Multi-factor authentication in Windows - Part 1: USB tokens and smart cards

Until now, passwords were often used as a required authentication mechanism or it was a preferred mechanism when accessing sensitive systems and data. However, due to security needs, it requires more and more convenience, reducing the complexity and need to implement it

Martin Kiaer

Until now, passwords were often used as a required authentication mechanism or it was a preferred mechanism when accessing sensitive systems and data. However, due to the need for security, which requires increasing convenience, less complexity and the need to deploy additional authentication technologies, in this series we will introduce the multi-authentication technologies. Numbers used with Windows. In this first section we will begin to look at the basics of chip-based authentication.

When the password does not work

Back in 1956, George A. Miller wrote the article ' *Number 7 miraculously, plus or minus 2: Some limitations on information processing ability* ', it was an article describing the limitations of when you want to remember the pieces of information. One of the conclusions in the article is that an average person has the ability to remember 7 pieces of information at the same time the error can add / subtract 2. Other scientists then tried to improve, The average person can only remember 5 pieces of information at a time. However, the way to admit this theory challenges the problems associated with the length and complexity that come with this problem we can see in many other articles.

Complexity is often said to be one of the biggest threats to security. One of the areas in which we consider this issue is authenticated when users and administrators require a complex password policy to be followed. At the same time, this issue is always on the list of top 5 issues for the support of any organization. Gartner and Forrester predict that calls to the support team (or support group) involve forgetting passwords that cost approximately $ 10 per call. So doing an cost-benefit analysis for an organization's current password policy is a good thing to do now.

The password will be an authentic authentication mechanism when the length of the password is greater than 15 characters and has at least one non-English alphabet character. The clusters used are long passwords, so make sure the characters are easily remembered by the user. This will ensure that most 'rainbow' attacks, even 8-bit attacks, will fail, thanks to the added complexity of other characters.

Note :
Since Windows 2000, passwords can be supported up to 127 characters. However, the reason why passwords are just an inadequate authentication mechanism is because users often miss them well and protect unsecured

passwords. You may also find that the password is not properly protected. Fortunately, however, we have a number of other security solutions that will enable both security and convenience by using an easy-to-remember short password.

Authentication based on chips

One of these security solutions is chip-based authentication, which is often thought of as two-factor authentication. Certification of these two coefficients uses the combination of the following components:

1. Can be a smart card or USB token

2. Sometimes a personal identification number (PIN). A PIN may allow users to access digital certificates that are stored on a smart card.

Figure 1 illustrates two different solutions, but basically it has the same technology. Strictly speaking, it only varies in shape, cost and some components that make up the difference, although each solution may have some additional features that we will look at below.

Examples of smart cards can be used for both remote authentication and Windows authentication, physical access and billing.

Examples of USB tokens with chip-based authentication and flash memory to store files and documents .

Figure 1: Two examples of chip-based authentication devices

Both smart cards and USB tokens have chips attached. The chip requires a 32-bit microprocessor and normally has EEPROM (Electrically Erasable Programmable Read-only Memory) about 32KB or 64KB, the RAM chip is embedded on a smart card or USB token. Today, smart cards or USB tokens can be up to 256KB of RAM for secure data storage.

Note :
When talking about storage in this article, we only talk about the storage embedded in the security chip, not the device itself.

This chip has a small operating system and memory to store certificates, which is used for authentication. The on-chip operating system varies among different manufacturers, so make sure you use CSP (Cryptographic Service Provider) in Windows, which supports the on-chip operating system. We will look at the CSP in the next section. Chip-based solutions have some advantages over other multifactor authentication solutions because they can be used to store certificates for authentication, identification and signatures. As mentioned above, everything is protected by PIN, PIN can allow users to access data stored on the chip. Since an organization often maintains and issues smart cards or USB tokens for themselves, they also define certain policies related to the solution. For example, the card may be locked or deleted after a number of incorrect PIN entries. Because you can combine these policies with PINs, the length of the PIN may be shorter and thus easier to remember without being vulnerable to security breaches. All these parameters are saved on the smart card when it is released. The chip-based solution is also able to withstand interference problems, so in addition to the correct PIN, the data (certificates and personal information) stored on the chip cannot be accessed and thus cannot be used. on something else.

Smart card or USB token?

A difference between smart card and USB token is external appearance. Both solutions address basic needs, with

two-factor authentication, but each solution has its own advantages and disadvantages. Smart cards can be used for image recognition, because you can print photos and names on it. USB tokens may have flash memory for storing other documents and files. Both devices are used to control physical access in their own way. Smart cards can also have a circuit, magnetic magnets, bar codes like USB devices.

The smart card requires a card reader, while the USB token can use the existing USB port on the computer and that is the problem for this solution to compete with the smart card reader. Today, smart card readers need to use interfaces such as PC Card, ExpressCard, USB or built-in, some notebook computers and keyboards have implemented their models. Smart card readers are considered as Windows devices, completely independent of the chip operating system and they have security descriptors and PnP identifiers. Both readers and USB tokens require a Windows device driver before they can be used and you should always make sure to use the latest drivers, which comes from reasons for transparent performance. certification of two coefficients.

The initial cost may be slightly affected when you choose the chip solution to use. Smart cards and basic credit cards are similar. Many companies use smart cards for physical access at the office and pay for lunch, . That means that it has both convenient and monetary values ??and therefore users can protect and just bring their smart card with them all the time. It is also suitable for carrying in a wallet, which also helps it to be better protected.

Some issues to consider

When choosing a chip-based authentication solution, there are some issues and some tips that you should consider here:

1. ***Compatibility*** - Make sure that the chip operating system is compatible with the CSP you want to use. In the next part of this series, we will introduce CSP, the software that links the chip operating system and Windows, and it is also responsible for the security policy being applied to the chip.

2. ***Management issues*** - If you have to add smart cards or USB tokens to use for many people, choose the chip

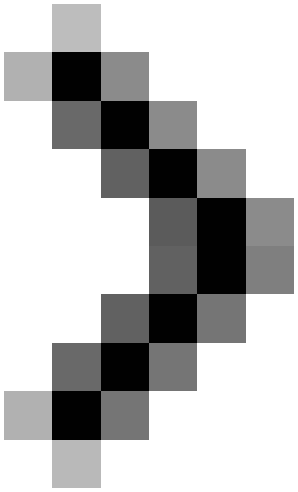
operating system compatible with the Card Management System (CMS) you have chosen.

3. ***Scalability*** - Ensure that the operating system chip can be used by all the required applications and the authentication needs you need. You may have future needs for adding additional certificates to this smart card or USB token, such as signing and encryption in email. Check out the DoD Common Access Card (CAC) specifications, details that have been used to store a lot of user information. Be sure to consider privacy issues when adding more information. We will consider this in the next section.

4. ***Usability*** - Make sure to select and add a chip-based solution, both for user-friendliness and manipulation. One of the biggest challenges with multifactor authentication solutions is that everyone has a tendency to forget or lose their smart card or USB device or forget the PIN if it is not used regularly.

Conclude

In the next section, we will show you how to best add smart cards or USB tokens to the Windows environment, and will also show you how to configure a CSP client and the differences between CSP configuration in Windows XP / Windows Server 2003 and Windows Vista / Windows Server 2008.



Part 2: Prepare devices for XP and Windows 2003