

# Secure Email for the Real World

A CertifiedMail Technology Paper



**Microsoft**<sup>®</sup>  
**GOLD CERTIFIED**  
*Partner*

**CertifiedMail, Inc**  
through ReSoft International LLC  
[www.re-soft.com](http://www.re-soft.com)  
Phone 203 972 8462      [info@re-soft.com](mailto:info@re-soft.com)



## Executive Summary

Since written communications began, there has been a need for some of those communications to be more secure or secret than others. The need for medieval monarchs to maintain a 'need-to-know only' communications policy to protect their empire-building plans is no different than the need for Silicon Valley entrepreneurs to protect their business plans from potential competitors.

Add to that the requirements that governments have now put in place to protect personal and institutional privacy with legislation such as the Health Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, and Sarbanes-Oxley, and secure email has become a must-have, rather than a would-be-nice, for most businesses today.

Historically, email security has been a black art, the province of specialists in encryption, digital certificates, virtual private networks, and key algorithms of various degrees of complexity. But with everyday human resources tasks now requiring the use of secure email, such an approach is no longer viable. Non-technical users need to be able to send secure communications at the touch of a button. And IT staffs need a standardized approach so that they're able to easily manage secure email systems alongside all their other tasks.

This paper describes how CertifiedMail has, over the past decade, developed and implemented a range of secure email solutions that are easy to install, maintain, and use, and that meet all government-mandated security standards. CertifiedMail solutions are built on standard platforms, integrate with all major commercial email systems, and use commonly-implemented security standards. A common code base ensures scalability and portability; through its hosted and in-house solutions, CertifiedMail is involved in the lives of seven million customers and supports monthly outbound messaging requirements that can reach into the millions.



# Table of Contents

|  |           |
|--|-----------|
| <b>EXECUTIVE SUMMARY</b>                                   | <b>2</b>  |
| <b>TABLE OF CONTENTS</b>                                   | <b>3</b>  |
| <b>INTRODUCTION</b>  | <b>4</b>  |
| <b>A SHORT HISTORY OF SECURE EMAIL</b>                     | <b>4</b>  |
| <b>ENTER CERTIFIEDMAIL</b>                                 | <b>5</b>  |
| <b>FOUNDATIONS</b>   | <b>5</b>  |
| <b>CERTIFIEDMAIL SOLUTIONS TO FIT MANY DIFFERENT NEEDS</b> | <b>6</b>  |
| <b>EASE OF IMPLEMENTATION AND MAINTENANCE</b>              | <b>7</b>  |
| <b>OUR CUSTOMERS ARE OUR BEST ADVOCATES</b>                | <b>8</b>  |
| <b>CORE FUNCTIONALITY OF CERTIFIEDMAIL</b>                 | <b>9</b>  |
| <b>THE CERTIFIEDMAIL DATA CENTER</b>                       | <b>11</b> |
| <b>TRY IT FOR YOURSELF</b>                                 | <b>11</b> |
| <b>ABOUT CERTIFIEDMAIL, INC</b>                            | <b>12</b> |

CertifiedMail.com, the CertifiedMail logo and Send Certified are trademarks or registered trademarks of CertifiedMail, Inc. Other product names may be trademarks or registered trademarks of their respective companies.

## Introduction

For a security solution to deliver, it must be easy to use for both end users and administrators. Since 1989, CertifiedMail has been creating commercial security products that follow this mandate, not the least of which were military-strength security solutions for the US Navy's nuclear submarine fleet. As a result, the company's state-of-the-art fourth-generation secure communication system, integrating secure email, large file transfer, content filtering and web plug-ins, not only deliver high levels of security but also set new standards for ease of use, interoperability and functionality.

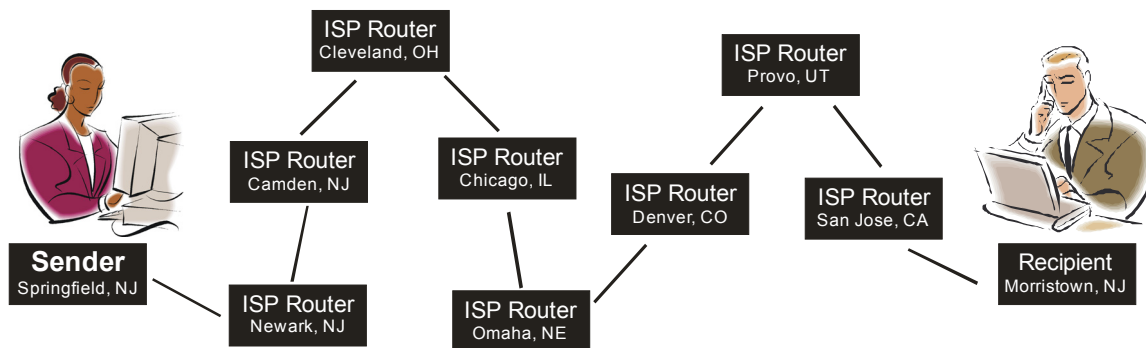
Secure email is now a requirement for most businesses because of government privacy mandates imposed by HIPAA (Health Information Portability and Accountability Act), Gramm-Leach-Bliley, Sarbanes-Oxley and various SEC regulations. Historically, secure email has been the province of technical users familiar with encryption, digital certificates, virtual private networks, and key algorithms. But as privacy requirements have spread to fundamental business tasks, non-technical users in HR and accounting, along with those in specialized fields such as healthcare, must secure many of their communications. The challenge for effective secure email is to ensure that these users can seamlessly send and receive secure messages without needing special knowledge or software, and without changing the way they already work.

CertifiedMail solutions are transparent to end users, and are designed to be easy to implement and manage. They are built on standard platforms, integrate with all major commercial email systems, use widely-accepted security standards, and meet all government-mandated security and privacy standards.

## A Short History of Secure Email

Secure email using Public Key Infrastructure (PKI) was defined by the Internet standards committee in October 1995 and is commonly referred to as S/MIME. To date, S/MIME has been integrated into most popular desktop email clients, but has not achieved significant market acceptance because of the high levels of complexity inherent in this approach. This complexity has also prevented S/MIME from being implemented at the email server level.

Figure 1 below shows just how many points of vulnerability can exist between an email's departure from the sender's email outbox and its arrival in the recipient's inbox when regular transmission is used:



*Figure 1: With regular 'clear text' email transmission, a message might be accessed at any one of as many as 25 different unsecured ISPs in the course of a seven-mile journey from Springfield, New Jersey to Morristown, New Jersey*



To be a cost-effective, viable alternative to courier services for confidential information distribution, an electronic communication solution should offer most, if not all, of the following attributes:

- No significant IT administrative overhead
- Scalable for use with large numbers of senders and recipients.
- As ubiquitous as the most common Internet technology
- No effective limit on document size
- No pre-established coordination requirements between the sender and recipients
- No special software required for sender or recipient.
- No user training requirements
- Integration with internal and trusted partner email systems
- Message tracking and status reports

## **Enter CertifiedMail**

The CertifiedMail approach was developed with all of these needs – as well as the full range of regulatory requirements issued by federal and state legislation over the past several years – in mind.

According to Bob Janacek, executive vice president and chief technical officer for CertifiedMail, “Over the past almost twenty years of developing commercial security software, if we’ve learned one significant lesson, it’s this: Besides offering the highest levels of protection available, if a security product is not easy to use and administer, it will be abandoned by end users. By applying these lessons every day, we have achieved a loyal customer following with many long-term relationships.”

## ***Foundations***

CertifiedMail solutions are built on a common code base, using widely-implemented standards. Because corporations operate on mixed IT platforms, using a standardized approach enables CertifiedMail solutions to easily interoperate with existing IT environments, allowing for virtually any integration possibility.

CertifiedMail leverages the flexibility of Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP), alongside the CryptoAPI built into Windows Server for message encryption and proof that messages are original. In addition, CertifiedMail leverages several built-in RSA algorithms to protect sensitive data. Use of the .NET platform also brings two key benefits to end users – universal access and 24x7 availability. The system must be everywhere the customer needs it to be, whether it’s inside a desktop application or embedded in a financial statement, and they don’t want to have to authenticate or put their password in many different places.

As a result, CertifiedMail enables secure, trackable messaging between any Internet users with access to an email client and a web browser. Senders create messages from a secure website running the CertifiedMail software, or by clicking a “Send Certified” button in their email client. Once a message has been received by the CertifiedMail secure server, a “message waiting” email is automatically sent to the recipient. This email contains an embedded SSL web link that brings the recipient back to the CertifiedMail secure website to pickup their message(s). RSA and PKI technologies are used behind-the-scenes in this process to protect data in transit and at rest.



Figure 2 below shows how CertifiedMail messages retain their integrity throughout the transmission from the sender's outbox to the recipient's inbox:

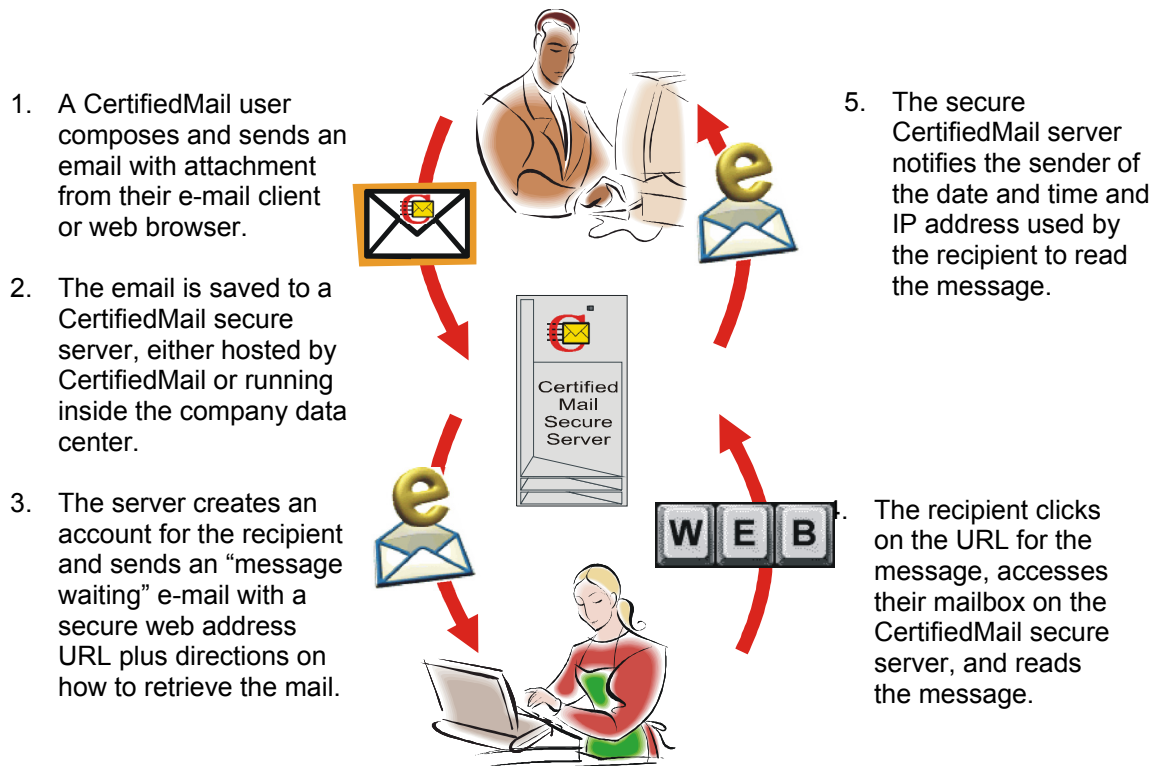


Figure 2: Secure email transmission using internal or external CertifiedMail secure servers.

Business partners, agents and privileged remote users can thus directly communicate via a secure CertifiedMail server using their existing email servers and clients. For partners running their own mail servers, an encrypted pipe can be established between their server and a secure CertifiedMail server without additional hardware or software. This technique uses the SMTP routing and TLS encryption that is integrated into the mail servers. For remote email users, CertifiedMail also supports secure SMTP and POP3 connections, once again without requiring additional hardware or software for end users.

## **CertifiedMail Solutions to Fit Many Different Needs**

The CertifiedMail system is provided as a hosted service with customers ranging from SOHO to large enterprises; a CertifiedMail Appliance for installation in small and mid-sized firms; and a CertifiedMail Server for enterprise person-to-person and automated application-to-person use. Every CertifiedMail Appliance and CertifiedMail Server must have a licensed SSL certificate installed in order to achieve secure communications.

The use of a common code base ensures that improvements made to any particular implementation easily become available and supported for other implementations if appropriate.

Other options include:

- "Send Certified" email client add-in
- CertifiedMail Compliance Manager for content inspection and regulatory enforcement
- "Secure Contact Us" for integration with web forms
- CertifiedMail Automation Engine



- CertifiedMail Large File Transfer
- CertifiedMail Director (gateway content filter and secure business partner communication)

Further details of individual products may be found on the web at [www.re-soft.com/encrypt](http://www.re-soft.com/encrypt).

## Ease of Implementation and Maintenance

The process of creating and transmitting a secure email message within a medical systems environment is illustrated in the schematic below:

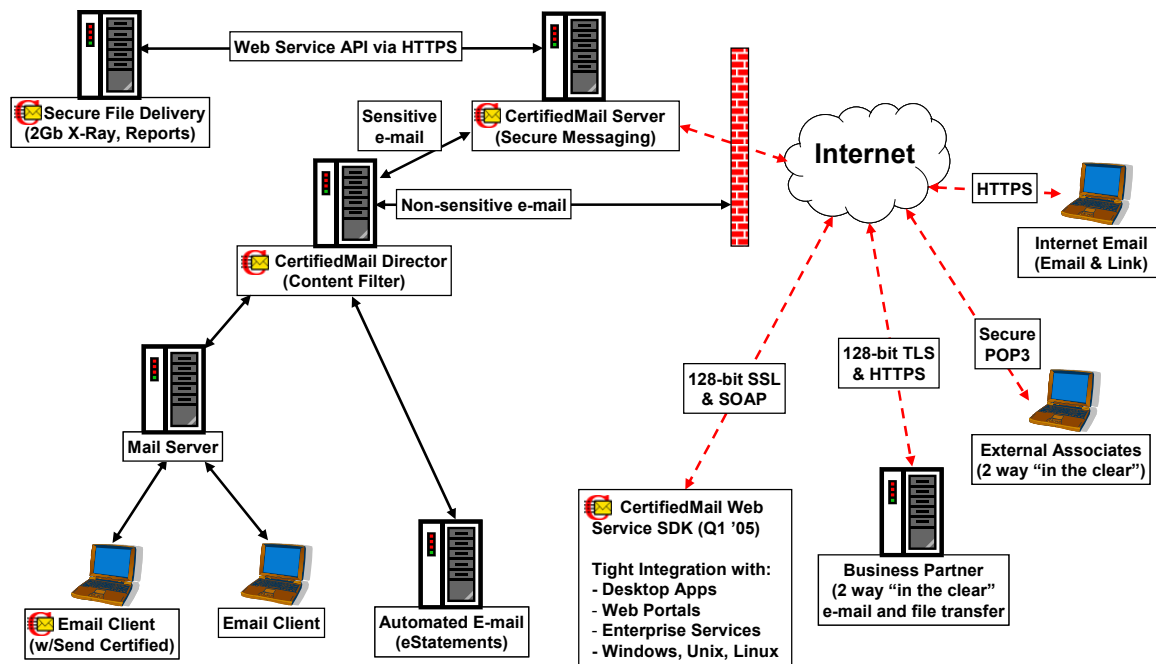


Figure 3: Mapping the CertifiedMail secure email universe

- An email notice is sent to the recipient with an embedded secure web link.
- First-time recipients type in their email address, via a secure SSL connection. Single Sign-On (SSO) Integration is also available.
- The first-time recipient creates a password, verifies it, and views their message – all via a secure SSL connection.
- Previously-registered recipients simply login via a secure SSL connection.
- Recipients can view and securely reply to their message via an encrypted SSL web browser connection.
- When their message is opened, the sender receives a receipt containing the date and time when their message was opened.
- A CertifiedMail message sent to an employee can be automatically decrypted, tagged and securely forwarded through their internal mail server to their email Inbox .

From an IT administrator's perspective, a single CertifiedMail message addressed to many employees automatically creates an account for each employee. At the click of a button, individuals, groups or the entire organization can be configured to begin sending CertifiedMail messages.



## Our Customers Are Our Best Advocates

“The CertifiedMail solution is very flexible and it easily adapts to any changes we make in our UNIX environment,” says James Cassata, Web Services Manager at Fiduciary Trust. “Using CertifiedMail and Windows 2000 we are getting excellent performance, top-level security and great functionality at a low cost. The CertifiedMail solution requires very little maintenance and people can quickly learn how to maintain the environment. Another advantage is the ability to cluster the servers using Microsoft’s clustering technology. As far as adding boxes to the environment, it’s very seamless. The CertifiedMail solution has been very good at installation and continued operation.”

Stephen Tall, Fiduciary Executive Vice President and Chief Technology Officer, recognizes the advantage of developing on one platform. “We are seeking to consolidate on one common platform, which is Windows 2000. From the desktop to the server, Windows 2000 provides a very widely available standard that simplifies our management and allowing us to spend more time adding value for our clients and less time managing a variety of standards. In addition, we can enhance our client usability features using the CertifiedMail Server solution.”

“A core part of our business is the transmission of confidential medical information and PHI. HIPAA, GLB, and other regulations require we make every effort to protect the privacy of our customers’ confidential information”, says Kerwin Smith, Director of Infrastructure at Examination Management Services Inc, a leading provider of medical information, risk management and investigation services to the insurance, legal, clinical and business communities.

“The flexibility provided by the combination of CertifiedMail’s outsourced secure email service, their in-house content filtering solution and the seamless integration between the two components convinced us that the company had the right solution for us. With CertifiedMail, we can control to the username and domain level which emails are encrypted. The hosted implementation means the benefits were available immediately – we were up and running with the first twenty users in just two hours. Our customers don’t have to install any special software or hardware at their end, and we don’t have to maintain production software.”

CertifiedMail customers receive a tremendous return on investment when they replace traditional hard-copy mail operations with CertifiedMail email messages. Costs for preparation, printing, labor and postal delivery can range from \$1.50 to \$10 per item, depending on the degree of automation; secure messages sent via CertifiedMail cost less than \$.10 per item. CertifiedMail can manage 2 million secure messages per day on less than \$100,000 worth of hardware using Windows 2000/2003 server load balancing and clustering.

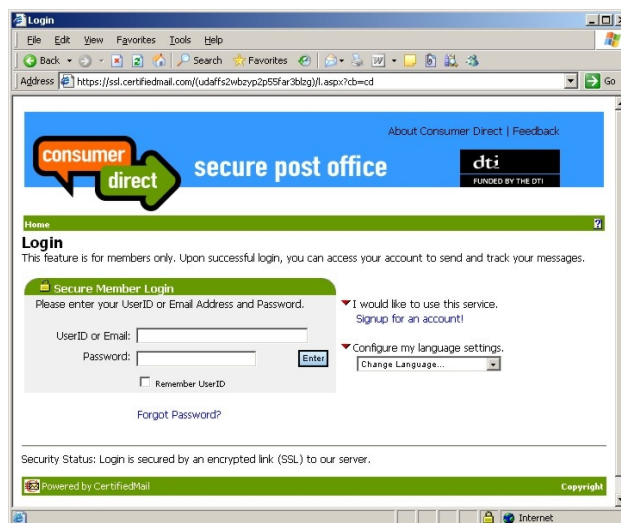
## Core Functionality of CertifiedMail

CertifiedMail combines secure email, secure large file transfer (up to 2 gigabytes), secure web forms, and secure website communications capabilities in a seamlessly integrated suite of interoperable solutions, enabling person to person, application to person, and application to application communications.

CertifiedMail has been described as a “Swiss Army Knife” of inputs and outputs:

- Internal users get integration with outbound SMTP messages, an https portal interface with transparent single sign-on option, and drag-and-drop secure large file transfer
- External users get an https portal interface for peer-to-peer messaging, mass automated communications (such as statement distribution), and large file transfer capabilities; secure POP3 for email client integration; secure TLS for two-way encrypted transmission of standard messages; and background retrieval and storage of large files

The server application and hosted service offer users a custom inbox, outbox with track sent and retract message capability, message tracking by recipient or by attachment, automated decryption, automated integrity checking, and the ability to create and send messages with a range of attributes such as forwarding prevention.



The “Send Certified” button integration is available for Microsoft Outlook/Outlook Express, Lotus Notes, and Novell GroupWise mail applications for user-selectable secure messaging:

The 200K download installs without user intervention, and also supports multi-user environments such as Citrix. It is available in encrypting and non-encrypting versions; the non-encrypting version enables compatibility with email anti-virus and archiving systems, and the encrypting version prevents plain text messages from being stored on the internal mail server.

Messages sent using the Send Certified system are assigned a user-applied mark to indicate secure delivery with corresponding content filter rule – for example, users may be instructed to add an asterisk at the beginning of a message subject to send it securely, or set the Importance level to High.

CertifiedMail also offers policy-based secure messaging, either through direct integration with the CertifiedMail Director content filter or through third-party content filters.



For internal users, this provides the ability to:

- Send messages from their existing email client (no training required)
- Optionally receive incoming secure messages and replies in plain text format, since the organization's CertifiedMail system is behind their firewall
- Selectively receive inbound secure messages as an "email waiting" notice with embedded SSL URL
- Use an intranet-based single sign-on for transparent integration with existing network login
- Use an extranet-based single sign-on when traveling to ensure continuing access to secure email
- Optionally send messages from a secure web portal interface

Standard external users with no special privileges can:

- Receive email waiting notices and embedded https URL
- Retrieve messages through a secure portal interface using their web browser without the need for any special software, certificates, or plug-ins.

Business partners may be allocated special privileges as part of the CertifiedMail system:

- Receive and send secure messages via SMTP TLS with the CertifiedMail user organization
  - TLS built into all commercial SMTP servers
  - Unlike S/MIME gateway solutions, there's no need for any additional gateway software (just an X.509 certificate) or infrastructure changes
  - Highly secure, automatic RSA public/private key encryption (same SSL encryption used for browser-based online banking)
- Download large file transfers from same webmail portal interface
- For more frequent large file transfers (e.g. daily consolidation reports), a background Windows Service is available that will automatically poll and pull down large files over an encrypted SSL session, and save them to a local directory for further processing



## The CertifiedMail Data Center

The CertifiedMail Secure Data Center resides in the \$100+ million NAC.Net complex, one of the largest and most prestigious data centers in the Eastern United States. This data center allows both the CertifiedMail Hosted Service and Dedicated Customer Systems to meet industry-mandated compliance, security and fault tolerance requirements.



### Security

- Data center is staffed 24 x 7 x 365
- Diesel generator UPS, Liebert environmental units, FM200 automatic fire suppression
- Biometric identification and PIN required for data center access
- Data center access strictly limited to pre-approved individuals
- CCTV surveillance cameras
- Multi-layered best practices security architecture
- On-site and remote system monitoring
- Local and off site automatic data backups
- All stored data is compressed and then protected using strong encryption
- All passwords are stored as a one-way hash and cannot be reverse engineered

### Performance

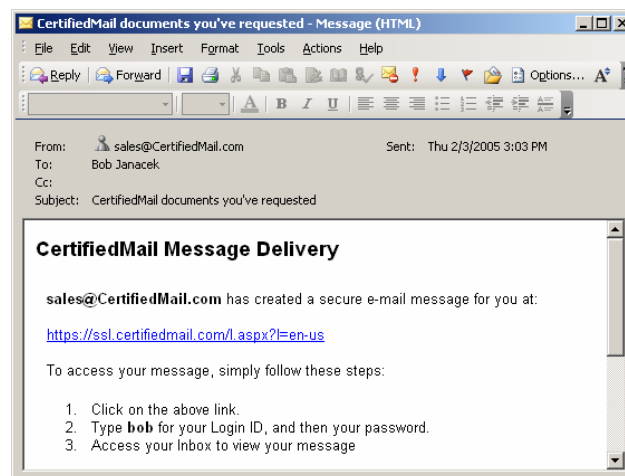
- Full mesh of OC3 (155 Megabit) and OC12 (622 Megabit) links
- Redundant infrastructure using Lucent and Cisco hardware
- Connected to Internet backbones at redundant data centers (see Appendix)
- Linked directly to major Internet networks including UUNET, AOL, Genuity, and others
- Scalable multi-tier architecture with load balancing and clustering capabilities
- Porting currently underway to a state-of-the-art 64-bit architecture, allowing expansion to terabytes of main memory and unlimited directly addressable storage

Call 1-800-672-7233 to request a more detailed technical paper on the CertifiedMail Data Center.

## Try It for Yourself

The simplest way to see how easy it would be to start securing your email with CertifiedMail is to try it for yourself. Visit the CertifiedMail website at <http://www.re-soft.com/encrypt> and select one or more data sheets, case studies or white papers. Enter your email address, and voila! A message will arrive in your inbox with an embedded SSL URL link to a message box at the CertifiedMail Data Center.

Or, give us a call at 1-800-672-7233, and we'll set you up with a 30-day trial account for the hosted service. No strings attached.





## About CertifiedMail, Inc

CertifiedMail is an established software infrastructure provider for secure messaging and file transfer leveraging existing email and Internet systems. Our standards-based, fourth generation software has been developed in-house in the United States for our own needs as well as for our customers' needs since 1995. We run the same code that we shrink-wrap for corporations, code that scales from a single server to enterprise cluster.

Founded by experts in data security, each with more than a decade of information security experience, CertifiedMail overcomes the inherent insecurity of the Internet as a transport mechanism for confidential data by enabling organizations to send and track sensitive information over the Internet using regular email. CertifiedMail solutions support HIPAA compliance for healthcare organizations such as Sutter Health, Covenant Health, and Rite Aid Corporation. Sovereign Bank, Sacramento Bank, Conseco Finance (now Green Tree), and other financial institutions use CertifiedMail as an integral part of their SEC, Sarbanes Oxley, or Gramm-Leach-Bliley Act compliance solutions. Law firms take advantage of its secure, trackable messaging to deliver sensitive intellectual property information and protect client confidentiality. Whatever the industry, CertifiedMail solutions save significant time and cost while greatly increasing the privacy and accountability of communications. For more information, visit [www.re-soft.com](http://www.re-soft.com).