

## Authentication Protocols

You can use Network Connections with the following authentication protocols and methods.

### PAP

Password Authentication Protocol (PAP) uses plaintext (unencrypted) passwords and is the least sophisticated authentication protocol. PAP is typically used when your connection and the server cannot negotiate a more secure form of validation. You might need to use this protocol when you are attempting to connect to a non-Windows-based server.

### SPAP

Shiva Password Authentication Protocol (SPAP) uses a two-way encryption scheme to encrypt passwords. By using SPAP, Shiva clients can dial in to computers running Windows 2000 Server and Windows XP Professional clients can dial in to Shiva network access servers.

### CHAP

The Challenge Handshake Authentication Protocol (CHAP) negotiates a secure form of encrypted authentication by using Message Digest 5 (MD5), an industry-standard hashing scheme. A *hashing scheme* is a method for transforming data (for example, a password) in such a way that the result is unique and cannot be changed back to its original form. CHAP uses challenge-response with one-way MD5 hashing on the response. In this way, you can prove to the server that you know your password without actually sending the password over the network. By supporting CHAP and MD5, Network Connections can authenticate users to almost all third-party PPP servers.

#### Note

- If your server requires you to use PAP, SPAP, or CHAP, you cannot use data encryption for dial-up or PPTP connections.
- If the connection is configured to require data encryption, and connects to a server that is only configured for PAP, SPAP, or CHAP authentication, the client terminates the connection.

### MS-CHAP

Microsoft created *Microsoft Challenge Handshake Authentication Protocol* (MS-CHAP), an extension of CHAP, to authenticate remote Windows-based workstations. Like CHAP, MS-CHAP uses a challenge-response mechanism.

Where possible, MS-CHAP is consistent with standard CHAP. Its response packet is in a format specifically designed for networks with computers running Windows XP Professional, Windows XP Home Edition, Windows 2000, Windows NT, Windows Me, Windows 98, and Windows 95.

A version of MS-CHAP is available specifically for connecting to a Windows 95-based computer. It is available as part of the Windows Dial-up Networking 1.3 Performance and Security Upgrade for Windows 95. This is required only if your connection is being made to a Windows 95-based computer.

### MS-CHAPv2

Windows XP Professional also includes Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). This protocol provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving. To minimize the risk of password compromise during MS-CHAP exchanges, MS-CHAPv2 supports only a newer, more secure, version of the MS-CHAP password change process.

In Windows XP Professional and Windows 2000, both dial-up and VPN connections can use MS-CHAPv2. Windows NT 4.0, Windows 98, and Windows 95-based computers can only use MS-CHAPv2 authentication for VPN connections.

For VPN connections, Windows 2000 Server offers MS-CHAPv2 before offering MS-CHAP. Updated Windows-based

clients accept MS-CHAPv2 when it is offered and MS-CHAP is enabled. Dial-up connections are not affected.

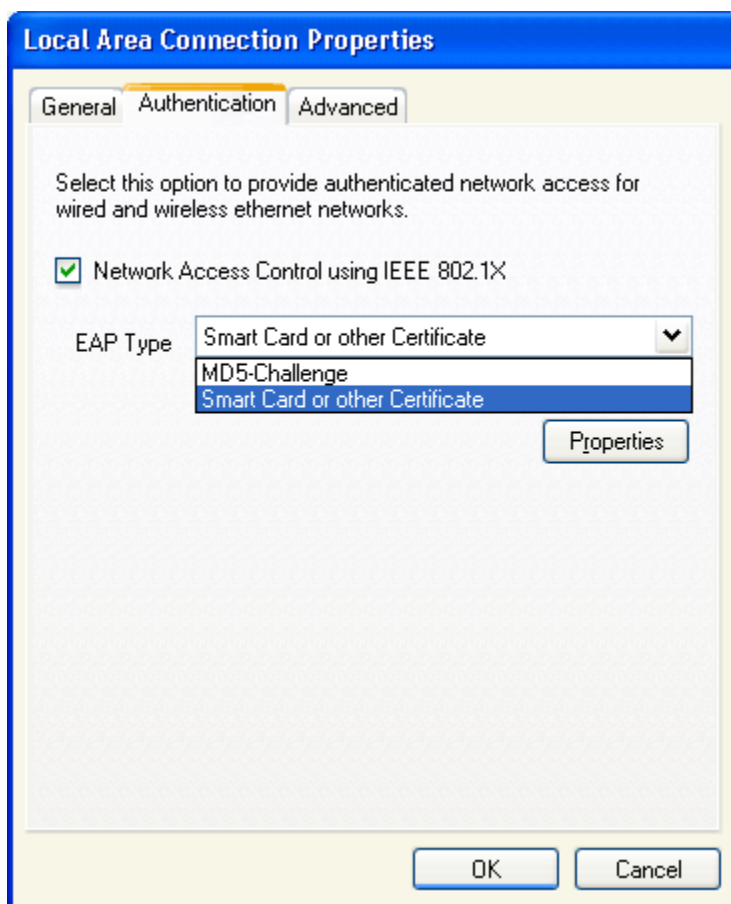
## EAP

The *Extensible Authentication Protocol* (EAP) is an extension to the Point-to-Point Protocol (PPP). EAP was developed in response to an increasing demand for remote access user authentication that uses third-party security devices. EAP provides an infrastructure to support additional authentication methods within PPP. By using EAP, support for any number of authentication methods might be added, including token cards, one-time passwords, public key authentication using smart cards, certificates, and others. EAP is a critical technology component for secure VPN connections, because it offers stronger authentication methods (such as public key certificates) that are more secure against brute-force attacks, dictionary attacks, and password guessing than older password-based authentication methods.

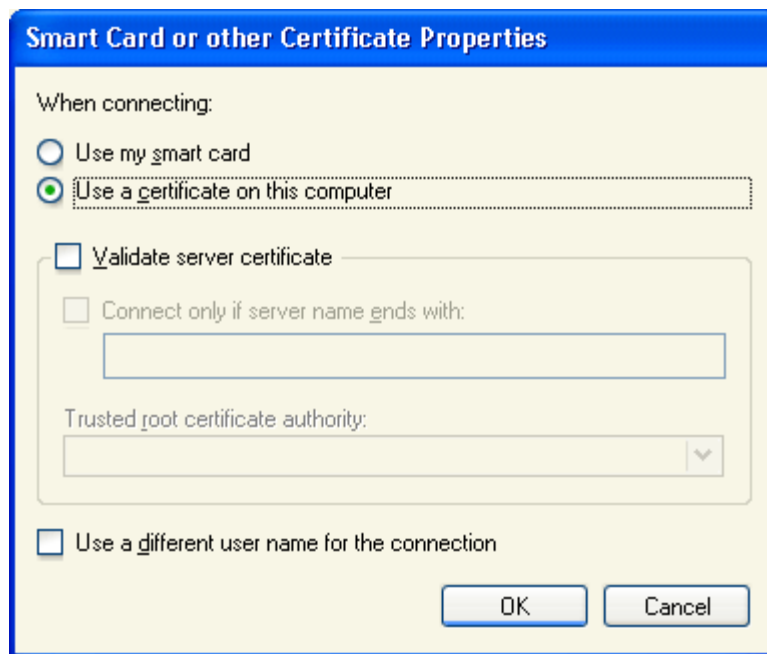
## Certificate Authentication

A certificate is an encrypted set of authentication credentials, including a digital signature from the certification authority that issued the certificate. In the certificate authentication process, your computer presents its user certificate to the server, and the server presents its computer certificate to your computer, enabling mutual authentication. As shown in Figures 21.4 and 21.5, if a user certificate is installed either in the certificate store on your computer or on a smart card, and EAP-TLS is enabled, you can use certificate-based authentication in a single network logon process. This provides tamper-resistant storage of authentication information.

**Figure 21.4 Authentication tab on the Local Area Connection Properties sheet**



**Figure 21.5 Smart Card or other Certificate Properties dialog box**



Certificates are validated by verifying the digital signature by means of a public key. The public key is contained in a trusted authority root certificate of the certification authority that issued the certificate. These root certificates are the basis for certificate verification and are supplied only by a system administrator.

### Smart Cards

A smart card is a credit card–sized device that is inserted into a smart card reader, which is either installed internally in your computer or connected externally to your computer.

Certificates can reside either in the certificate store on your computer or on a smart card. When setting the security options of a connection, you can use a smart card or other certificate, and you can specify particular certificate requirements. For example, you can specify that the server's certificate must be validated.

When you double-click **New Connection** in the Network Connections folder, if a smart-card reader is installed, Windows XP Professional detects it and prompts you to use it as the authentication method for the connection. If you decide not to use the smart card at the time you create a connection, you can later modify the connection to use another certificate or authentication method.

---

[Manage Your Profile](#) | [Legal](#) | [Contact Us](#)

© 2005 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)