GeoRoot™

The power of your own trusted Certificate Authority

PROTECT YOUR BUSINESS WITH YOUR OWN CERTIFICATE AUTHORITY

The growing demand for secure e-business environments makes user and transaction identity certification a necessity. One of the most important steps toward achieving enterprise-wide protection is to issue digital certificates through a Certificate Authority (CA). Yet, organizations that choose to run their own private CA often grapple with a common obstacle -- a lack of global recognition for their "self-signed" certificates.

GeoRoot is an ideal solution that allows enterprises to retain full control over Registration Authority (RA) functions for the issuance of SSL server certificates for domains and client certificates (x.509). With GeoRoot, your organization will gain the inherent security, confidence and recognition that result from being chained to one of GeoTrust's trusted roots.

COMPATIBLE WITH 99% OF ALL BROWSERS

Lack of certificate recognition can be costly resulting in the loss of critical business or the denial of user access to vital information. If a certificate is not recognized, the result is that the recipient may receive an error message or complaint from the browser, and consequently not trust either the server or the source.

GeoTrust certificates are recognized by 99% of all browsers, and are compatible with most digital certificate and public key security applications, including commerce sites, intranet, extranet, S/MIME, and VPN hardware and clients. Enterprises using GeoRoot can also issue digital certificates for customized internal applications, and to partners and other affiliated organizations that need to securely exchange data. It's this type of ubiquitous recognition that gives enterprises the confidence of knowing that their certificates, whether for electronic documents, secure email or other transactions, will be trusted globally.

MAINTAIN CONTROL, BRAND IDENTITY AND COSTS

GeoRoot allows enterprises to maintain complete control over certificate lifecycle management, including issuance, renewal and revocation. Functions such as authenticating individuals, deploying and managing SSL server certificates and client certificates, and managing the distribution of public keys to appropriate parties all lie internally - providing maximum flexibility for securing enterprise-wide business applications.

In addition, GeoRoot allows an enterprise to maintain its own brand identity when issuing certificates - helping win the confidence of everyone they do business with. With privately-branded certificates, organizations build and maintain their own reputation for secure and trusted e-business transactions. The predictability of GeoRoot's low fixed annual fees and cost-effective licensing model help maximize IT budgets and minimize Total Cost of Ownership.

SEAMLESS INTEGRATION WITH MICROSOFT BACK OFFICE ENVIRONMENTS

GeoRoot works seamlessly with Microsoft Active Directory and Certificate Server for the authentication and delivery of GeoTrust-signed certificates. In most instances, once a certificate is generated by MS Certificate Server and signed in GeoRoot, the information about that certificate automatically flows directly into Active Directory.

GENERAL GEOROOT REQUIREMENTS AND GUIDELINES

To prevent any security compromises caused by malicious intent, system failures or inadvertent errors, GeoRoot customers are required to meet and adhere to guidelines for generating and managing certificates in a trustworthy fashion.

To become a GeoRoot customer, your organization must meet the following eligibility requirements:
- Net worth of $5M or more
- Carry a minimum of $5M in Errors and Omissions insurance
- Provide Articles of Incorporation (or similar) and an incumbency certificate
- Provide a Certificate Practice Statement (CPS)
- Provide hardware key generation and storage on a FIPS 140-1 Level 2 compliant device
- Utilize an approved CA product from Baltimore/Betrusted, Entrust, Microsoft, Netscape or RSA

GeoRoot customers must adhere to the following guidelines:
- Submit the certificate profiles for the company CA certificates and certificate to GeoTrust for review and approval before issuing such certificates
- Maintain an accurate Certificate Revocation List (CRL) for all company issued certificates
- GeoTrust may request a statement of compliance, or may perform an audit

GEOROOT SSL SERVER CERTIFICATE GUIDELINES

The following domain guidelines apply to GeoRoot customers:
- SSL certificates can be issued for one or multiple years
- All domains must be owned by the enterprise customer
- The certificates can be installed on as many servers as needed
- The SSL certificates must include the standard set of X.509 extensions

GEOROOT CLIENT CERTIFICATE GUIDELINES

The following guidelines apply to GeoRoot customers for the issuance of client certificates for S/MIME or secure mail:
- Client certificates can be issued for one or multiple years
- Certificates can be issued to company employees and company partners only for use and may not be resold or provided to users with no affiliation with company
- The certificates must include the standard set of X.509 extensions

ABOUT GEOTRUST.

GeoTrust is a leader in identity verification and trust services for e-business. Its products include web security services for secure e-commerce transactions, identity verification, managed security services and TrustWatch (www.trustwatch.com), a free toolbar and search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information. With more than 100,000 companies in over 140 countries using its technology for online security, GeoTrust has rapidly become the second largest identity verification provider in the world. Visit www.geotrust.com or call +44 1622 764789 for more information.

GeoTrust®

6 Kings Row, Armstrong Road
Maidstone, Kent, UK
Phone: +44 1622 764789
E-mail: info@geotrusteurope.com
www.geotrusteurope.com