



# OmniRoot™ for Microsoft Users

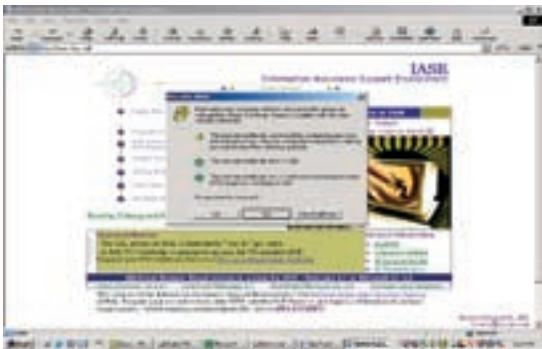
## Providing Public Trust to Organizations Issuing SSL Certificates

### ESTABLISHING TRUST TO DRIVE BUSINESS

Consumers and businesses now conduct business online using devices, such as PDAs, phones and appliances, going well beyond PC's and Laptops. The ongoing success of today's web-based services requires that users trust these services and are able to perform transactions securely from any web-enabled device. It has become the industry standard to secure the web properties running these services using SSL server certificates. Publicly recognized SSL certificates ensure the identity and authenticity of the web property and maintain the privacy, security and integrity required for these transactions.

### THE IMPORTANCE OF ROOTS

Organizations rely on SSL certificates issued by reputable public certificate vendors to provide security and trust for their users — if a certificate is not trusted then the user will receive a security warning. A security warning will decrease trust in the online service or mobile carrier. To prevent the user from receiving a warning, the device they are using needs to have a root certificate from within the same hierarchy as that used to issue the SSL certificate on the server being accessed.



Example Security warning - No embedded root

### ESTABLISHING A TRUSTED ROOT

You may set up a mechanism whereby the user installs your root certificate as a trusted root within their browser, but this can be complicated and frustrating for users and is particularly difficult to manage when you are faced with a broad-based user community with numerous versions of browsers.

Alternatively you can seek to have your own root certificate embedded in web browsers but it will take a minimum of two years for those browsers to become widespread in the marketplace and you will also have to dedicate resources to the ongoing management of the embedded root.

### GREATER CONTROL AND REDUCED COSTS

For organizations hosting large numbers of web servers secured by SSL, or issuing numerous client certificates the OmniRoot is unbeatable. By simply leveraging your existing CA, you can take control of the complete certificate management process to secure your own web sites and communications, while reaping significant annual savings over the cost of purchasing comparable certificates on the retail market.

### LEVERAGING YOUR MICROSOFT CA

OmniRoot extends Microsoft Windows® 2000 and .NET® Certification Authority usability by allowing customers who are using or plan to use the Microsoft PKI with the opportunity to chain to Cybertrust's pre-distributed root certificate. The use of Cybertrust's OmniRoot facilitates quick deployment and use of digital certificates. Cybertrust is among a select group of CA providers who currently have root certificates embedded in the most popular browser and server software such as Microsoft Internet Explorer and Internet Information Server. Certificates issued under Cybertrust's hierarchy reduce the cost, time, and security concerns associated with deploying a new root certificate to establish a new certification hierarchy.



# OmniRoot for Microsoft Users

## Providing Public Trust to Organizations Issuing SSL Certificates

### UNIQUELY VALUABLE TO MICROSOFT USERS

#### Maximize features of Windows 2000 and XP

Cybertrust OmniRoot creates unique enhancements to Microsoft's PKI capabilities. By making its predistributed root available, Cybertrust enables Microsoft users to more fully leverage the built-in security features of Windows 2000 and XP.

#### Go Beyond the Enterprise

Using OmniRoot with a Microsoft PKI, certificates can cross enterprise boundaries and enjoy worldwide acceptance.

### ADDITIONAL BENEFITS

#### Enhance usability and user experience

OmniRoot simplifies deployment for an enterprise by leveraging Cybertrust's pre-distributed root certificate, which is already embedded in the majority of web and micro browsers in use. This seamless approach to root certificate distribution and usage will significantly reduce incoming help-desk calls, thereby eliminating an unnecessary IT burden.

#### Build and maintain trusted relationships while promoting your brand

Certificates carry your brand, yet they can be validated in the hierarchy under the Cybertrust root. This gives you operational ease while preserving your identity and branding since you remain the issuer of the certificates.

#### Address Clients & Servers

Client or Server? OmniRoot eliminates the need to deploy a root certificate to end-user clients everywhere. Once a your OmniRoot certificate hierarchy is established, end-users receiving client certificates will be able to seamlessly interact with each other and will also be able to securely communicate with certificate-enabled application servers.



### HIGH UBIQUITY & CONSUMER RELIANCE

The ongoing success of today's internet-based commerce requires that consumers and businesses are able to communicate securely on multiple devices.

The Cybertrust root is present in the widest variety of browsers, servers, phones, secure email programs, operating systems and applications. In addition, some of the largest organizations online rely on certificates issued from the Cybertrust root. With millions of users relying on our technology, Cybertrust is dedicated to maintaining the highest ubiquity and ensuring the continued success of online commerce.

### NEAR UNIVERSAL INTEROPERABILITY

#### Leading Applications, Browsers and Clients

Apple	FireFox
Microsoft	Citrix
Lotus	AOL
Netscape	Opera
Qualcomm Eudora	Mozilla
Sun	Red Hat Linux Konqueror

#### Leading Mobile and Handheld Devices

Openwave	Palm/ Handspring
Motorola	Microsoft Pocket PC
Nokia	AT&T
NTT DoCoMo	RIM
Panasonic Mobile	SonyEricsson
Philips	Vodafone J-Phone

Complete listing available upon request

#### ABOUT CYBERTRUST

Cybertrust is a global information security company that offers business-driven consulting, managed services and enabling technologies to help businesses and governments gain greater visibility and control of their risk. By aligning information security to business objectives, Cybertrust can help customers improve their overall information security — often with the people, processes and technologies already in place. Cybertrust is 100 percent focused on information security and is vendor- and product-neutral. Its intelligence and resources are applied to deliver the best possible information security practices and strategies for each customer's business, specifically focusing on critical identity and access, threat and vulnerability, and compliance management challenges. Cybertrust has earned the trust of thousands of customers worldwide, has been recognized as the global market leader in managed security services, and is one of the world's largest providers of information security. Headquartered in Herndon, Virginia, USA, Cybertrust has 30 offices around the world. For more information, visit [www.cybertrust.com](http://www.cybertrust.com).



13650 DULLES TECHNOLOGY DRIVE, SUITE 500, HERNDON, VA 20171-4602, USA  
1.888.396.8348 » [WWW.CYBERTRUST.COM](http://WWW.CYBERTRUST.COM)

Cybertrust combines the expertise of Betrustrusted®, TruSecure®, and Ubizen®. We deliver information security consulting, managed services, and technology.