



CertainKey
Cryptosystems

Understanding Gatekeeper – White Paper

Table of Contents:

What do all these terms mean?	2
Why do I need Gatekeeper?	2
What is CertainKey Gatekeeper?	3
Can you explain the issue of trust?.....	3
How can Gatekeeper help me?	4
What does Gatekeeper do?.....	4
What does Gatekeeper do differently?	4
How does Gatekeeper work?.....	5
Which standards does Gatekeeper support?	5
How do I get Gatekeeper?	6

What do all these terms mean?

Some of the terms used to describe what Gatekeeper is, and to describe its functionality, may be considered obscure. Below we review some fundamental terms:

CertainKey digital certificate: see *digital certificate*

cipher: the algorithm or function used for encryption and decryption

cipher text: the text outputted from the encryption process (the original text can be retrieved through the decryption process).

plain text: as opposed to *cipher text*, plain text is what you are looking at right now.

encryption: the method of concealing the contents of a message by altering it.

decryption: the reverse operation of encryption

key: unique data used in the encryption and/or decryption process

private key: the portion of your digital certificate that is kept private. It is stored on your computer and protected with a password.

public key: the portion of your digital certificate that is made public. It is stored on CertainKey computers and anyone can access it.

digital certificate: sometimes referred to as a key pair, it is the combination of your *private key* and *public key* along with information like the date it was created.

Why do I need Gatekeeper?

Digital communications are increasingly becoming the principal method of communicating between organizations. Timely and accurate information delivery is crucial for increased productivity and geographic reach. In the past, paper was the medium of choice and few people worried about the security or integrity of their communications. More often than not, this was a function of their trust in a courier service. For example, ask yourself if your lawyer has ever sent confidential documents via courier. Did you worry about their authenticity or whether they were tampered with?

With digital communications, and email is only one example, security and authenticity are more difficult to guarantee and detect. Would you know if someone tampered with your email message while it was en route to its recipient? The answer is likely 'no'. The same is true with web traffic, file transfers and any other data sent over the Internet.

With a traditional courier service it is possible, to a degree, to guarantee the integrity of a package. The Internet, however, is full of intermediaries. Your messages often do not travel in the most direct way from the sender to the recipient. In fact, the path they take is usually difficult to predict.

The CertainKey Gatekeeper solution solves the problem of digital eavesdroppers with a cryptographically secure means of sending and receiving email. Other comparable solutions leave large gaps in their security while Gatekeeper leaves all security in the hands of the individual. CertainKey never receives any confidential information and cannot intercept or modify messages. You can choose to send your messages with low security (e.g. an update email to your mother), high security (e.g. confidential business communications) or anywhere in between.

What is CertainKey Gatekeeper?

CertainKey Gatekeeper gives you a secure and trusted means of communication. Our managed service provides a mechanism for transmitting email, and other Internet communications, in a way that enables the receiver to verify the origin of the message and the sender to guarantee the integrity of the message. In a similar way, any Internet protocol can be adapted, using CertainKey Gatekeeper, to enable secure authentication or communications.

Can you explain the issue of trust?

When you last received that junk email message proclaiming how good it was to be your own boss, and that you could make obscene amounts of money, did you wonder about its authenticity? Could you have determined whom it was from even if you wanted to spend the time? This is one problem solved by using Gatekeeper. You can verify who the sender of a message was by their CertainKey digital certificate. Along with this authenticity guarantee it is also impossible for a malicious eavesdropper to modify the message so that the integrity of the message is guaranteed.

Just because you can verify who sent a particular email, if you cannot also guarantee its integrity it is not much good. As an example, if your human resources people are sending “electronic pink slips” you do not want those to be tampered with along the way. Sure it is great that you can verify that human resources sent the message, but if the contents have changed, the intended recipient may not receive the correct message and there is a chance the employer may be held liable for the contents. By using a cryptographically secure digital signature and strong encryption, Gatekeeper solves the integrity and authenticity problems

In summary, email sent without a system of security in place, such as Gatekeeper, is in-fact the electronic equivalent of a postcard and the information should not be trusted.

How can Gatekeeper help me?

Gatekeeper will keep your sensitive corporate information within the company and keep it private from eavesdroppers or malicious crackers. Your data is sent securely and can only be read by recipients that are chosen by the sender. If you send mail to your colleague, and she has a CertainKey digital certificate, the message will be automatically encrypted in a way that can only be decrypted by your colleague. Your Carbon Copy (Cc:) and Blind Carbon Copy (Bcc:) fields in email work the same way that you are used to. Only those people that are on the Cc: or Bcc: lists will be able to decrypt the message.

If you want to be guaranteed that there are no eavesdroppers lurking between you and the recipients of your message then your mail reader alone is inadequate.

What does Gatekeeper do?

Gatekeeper sits between your email program and your Internet connection. It acts as a proxy, creating a transparent, yet secure, means of sending and receiving mail. You can use your existing email reader and let Gatekeeper worry about keeping things secure. Gatekeeper encrypts outgoing messages so only the intended recipient or recipients can read them and also automatically decrypts incoming messages so that your email reader can display them. The software does this by means of CertainKey digital certificates.

What does Gatekeeper do differently?

The problem we are trying to solve is the lack of trust on the Internet. How do you know who is sending you that email and how does a recipient of your email know it was you who sent it? Other companies have come up with their own solutions to the problem. Typically they involve a publickey scheme similar to the methods used by Gatekeeper. The biggest difference between Gatekeeper and its competitors is that your private keys stay private. Other solutions will hold your private key in escrow to help with key recovery, but this does not make sense. For example, our house keys are not held in escrow. But that is not to say that key escrow does not work just that it has historically been done incorrectly.

Various governments to allow intelligence agencies access to encrypted information have promoted key escrow. Even in situations where a business controls its own keys, the mechanism for key recovery is such that an individual would not know that decrypted information had been released. Key escrows provide attackers (terrorists, teenage hackers, etc) with the ultimate back door entry to everyone utilizing the escrow service.

Another notable difference CertainKey Gatekeeper possesses, is not being tied to any one cipher or algorithm. If CertainKey Gatekeeper finds vulnerability with any of the ciphers in use, and this does happen on occasion, the software will adapt and use any one of many available ciphers. Gatekeeper already knows how to use most of the popular

ciphers and updates to the existing ciphers automatically. Gatekeeper will also automatically add new ciphers as they become available.

Our solution has a well-designed method for expiring old keys. Traditional schemes do not expire keys very often. The key that your bank uses, as an example, for enabling secure web-based banking is likely required to expire on a yearly basis, possibly longer. Business and home users of the Gatekeeper software can expire their digital certificates at arbitrary times. CertainKey certificates are renewed every 90 days. This obviously improves the security of your encrypted data because even if a potential eavesdropper somehow guessed your private key, the amount of data encrypted with that key is kept to a minimum.

How does Gatekeeper work?

Gatekeeper is an application that runs on your desktop computer. It works in the background, handling outgoing and incoming email. The application checks to see if the recipients of outgoing mail have CertainKey digital certificates and those that do are sent the message in encrypted form. If the sender encrypted an incoming email message, the message is decrypted using your personal digital certificate and your email software displays it as before.

Every user of the CertainKey Gatekeeper software has their own personal digital certificate. It is actually impossible to use the software without one, they are created the first time you start the program. Roughly speaking, the CertainKey digital certificates have two halves to them, the private key and the public key. The public key is stored on CertainKey servers and is available for everyone to see. Your private key is stored on your computer and is protected by a password. The keys are related in such a way that messages encrypted by the public key can only be decrypted by the private key and vice versa.

To send someone a secure message, you first compose the message in your mail reader and send it off as you normally would. This is where the Gatekeeper software steps in. It checks to see if the recipient or recipients have digital certificates by asking the CertainKey KeyMasters. If there is a suitable digital certificate to use, the message is sent in an encrypted form, otherwise it is sent in plain text.

At the recipient's end, incoming messages are checked by Gatekeeper to see if they are encrypted. When an encrypted message comes into CertainKey Gatekeeper, the software decrypts it using the recipient's private key.

Which standards does Gatekeeper support?

Gatekeeper currently provides support for such protocols as IMAP, SMTP, POP3, and HTTP1.1 (*RFC2060, RFC2821, RFC1935, RFC2616*). Other protocols will be added in the future such as FTP, telnet, and ICQ (*RFC959, RFC495*). The power the XML standard is

used extensively by CertainKey to store digital certificates, protected documents and email, and virtually all PKI communications (<http://www.w3c.org/XML>).

How do I get Gatekeeper?

You should first check to see if your Internet provider already offers our service as an addition to your existing access package. If your provider offers our service, contact them for further information.

If your Internet provider does not provide our service as an addition to a monthly package, you can sign-up directly with CertainKey. There are different packages for business and home customers. Contact sales@certainkey.com or 613-261-1749 with questions.