WatchGuard

Email Encryption

When Data Loss Prevention Is Not Enough:

Secure Business Communications with Email Encryption

Technical Brief

WatchGuard® Technologies, Inc.

Need for Email Encryption Is at Its Peak

Based on the growing volumes of confidential and sensitive information traversing networks on a daily basis, regulatory bodies and business executives have turned their concerns to ensuring messaging is protected from unauthorized viewing. Regulations such as Sarbanes-Oxley (SOX), PCI, HIPAA, GLBA and others have been introduced to mandate that email messages containing sensitive or confidential data are handled securely.

Email encryption has emerged as a vital aspect of an overall email security solution to secure confidential data and yet continue to allow the free flow of communications between colleagues, customers, and partners.

The Solution: Seamless Email Encryption from WatchGuard®

WatchGuard XCS SecureMail Email Encryption (XCS SecureMail) technology, powered by Voltage, provides easy-to-use, business-class encryption to enable organizations to securely transmit and receive private and sensitive data. This encryption solution, available as an add-on subscription for all WatchGuard XCS appliances, provides transparent, policy-driven email encryption, supporting the encryption of large messages up to 100 MB.

The transparent nature of XCS SecureMail adds to its ease of use. The WatchGuard XCS data loss prevention engine identifies outgoing messages that meet pre-defined policies for confidentiality and automatically encrypts messages with no special action required by the sender. Encrypted messages are sent as HTML attachments to ordinary email messages, and are directly delivered to the recipient who can decode and view the encrypted messages using any web browser, including those on mobile devices.

XCS SecureMail enables organizations to:

- **Secure Confidential Information.** Outgoing messages containing sensitive information are transparently encrypted, delivered to any mailbox, and are easy for recipients to decrypt and view.
- **Adhere to Privacy and Compliance Regulations.** Sensitive messages are handled in compliance with industry regulations including HIPAA, PCI, SOX, GLBA and others without any effort on the part of the sender.

XCS SecureMail Email Encryption Architecture

XCS SecureMail delivers an easy-to-use secure envelope solution which can be implemented for employees, customers, vendors, and other business partners. As shown in Figure 1, XCS SecureMail Email Encryption is an instant-on feature of the WatchGuard XCS.
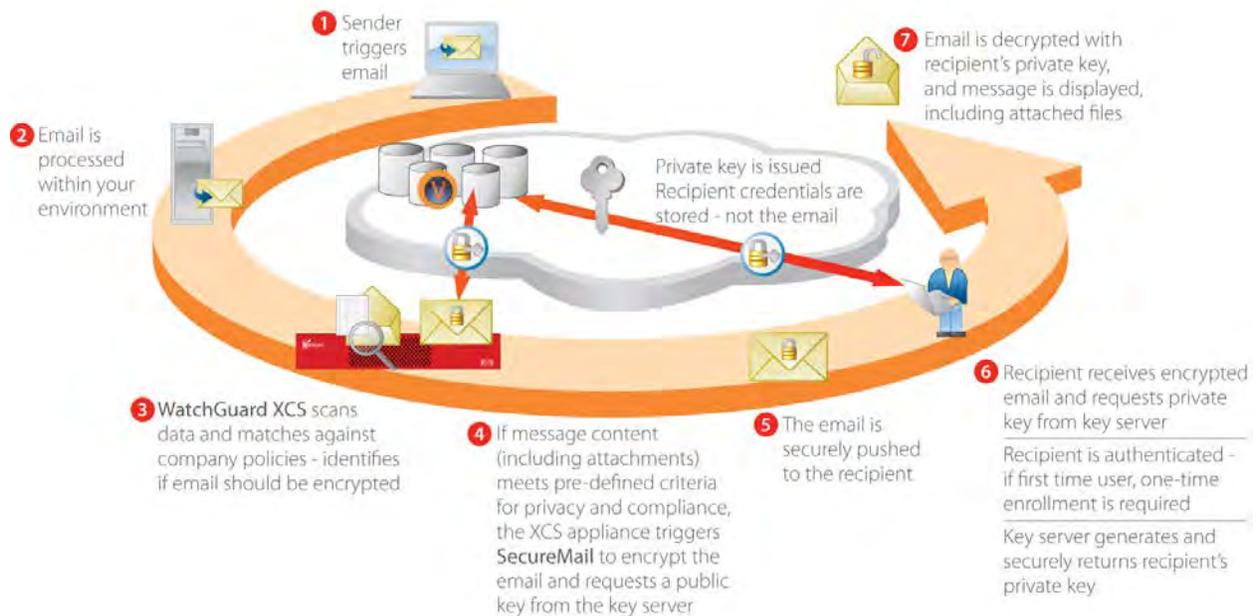
Figure 1. Instant-On Encryption

How XCS SecureMail Encryption Works:

1. A sender from within the organization triggers an email.

2. The email is processed within the organization's email environment and the email is routed to the WatchGuard XCS appliance for scanning.

3. The email passes through the XCS data loss prevention engine's pattern and content filters, which scans the data and matches it against pre-defined company and regulatory policies. Each message is checked to determine if it needs to be encrypted, quarantined, bounced, or handled in other ways as established by the policies created up by the Administrator (see Figure 2).

4. If the message meets the requirements of a specific encryption policy, the XCS SecureMail engine communicates with the Voltage SecureMail Cloud to generate encryption keys, any branding data, and creates the notification message. XCS SecureMail uses Identity-Based Encryption (IBE) technology which generates encryption keys based on the sender and recipient email addresses. The message is signed with the sender's public key and is securely pushed by the WatchGuard XCS appliance to the intended recipient.

5. The recipient opens the attachment, and, if it is his or her first time receiving an encrypted email via XCS SecureMail, he or she completes a one-time registration and authenticates his or her email address.

6. Once the recipient has authenticated with the service, the private session key is issued based on the recipient's identity.

7. The entire email, including attachments, is decrypted and the recipient can now view the message securely.

Recipients of encrypted messages do not require special software or applications to open an encrypted email. Encrypted messages can be opened with any browser running on any operating system or mobile device. The process is quite simple: recipients open an HTML email attachment, it authenticates using their identity, and they can view the secure message.

Next-Generation Identity-Based Encryption

XCS SecureMail Email Encryption is based on IBE technology, a unique approach that uses a simple identity – an email address – as the public key in a public/private key pair.

IBE came about because of the shortcomings of legacy encryption methods, which have prevented their widespread adoption. One of the main problems with other email encryption technologies is that senders and recipients must exchange certificates or keys before any communication can take place. This can be painful for users.

Figure 2. Discovery, Remediation and Inspection of Outgoing Messages

These other email encryption technologies also assume static relationships and authentication policies, which do not reflect contemporary business processes and dynamics. There are also administrative problems, such as key management, certificate lifecycle management (e.g., revocation and renewal), and ensuring availability, recoverability, and accessibility of keys. For example, keys need to be backed up and highly available. They also need to be revoked if the user is no longer with the organization. Simply put, these legacy technologies lack usability, they do not scale to support many users, and they are costly to manage.

IBE overcomes these issues. Senders can encrypt a message to a recipient simply by knowing that person's email address. IBE not only solves the usability problem, it solves the scalability and administration problems. Keys to encrypt and decrypt are generated dynamically when they are needed. This means you don't need a key database or escrow system to store and archive keys. And because keys are issued on-the-fly, there is no risk of losing data in email due to lost or corrupted keys.

IBE uses any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the mapping of identities to decryption keys. Using IBE radically simplifies key management because the sender does not need to contact the key server to get an encryption key. Instead, the encryption key is mathematically derived from the receiver's identity. The receiver must only contact the key server once to authenticate and get the required decryption key. The key server is able to construct the receiver's decryption key

mathematically, eliminating the need for a database at the key server and making key recovery extremely straightforward.

Because keys are generated on-the-fly and are never stored, IBE provides greater ease of implementation and management over traditional public key cryptography technologies and enables message encryption at the gateway without the complexity of certificates, Certificate Revocation Lists or other infrastructure requirements.

And because IBE has solved all of the key management complexities, it also means the technology can easily scale to any number of users.

Benefits of XCS SecureMail Email Encryption

The technical innovations of the IBE technology featured within the WatchGuard XCS SecureMail Email Encryption subscription translate into many tangible benefits for organizations seeking to secure their most critical business communications. When compared to other email encryption technologies such as symmetric key management and PKI (see table below), XCS SecureMail offers significantly more benefits at a lower total cost of ownership.

REQUIREMENT	SYMMETRIC KEY MANAGEMENT	PKI	WATCHGUARD XCS SECUREMAIL (IBE)
ENCRYPT	Yes, but online connection required	Often no, when no recipient certificate is available	Yes, to anyone including groups
DECRYPT	Yes, but online connection required	Yes	Yes, without pre-enrollment required
INTEGRATION WITH INFRASTRUCTURE	Yes, but requires a per-decryption lookup	Not without complex key escrow and sharing	Yes, no per message lookup or key escrow required
KEY RECOVERY	Must maintain a key database	Must maintain a key database	Yes, no database required
SCALABILITY	Limited by per-transaction key server operations	Limited by operational complexity	Yes, messages and keys are never stored, and keys are generated on-demand

Filters and Lexicons for Compliance & Policy Management

XCS SecureMail draws on the capabilities of the WatchGuard XCS compliance and policy dictionaries or custom dictionaries created by the administrator, as well as policies that search the subject headers and body text of email messages and attachments, assisting organizations to comply with industry regulations including:

- HIPAA (Health Insurance Portability and Accountability Act)
- GLBA (Graham-Leach-Bliley Act)

- SOX (Sarbanes-Oxley Act)
- European Privacy Initiative
- NASD 3010
- USA PATRIOT Act
- SEC Rule 17

WatchGuard's pre-defined compliance and privacy lexicons, which include terms, phrases, and alpha-numeric listings related to financial, health, and other private information, assist enterprises to be compliant with industry regulations and alleviate the burdens and time required to set manual policies to identify sensitive information.

Transparent, Policy-Based Encryption

Because the XCS SecureMail technology is tightly integrated into the WatchGuard XCS appliances, content control and secure messaging policies are managed and enforced centrally from a single location, without the need for a dedicated, costly management appliance.

Centralized, Granular Control of Encryption Policies

Message encryption policies can be extremely granular and, once defined, applied automatically at the gateway. This ensures encryption and email privacy is handled consistently, and eliminates the risk of user error by removing the need for senders to make decisions as to whether or not to secure an email and its content.

When encryption is enabled, you can use XCS policy and content filtering features to scan for specific patterns in email messages that indicate the message must be encrypted, including:

- Pattern Filters
- Objectionable Content Filters
- Content Scanning
- Content Rules
- Document Fingerprinting

For example, you can create a Pattern Filter to search for the word "[Encrypt]" in the subject field of a message. An end user can add this phrase to their message subject header to indicate the message must be encrypted before it is delivered.

Policies can be set to encrypt messages based on header, subject line, sender, recipient, content, attachments, and many other attributes of an email message, including:

Header or Subject Line: Emails can be set to be encrypted based on keywords within the header or subject line.

Sender or Recipient: Encrypt messages based on destination (e.g. auditors, Board of Directors, a specific business partner or supplier) or sender. For example, a policy can be set that defines that

any emails from John Smith, the CFO of an organization, to the company's auditor, Jane Doe at auditfirm.com are sent encrypted.

User, Group, or Domain: Messages can be encrypted based on user, group, or domain, providing secure, enhanced flexibility of data-in-motion privacy without hindering the flow of data. For example, all emails sent out of the organization by the HR department can be set to be encrypted.

Email Body: Searches for text in an outgoing message that identifies it as a message to be encrypted.

Private Data and Objectionable Content: Searches from a pre-defined dictionary of words that is checked against a message to determine if the message should be encrypted. For example, you may require that any outgoing messages that contain certain confidential information, for example, credit card information or medical records, must be encrypted.

Keywords and Regular Expressions: Keywords and regular expressions found in the subject line or content of messages as defined within WatchGuard XCS content control policies.

Attachment Type: Messages can also be encrypted based on other message attributes such as attachment type. For example, you can set encryption to be triggered on all .xls or .csv documents.

Attachment Content: WatchGuard XCS has the ability to scan content of over 150 file types for keywords, phrases, or patterns which, upon detection of policy-based content can then trigger the email for encryption without user intervention.

The SEAMLESS User Experience

WatchGuard XCS SecureMail Email Encryption has been specifically designed with ease-of-use so that employees, customers and other business partners can immediately appreciate the benefits associated with encrypted email communications.

Sending Encrypted Email

Transparent Encryption

XCS SecureMail is transparent to employees. When sending an encrypted email, the user simply composes and sends the email as he would at any other time. As shown in Figure 3, the content of the outgoing email is then automatically scanned and, if deemed to contain sensitive material as pre-defined by your organization's policies, it is automatically encrypted.
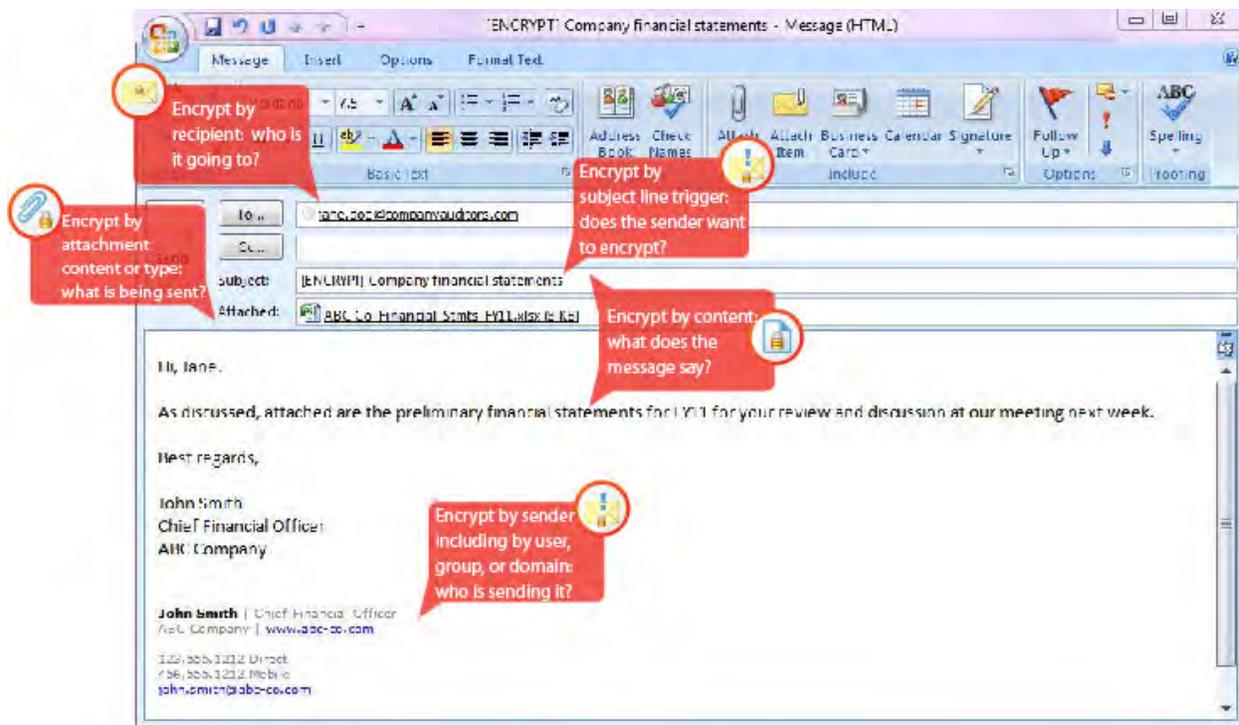
Figure 3. Transparent encryption based on pre-defined organizational policies

Manual Encryption

XCS SecureMail also allows a sender to clearly flag a message for encryption by adding the trigger [ENCRYPT], for example, in the subject line. This is then automatically identified by the system filter and the message is encrypted before being sent.

Secure Replies and Forwards

Once an encrypted message is received and opened by the recipient, reply, reply all, or forward actions of the encrypted email are also encrypted for ongoing secure communication of the encrypted message once it is sent.

Encrypt Large Messages Up to 100 MB

WatchGuard XCS SecureMail Email Encryption provides the ability to support the encryption of large messages spanning in size upwards of 20 MB and up to 100 MB.

Simple Mobile Device Decryption Experience

XCS SecureMail provides a simple mobile device decryption experience for iOS, Android, and BlackBerry users. A reader application is available for download for seamless decryption of encrypted messages. The message can be decrypted simply by choosing to use the Voltage app to open the attachment in the envelope. Any replies or forwards are also encrypted to ensure secure communications. The application is available at no additional cost and can be downloaded using links in the secure message envelope received by the recipient with the encrypted message. For all other mobile devices, the recipient simply clicks on the "Other Mobile Users" link in the notification message, and the message is forwarded to the SecureMail cloud. The message is then routed to the ZDM proxy mail store, and the recipient receives a

new message with an email link to the secure message. The message is temporarily stored and then deleted.

Receiving Encrypted Email

As mentioned previously, no special software is required to receive and read encrypted messages with XCS SecureMail Email Encryption. Recipients can open encrypted messages with any desktop email program or any web browser running on any operating system.

When receiving an encrypted email using XCS SecureMail, the recipient receives a notification message which arrives in his or her email inbox. The notification envelope can be fully customizable with the sending organization's logo and branding with the purchase of an XCS SecureMail Branding subscription.

On opening the email, the recipient receives the following notification of receipt of an encrypted message from WatchGuard XCS SecureMail:
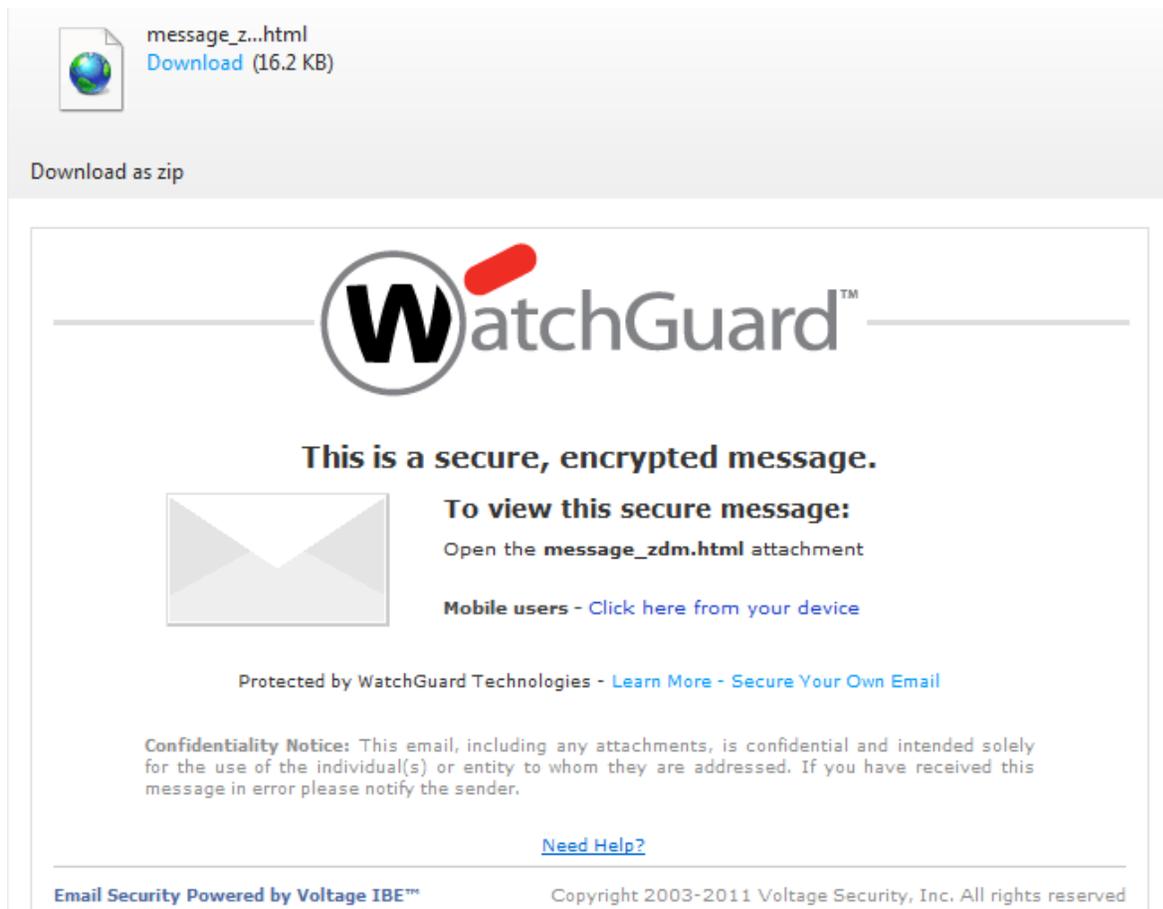
Figure 4. Recipient notification of encrypted message

The recipient then simply clicks on the message_zdm.html attachment and clicks on the "Read Message" button shown in Figure 5.
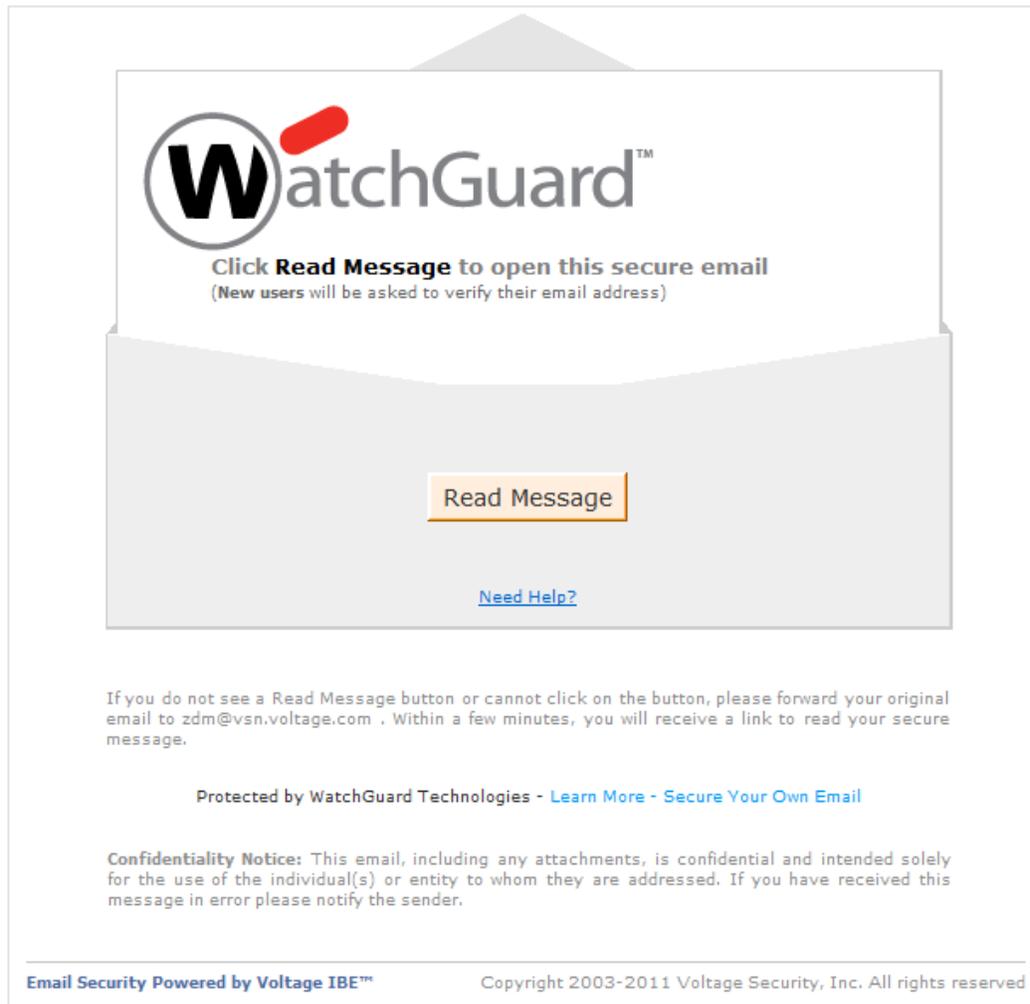

Figure 5. Read Message screen to open a SecureMail encrypted message

Those receiving encrypted emails for the first time are not required to set up an account in advance of using the system. Rather, they are directed to a screen, as shown in Figure 6, to create an account on the SecureMail site. The need for first-time user registration is automatically detected when no account exists for the recipient's email address. Once a recipient has set up an account on SecureMail, they can receive secure messages from any number of senders using SecureMail email encryption using the same login credentials.
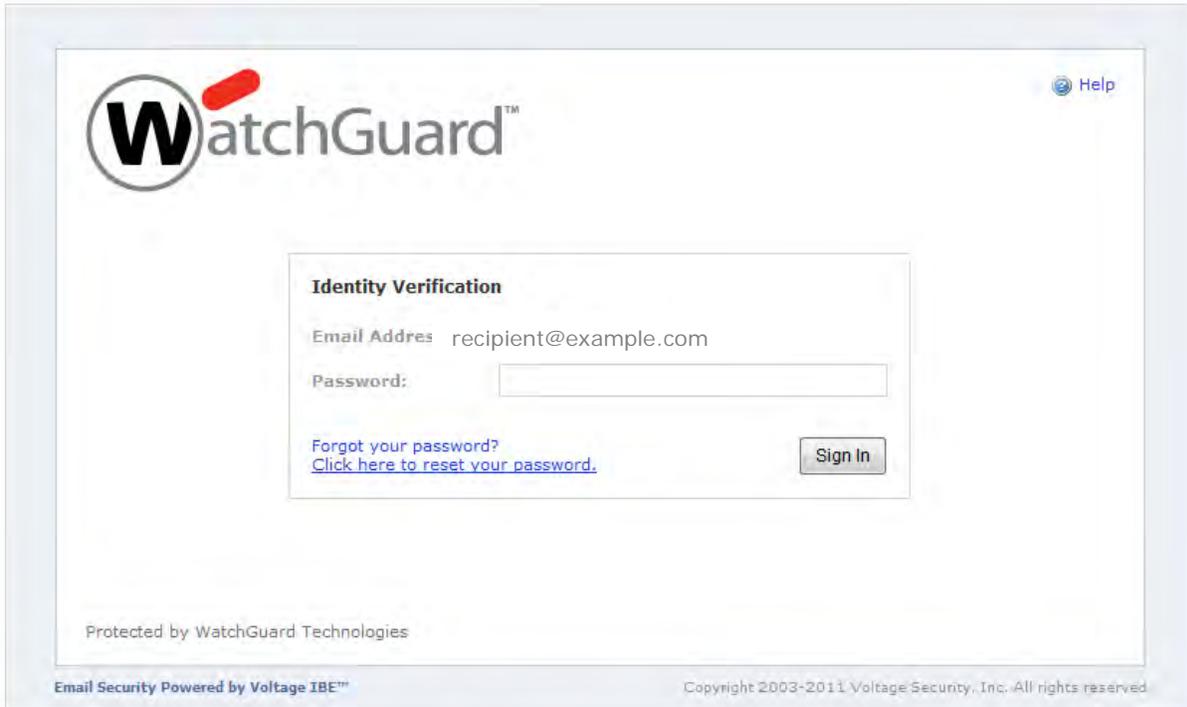
Figure 6. First-time recipient registration

Once recipients have created their passwords, a verification message is sent to the recipient's inbox for them to verify their account and finalize the one-time registration process, as shown in Figure 7.
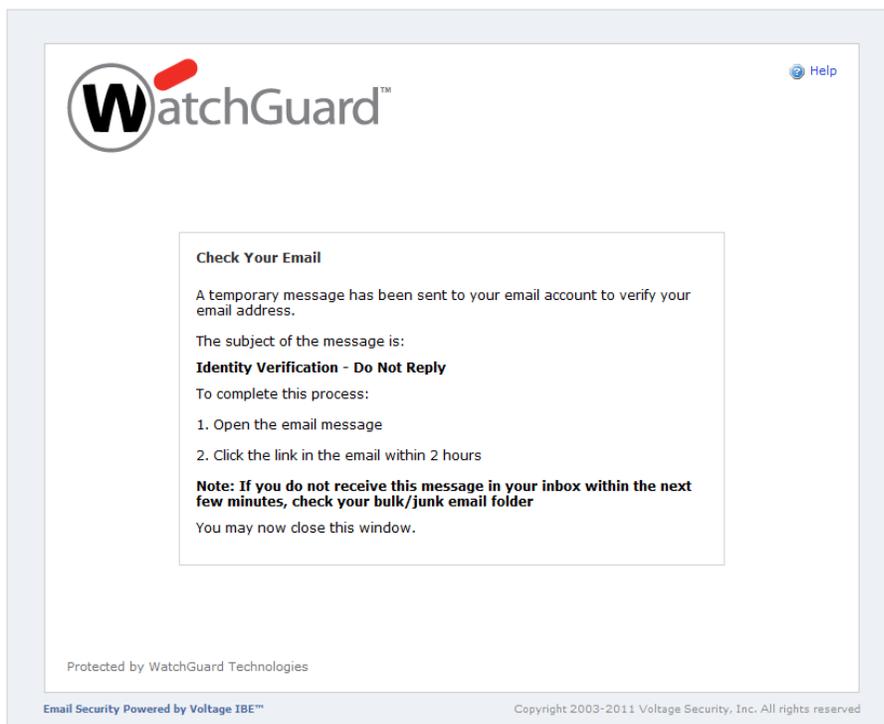

Figure 7. Verification Screen upon Completing One-Time Registration

If the recipient has already registered with XCS SecureMail, he would simply authenticate his ID as shown in Figure 8.
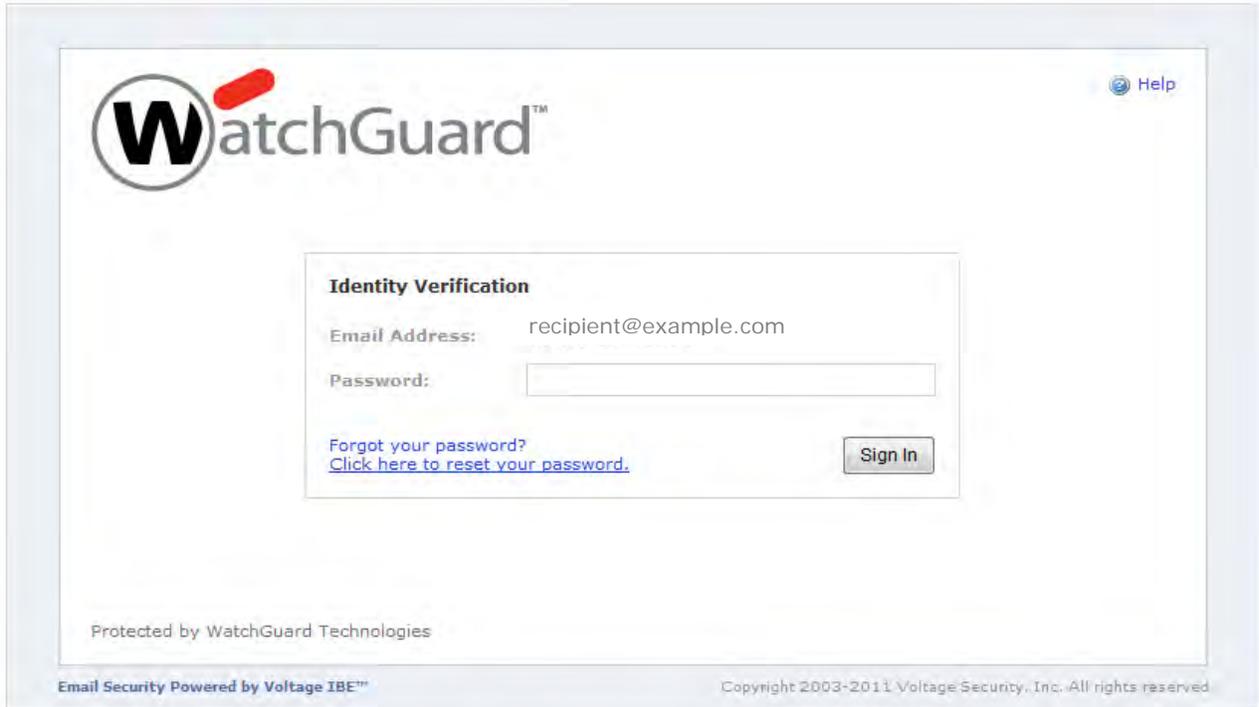

Figure 8. Identity verification for on-going authentication when receiving SecureMail messages

Once this initial registration or authentication process is complete, the recipient can view the decrypted message, which is automatically displayed in the browser window, as shown below in Figure 9.

Figure 9. Decrypted message displayed in browser

When access to the decrypted message is obtained, the recipient has the ability to securely Reply, Reply All, and Forward, without requiring any special software. Once a recipient clicks on any of these actions within the encrypted email, a "Send Secure" screen, as shown in Figure 10 below, will appear and provide the recipient with the ability to continue the email communication securely. This ensures that the entire email conversation is secured from the moment it is triggered and throughout its communication trail.

Figure 10. Secure reply, reply all, and forward of encrypted messages

The Message Decoding Process

Messages are encrypted using 1024-bit RSA-equivalent (highly secure) industry standards. The HTML attachment in the notification eliminates the need to install special software, ensures the highest delivery rate, and enables the solution to have universal reach with high usability. For example, other cloud-based services that rely on JavaScript, which is not always available and is often stripped out at the receiving gateway or disabled in the recipient's browser, resulting in higher delivery failure rates, user frustration and higher help desk costs to increased number of support calls.

Conclusion

No other solution on the market provides greater flexibility and ease-of-use. With its transparent application and universal reach, messages encrypted with WatchGuard XCS SecureMail Email Encryption can be sent to any email inbox without cumbersome and costly administration or infrastructure

requirements, or needing on the part of the recipient to install client software. Thus, confidential communication with business partners and customers is simplified and scalable.

XCS SecureMail provides maximum security to organizations with its transparent encryption capabilities using custom or pre-defined policies, data loss prevention, and compliance dictionaries. Also, since messages are never stored on the same server as their keys, XCS SecureMail ensures that only those with permission to view the encrypted message have access to its content.

It has never been easier to deploy encryption as part of an overall email security solution. WatchGuard XCS SecureMail Email Encryption provides the necessary infrastructure so that all you have to do is enable it on the WatchGuard XCS, set data loss prevention policies and compliance rules, and your outgoing emails and data will be protected from unintended viewers.

Next Steps

For more information on the powerful WatchGuard XCS family of extensible content security products with next-generation email encryption capabilities, visit www.watchguard.com/xcs.

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.