

## Re: Certificates

**Source:**

<http://www.tech-archive.net/Archive/Certification/microsoft.public.cert.exam.mcse/2004-03/4653.html>

---

**From:** Steven Umbach (*n9rou\_at\_n0spam-comcast.net*)

**Date:** 03/29/04

Date: Mon, 29 Mar 2004 00:36:51 GMT

Certificates in Windows 2000/2003 are part of the Public Key Infrastructure used as more secure or additional authentication for users AND computers. PKI uses a public/private keypair. The certificate is the public key that is distributed to anyone while the private key is very sensitive and must be secured and guarded. The domain recovery agent for EFS is an example of a private key used to recover domain users EFS files.

Certificates are used to issue a challenge to a computer [such as in ssl] or user by encrypting a string and sending it to the computer along with a session key. Only the holder of the matching private key can decrypt that string and send it back to computer issuing the challenge by encrypting it with the session key that was encrypted with the challenge assuring that ONLY the original computer issuing the challenge will be able to decrypt the response and then if the string was successfully decrypted by the challenged computer then authentication occurs. This assures a very high level of security in authentication as long as the private keys are secure.

Windows 2000/2003 server can be a Certificate Authority and issue certificates for domain users/computers or even non domain users. A private CA is usually only trusted within the domain or organization and would be useless for something like a IIS web server certificate for the general public since their computers/browsers would not trust the private certificates. However for a domain or organization, private certificates/private keys can be very useful in increasing security for things like ipsec, l2tp, EFS, email, smart cards, and user authentication. For instance l2tp requires a machine certificate/private key while pptp does not. The advantage is that if your organization uses l2tp, only computers with machine certificates/private keys issued by your CA will be able to access your network via vpn greatly increasing remote access security by eliminating the risk of password guessing from non domain machines. Smart cards are another example of using PKI in the domain. The smart card contains your user private key stored in a chip. With smart card access required, no one will be authenticated to the computer without the smart card being physically present and the user needs to enter a numeric code which usually locks out the user after a few bad attempts. These are the ways in which PKI can greatly increase security over traditional logon name/password. --- Steve

microsoft.public.cert.exam.mcse: Re: Certificates

"Tim Kettring" <tim6kettring@e-garfield.com> wrote in message  
news:c44ek2\$2ehq8m\$1@ID-212626.news.uni-berlin.de...

> *I am studying for win-2k-server , and dont understand what certificates (*  
> *from verasign etc... ) are good for . Why would a person need a root*  
> *certificate , when they supply a user name and password ?*

>  
> *Thanks , tim*

>  
>  
>