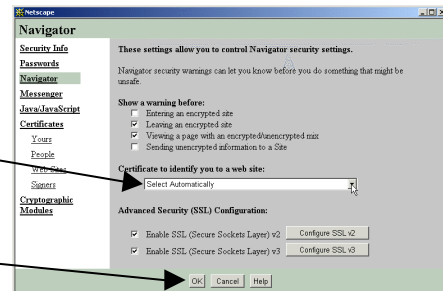
- In the Netscape navigation toolbar, click the **Security** icon.



- In the Security Info window, select **Navigator**.



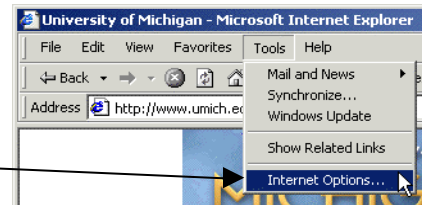
- In the Navigator window, choose **Select Automatically** pull down menu under “Certificate to identify you to a web site.”



- Click **OK**.

INTERNET EXPLORER 5.5 or later

- From the Internet Explorer **Tools** menu, select **Internet Options**.



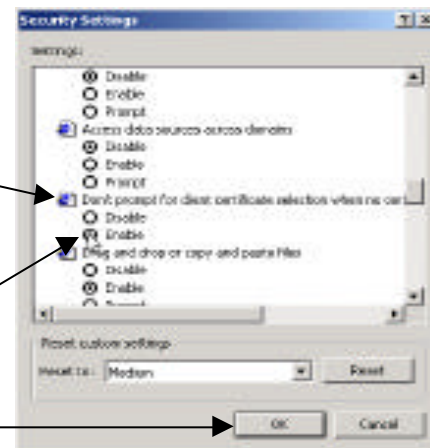
- In the Internet Options window:

- Select the **Security** tab.
- Select the **Internet** icon.
- Click the **Custom Level** button.



- In the Security Settings window:

- Scroll about halfway down the list to the heading “Don’t prompt for client certificate when no certificate or only one certificate exists.”
- Under “Don’t prompt for client certificate selection when no certificates or only one certificate exists,” activate the **Enable** radio button.
- Click **OK**.



- In the Internet Options window, click **OK**.
- You may now delete the **KX509Setup** program from your computer.

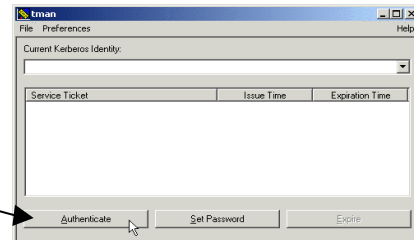
F. Creating a Kerberos Ticket and Kx509 Certificate

CAUTION! Before benefiting from Kx509 security, you must have an active Kerberos ticket. A Kerberos ticket automatically expires after seven (7) hours. If your Kerberos ticket expires, you will need to create another Kerberos ticket and Kx509 certification.

1. Use the Windows **Find** or **Search** command (under the **Start** menu) to find and open Ticket Manager, more commonly known as **tman** (or tman.exe).

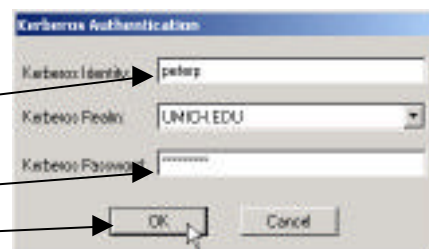
HELPFUL HINT: Create a shortcut for tman on your desktop.

2. In the tman window, click **Authenticate**.

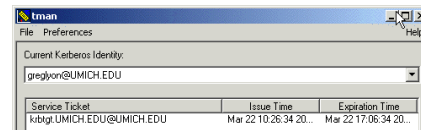


3. In the Kerberos Authentication window:

- a. In the **Kerberos Identity** field, enter your **username**.
- b. In the **Kerberos Password** field, enter your **UMICH password**.
- c. Click **OK**.

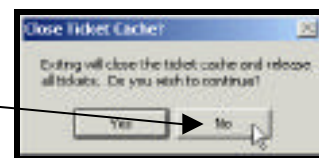


4. In the tman window, you will now have a Kerberos ticket. Note the time the ticket was created and that it will expire seven (7) hours later.



5. You may now minimize the tman window but note that, when minimized, it only appears as an icon (not as a button) in the taskbar.

CAUTION! Do not close the tman window; closing it expires both Kerberos and Kx509 certificates. You will receive a warning if you try to close the window. Click **No** to keep your security active.



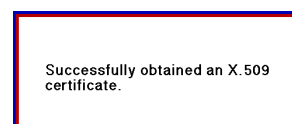
NOTE: To access the tman window after minimizing it:

- click the **tman** icon in the Windows taskbar
- if you created a shortcut, double-click the **Shortcut to tman** icon on your desktop



6. On your desktop, double-click the KX509 shortcut.

7. After a few seconds, you will receive notification that you have received a certificate.



NOTE: If you had not previously created a Kerberos ticket, you will receive the following message. Correct this problem by following steps 1-3 in this section.

Have you authenticated to Kerberos?
Your ticket file is invalid.

G. Time Limits for Your Kerberos Ticket and Kx509 Certificate

Your Kx509 certificate is valid for only as long as your Kerberos ticket is valid. Kerberos tickets automatically expire after seven (7) hours. If, for example, you obtained your Kx509 certificate three hours after obtaining your Kerberos ticket, the certificate would expire in four (4) hours

You can check the status of your Kerberos and Kx509 security by accessing the tman window. See the note under step 5 of the Section F, “Creating a Kerberos Ticket and Kx509 Certificate.”

H. Ending Your Kx509 Session

WARNING! For maximum security, you should terminate your Kerberos and Kx509 protection whenever you leave your computer. With either Kerberos or Kx509 active, anyone can use your computer and pretend to be you.

1. On the **Desktop**, double-click the **Logout KX509** icon.



2. Make certain you receive the confirmation window.

[Graphic of confirmation window]

3. To terminate your Kerberos tickets, activate the **tman** window by either:

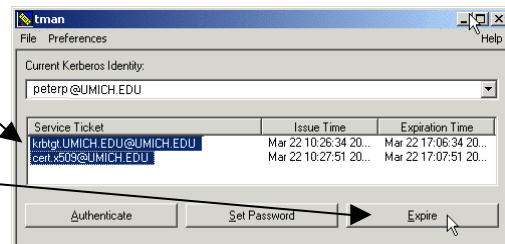
- click the **tman** icon in the Windows taskbar
- if you created a desktop shortcut, double-click the **Shortcut to tman** icon



4. In the **Service Ticket** field, select each item by clicking on it.

HELPFUL HINT: Holding down the **Ctrl** key allows you to select multiple items.

5. Click the **Expire** button so that all items are removed. Your entry in the Current Kerberos Identity field will also disappear.



6. To reestablish Kerberos and Kx509 security, follow the steps under “Creating a Kerberos Ticket and Kx509 Certificate.”

I. Kx509 Benefits

- You only need to authenticate (provide your unickname and UMICH password) once at the beginning of a session in order to access U-M electronic services that use Kerberos or Kx509 security. However, read the **WARNING!** under “Ending Your Kx509 Session.”
- Kx509 works with the most popular web browsers.
- Your UMICH password is especially secure because it is never sent over the Internet.
- Web service providers can create personalized and customized services for individuals.
- Kx509 allows secure web transactions at the University of Michigan.
- Kx509 allows for the possibility of secure web transactions between universities and other institutions.

J. Verifying that Your Web Browser Is Able to Offer Kx509 Security

NETSCAPE 4 or later

1. In the Netscape navigation toolbar, click the **Security** icon.



2. In the Security Info window, select **Yours** under the Certificates heading.

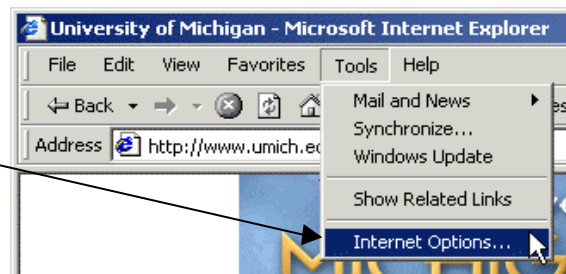


3. The “Your Certificates” window should have an entry similar to that seen at the right.
4. Click **OK** to close the window.



INTERNET EXPLORER 5.5 or later

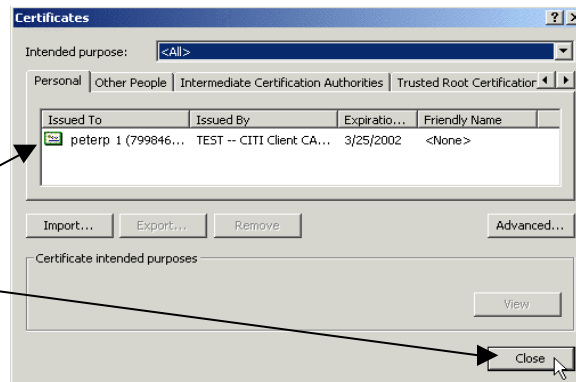
1. From the Internet Explorer **Tools** menu, select **Internet Options**.



2. In the Internet Options window:
 - a. Select the **Content** tab.
 - b. Click the **Certificates** button.



3. In the Certificates window:
 - a. You should see an entry similar to that seen at the right.
 - b. Click **Close**.



4. In the Internet Options window, click **OK**.

K. Additional Resources

Visit **ITCS's Information System** (<http://www.itd.umich.edu/itddoc/>) to obtain ITCS computer documentation and other resources. A list of relevant documents follows:

Obtaining Software from the ITCS Software Distribution Directory, S4147

Windows 95/98/ME/NT/2000 Internet Access Kit, S4269

We welcome your comments; please send e-mail to itd.doc.comments@umich.edu.

ITCS's Online Help Desk (www.itd.umich.edu/help/) provides a variety of computing help resources.

For further help with Kx509, send e-mail to online.consulting@umich.edu or phone 734) 764-HELP.