Compliancy for Massachusetts Data Protection Policy 201 CMR 17

E-mail encryption for the protection of personal information

Effective March 1, 2010 all organizations large and small that store, own, or maintain information of Massachusetts residents will be required to comply with new data protection regulation, 201 CMR 17. The regulation mandates security standards that must be met by all persons and organizations that own or license personal information about a resident of the commonwealth in either paper or electronic forms.

Explanation of 201 CMR 17

Effective March 1, 2010 organizations that store, own, or maintain information of Massachusetts residents will be required to comply with new data protection regulation, 201 CMR 17. The regulation mandates security standards that must be met by all persons and organizations that own or license personal information about a resident of the commonwealth in either paper or electronic forms.

Personal Information- defined as a Massachusetts resident's first and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

- Social Security Number
- Driver's License Number or state-issued identification card number
- Financial Account Number
- Credit or Debit Card Number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account

Do I need to Comply?

- Do you transmit personal information via e-mail?
- Do you maintain personal information on a desktop computer?
- Do you maintain personal information on a laptop computer or removable device?
- Do you make periodic backups of any data containing personal information?

If you answered yes to any of the above questions you need to begin using encryption when handling, storing, and transmitting all personal information.

*Please note this is only a minimal list of business activities that require compliance, please see the full list at http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

How do I Comply?

-All files and documents containing personal information should be encrypted

-All e-mail communications that contain personal information (credit card numbers, social security numbers, driver license numbers, etc) must be encrypted. **The use of a digital certificate allows you to encrypt e-mail messages.**

-Establish a secure website that requires safeguards such as cryptographic technology and/or tokens to conduct transactions involving personal information. **The use of digital certificates allows you to implement cryptographic technology.**

To address the concerned highlighted above, many organizations have turned to secure e-mail as a method to protect personal information using their current e-mail client like Outlook, Outlook Express, Mozilla Thunderbird and Apple Safari. These popular e-mail clients among others support the Secure/ Multipurpose Internet Mail Extensions (S/MIME) standard for encrypting e-mail.

What is Encryption?

Encryption is the process of transforming text such as e-mail messages and attachments to make it unreadable by anyone except the person the message is intended for. The recipient (as well as the sender) needs to hold a digital certificate and accompanying private key, where the senders' and recipient's public keys are shared.

What is a Digital Certificate?

A digital certificate contains a public key and a private key; the purpose of the public key is to give out to anyone publicly so they can send you encrypted emails. Your private key is a key/algorithm that you will want to keep private and not give out to anyone. When someone sends you an encrypted e-mail only your private key will be able to open the e-mail. Giving out your public key is easy, you simply digitally sign an e-mail and send to a recipient.

For more information about GlobalSign solutions, please call 1-877-SSL-GLOBAL

Visit www.globalsign.com for more information

GlobalSign Certificates for E-mail Encryption

GlobalSign offers a range of digital certificates with varying trust levels for individual consumers and enterprises. GlobalSign's enterprise solutions include digital certificates for individuals e.g. Sally Jones, or organization departments e.g. Marketing Department.

Personal Level Certificates

PersonalSign1- Low cost, immediately issued Digital ID that can be readily used to secure e-mail. For personal use to secure e-mail communications only an e-mail validation is completed.

PersonalSign2- Used for individuals (not representing an organization) to secure e-mail (S/MIME), authenticate to online services, and digitally sign Microsoft Office Documents. PersonalSign 2 provides more identity authentication as GlobalSign checks to verify you are who you claim to be

Enterprise Level

PersonalSign 2 Pro- Used for individuals representing organizations to secure e-mail (S/MIME), authenticate to enterprise online services, and digitally sign Microsoft Office Documents.

PersonalSign2 Department- Used for departmental identities (such as Marketing) to secure e-mail (S/MIME), authenticate enterprise online services, and digitally sign Microsoft Office documents.

Managing Multiple Digital Certificates

GlobalSign's Enterprise PKI (ePKI) can issue Digital IDs to multiple employees, suppliers, and extranet users for authentication, secure e-mail, and document security. ePKI offers complete life cycle management and online identity management. By using ePKI, issuing, reissuing, renewing, and revoking is made easy across numerous departments and office locations. The one-time vetting process means that once the organization is vetted, staff can issue secure client certificates on demand against a single or multiple certificate profiles.

The ePKI solution is a web-based portal that allows an appointed Administrator to acquire complete control of certificates issued to individuals or roles under their fully vetted organization identity. Administrators can manage all standard Client and SSL Certificates through the same GlobalSign Certificate Center (GCC). ePKI administrators just log-in their ePKI portal, select which Profile and certificate type they wish to register an end user for and invitations are issued immediately.

About GlobalSign

Established in 1996 and as a WebTrust accredited public certificate authority, GlobalSign offers publicly trusted SSL Certificates, EV SSL, Managed SSL Services, S/MIME e-mail security and Code Signing for use on all platforms including mobile devices. Its Trusted Root solution uses the widely embedded GlobalSign Root CA certificates to provide immediate PKI trust for Microsoft Certificate Services and internal PKI, eliminating the costs of using untrusted Root Certificates. Its partnership with Adobe to provide Certified Document Services (CDS) enables secure digitally signed PDF documents, certified transcripts and invoices. These core Digital Certificate solutions allow its thousands of authenticated customers to conduct secure online transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure e-mail and access control. The company has a history of innovation within the online security industry and has offices in the US, UK, Belgium, Japan, and China.

GlobalSign, Inc
Two International Drive
Suite 105
Portsmouth, NH 03801
http://www.globalsign.com

Massachusetts -CMR-201 v1.0. Published 29-03-2010.