

White Paper

Banking, E-mail

and GLB Security Requirements



© 2001-2002 CertifiedMail.com, Inc.

<http://www.re-soft.com>

E-Mail In Banking

According to industry estimates, more than half of the US population is currently using Internet e-mail. Increasingly, e-mail is taking the place of postal mail to communicate between financial institutions and consumers. E-mail is also popular with financial workers to send data and attachments to colleagues for collaboration and review. E-mail empowers the financial industry in new ways and brings new expectations as well.

Significant productivity gains and cost savings will further entrench e-mail into the financial industry. But before e-mail can be used as a universal communication tool for sensitive data, several significant drawbacks must be addressed. E-mail was designed for easy, rapid flow of information, without considering accountability and security of information. These are important attributes to the financial industry, especially when sending consumer account information. In the same way that financial records would never be sent on the back of a postcard, e-mailing the same data exposes this information as plain text to the Internet.

GLB Overview

Federal legislators are aware of these limitations, and have passed new regulations ensuring the privacy of financial data. The Gramm-Leach-Bliley Act (GLB) mandates the privacy of consumer financial data. It is resulting in sweeping changes in banking transaction and administrative information systems. GLB is quite far reaching, since it defines “financial institution” to be any institution engaged in activities that have been determined to be financial in nature under the Bank Holding Company Act. There is no requirement that the company be a bank or be affiliated with a bank. As a result, every time the Federal Reserve and the Treasury determine that an activity is financial in nature and therefore a permissible activity for a financial holding company, a side-effect is that the GLB privacy rules cover a new industry.

CertifiedMail Solution

The ideal scenario for financial organizations would be to maintain the benefits of their existing e-mail system, expand its use to gain more efficiency, and comply with GLB requirements. By leveraging widely adopted open standards for security, and supplementing existing e-mail systems with these standards, this ideal scenario can be attained.



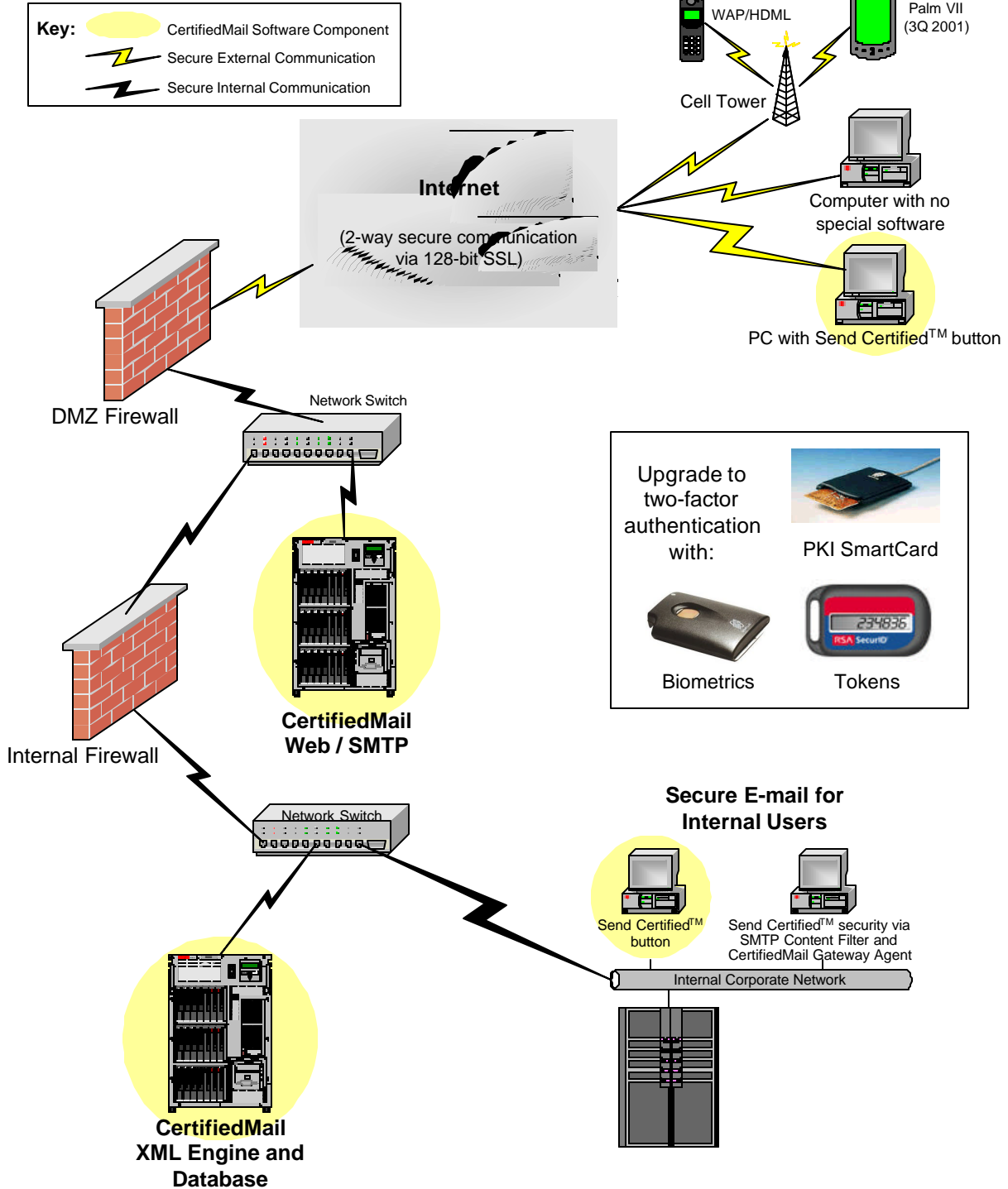
CertifiedMail.com Inc. is a security company that provides GLB-compliant e-mail for financial organizations. Based on open standards, CertifiedMail enables enterprises to rapidly establish secure, accountable, scalable communication with thousands or millions of recipients, including customers, colleagues and vendors. The CertifiedMail solution is installed in the organization's Datacenter, and enhances existing e-mail platforms. With CertifiedMail, financial employees use their current e-mail client, such as MS-Outlook or Lotus Notes, to send secure e-mail. This eliminates the need for retraining, and results in rapid adoption. Another key feature is ease of use for Internet-based recipients and employees who are traveling or at home, with no special system requirements or software to download.

The CertifiedMail solution is designed to be easy and ubiquitous, yet offer the high level of security needed to comply with privacy regulations. Features such as end to end message security, transparent encryption, digital fingerprints to verify document originality, strong authentication of senders and recipients, and two-factor authentication with smart cards, X.509 certificates and SecurID provide a very robust security environment. But even with these advanced features, a security system should be easy to use by senders, recipients and By leveraging open standards, using decades of experience in software and security design, and continually learning from customer feedback, the CertifiedMail system is easy for administrators to manage and maintain, and for users to send, receive and track secure e-mail.



Appendix A

CertifiedMail Architecture



For more information, visit us at <http://CertifiedMail.com>



Appendix B

Following are key elements of the CertifiedMail GLB-compliant messaging system.

Design Element	CertifiedMail	Benefit
Secure Messaging Implementation		
E-mail client integration	Send Certified but- ton for Outlook, Lotus Notes	One-click security from popular e-mail clients eliminates training and mistakes.
E-mail Gateway interface	Yes	Supports policy-based content filters. No client software needed to send secure messages from the desktop.
Wireless Support	Yes	All secure messaging features have been extended to WAP/HDML-enabled devices such as Internet cell phones.
Authentication, En- ryption, Integrity	Yes	User Authentication, end-to-end transparent encryption and message integrity using RSA MD5 digital fingerprint.
RSA SecureID Authentication	Yes	Integrate the CertifiedMail login with your existing SecureID ACE Server, providing strong user authentication.
PKI Authentication	Yes	PKI certificates can be queried for strong authentication.
eSign Electronic Signatures	Yes	Embed digital signatures into documents and HTML pages in compliance with the eSign Act.
Any Internet recipi- ent can receive a secure message	Yes	Universal system-wide secure e-mail platform.
Message tracking	Yes	Confirmation when the recipient opened a message.
Retract message not yet opened.	Yes	Undo costly errors when e-mail is sent to the wrong recipient.
Unlimited attach- ments per message	Yes	Transmit any number of attachments, including very large documents, even though the recipient's e-mail system has message size or storage space limitations.
Server Technology		
OS platform	Intel-based servers and Windows 2000 operating system	Low cost hardware, software and on-going maintenance. Enterprise ready. Easy to maintain.
Data interfaces	XML, SQL and SMTP	Rapid integration with legacy systems and enterprise appli- cations, including call center and billing systems.
Server Version	Yes	Fault-tolerant, clustered and load-balanced configuration based on capacity requirements. Designed for mission criti- cal enterprise needs and installed in your DataCenter.
Appliance Version	Yes	CertifiedMail Appliance is appropriate for departmental us- age, and can be upgraded to a full server without losing data.

