

## Re: CIFS / Kerberos question

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-02/0126.html>

---

**From:** Mike ([mjl000@hotmail.com](mailto:mjl000@hotmail.com))

**Date:** 02/04/03

From: "Mike" <[mjl000@hotmail.com](mailto:mjl000@hotmail.com)>  
Date: Tue, 04 Feb 2003 07:59:21 GMT

Here's some info that may help with your second and third questions.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:279815>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:180548>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:266080>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:274062>

<http://web.mit.edu/is/help/kerberos/>

<http://web.mit.edu/kerberos/www/>

news:comp.protocols.kerberos

<http://www.ornl.gov/~jar/HowToKerb.html>

There are many other web pages which can provide appropriate info like military sites.

Packet sniffing from a connected hub (for server, clients and network sniffer) is also a way to observe actual operations of traffic.

Additionally a network monitor or packet capture utility can operate from a server to capture traffic from a server.

"Naomaru Itoi" <[nittoi@activcard.com](mailto:nittoi@activcard.com)> wrote in message  
news:6c96015.0212131536.2f8ab8c7@posting.google.com...

> Hi,

>

> *This is a rather complicated question related to many subjects, so  
> please allow me to crosspost ...*

>

> *I am trying to achieve PKI authentication and SMB access to Windows*

> *Domain from a UNIX box. In other words:*

> *- From a UNIX box (let's say MacOS X), a user gets authenticated by a*

> *Domain Controller (which uses Active Directory for authenticating*

> *users) with digital signature with a smartcard*

> *- The user mounts a directory on a Windows PC, which is in the domain,  
> through SMB/CIFS.*

> *- The user accesses the files through SMB/CIFS.*

>

> *To achieve this, I need to gather some information about Kerberos and*

> *SMB/CIFS on Windows.*

>  
> *By reading documents in MSDN Library and on the Internet, I am*  
> *guessing the following are the architectures of Windows filesystem*  
> *client and server.*  
>  
> *Microsoft Client Microsoft Server*  
>  
> *Filesystem Filesystem*  
> -----  
> *SSPI-Krb5 SSPI-Krb5*  
> -----  
> *Kerberos / CSP Kerberos*  
> -----  
> *TCP/IP / PC/SC*  
>  
> *- Filesystem relies on SSPI-KerberosV to provide security services.*  
> *- SSPI-KerberosV5 uses KerberosV5 (and its PKI extension, PKINIT) to*  
> *authenticate a user (and maybe establish a secure channel).*  
> *- SSPI-KerberosV5 uses CSP/CAPI for smartcard services.*  
>  
> *[Question 1. Is this guess correct?]*  
>  
> *Assuming the answer to Question 1. is yes or almost yes, I believe I*  
> *can achieve the goal with an architecture like this:*  
>  
> *My Client MicroSoft Server*  
>  
> *Filesystem Filesystem*  
> -----  
> *GSSAPI-Krb5 SSPI-Krb5*  
> -----  
> *Kerberos / PC/SC Kerberos*  
> -----  
> *TCP/IP*  
>  
> *- Fortunately, since there are open source implementations of SMB/CIFS*  
> *filesystems (e.g. on MacOS X and on Linux), I don't have to write a*  
> *filesystem.*  
>  
> *Then, the next question is, what exactly do I have to do in*  
> *Kerberizing SMBFS.*  
>  
> *[Question 2. What exactly does Kerberos do in the server? If Kerberos*  
> *is used only for initial authentication, then all I need to do is*  
> *PKINIT in the filesystem on UNIX, right? Or, does the fileserver*  
> *actually check a ticket per each message, and even more, encrypt the*  
> *data transferred between the client and the server? If so, what*  
> *exactly do I have to do? Encrypt packets with Kerberos functions*  
> *(krb5\_mk\_priv(), etc.)?]*  
>  
> *[Question 3. Is there any documents, or maybe piece of code, which*

microsoft.public.win2000.security: Re: CIFS / Kerberos question

> *describe internals of SSPI, Microsoft filesystem implementation,*  
> *etc.?]*  
>  
> *As these are very detailed questions, I will appreciate any help ...*  
> *advices on how I should proceed, where to get more information, etc.*  
>  
> *Thank you.*  
>  
>  
> -----  
> *Naomaru Itoi, Ph.D.*  
> *ActivCard, Inc.*  
> *Researcher / Architect*  
> *Phone: 510-745-6270*