Using Smartcards in Windows Server 2000/3/XP

Nowadays everyone is concerned about network security. The concern leads to highly secured networks. But one week point is still left – your users passwords. Do you believe that everyone is only using long secure passwords with special characters etc? Well, you might have done a system policy. But are sure your users are not writing the passwords on a sticky note or somewhere else?
In the following article I would like to discuss how you could get rid of all the password problems with the introduction of smartcards. Your users would be very happy about such an introduction. Proper configured smartcards can also be used as a single logon mechanism.
All you need is a Windows 2000/2003 Active Directory Infrastructure. Below I will explain briefly how to set it up.

Installing the Enterprise CA

After you've acquired the PC/SC compatible smartcard readers such as the Aloaha Card Reader 38 and installed them on each computer, you need to prepare the smartcards. Each smartcard requires a certificate. To get that certificate on each smartcard, you need a certification authority (CA). To issue smartcard certificates, you need an Enterprise CA server. Most of the particulars for the installation of the CA are not significant when it comes to simply issuing the smartcard logon certificates. However, they may be important if you have other things planned for your CA.

If you don't already have a CA and you have no real preference on how to install it, you can follow these steps:

1. Log on as a member of the Enterprise Admins group.
2. Open the Windows Control Panel, open Add/Remove Programs, and click Add/Remove Windows Components.
3. The Certificate Services option is in the list of Windows components. Select that option and follow the wizard to install. The first thing you'll see is a warning message telling you that you cannot change your machine name or domain membership. Keep that in mind, click OK, and then click Next.
4. When the CA Type selection box appears, make sure that you're installing an Enterprise CA and then click Next.
5. In the CA Identifying Information box, enter a name for your CA and then click Next.
6. In the Certificate Database Settings dialog box, leave the default settings (unless you know that you want to change them) and click Next. You'll need the CD-ROM or installation files in a couple of seconds.
7. If you don't have Internet Information Services (IIS) installed, you'll be prompted to install IIS to get web enrollment working. If you don't plan to do any web enrollment, you can just click OK and don't worry about it. Click Finish when it's all over.

Next, you need a smartcard logon certificate template.

Creating the Template

After you have the CA installed, you need to manage it a bit. Create an MMC with the following snap-ins:

1. Active Directory Users and Computers
2. Certification Authority
3. Certificate Templates

Now that you have the console configured, click Certificate Templates and look for the Smartcard Logon certificate in the right-hand pane. Right-click the Smartcard Logon template and select Duplicate Template.

At this point, you get a Properties of New Template dialog box. (Name your template whatever you want.) Be sure to select Publish Certificate in Active Directory if the box isn't already checked.

Click the Request Handling tab and then select Signature and Smartcard Logon in the Purpose drop-down list. You want the user to be prompted to insert a smartcard during logon, so select the option Prompt the User During Enrollment.

Before you leave this dialog box, click the CSPs button near the bottom to open the CSP Selection dialog box, where you can select the appropriate cryptographic service provider (CSP). For example, I use a smartcard produced by Schlumberger, so I chose the Schlumberger CSP.

CAUTION

Some people think that they can choose pretty much anything here, but that isn't quite the case. What you select affects what the user sees on the other end. For example, if I selected the Infineon SICRYPT Base Smartcard CSP, I'd be prompted to insert my SICRYPT smartcard on the client side.

Select only the applicable CSP(s) for the smartcards you purchased. As I said earlier, this process is easier if you have only one type of smartcard and reader. If you have more than one smartcard type, you'll have to select multiple CSPs. Later in this article, you'll see how having multiple CSPs affects the user.

After clicking OK in the CSP Selection dialog box, you return to the Properties dialog box for the template you're setting up. Click the Security tab. If you want to allow all users in your Domain Users group to receive certificates during logon, you must add them to the Access Control List (ACL) for this template. Be sure to give them the rights to Read, Enroll, and Autoenroll.

Click OK. The template is ready. Now that you have the smartcard logon template duplicated, you need to issue it from the CA.

Issuing the Certificate

Issuing the certificate is a simple process: Expand the Certification Authority object in your MMC, expand your CA name, right-click Certificate Templates, click New, and then click Certificate Template to Issue. After that, you simply locate and select your newly created and configured certificate and click OK. The new certificate appears in the right-hand pane.

You're done with the Certification Authority. Now, you need to perform the final administrative step: configuring autoenrollment in Group Policy.

Configuring Autoenrollment

To deploy smartcard certificates in Windows 2000, you had to set up a smartcard enrollment station (a computer with a smartcard reader) and assign at least one person to put the certificates on the smartcards. To perform this job, the person had to physically insert the smartcard, download the certificate, maybe set the PIN, and then pull out the smartcard, repeating that process for each smartcard user. Although you may know someone who is just perfect for that job, this is a real problem for some organizations.

Although you can still set up an enrollment station and enrollment user in Windows Server 2003, you also have the option to distribute the workload of certificate deployment. This option, called autoenrollment, automates the deployment of certificates to the users' smartcards.

You can activate autoenrollment through Group Policy. Let's assume that you want to deploy smartcards to every user on your domain. Using that assumption, we'll configure the Default Domain Policy to enable autoenrollment.

Probably the quickest way to get to that Default Domain Policy is to right-click the domain object in Active Directory Users and Computers, click Properties, click Group Policy, and then click the Edit button (while the Default Domain Policy is selected). Find Autoenrollment in the right-hand pane and then click Properties.

The Autoenrollment Settings Properties dialog box appears - select both check boxes, or you are headed for disappointment.

Click OK and then close your Group Policy window. That's all for the configuration. Now you need to know what is about to happen to the users.

What the User Sees

You'll probably have to send out distribution email or some other communication to your network users, explaining the use of smartcards and describing the enrollment process. Essentially, it goes like this:

In the user's Welcome to Windows logon dialog box, the user should see the words "Insert your card or press Ctrl-Alt-Del to logon." This prompt is merely an indication that the smartcard driver and hardware were installed.

Sometime after the user logs on by the standard process of entering a username and password, a certificate icon appears in the user's system tray. The user must click the certificate icon, which opens a Certificate Enrollment dialog box. The user should click the Start button in this dialog box.

If you have multiple types of smartcards on your network and you selected multiple CSPs, users should be prompted to insert smartcards of all types (as many as you have). Each user must cancel enrollment requests for all smartcard types he doesn't have, and start enrollment only for the type of smartcard he has.

The user is then prompted to insert the smartcard and enter the PIN for the card. Most smartcards come with a default PIN, but you should remind users to change the default PIN during autoenrollment if that option is available, as it is for most smartcard readers.

NOTE

Check your smartcard manufacturer's documentation concerning PIN entry rules. If I enter the PIN incorrectly three times in a row on my smartcard, Schlumberger tells me that the card will be unusable. Now there's a failsafe for you!

After the user enters the default PIN and changes it to a new PIN, the certificate is automatically downloaded to the card. This step completes the process of distributing smartcards.

Forcing Smartcard Logons

When users have completed the process successfully, consider forcing smartcard logon by modifying the user's account properties to require smartcards for interactive logons. With this technique, you don't have to worry about someone logging onto one of your workstations without a smartcard. To configure this option, open Active Directory Users and Computers and access the user account properties. Select the option Smartcard Is Required for Interactive Logon.

If you require smartcard logon for all your network users, you can scour your domain for any remaining passwords that cannot be replaced. For example, some service accounts (those for Internet Information Server, Exchange Server, backup programs, etc.) still require passwords, so you still need a good password policy to secure those accounts. However, because you can control these passwords, they can be long, complex, and recorded on a piece of paper that's locked in a safe. Further, you can create an extremely stringent account policy to thwart any attempts to crack those passwords.

When you are done, take a few minutes to appreciate all your hard work. You've increased the security of your network and provided solid protection from password-cracking programs.

Additional Advantages

As already mentioned above you just removed the weakest point of your network. Besides that you also gave your company and users a huge added value. In most countries documents involved in electronic document exchange have to be signed digitally. Outlook together with the Aloaha Card Reader 38 now allows every user to send secure, digitally signed s/mime emails. Furthermore your users are now able to digitally sign any PDF file they created with the Aloaha PDF Suite. I am sure that based on this document you as an systems administrator can create some very strong points to get the permission to purchase some readers/smartcards.

Is Active Directory a must?

Active Directory helps to roll out such a smartcard system easily but is not needed. Instead of the Active Directory a normal Web browser could be used to roll out the certificates to any Infineon or Schlumberger Smartcard together with the Aloaha Card Reader. You can try it out:

Go to http://certserv.wrocklage.de/certsrv/ and choose “Request a Certificate”. Then choose “submit an advanced certificate request”. Once you clicked “Create and submit a request to this CA” you can chose your CSP under Key Options.