IronPort PXE Encryption Technology: Safeguarding Business Email

WHITE PAPER

TABLE OF CONTENTS

Executive Summary

Using encryption to secure message content and provide unprecedented visibility and control over email.

The more that businesses rely on email, the more critical it becomes to protect confidential email messages from unauthorized eyes. IronPort PXE™ encryption technology combines robust encryption with ease of use to ensure that vital business information is properly secured, yet continues to flow freely between senders and recipients.

IronPort PXE encryption technology has been rigorously designed to protect the integrity of messages identified as confidential. It integrates easily into existing enterprise mail systems.

Just as important, IronPort PXE is convenient for users. The advanced content filters of IronPort C-Series™ email security appliances identify outgoing messages that meet defined policies for confidentiality, and hand those messages to the IronPort PXE engine for encryption. No special action is required by the sender to protect sensitive information. Encrypted messages are sent as HTML attachments to ordinary email messages, delivered directly to recipients' inboxes. Recipients can decode and view the encrypted messages using any Web browser.

Detailed delivery and response tracking and comprehensive message activity reporting enable users and administrators to view the status of individual messages, and to monitor the effectiveness of corporate confidentiality policies.

INTRODUCTION

Email has become a prevalent medium for business communications, and its popularity continues to grow. Every day, sensitive information is shared with business partners and customers via email.

Although email is critical to the rapid pace of business today, the general lack of message security is a source of concern, both for regulators and business executives. Regulations such as Sarbanes-Oxley and HIPAA require that email messages containing sensitive or confidential data must be handled securely. Additionally, executive correspondence and exchanges concerning personnel, legal and other confidential matters must be protected from unauthorized viewing.

Encryption is a vital aspect of an overall email security solution. Working with IronPort C-Series email security appliances, IronPort PXE encryption technology enables enterprises to:

- **Secure confidential communications.** IronPort PXE encryption is robust, versatile and easy-to-use. It encrypts messages transparently to senders, can deliver encrypted email to any mailbox, and makes it easy for recipients to decrypt and view their mail.
- **Guarantee compliance.** Sensitive messages are auditably handled in compliance with HIPAA, SOX, GLB and other industry regulations—without any effort on the part of the sender.
- **Enhance email visibility and control.** Features such as guaranteed read receipts, message locking and message expiration provide a truly business-class email solution.

THE IRONPORT PXE ARCHITECTURE

An email message can easily pass through a dozen waypoints and multiple companies, each with different policies and security settings, on its way from sender to recipient. It only takes one weak link (a worm, a hacker, an unsecured WiFi network, a dishonest employee) for a message to be intercepted. If that message contains confidential information, the public release of its contents could lead to embarrassment—or even financial consequences—for the company that sent it. Just as putting a letter in an envelope is more secure than writing the information on a postcard, encryption provides extra protection for the contents of email messages.

IronPort PXE encryption technology works with IronPort C-Series appliances and your own mail servers to deliver easy-to-use secure email for employees, customers, vendors and other business partners.

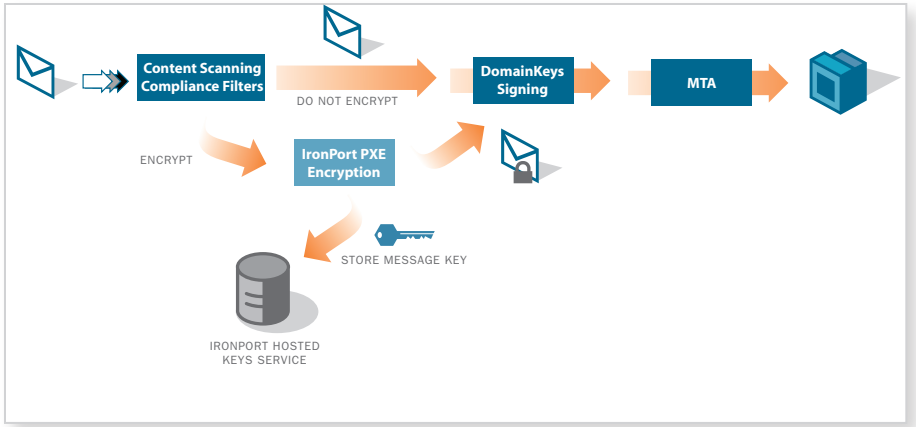

Figure 1: *Messages that fall under corporate confidentiality policies are automatically routed for encryption.*

As shown in Figure 1, IronPort PXE encryption technology is a simple add-on to the IronPort C-Series' mail flow. All email sent from the organization passes through the powerful and versatile IronPort content filters, which check for messages that need to be encrypted, quarantined, bounced, or handled in other special ways.

If the content of a message (or an attachment) matches any policy specified for encryption, that message is automatically processed by the IronPort PXE encryption engine. The key used to encrypt the message is stored by the IronPort Hosted Keys Service, while the message itself is queued for outbound delivery.

Messages sent using IronPort PXE technology can be opened with any email program and any Web browser running on any operating system. Recipients simply open an email attachment, enter a password and view the secure message.

Digital signing is a recommended option for use with messages encrypted by IronPort PXE. A digital signature authenticates the sender, allowing the recipient to open the message with confidence. Further, digital signing provides the receiving gateway with a mechanism to choose whether or not to pass encrypted messages, which cannot be properly scanned for viruses and spam. The gateway can then accept those from trustworthy domains while rejecting others. IronPort supports the DomainKeys Identified Mail (DKIM) standard for domain authentication.

IRONPORT

Note: *IronPort Hosted Keys Service provides a simple, economical solution for key management.*

IronPort Hosted Keys Service

Organizations wishing to implement IronPort PXE encryption technology solutions can do so with instant deployment and zero management costs. The IronPort Hosted Keys Service provides:

- Automated user enrollment and account creation
- User authentication and message key delivery
- Message tracking
- SecureReply capability for responding to encrypted messages

The key server never holds actual email messages; only encryption keys and management information. Therefore, it offers significant security benefits over solutions that store both messages and encryption keys on the same system.

Filters and Lexicons

IronPort Compliance Filters™ search the headers and bodies of both messages and attachments. These best-of-breed filters enable an organization to comply with regulations such as:

- Health Insurance Portability and Accountability Act (HIPAA)
- Graham-Leach-Bliley Act (GLB)
- Sarbanes-Oxley Act (SOX)
- European Privacy Initiative
- NASD 3010
- USA PATRIOT Act
- SEC Rule 17

By providing health and privacy lexicons, IronPort assists enterprises in establishing automated email compliance with HIPAA, GLB and other regulations. These libraries include terms, phrases and alphanumeric listings related to financial, health and other private information. IronPort's predefined lexicons minimize the burden of establishing the rule sets used to identify sensitive email.

Because of its extensive HIPAA lexicon and robust encryption capabilities, IronPort's secure messaging solution is the only one to have received the endorsement of the American Hospital Association (AHA).

Enhanced Visibility and Control

In addition to robust content filtering and encryption, IronPort PXE offers exceptional control over business email with:

- **Guaranteed read receipts.** Normally, senders wanting acknowledgment that an email message has arrived must depend on the recipient to initiate a reply, or at least to click on a receipt request. With IronPort PXE, because recipients have to retrieve a decryption key before they can read a message, the system knows when that has happened. This provides absolute proof that the recipient has actually opened the message. Similarly, IronPort technology can automatically notify a sender if email is not opened within a specified period of time, thereby alerting senders to follow up on important messages.
- **Message locking**. Senders can lock a message to prevent it from being viewed even after it has been delivered to the recipient's inbox. This feature can reduce the consequences of email that contains inaccurate or inappropriate content, that was sent out prematurely, or accidentally sent to the wrong recipient(s).
- **Message expiration.** Similarly, messages can be given an expiration date after which they cannot be opened. For example, retailers can use this feature to send limited-time product offers to customers. Messages can also be expired manually.

Note: *Wayward email can damage an organization's reputation.*

Email Embarrassments

- A public relations person at Sony Ericsson in London sent an earnings report to several internal personnel a day before its public release. Unfortunately, he misaddressed one of the recipients, inadvertently sending the message to a similarly named person at the Dow Jones news service office in Stockholm. The sender immediately realized the mistake, but had no way to prevent the Dow Jones employee from reading the message. Dow Jones published the release before Sony-Ericsson, causing a significant move in Ericsson stock.
- An employee of the Palm Beach (Florida) County Health Department emailed a routine update on HIV/AIDS statistics to other members of the department. He inadvertently attached a list containing the names and addresses of HIV/AIDS patients. The agency's IT staff shut down the email system for about an hour to remove all traces of the message, although some people had already viewed it.

IronPort PXE vs. Secure Webmail

IronPort PXE is not a Web-based secure email solution. In the IronPort architecture, a Web browser is used to authenticate users and display decrypted messages, but there is no Web server storing mail. This makes it is a more efficient, secure and cost-effective solution for secure email than Web-based systems because:

- The actual incoming messages—not just links—are delivered directly to users' mailboxes. There is no concern about confidential messages being kept on a remote system.

- Messages are never stored on the IronPort Hosted Keys Service server. The only time an encrypted message and its key are combined is on the recipient's computer. This is a more secure approach than storing both messages and decryption keys on the same server.
- There is no need to set up a new mail system. By leveraging existing mail servers, IronPort PXE avoids the deployment and administration costs of a secure webmail server—and the expense of expanding such a system to keep pace with increasing email usage.
- IronPort PXE does not require allowing inbound HTTPS access to enable webmail retrieval.

THE IRONPORT PXE USER EXPERIENCE

IronPort PXE encryption technology has been designed for the simplest possible use—so your employees, customers, vendors and other business partners will quickly appreciate the benefits of encrypted communications.

Sending Encrypted Email

The encryption process is transparent to your employees; they compose and send mail as usual. Material deemed sensitive by your organization's policies is automatically encrypted before it is relayed to the outbound mail server.

If they wish, senders can explicitly flag a message for encryption. This is typically done by adding a specific phrase to the subject line, which is then identified by an IronPort content filter.

Not all people wishing to send encrypted messages are within your organization. Increasingly, customers and prospects expect to be able to get product and service information on websites and through email. In some cases, they may wish to initiate confidential correspondence. IronPort PXE encryption technology offers a quick and easy way to generate secure email, without the expense and effort of solutions that require the destination organization to set up secure mailboxes before new users can send encrypted messages.

Once your organization has deployed IronPort PXE encryption technology, you can place links to it on your public website. When a website visitor selects your "Contact Us" (or similarly named) link and completes the simple registration process, IronPort PXE launches a browser-based message form. The remote user can then compose and send a message, which is encrypted and forwarded to the designated recipient.

Receiving Encrypted Email

No special software is needed to receive and read IronPort PXE messages. Recipients can use a desktop email application such as Microsoft Outlook, Lotus Notes, or Novell GroupWise—or a Web-based system such as AOL Mail, Yahoo! Mail, Gmail, or Hotmail.

An IronPort PXE-encrypted message arrives as a plain-text email with an HTML attachment. As shown in Figure 2, the plain text directs the recipient to open the HTML attachment. This notification message is fully customizable and supports both HTML and text.

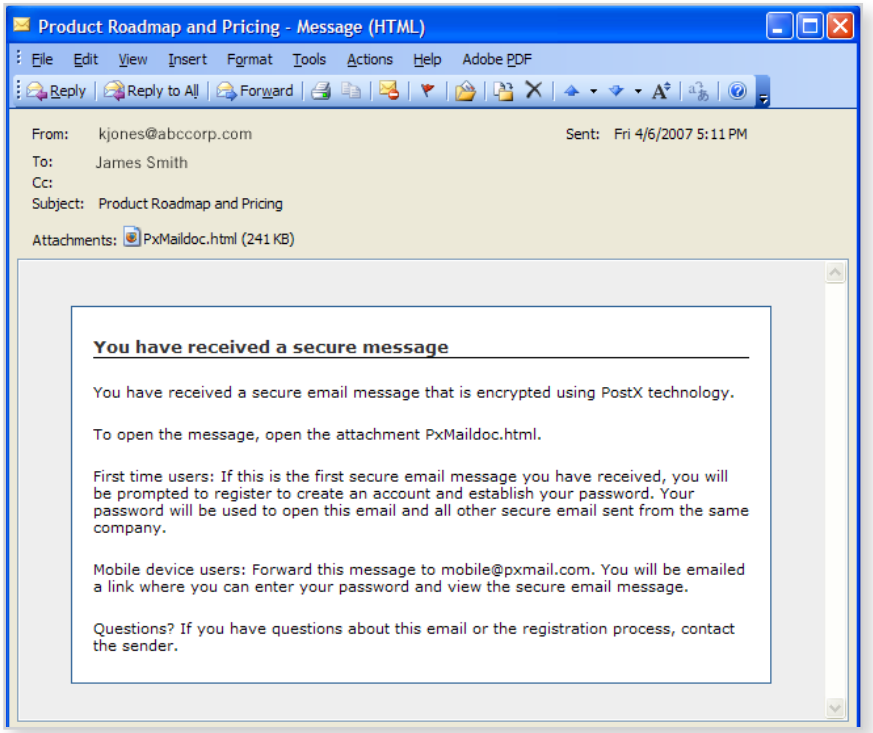

Figure 2: *The recipient is given clear instructions for decrypting the secure message.*

The attachment opens in a Web browser, and the recipient is prompted to enter his or her password, as shown in Figure 3.

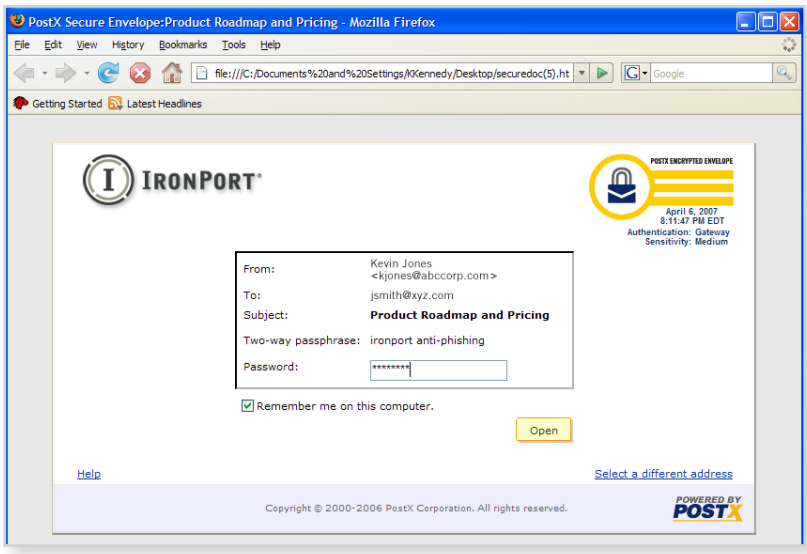

Figure 3: *The HTML document first displays a password-entry screen.*

IRONPORT

The password is authenticated by the IronPort Hosted Keys Service. Upon successful authentication, the decryption key is sent to the user's system, which then automatically displays the decrypted message in the browser window, as shown in Figure 4.

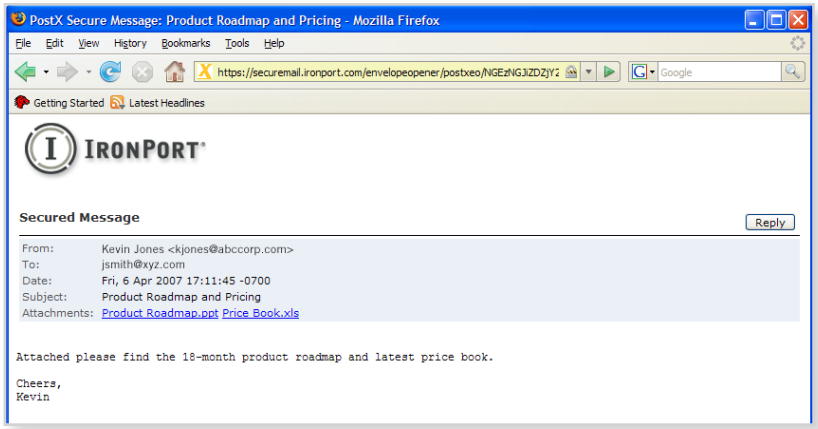

Figure 4: *Upon authentication, the decrypted message displays in the user's Web browser.*

The decryption key must be retrieved from the server each time the message is read—allowing messages to be locked by the sender even after they have been read.

Recipients can respond to messages in a secure manner by clicking on the "Reply" button at the bottom of the screen.

First-time recipients do not need to set up an account in advance of using the system. When they attempt to open their first IronPort PXE-encrypted message, they are guided through a simple Web-based registration process to set a password. An account is automatically created on the IronPort Hosted Keys Service. That account can then be used to receive IronPort PXE-encrypted messages from any sender. Users can also log into their account at any time to compose new encrypted messages.

For all users, the password screen also displays the two-way passphrase chosen by the user during account setup. This passphrase is an anti-phishing measure; it assures recipients that a message has come from a trusted email server.

The "envelope" in which the encrypted message is sent can be customized to meet branding the needs of individual organizations.

How Messages Are Decoded

The HTML attachment contains the encrypted message content (encrypted using either AES or RC4—both highly secure, industry standard algorithms) as well as JavaScript to decrypt the content.

JavaScript provides an effective local decryption mechanism without requiring the installation of any software—a critical requirement in attaining universal reach with high usability. However, JavaScript is not always available: it may be stripped out at the receiving gateway or disabled in the recipient's browser. In these cases, recipients can still decode encrypted messages easily. After they enter their password, the encrypted message is automatically posted to the IronPort Hosted Keys Service for decryption. Then, the resulting decrypted message is sent back to the user's browser for display. This communication is performed over a link, secured with the SSL protocol. Decoding messages in this "triple-trip" fashion is slower and less scalable than decoding them locally, but it does provide a viable alternative when it is not possible to use JavaScript to open the message.

MESSAGE TRACKING AND REPORTING

Users and administrators of IronPort PXE technology can use the system's Web-based interface to track messages and get reports on message activity.

- **Delivery and response tracking.** Messages send notifications to the server when they are opened, optionally generating read receipts for senders. Administrators can configure time-based triggers to monitor message opening and signal when messages are not opened within a certain time period.
- **Message activity reporting.** IronPort C-Series email security appliances provide extensive reporting on content filtering. For encryption, it can indicate how many messages were flagged by each specific policy, and how many from each user.

CONCLUSION

IronPort PXE is a comprehensive yet easy-to-use encryption solution that offers the following benefits:

- **Security.** Messages containing sensitive or confidential information are automatically encrypted to protect the message content. Encrypted messages are never stored on the same server as their keys, providing maximum security.
- **Compliance.** IronPort PXE helps organizations comply with both regulatory and internal policies. All outbound messages are scanned by content filters, and messages containing confidential and sensitive information are encrypted. Predefined lexicons can easily be extended and customized to meet individual needs regarding confidential information. This policy-driven approach, enforced at the gateway, ensures that rules are consistently and auditably applied.

- **Visibility and control.** Features such as guaranteed read receipts, message locking and message expiration give organizations greater control over business email.
- **Universal reach.** Messages encrypted by IronPort PXE can be sent to any email inbox without requiring a pre-existing relationship or client software. This enables the solution to scale for ad hoc communications for both business-to-business and business-to-consumer applications.
- **Ease of use.** Message encryption is transparent to senders. Message recipients can use their favorite email and Web clients running on any computer platform. Once the decryption key has been obtained, in most cases users do not even need to be online to reread a message.
- **Ease of deployment.** IronPort's Hosted Keys Service provides all necessary infrastructure. Simply enable IronPort PXE encryption in your email security appliance, define content filtering and compliance rules, and you are ready to go.

IRONPORT

IronPort Systems
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

IronPort is now part of Cisco.

CISCO