An *IT Briefing* produced by SearchSecurity.com

PGP Education Series: The Dawn of Pervasive Encryption

By Jon Callas, PGP Corporation and
Jim Reavis, Reavis Consulting Group

PGP Education Series: The Dawn of Pervasive Encryption

By Jon Callas and Jim Reavis

BIO

Jon Callas—Jon Callas is the Chief Technology Officer, Chief Security Officer, and a founder of PGP Corporation. He served as Chief Scientist at PGP Inc. and as CTO of the Network Security Division for Network Associates Technologies Inc. He previously served as Director of Software Engineering at Counterpane Internet Security and was a co-architect of Counterpane's Managed Security Monitoring system. Most recently, Mr. Callas was Senior Systems Architect at Wave Systems Corporation. His career includes work at Digital Equipment Corporation, World Benders, and Apple Computer. He is the principal author of the Internet Engineering Task Force's (IETF's) OpenPGP standard and writer and frequent lecturer on systems security and intellectual property issues.

Jim Reavis—Jim Reavis is the President of Reavis Consulting Group and editor of the *CSOinformer* newsletter. He is also an Appointed Advisor to the President of the Information Systems Security Association (ISSA). For more than 12 years, Mr. Reavis has worked in the information security industry as an entrepreneur, writer, speaker, technologist, and business strategist. He founded SecurityPortal in 1998, and has been an advisor on the launch of many industry ventures.

This IT Briefing is based on a PGP Corporation/TechTarget Webcast, The Dawn of Pervasive Encryption. To view the Webcast, simply click on the link.

The Dawn of Pervasive Encryption covers these topics:

- PGP Encryption: The Gold Standard
- What's Driving Encryption?
- Comparison: Pervasive Web and Pervasive Encryption
- PGP Universal: An Enabling Technology
- Sending Secure Email
- Impact of Secure Messaging on Society
- Summary
- Common Questions

About PGP Corporation

The recognized worldwide leader in secure messaging and information storage, PGP Corporation develops, markets, and supports products used by a broad installed base of enterprises, businesses, governments, individuals, and cryptography experts to secure proprietary and confidential information. During the past ten years, PGP® technology has built a global reputation for open and trusted security products. The PGP Corporation family of products includes PGP® Universal—an automatic, self-managing, network-based solution for enterprises—as well as desktop, mobile, and SDK solutions.

PGP Universal is the world's first security architecture to shift the burden of securing email messages and attachments from the desktop to the network in a way that is automatic and entirely transparent to users. Secure up to 100% of your internal email and business partner communications today. Go to www.pgp.com for more information.

About TechTarget *IT Briefings*

TechTarget IT Briefings provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced IT Briefings turn Webcasts into easy-to-follow technical briefs, similar to white papers.

For inquiries and additional information, contact:
Tina Hills
Director of Product Marketing, Webcasts, TechTarget
thills@techtarget.com

PGP Education Series: The Dawn of Pervasive Encryption

PGP Encryption: The Gold Standard

The history of PGP technology dates back to 1991, when inventor Phil Zimmermann released the first version of the product. Over more than a decade, PGP technology has built a global reputation for open and trusted security products. Currently, a wide majority of all encrypted email relies on the OpenPGP standard, otherwise known as RFC 2440.

PGP Corporation is the global leader in digital information security, and PGP products are used by a broad installed base of enterprises, businesses, governments, individuals, and cryptography experts to secure proprietary and confidential digital information assets. As described in this paper, the Company offers a diverse collection of digital security products, ranging from PGP Universal—an automatic, self-managing, network-based solution for enterprises—to desktop, mobile, and SDK solutions.

What's Driving Encryption?

Corporate Governance and Legislation
Both corporate governance and legislation have begun to mandate increased use of encryption, reinforcing its recognition as a best practice across industries (see Figure 1). Recent developments in the computer industry indicate that encryption is needed now more than ever before. From the viewpoint of Chief Information Security Officers—tasked with developing, refining, and improving their corporate security assurance programs—encryption has become an important best practice for corporate governance. Security professionals are also sometimes called Chief Risk Officers because they take a risk management approach to protecting corporate information assets.

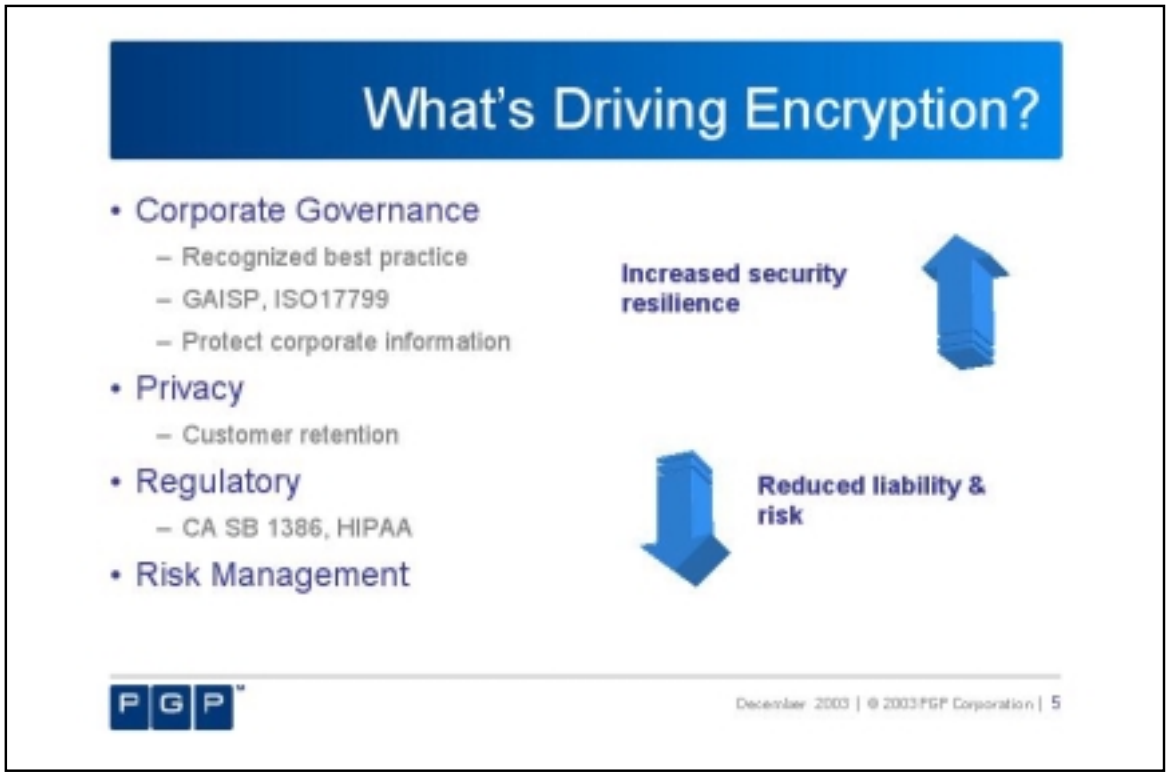

Figure 1

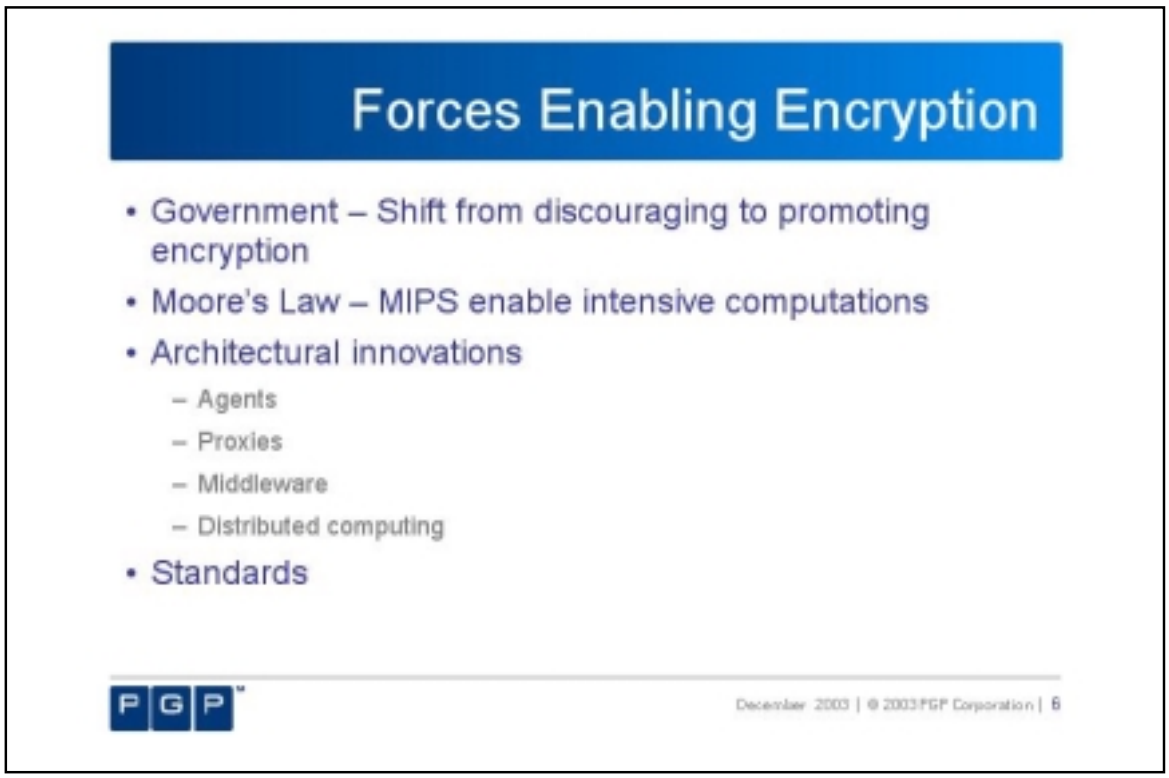

Figure 2

Government
Government has also changed its attitude to one of actively promoting encryption rather than discouraging its use, thereby helping to validate the technology. However, the same encryption techniques used to secure electronic communications can also hide those individuals intent on using the technology for illegal or unethical activities. As a result, government legislative bodies throughout the world now recognize that computer networks and the information assets they contain must be protected. New regulations now require organizations to maintain comprehensive network and messaging security.

Moore's Law
As shown in Figure 2, Moore's Law[1] and its effects on the price-performance ratios of computer platforms have provided a boost in terms of more cost-effective processing power for executing encryption operations. Moore's Law predicts that every year we can accomplish more on a mainstream computer because of increased processing power. With current market conditions making it possible to acquire a 2.5 or 3.0GHz processor for less than $1,000, developers can rethink the way they approach design issues involving encryption. Encryption techniques that used to be very expensive—partly because of processing requirements—can now be used within a streamlined infrastructure supporting pervasive encryption. Increased throughput in modern computer hardware also makes it possible to incorporate encryption techniques that were impractical even five years ago.

Architectural Innovations and Standards
From an architectural perspective, there has been a shift from the model of monolithic code existing on one workstation to a distributed model based on cooperating, federated computing proxies. PGP Universal's architecture relies on technologies that are reasonably mature. Rather than requiring new technologies, PGP Universal uses existing technologies differently, moving the operation of securing communications from the desktop to the network level. Because PGP Universal uses established technologies and standards, developers and system designers are not required to redo existing system architectures to achieve interoperability.

[1]Moore's Law predicts that the transistor density on integrated circuits doubles every couple of years. This exponential growth and ever-shrinking transistor size result in increased performance and decreased cost. http://www.intel.com/labs/eml/

Pervasive Encryption: Replay of the World Wide Web

Anyone older than high-school age realizes that the Internet has been in existence for a number of years; however, in the early days, only a small number of people primarily in the academic and research communities used it (see Figure 3). A convergence of trends—increasing ease of use of the World Wide Web, the introduction of search engines, and new options for and the speed of connectivity—catapulted the Web from an obscure communication channel to a major, pervasive worldwide medium for exchanging information and transacting commerce.

The acceptance and widespread adoption and use of encryption have, to some degree, followed a course similar to the acceptance and widespread adoption and use of the Web. As illustrated in Figure 4, encryption was initially considered an arcane playground primarily for the elite who were comfortable with the complex mathematical algorithms on which most encryption ciphers are based. The average person often did not understand how encryption worked and rarely had occasion to use it.

In the last decade, however, the situation has changed dramatically. Most people now have some type of access to the Internet and to email. For individuals to be able to send secure email effectively and easily to a wide range of email-capable devices, users must be shielded from the complexities of encryption by the supporting technology. This situation is similar to the way the Domain Name Service (DNS) and search engines hide the technical inner workings of the Web. Use of an automatic encryption proxy can bridge this gap and enable easy-to-use secure messaging.

The impetus for PGP Universal arose from that same desire to automate and simplify the encryption process. As Jon Callas describes it, "The first idea that I had for PGP Universal came from a dinner table conversation with a friend of mine on how—even as experts—we were not able to use encryption correctly, that we would forget to encrypt a reply every so often, that we would tend not to use it because it required one extra step. I started into a somewhat animated, 'You know what I would do? If I could go and build something brand new, this is what I would do.' This was, in fact, building something that is a proxy agent—something that does the security for me so that I don't have to think about it."

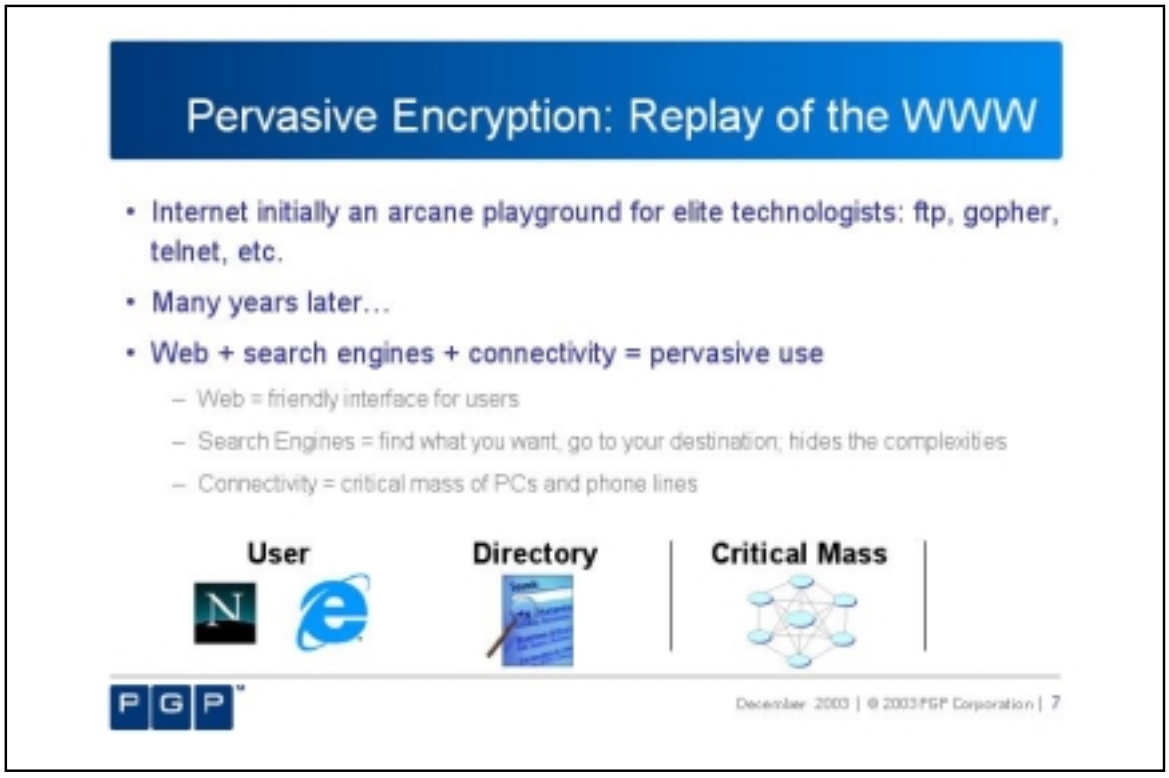

Figure 3

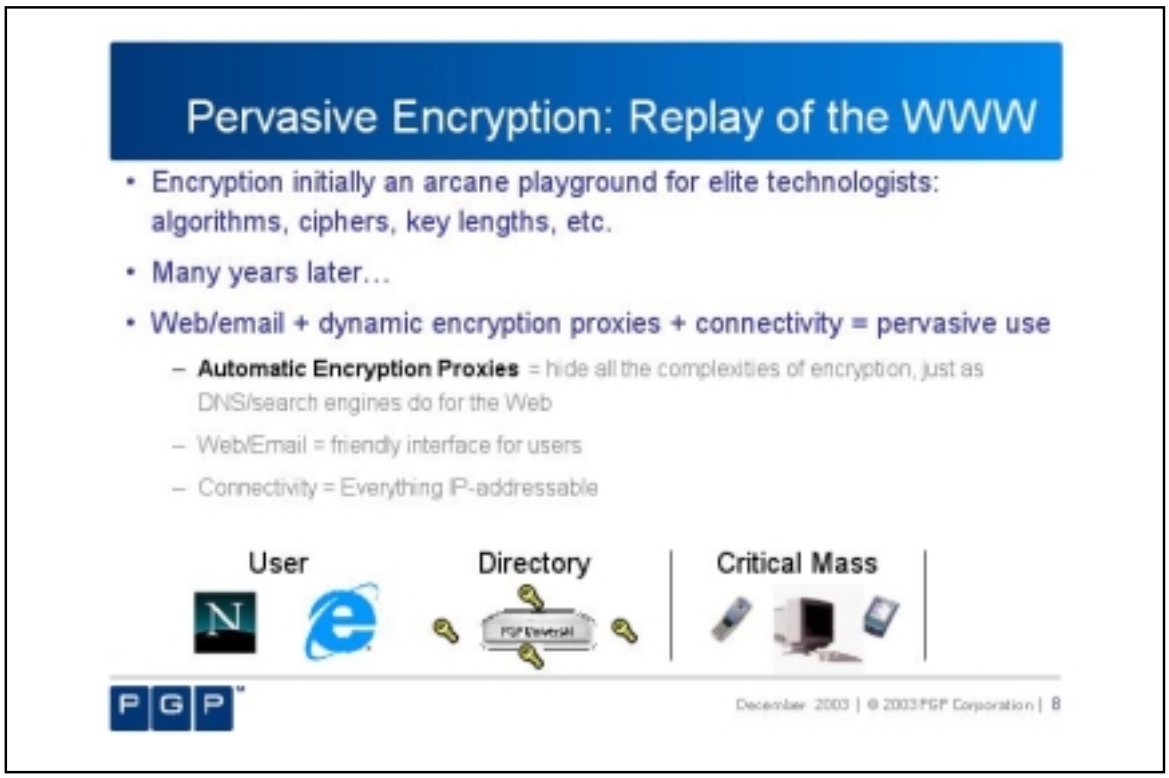

Figure 4

PGP Universal and Pervasive Encryption

Many users may be reluctant to adopt encryption as a part of their routine communications unless the process is relatively painless. To gain acceptance, encryption needs to be something that happens in the background, invisible to users (see Figure 5).

To deliver this degree of transparency, encryption needs to be transformed from a desktop function performed by an individual user to a network service that encrypts data for all users. PGP Universal provides an automatic encryption proxy to simplify and expedite the encryption process. Organizations can leverage this process, which, in turn, will multiply the instances of encryption and the keys that support it, resulting in a significantly more secure network environment.

The relationship of the Open Systems Interconnection (OSI) protocol stack layers, shown in Figure 6, illustrates the mechanism by which PGP Universal works. PGP Universal moves the complexity of encryption from Layer 7—the application layer—down to Layer 4—the transport layer. In this part of the system there are simpler ways to perform operations because the interfaces are more fully defined. Moving the process to the transport layer also eliminates the expectation that any of the numerous email-capable client devices currently available will perform encryption operations. The increase in the number of handheld devices, both wireless and wired, makes it difficult to develop secure-messaging solutions that accommodate every client. The diversity of systems adds to the complexity of the challenge as well.

To design a security system that works pervasively, the security mechanisms must be able to work effectively in nearly every situation. Moving the security functions to the network takes advantage of the fact that all users already communicate with the network using secure connections such as Secure Sockets Layer (SSL). A key advantage of this approach, therefore, is that any device able to handle POP, IMAP, SMTP, or MAPI over SSL can use PGP Universal. For example, PGP Universal interoperates with smart phones that use a standard email client with SSL support. Moving this functionality to the network results in systems that are more stable, more secure, and less subject to frequent architecture changes.

Security policy typically fails when email recipients do not have secure messaging. PGP Universal offers

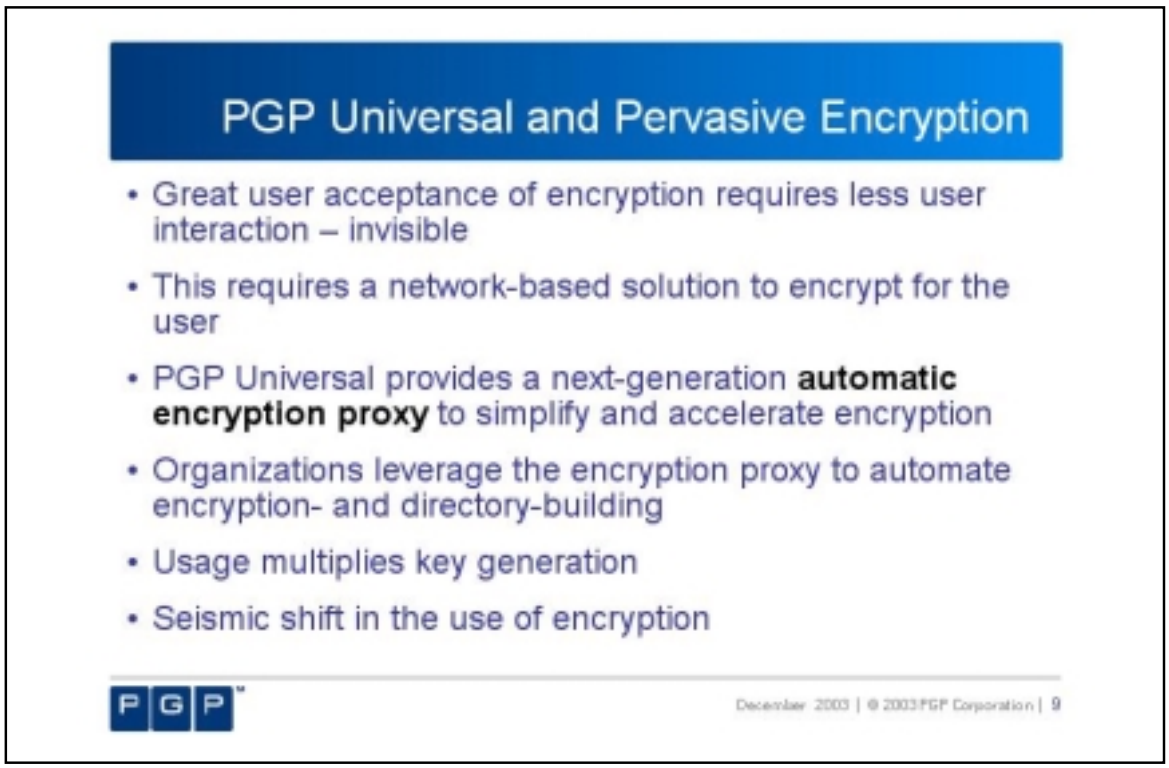

Figure 5

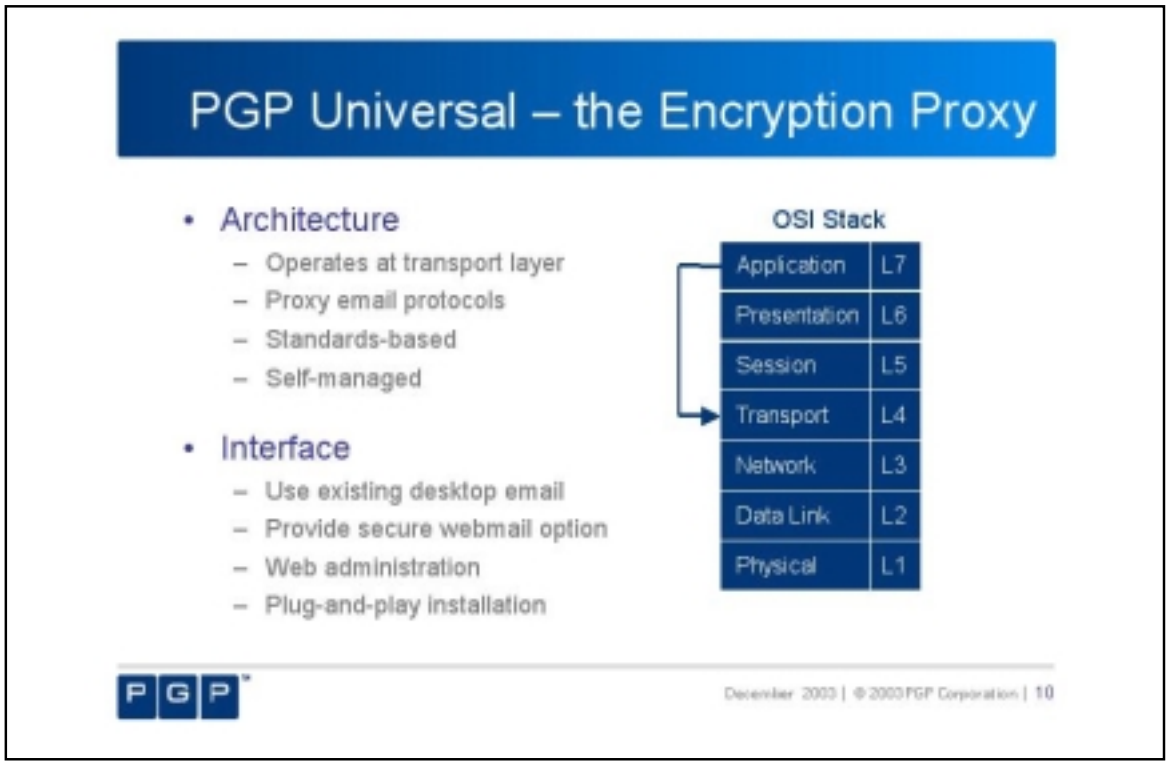

Figure 6

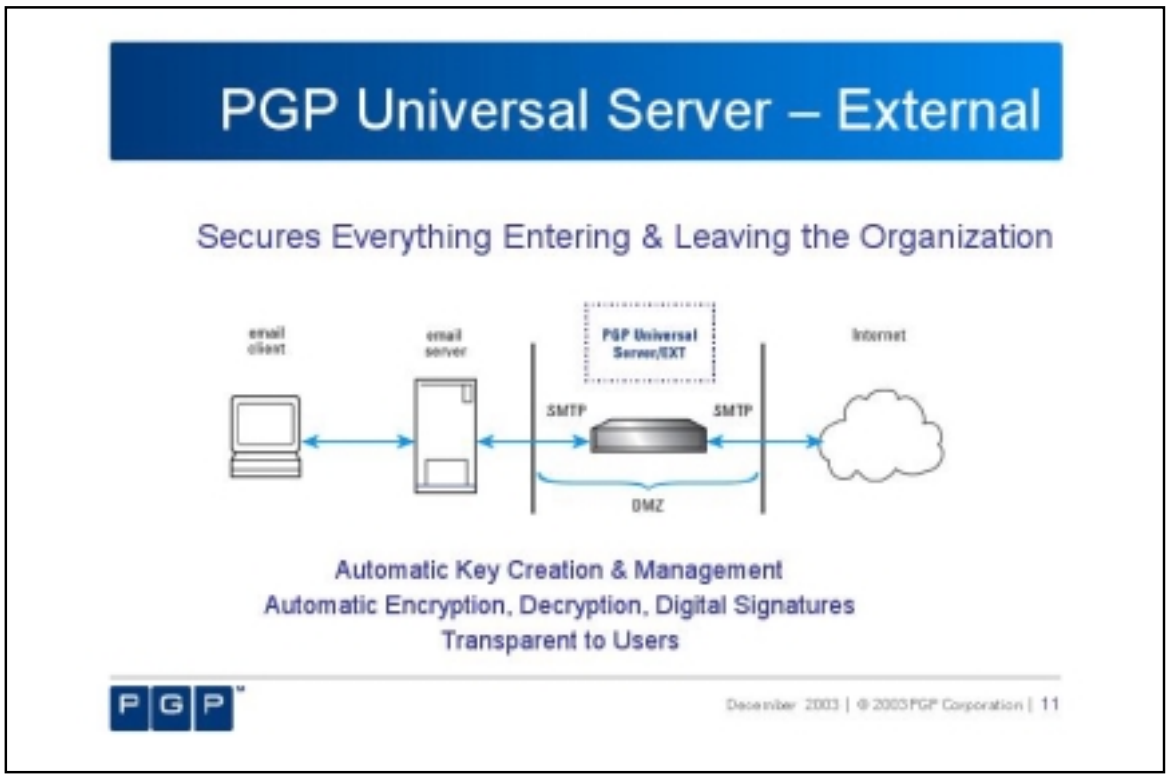

Figure 7

a secure webmail option for email recipients without an installed encryption solution. In such cases, PGP Universal retains the original secure message and sends an "in-the-clear" email message notifying the recipient that a secure message is available. The PGP Universal Web Messenger feature then allows recipients to use their Web browser to create a secure SSL/TLS session and retrieve their message through a webmail-like session. The goal is to create security mechanisms that are more powerful as well as easier to build, easier to deploy, and easier to maintain.

The simplest way to deploy PGP Universal is shown in Figure 7. Here, PGP Universal operates in the DMZ, securing messages entering and leaving the organization with the SMTP email protocol. When messages are transmitted, PGP Universal automatically encrypts them. When secure messages are received, PGP Universal automatically decrypts them. The software performs full key management, key creation, and key lifecycle management as well as digital signatures for all users on the PGP Universal system.

Placing these functions at the edge of the network's email subsystem ensures minimal disruption because security is added without manual intervention once PGP Universal is deployed (see Figure 8).

This approach is particularly useful for large enterprises that are required to archive messages. From an email end user's perspective, this approach also ensures transparency because there is no software to install or other configurations to change. PGP Universal automatically encrypts the email as it leaves the organization and adds a digital signature, if required. Such a configuration resembles that of a typical corporate firewall—once it is implemented, end users are not aware of its existence. In addition, PGP Universal's Self-Managing Security Architecture reduces the need for ongoing IT management and support once it is deployed.

According to Jon Callas, "This is really where the innovation of PGP Universal comes in. Gateway SMTP encryptors and decryptors are not news. They are things that people have done in the past—something that people have thought about for years. What we did is say, 'Let's proxy everything. Let's take POP, let's take IMAP or SMTP, and let's make it work for Microsoft MAPI protocols, too.'"

"With this approach," Callas continued, "you connect to PGP Universal with SSL just like you connect to any other email server. PGP Universal takes your connection and sends it to the real email server. It doesn't

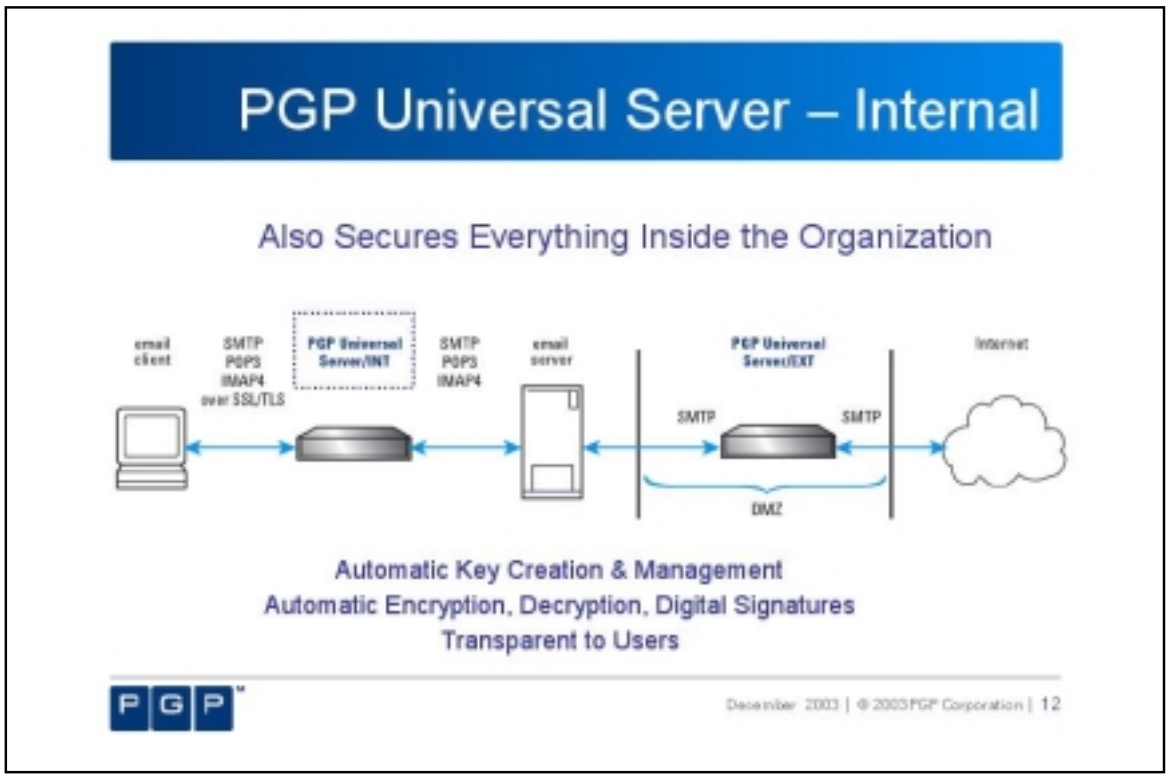

Figure 8

have to store your messages; it operates on them in transit. In that particular case, it can take your messages and not only have them encrypted right out of the network, but also while they are in your network. The benefit of this approach is that you end up with your information and your partner's information encrypted even when it is on the server. This results in ciphertext everywhere and plaintext on your computer. You can still do all the searching and indexing that you did before because PGP Universal is handling your client and what it would consider to be plaintext. It is inserting little markers, telling you that it was decrypted, telling you that the signatures were verified correctly, and so on."

Communicating securely with users outside the organization is difficult. Even when outgoing email security policy is followed, there is no guarantee recipients will reply securely. PGP Universal Satellite resolves this problem by offering two-way policy enforcement—extending security to inbound email messages originating outside the organization. PGP Universal Server downloads PGP Universal Satellite—a small, no-user-interface, invisible piece of software—to the recipient's Windows or Mac OS X desktop client along with a key and associated security policy. Once installed, PGP Universal Satellite automatically encrypts and decrypts and enforces policy on all email sent to and from the PGP Universal Server.

PGP Corporation applied knowledge gained from developing firewalls and virtual private networks (VPNs) to developing PGP Universal Satellite. Essentially, PGP Universal Satellite transparently pushes network encryption out to the client itself. Once installed on the client, it operates much like a firewall, listening to the email protocols. PGP Universal Satellite offers an additional advantage as well: end users can manage the private key of their key pairs, if desired. In what is called Client Key Mode, all cryptographic operations are performed by the end-user computer on which PGP Universal Satellite is installed. The private key never leaves the user's computer; the user's computer also handles all private key management. This approach ensures that signing keys remain within the user's direct control at all times, meeting the most stringent non-repudiation requirements.

Pushing encryption out to the client allows the servers to gain more throughput. A potential disadvantage to this approach, however, is the fact that individual users have to manage the process. From its earliest

days, cryptography has suffered from a serious limitation: no matter what mechanism users chose to lock their data—a passphrase or a token, for example—they could find themselves unable to access their data if they forgot that passphrase or token.

To address that limitation, PGP Universal offers another option called Server Key Mode. In Server Key Mode, the server from which PGP Universal Satellite is installed performs cryptographic operations. When PGP Universal Satellite is used, the server temporarily—yet securely—sends the private key to PGP Universal Satellite. This approach provides for transparent roaming on additional authorized computers or email-capable client devices without manual migration of the key. For example, Server Key Mode enables end-to-end security and authentication when used with personal digital assistants (PDAs) and smart phones.

Implementation of PGP Universal can be determined on a user-by-user basis, with some users relying on server-based encryption (Server Key Mode) and others set up to use client-based encryption (Client Key Mode). The decision of how to handle the issue of users managing keys may be mandated by corporate security policy or regulatory requirement, or administrators can opt to ensure the server keeps track of all keys so no one can lose them.

Sending Secure Email

Figure 9 illustrates the technique of sending a secure email using PGP Universal between two fictional characters: Bob and Sue.

In this example, Bob composes an email message using a standard email client in the same manner he always composes messages. When the message is complete, he clicks "Send." In earlier versions, PGP email plug-ins required senders to click a "Send Secure" or "Please Encrypt This" button to activate the encryption function. Responses from product testers suggested that removing this requirement would make the product easier to use, which is why Bob now simply clicks "Send."

Bob's message gets picked up by PGP Universal, either by PGP Universal Satellite on the client machine or through SSL to a PGP Universal Server. The server examines the destination of the message and recognizes it is being directed to Sue. The server identifies Sue's domain and examines LDAP information associated with the account to determine

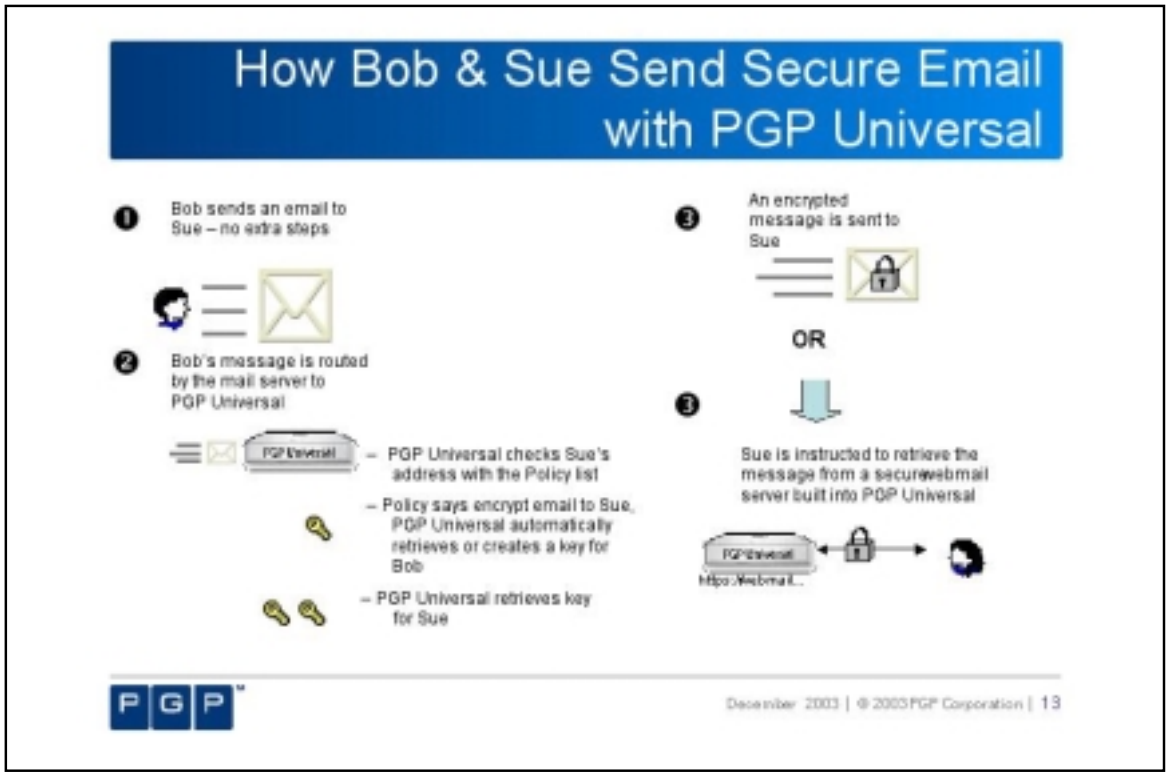

Figure 9

that the policy to Sue's domain is to encrypt the message, but not to sign it. To accomplish this goal, the server needs to have a key for Sue.

The server might have Sue's key itself, access her key through a global PKI-like certificate server, communicate with an LDAP server at Sue's company to retrieve her key, or ask another PGP Universal Server for the key. If the server finds a certificate for Sue, it can obtain the public key from it, encrypt the message, format it, and send it on to the recipient (Sue).

PGP Universal's approach is format-agnostic because it does not require a PGP key or PGP certificate but can also use an X.509 certificate or S/MIME-formatted email. OpenPGP and S/MIME are fully realized IETF standards. The National Institute of Standards and Technology (NIST) mandates the use of either protocol for communications between the government and government contractors. Similarly, there are both S/MIME and OpenPGP versions of EDI specifications. Although these two standards have been vying for prominence for some time, indications are that both will continue to be used in the short term. As XML-based formats become increasingly important in the next few years, PGP Universal will interoperate with these formats effectively as well.

Returning to the earlier Web metaphor, there are two primary ways to place an image within a Web page: in GIF format or JPEG format. When viewing the image, the user doesn't know or care what the format is. In the same manner, people working with secure email often want to be able to move freely between standards, using either S/MIME or OpenPGP where appropriate. PGP Universal makes it possible to perform pervasive encryption regardless of the choice of standards at the organizational level.

In the PGP Universal world, the certificate type defines what the message type should be. If the PGP Universal Server determines that Sue has an X.509 cert stored in the VeriSign public directory, the underlying assumption is that Sue will probably want to receive an S/MIME message, and PGP Universal codes it that way. If Bob sends a single message to two people, such as Sue and Alice, and Sue has an X.509 certificate and Alice has a PGP certificate, PGP Universal automatically sends an S/MIME-formatted message to Sue and a PGP-formatted message to Alice. In this way, Sue and Alice each receive secure messages delivered in the format appropriate to their respective email configuration.

If a recipient doesn't have a certificate, the PGP Universal Server has several options. The simplest technique is to send the message in plaintext format, which might be appropriate for certain domains. For example, the server might receive a message going to an AOL account and determine that the message should be encrypted if it can locate the recipient's key, but if not, should be sent to the recipient in plaintext.

In some enterprises, policy states that messages should be exchanged with business partners through the email VPN and, if security cannot be ensured, the message exchange should fail. If Bob attempted to send a plaintext message to someone where this policy is in effect, for example, PGP Universal could bounce the message back to him. However, in many cases, the message must be delivered even if the recipient, Sue, has no knowledge of email security. In this case, PGP Universal sends a message to Sue reading, "Bob would like to send you a secure email message. Please click this link." The SSL HTTP link then connects Sue to a secure webmail server built into PGP Universal.

Authentication in this scenario can be handled in two different ways: The server may presume that Sue will be the first person to open the message Bob sends ("first time good"). Or, the server may send Bob a message containing a randomly generated password that must be given to Sue by some means other than email ("out of band"). Depending on the circumstances, one or the other of these approaches might be appropriate to maintaining the necessary level of messaging security.

In either case, Sue authenticates to the PGP Universal Server where she can access a webmail-like system. She can read the email, reply to it, and download PGP Universal Satellite, which will coordinate with PGP Universal Server. Thereafter, whenever Sue sends email back to Bob's domain, PGP Universal Satellite will encrypt it automatically. Any other email she sends will be handled normally. Sue can also download attachments and interact in other ways with the Web-based system. This Web-based system provides a useful way to maintain secure communications with infrequent recipients. In situations where secure communication needs to occur consistently and often, PGP Universal Satellite is a more effective approach.

PGP Universal itself performs the encryption functions, leading some to question whether it would be more efficient to apply encryption-accelerating hardware to the task. In practice, encryption-acceleration hardware encrypts at about the same speed as the processor on which it is running, so users can gain additional performance with two machines running in concert. Using two separate computers can be more cost-effective than purchasing an accelerator

card, however, particularly because the price-performance ratios of current-generation machines are so favorable. Multiple PGP Universal Servers can be clustered, providing performance gains and efficiency advantages. Clustered PGP Universal Servers communicate by trading keys and policy information and are centrally managed via the Administrative Interface on the Primary Server in the cluster This setup can be the least expensive way to implement a high-performance PGP Universal platform.

Impact of Secure Messaging on Society

Business agility has become an increasingly important factor in organizational growth (see Figure 10). In the past, an organization's business agility was often hampered by a variety of equipment requirements, different line setups, and disparate hardware needs, making it more difficult for systems to interoperate or new ventures to succeed. If an organization is assured that its key digital information assets are secured in transit both inside and outside the organization, it may have the confidence to modify its organizational structure, launch new business initiatives, and even move into new markets.

Explosive growth in online commerce imposes the need for improved security in electronic communications as well, whether a business is operating primarily online or in a more traditional bricks-and-mortar setting. All parties must be assured that electronic communications exchanged between a business, its partners, and its customers will be protected. As a result, consumers will gain increased confidence in online transactions, leading to a better climate for online commerce and increased revenues.

Identify theft is another serious concern for anyone who spends time online. Although most cases of identify theft still use offline techniques such as pilfering credit card receipts, projections point to increased online activity in this area in the future. Pervasive encryption can help reduce the risks for consumers as well as businesses involved in online commerce.

As Jon Callas points out, "When we were building PGP Universal, we talked to a number of people who have used PGP secure messaging a lot in the past. Many have told us that their CEO said, 'I want you to secure everything. I know you can't do it this year. I know you can't do it next year. But this is the goal I want to set for you. I want all email encrypted.' There are companies that have already said,

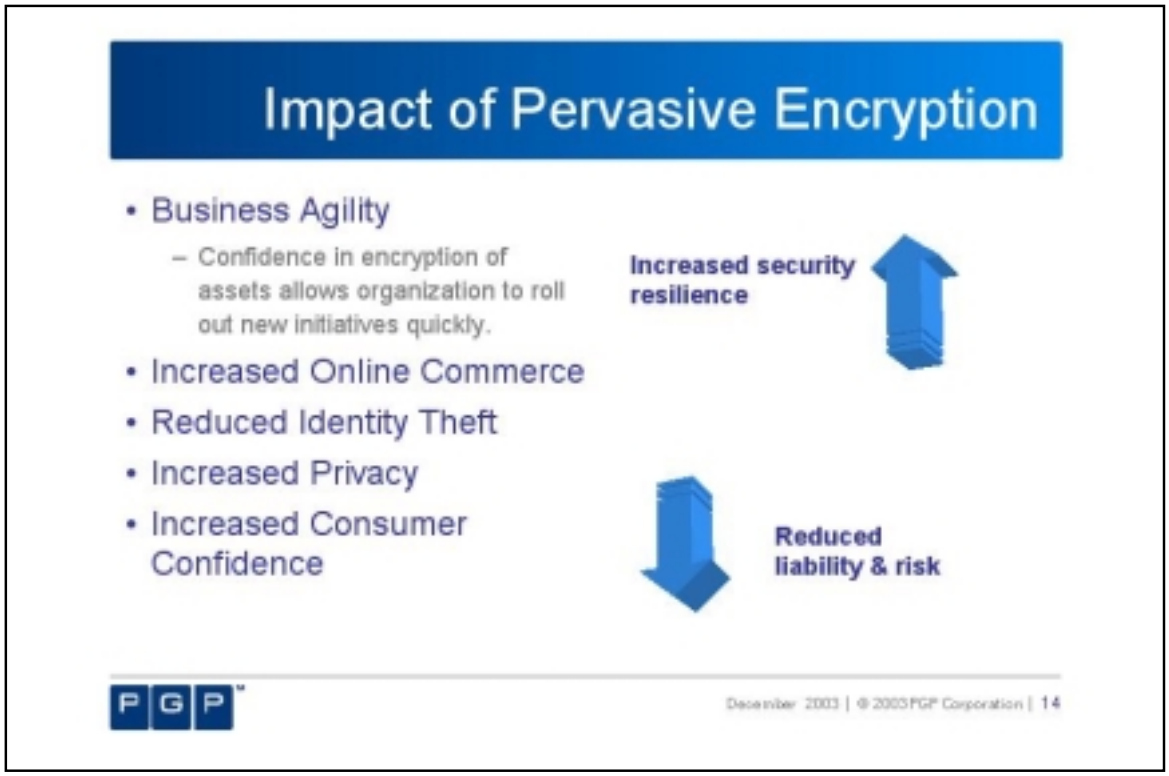

Figure 10

'Between us and our partners, we encrypt all of our email. That is our policy. If you want to be one of our partners, you have to encrypt your email.'"

This imperative, frequently now part of an enterprise strategy, can generate high costs as IT professionals and system architects learn how to implement encryption solutions and users learn to employ them. If the system requires user intervention, there's always the chance people will forget to encrypt something. If, however, a system allows policies to be centrally established and managed and messaging security policy to be completely defined, the servers can perform encryption automatically and transparently to the users. This approach not only satisfies everyone's goals, it also allows processes once accomplished by fax or physical mail to be moved to email.

Automating encryption is an important factor in lowering costs. Typically, security systems do not deliver a measurable return on investment. Messaging security, on the other hand, delivers a substantial return on investment because it enables the least expensive form of communication to be used in lieu of more costly methods. Pervasive encryption performed at the network level not only provides operational cost savings, it enhances productivity by eliminating the need for user training and support while centralizing system deployment and management.

Summary

The demand for pervasive encryption is becoming more widespread: Both government agencies and society are requiring that encryption be routinely used for communication over the Internet and intranets (see Figure 11). The technology and standards that make pervasive encryption possible have reached maturity. As PGP Universal demonstrates, the automatic encryption proxy makes encryption cost-effective and practical while being transparent to end users. Such a system becomes part of the network infrastructure, minimizing IT maintenance requirements and automating the fundamental work of creating keys or downloading them from other sites.

PGP Universal represents a next-generation, secure-messaging solution that enables pervasive encryption. As pervasive encryption takes hold throughout the industry, confidence among individual users and businesses will rise, leading to increased use of the Internet for inexpensive, secure communications.

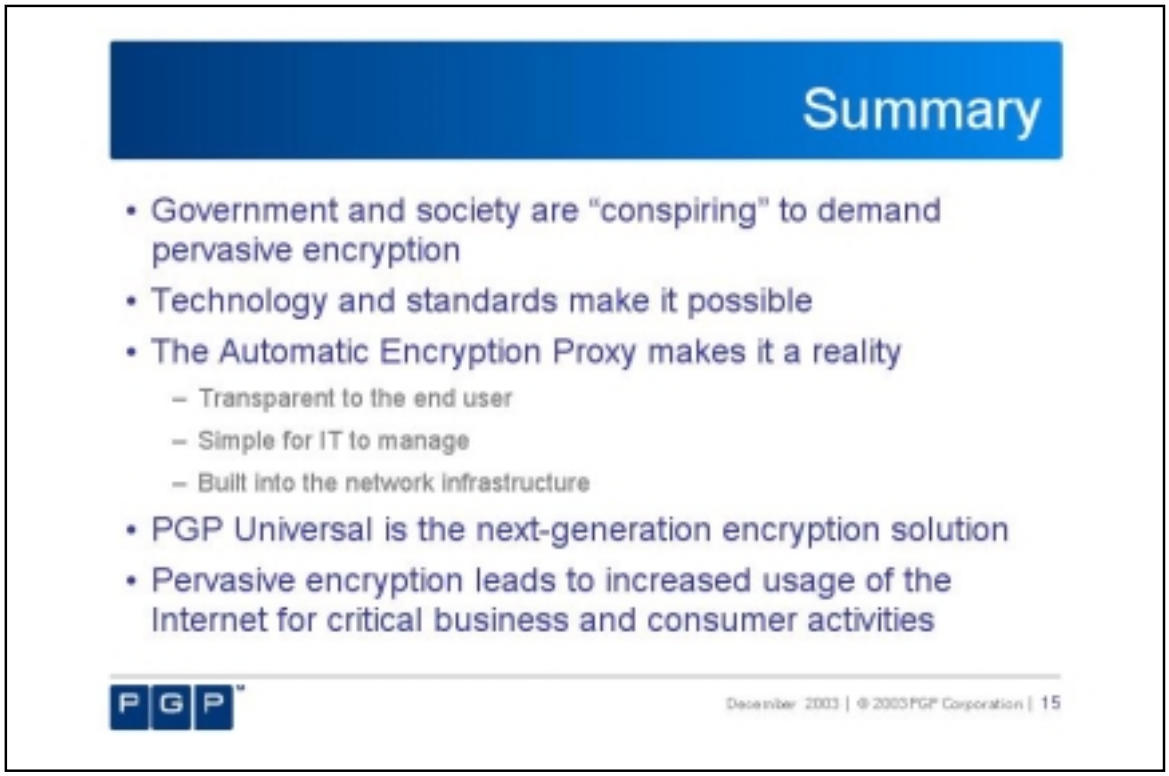

Figure 11

Common Questions

Question: A major historical complaint about email encryption is the issue of portability and user mobility. For example, a user might have multiple PCs or a smart phone or a BlackBerry handheld device. How does PGP Universal address the problem of encryption when someone is using multiple devices?

Answer: Using a clientless operation model, PGP Universal works with any device that can handle SSL. Regardless of the type of device, if it has an email client with SSL capabilities, the user enjoys full messaging security. By using industry-standard protocols such as X.509, OpenPGP, and S/MIME, PGP Universal is flexible enough to interoperate with the majority of other systems. PGP Universal can work with companies that have a PKI certificate process as well as users with smart phones. Users who travel frequently with laptop computers can plug into the hotel network and exchange email as securely as if residing in their office. Regardless of where a user is or what device she or he is using, PGP Universal ensures that email is always secure.

Question: Authentication is an important concern because people worry about identity theft or "spoofed" email messages. What are the key trends in the authentication of email messages and how does PGP Universal address them?

Answer: Digitally signing messages is the best way to ensure authentication. PGP Universal includes mechanisms that construct a signing PKI as well as an encryption PKI to positively identify the origin of a particular message.

Question: The concept of a self-managing keyserver and the supporting architecture could be leveraged for other types of communication beyond email. Can PGP Universal be used to implement other types of communication applications?

Answer: The four main Internet messaging protocols have already been implemented in PGP Universal, and a Lotus Notes version is underway. Instant messaging essentially represents a set of additional protocols, and a version of PGP Universal that supports instant messaging is already in development. The PGP Universal architecture uses a model by which the actual proxy engine can be a pluggable component so new functionality can be added as needed. PGP Universal can also handle Voice over IP (VoIP). With an infrastructure that has been set up for VoIP, a PGP Universal Server can transparently take messages, encrypt them, and send them along to the recipient, where they can be decrypted by the other gateway. Once developers fully explore the value and utility of smart security proxies, they'll be able to use this technology to add a layer of security to a wide range of existing systems.

Question: For these extended types of applications, would you use one set of keys, one hierarchy or structure of keyservers to control the operations?

Answer: Yes. In most cases, this would involve distributing objects. Clustering architectures work well in this regard. One possible approach would be to have one server act as the certificate server. Theoretically, you could have a variety of servers performing different tasks, such as webmail pickup, message delivery, instant messaging, and so on. These servers share keys. They share all necessary information to perform secure information exchange.

Question: The government has made a 180-degree change in attitude from demonizing encryption to now proactively encouraging and even mandating encryption. Is the pro-encryption position within the government likely to continue?

Answer: The current position will most likely continue. The government is just beginning to understand the basic nature of an information economy. To protect information, you must encrypt it. That has been the case ever since the invention of writing—whenever you want to protect something that has been written, you encrypt it. There is no other reasonable way to accomplish this task.

Question: What is the overhead in terms of bandwidth, time delay, and processing on the local client and email servers? How much extra hardware and bandwidth is required to jump from a voluntary (seldom-used) encryption policy to a pervasive policy?

Answer: PGP encryption often decreases the size of a message. The reason is that PGP encryption compresses the information before encrypting it. This approach not only improves security, but usually reduces storage and bandwidth requirements. We say usually because some content is already compressed. In the absolute worst case, encryption adds less than 10% to the size of a message, and this percentage is smaller with larger messages.

About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of industry-specific Web sites gives enterprise IT professionals access to experts and peers, original content and links to relevant information from across the Internet. Our conferences give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Practical technical advice and expert insights are distributed via more than 100 specialized e-mail newsletters, and our Webcasts allow IT pros to ask questions of technical experts in real time.

What makes us unique

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of conferences, the expert interaction of Webcasts and Web radio, the laser-targeting of e-mail newsletters and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals. For more information, visit www.techtarget.com.