Secure Messaging: Key to the Business Enabled Network

A Comodo White Paper

COMODO
ENTERPRISE™

> We must plan for freedom, and not only for security, if for no other reason than that only freedom can make security secure.
>
> - Karl Popper

Securing the Enterprise

A Paradigm Shift

With the Internet having achieved a state of utility for businesses and individuals alike, innovative forms of communications and business opportunities are proliferating between users, partners and customers. It is within this dynamic environment that we labor over how best to balance the constructive use and protection of sensitive data, not only over the Internet but across corporate intranets and extranets as well.

For security to protect and support the realization of benefits from open community commerce, users must not be confronted with complex demands or hindrances to their corporate mission. Applications must seamlessly facilitate trust and integrity amongst constituents and their transactions. Security must be transparent and pervasive to deliver such an obvious benefit.

History Often Repeats Itself

In the traditional, paper-based world of communications, companies rely on a number of guarantees for transactions: confidentiality, the guarantee that the contents of a message are private; authenticity, the guarantee that the message comes from the individual who sent it; integrity, the guarantee that the message contents have not been modified; and non-repudiation, the inability of an individual to renege on a transaction after the fact.

Before the Internet explosion, securing the corporate network – both physically and electronically – entailed using the same general concept employed during the Middle Ages: the perimeter defense. Feudal lords protected their castle through the use of moats and drawbridges; network administrators protected their networks by limiting access to only those individuals they had identified as trustworthy, and had pre-equipped with passwords, key cards, tokens, etc. Both strategies focused their energies on preventing external threats from passing through a reinforced and protected perimeter. The reasoning behind this strategy was simple: threats that cannot enter the network cannot damage it. This obviously and incorrectly presumed that all internal sources could be trusted to maintain policies and eliminate threats, and that sensitive data was always inside the perimeter. Facts speak differently as human error, non-malicious policy circumvention, physical theft and inherent operational risks continue to surface as the primary vulnerabilities – all internal or distributed from internal sources.

The Current Environment

While the well-accepted perimeter defense certainly has its merits in an overall enterprise security infrastructure (you'd be hard pressed to fi nd any corporate network that is not protected by a fi rewall), today's highly connected businesses must extend communications and corporate resources to customers, resellers, partners and diverse mobile clients. Most importantly in this environment, security strategies need to accommodate a variety of geographically distributed applications, hardware and data, all the while serving to protect the integrity and trust of each business transaction and participant.

As this paper begins to focus on secure email (messaging) for today's connected enterprise, we recognize that email is a business critical application that walks a fine line between being an open and dynamic commerce enabler with the need for comprehensive business protection. From a user's perspective this is all too often viewed as being between usability and security. Frequently at odds with one another, this situation is also a far cry from the threats considered by a perimeter defense strategy designed and employed decades ago.

To be certain, the Internet has not only brought the importance of security to the forefront of the business community, it has also brought about a signifi cant network security paradigm shift.

The Need for Secure Messaging

Enterprise E-mail – a once convenient means of inter-departmental communication between peers and co-workers has matured into a core element of the enterprise IT infrastructure. E-mail is relied upon for timely communication and workflow capabilities as well as for the promotion and facilitation of critical knowledge transfer among employees, business partners and customers.

As enterprise e-mail use has prevailed and thrived as a transport vehicle for a wide array of important documents, it becomes critical for organizations to investigate and actively manage the delivery of their confi dential and sensitive information.

This is especially important in today's more highly regulated business world, where now numerous governmental and industry mandates, e-mail-centric court decisions, and e-mail's expanding business role are all (re)defining a critical enterprise messaging landscape and corporate mandate. Legal and fi nancial responsibilities are directly attributable to e-mail use, and it is vitally important for organizations to not only understand these issues and risks, but to implement technologies that will mitigate them.

Unfortunately, while a genuine need for e-mail security currently exists in the enterprise, very few organizations have secure messaging infrastructures and policies in place.

Where Complexity Originates

Among the many prevalent security issues facing organizations are the need to:

- Integrate security technologies with existing enterprise applications, systems and processes – many of which may be legacy or highly customized.
- Ensure that any investment in security technologies will remain compatible with future applications and systems.
- Identify and account for all legal implications and requirements related to encrypting, monitoring and storing electronic documents and messages. eDiscovery mandates and cases are growing exponentially.
- Ensure that security administration does not overwhelm more important IT organizational duties.
- Make security solutions transparent to the end-user, negating the need for in-depth training, key/password management or having the user search for ways to circumvent policies.
- Implement security solutions that are compliant and compatible with continuously shifting regulations and legal requirements.

Thanks to several high-profi le world events originating with the signing of the fi rst national United States Digital Signature Law through the numerous security breaches that have been publicly announced, the very notion of what is secure and what is private in this electronic medium has fallen under close scrutiny and formal regulation. As a result, businesses worldwide need to re-evaluate their networks and systems from a security perspective, and make the integrity and protection of their messaging infrastructures a priority. Usage policies coupled with user awareness help to maximize investments and protection.

The Elements of Enterprise Messaging Security

An All or Nothing Proposition

Protecting a distributed network from a growing number – in frequency and variety – of security threats mandates much more than a perimeter monitor or the installation of additional fi rewall and AV equipment.

Comprehensive enterprise security measures must address and account for all fi ve essential security elements: Trust, Authentication, Privacy, Integrity and Non-Repudiation.

Trust

From the network and security administrator's viewpoint, not all users are created equal. Each member of an organization can be trusted with different types of information, depending upon their role, management status or any variety of other criteria. Networks and messaging systems must be able to account for these differential degrees of trust – for example; a message sent to a business partner must not contain sensitive information earmarked for the company's executive team.

Network administrators often enforce trust-based rules by implementing policy-based management (PBM) that classifies users into certain predefi ned groups, with specifi c access rights and capabilities assigned to each of the groups. In such a case, the messaging system should be integrated with the PBM technology to extend group privileges to each user's e-mail box.

Authentication

Authentication technologies are used to validate the identity of both the message sender and the message recipient(s).

One of the most familiar – though rudimentary – forms of authentication is the "cookie", which provides automatic authentication of users visiting Web sites supporting this technology. A cookie is a small fi le stored on an individual's computer that allows a site to tag the user with a unique identifi cation. When a person visits a site, the site's server requests a unique ID from the person's browser. If an ID is not found, the server will deliver one. Organizations that employ cookies in their e-commerce applications can track information about user behavior.

Obviously, much more potent and comprehensive forms of authentication are required in large enterprises, especially when they reach beyond the immediate corporate network and into the environments of their business partners, clients, and customers. Many networks and network operating systems rely on network authentication protocols, such as Kerberos, which authenticate clients when they attempt to connect with a server. On the Internet, digital certifi cates are often employed to authenticate people, applications, and services, and to provide access controls.

In a secure messaging system, these authentication technologies work in tandem with other technologies (e.g. public/private key, encryption) to provide comprehensive e-mail protection throughout the entire sending, transmission and reception process.

Privacy

Although an essential tool for increasing the productivity and effi ciency of employees, e-mail, like other electronic forms of communication, is susceptible to a wide range of threats – including interception by unintended or malicious users. As a result, privacy technologies are typically employed to ensure that messages are only viewable by their intended recipients.

The most common form of privacy protection for e-mail is encryption, in which an e-mail message is "scrambled" before sending, and "de scrambled" upon reception. This ensures that the message cannot be easily decoded if it is intercepted during transmission.

Encryption technologies – including shared secret and public key – can be used independently of other security technologies, but work best as part of a larger overall security solution that includes digital signatures and client certificates.

Integrity

Undeniably, one of greatest strengths of electronic media is the ease with which it can be manipulated and altered. When viewed from a security perspective, this strength is a tremendous liability, as it is critical for both senders and recipients to know that transmitted information has not been tampered with or altered.

One of the most bare-bones forms of maintaining the integrity of a message is through a checksum procedure called hashing. An algorithm is used to create a "hash" from the message; the algorithm is sent along with the message, which the recipient uses to create a second "hash". If the two hash marks match, the message has been unaltered, and validity of the message is ensured.

Non-Repudiation

Of all essential security elements, the non-repudiation element is one of the most technically challenging to implement. Non-repudiation prevents the sender of an electronic document from denying that he/she sent it, and prevents the recipient from denying that the document was received.

Digital signature technology enables non-repudiation by including a digital signature along with the e-mail, which is generated, in the context of a Public Key Infrastructure (PKI) solution, from a user's private key. Digital signatures are encrypted blocks of data that verify the sender's identity when decrypted (using the sender's public key) by the recipient.

Ease of Use

As Karl Popper noted, "only freedom can make security secure." Ease of use is necessary to ensure that security systems can be consistently and thoroughly implemented for a wide variety of applications without unduly restricting the ability of individuals or organizations to go about their daily business.

This last goal is frequently overlooked. Organizations must not only develop sound security measures, they must also fi nd a way to ensure consistent compliance. If users fi nd security measures cumbersome and time consuming, they are likely to fi nd ways to bypass them— thereby putting your Intranet and Extranet at risk. Organizations can ensure the consistent compliance to their security policy through:

- Systematic application - The system should automatically enforce the security policy, preventing human error or malicious action.
- Ease of end-user deployment - The more transparent the system is, the easier it is for end-users to use— the more likely they are to use it. Ideally, security polices should be built into the system, eliminating the need for users to read detailed manuals and follow elaborate procedures.
- Wide acceptance across multiple applications - The same security mechanisms should work for all applications a user is likely to employ. For example, you should be able to use the same security system whether you want to secure e-mail, e-commerce, server access via a browser, or remote communications over a virtual private network. PKI was designed with this multi-purpose application in mind.

A Foundation Built on Policy

In the enterprise setting, technology is typically implemented to support critical business functions and to reduce designated risks.

It is important to keep this tenet in mind when building a secure messaging infrastructure – often, organizations spend great amounts of effort, time and money on choosing and implementing a solution designed to increase enterprise security – while neglecting to spend equal effort fi guring out how this new technology will support day-to-day business operations, or how it will impact corporate users. This is a signifi cant mistake that, in essence, puts the cart before the horse.

All of the secure messaging technologies in the world will have little effect if they lack guidelines and rules establishing how they are to be used and integrated operationally into the enterprise.

Whether secure technologies are currently deployed in their enterprise environments or not, it is important for organizations to craft e-mail policies permitting various technologies and solutions to be used to build a secure messaging infrastructure. Creating such an e-mail policy involves a multitude of factors that are to be considered, including specific business, legal, and operational requirements, relationships with partners, clients, and customers, and the operational role(s) that e-mail supports in the corporate environment.

From a Technology Perspective

One of the most prevalent challenges in building a secure messaging infrastructure that incorporates all of the essential security elements is in fi nding a comprehensive and economical solution that can simplify and speed the deployment and adoption curve while minimizing administrative overhead.

Essential Security Element	Technology Group
Trust	Policy Based User Management, PKI Certificates
Authentication	PKI Certificates, Hardware Tokens
Privacy	Encryption (S/MIME, TLS, IPsec)
Integrity	Encryption, Message Hash Signatures
Non-Repudiation	Non-Repudiation Encryption, Digital Signature

On a global level, the essential element of trust infers the use of a policy based access technology; ensuring e-mail integrity and privacy requires encryption of some sort; authentication is most often achieved with public/private key infrastructure technology; and digital signature technology is essential for non-repudiation.

Bringing it All Together

Begin by evaluating the various email uses, groups and devices as well as the information classes being conveyed and their risks. This assessment becomes the basis for selecting available solutions and is integral to creating a messaging policy that complements and reinforces the technology choice.

For example, a large multinational legal fi rm has just implemented a secure messaging product that encrypts employee e-mail before it is sent. However, all 10,000 corporate users must manually enable this encryption function from within their messaging client. Unfortunately, this encryption solution has a detrimental impact on messaging bandwidth, and as a result, many users are choosing to deactivate the encryption feature in favor of increased performance. Also, an extremely sensitive fi le, sent by a user choosing to deactivate e-mail encryption, has fallen into the hands of a competitor.

In today's electronic communications-dominated world, problems such as these appear with increasing frequency. Many of them carry with them serious ramifi cations and consequences (fi nancial and otherwise), and all underscore the necessity of establishing a delicate and measured balance of security technologies and policies that govern their use within the business environment.

While a PKI solution ranks among the best security measures available, it is not an all-encompassing solution alone, and requires other monitoring technologies and human processes in addition to an e-mail usage policy to support its designated purpose.

The Reality of a Secure Messaging Infrastructure

Email is a prolifi c and important enterprise application, one that requires careful security and legal considerations. With email usage and content being a signifi cant risk to the enterprise, email security must be properly assessed and managed. There is a balance to achieve as businesses must maintain open communications with all stakeholders. Solutions and policies must be economical and easy to enforce, and critical information must be kept secure.

The need for trust, authentication, privacy, integrity and non-repudiation in email communications is a key business enabler just as they are critical, manageable and real elements of true security.

> “We must plan for freedom, and not only for security, if for no other reason than that only freedom can make security secure.”
>
> *The Open Society and Its Enemies (1945)*
> Karl Raimund Popper (28 July 1902 – 17 September 1994)

About Comodo

The Comodo companies provide the infrastructure that is essential in enabling e-merchants, other Internet-connected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and Email Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure email and fax services.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 10,000,000 users of our desktop security products.

For additional information on Comodo – Creating Trust Online™ visit http://www.enterprise.comodo.com

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay,
Trafford Road, Salford,
Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1.(888).266.6361
Email: Sales@Comodo.com