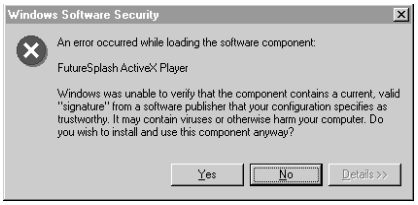
Security

With a built-in set of Internet security technologies, Microsoft Internet Explorer 3.0 lets you communicate privately, download code you can trust, and identify yourself to others across the Internet. This means you can conduct transactions and participate in consumer services on the Internet with the same privacy and security as in the real world.

The following security technologies are supported in Internet Explorer 3.0.

Authenticode ™ Technology

Authenticode enables developers to digitally sign their software code, allowing you to verify the publisher of the software before you download it from the Internet. Verifying the digital signature also ensures that the software hasn't been tampered with during downloading.

- 

- **Figure 8** Microsoft Internet Explorer checks to see if software or software components are authentic before you download them from the Internet.
-
- **Open.** Authenticode supports existing certificate standards, X.509 certificate format, and PKCS #7 signed data standards. This commitment to supporting security standards is also evidenced by Microsoft's recently submitted code signing proposal and presentation to the World Wide Web Consortium (W3C). Microsoft Authenticode technology is an implementation of this widely supported proposal.
- **Software Publishing Certificate program.** Microsoft is working with industry-leading certification authorities such as VeriSign and GTE who will issue certificates, based on standard X.509 and PKCS #7 formats, which software publishers can use to digitally sign their code. Tools for code-signing are available through the ActiveX SDK, and will be integrated into Microsoft and leading third-party development tools.

- **Figure 9** Publishers' Public Key Certificate

Secure Sockets Layer 2.0/3.0 (SSL), Private Communication Technology 1.0 (PCT)

Support for SSL 2.0/3.0 and PCT 1.0 ensures that your personal or business communications using the Internet or intranets are private. The SSL and PCT protocols create a secure channel, so that no one can eavesdrop on your communications. With secure communications guaranteed, you can send e-mail, buy consumer goods, reserve airplane tickets, or even conduct personal banking on the Internet.

Client authentication. Client authentication lets you present your personal certificates to Web servers that request it. In this way, Internet Explorer functions as your virtual wallet, storing your personal certificates and then presenting them to Web servers when they need to verify your identity.

Personal certificates also make it easier to connect to Web services. You no longer need to type your user name and password to connect to your favorite Web subscription service. Instead, it automatically requests your personal certificate and validates your identity. In future versions, the Microsoft Wallet will also store a wider variety of personal information such as credit card numbers, passwords, or private keys.

Server authentication. Server authentication ensures that you are communicating with your intended party. Internet Explorer caches site certificates of Web services that you can use to verify the identity of any Web merchant or other Web server before you purchase goods or communicate with them. In addition, you know that only the sender of the message could have sent the message, and the message has not been altered in transit.

With the release of Microsoft Internet Explorer 3.0 (Beta 2), Internet Explorer enables you to view personal, site, and certificate authority digital certificates. Soon, you will be able to obtain your personal certificates from Certificate Authorities, such as VeriSign and GTE, when they become available.

Microsoft is working with Netscape and others, as part of the Internet Engineering Task Force (IETF) Transport Layer Security working group, to create a unified, standard secure channel protocol. Microsoft has written a discussion draft that combines the best features of SSL 3.0 and PCT 2.0, using SSL 3.0 as a base and adding features from PCT 2.0 based on feedback from cryptographers and implementers.

"Cookie" Privacy

Some web sites use a technology called "cookies" to store a small amount of information on you computer. These "cookies" are usually used to provide web site customization features. With Internet Explorer 3.0 Beta 2, you can choose to be warned before a "cookie" is stored on your computer and then elect to accept the "cookie" or not.

SOCKS Firewall Support

Many corporations provide their employees access to the Internet through firewalls that protect the corporation from unwanted access. SOCKS is a standard protocol for traversing firewalls in a secure and controlled manner. This version of Internet Explorer is compatible with firewalls that use the SOCKS protocol. This support was provided by Hummingbird Communications Ltd., a leading provider of firewalls.

NTLM Challenge/Response

Corporations can take advantage of Windows NT Server's challenge/response authentication that may already be in use on their Windows NT Server network. This enables users to have increased password protection and security while remaining interoperable with their existing Internet information servers.

CryptoAPI 1.0

CryptoAPI, the foundation of the Microsoft Internet Security Framework, provides the underlying security services for secure channels and code signing. The delivery of CryptoAPI 1.0 through Internet Explorer 3.0 allows you to easily integrate strong cryptography in your applications. Cryptographic Service Provider (CSP) modules interface with CryptoAPI and perform functions including key generation and exchange, data encryption and decryption, hashing, digital signatures, and signature verification. Internet Explorer 3.0 will install the Microsoft RSA Base Provider CSP on Windows 95.

CryptoAPI 2.0, scheduled for beta release in third quarter of 1996, will provide high level APIs for authentication, signing, and encryption and decryption services as well as a complete public key infrastructure. With this infrastructure, your applications can take advantage of certificate management functionality such as requesting that a certificate be created, stored, or verified.

- **Extensible security.** CryptoAPI isolates the application from the CSP modules and allows different CSPs to be used without modifying application code. CryptoAPI allows vendors to develop and efficiently deliver strong encryption CSPs to customers to the maximum extent allowed by existing law.
- **Open.** CryptoAPI's open architecture allows you a choice of CSPs. CryptoAPI will also be made available across the Windows, Macintosh, and UNIX operating systems. In addition, CryptoAPI 2.0 will support the following standard certificate formats: X.509 version 3, ASN.1, and DER.
- **Leverages existing skills and solutions.** CryptoAPI lets you use your existing programming expertise to incorporate cryptography in applications or existing solutions.

Commitment to Internet Standards

This set of security technologies, which is part of the Microsoft Internet Security Framework, supports Internet standards such as X.509 and PKCS#7 certificate formats. In addition, Microsoft actively participates in the Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and other groups to develop Internet security standards. Recent Microsoft security initiatives include the code signing proposal submitted to the W3C and the Transport Layer Security (TLS) efforts through the IETF, aimed at creating a single secure channel standard.