

# Public Key Infrastructure (PKI) with Comtrust™



A Superior Way of Meeting HIPAA e-Security Requirements

## Contents

Introduction: Modern e-Security Issues and HIPAA .....	2
Two Perspectives on Security .....	2
e-Security: The Internal Perspective .....	2
e-Security: The External Perspective .....	3
The Bottom Line.....	3
Combining PKI with Typical Security .....	3
Non-roaming Users .....	3
Roaming Users: Public Key Infrastructure (PKI).....	3
What is PKI?.....	4
Weaknesses of Most PKI Systems.....	4
ComTrust™/VeriSign’s Approach to PKI.....	5
How It Works .....	5
Closed vs. Open PKI .....	5
Consistency of Service.....	6
Security .....	7
Scalability .....	7
Directory/Database Technology.....	7
ComTrust™/VeriSign’s Leadership in Establishing Certification Authority Standards .....	7
Summary/Review .....	8



---

## **Introduction: Modern e-Security Issues and HIPAA**

Several information-security issues face individuals and companies as they go about their everyday business in this digital age. This is particularly true in the healthcare industry as more and more information is handled and transmitted electronically. For healthcare, maintaining proper information security is not just good business; it is mandated by federal law under the Healthcare Insurance Portability and Accountability Act (HIPAA).

HIPAA addresses the issues of security, integrity, and non-repudiation. Addressing these issues is best done with a broad brush—high-value solutions do not simply focus on HIPAA, e-commerce, or any other single aspect of security. The highest-value solutions come from addressing the entire set of business needs as a whole. A total solution that encompasses the requirements of HIPAA, enables e-commerce, reduces long-term operational costs, and recognizes the increasingly important role of the Internet in healthcare operations will provide the greatest return-on-investment.

### **Two Perspectives on Security**

A complete look at e-security issues requires examining the internal and external points of view—the issues of importance to a company or individual and those concerning the parties with whom they are communicating.

#### *e-Security: The Internal Perspective*

From the internal viewpoint, there are two basic concerns: 1) verifying the authenticity of communications and 2) non-repudiation. To safely conduct electronic transactions, you need to know that electronic communications are from the source identified and that their contents have not been changed. This is analogous to knowing that a letter really came from the addresser and that no one has tampered with the envelope. Such communications come from a variety of sources, including fellow employees, suppliers, business partners, and customers. They may also come in some variety of forms, the most common of which are e-mail messages, World Wide Web pages, and file downloads from servers.

Non-repudiation is the ability to build a situation in which the sender of a message cannot easily deny having sent it. For most purposes, this is the electronic equivalent of a signature. (The service ComTrust™ offers more closely resembles a notarized signature.) The importance of non-repudiation in medical and financial messaging cannot be overstated.

Today, businesses and individuals routinely receive important memos and data from fellow employees, suppliers, and business partners, as well as orders from customers. As e-commerce becomes even more ubiquitous, one can see a time coming when even the most important transactions take place electronically, including major contract agreements between corporations. The banking industry already moves incredibly large fund amounts electronically. The ability to verify the authenticity of communications and hold the senders accountable has always been fundamental



---

to business; this is no less true in the electronic information age. Note also that the federal government has declared electronic signatures legally binding by law.

#### *e-Security: The External Perspective*

The view from the external perspective is essentially the same with the additional issue of secrecy. When a message is sent to a business partner, it is often intended for eyes of that person or company only. To successfully conduct business, a healthcare organization needs assurance that communications are not being monitored by others for whom they were not intended. This security is absolutely required for conducting any electronic transactions involving patient data over open networks, such as the Internet.

#### *e-Security: The Bottom Line*

Security is basic to business for both the senders and the receivers of information. If e-commerce is to flourish, individuals and business must feel confident that their communications are verifiable and confidential. Most of the hesitation shown toward e-commerce today is related to security/privacy. ComTrust™ will give a new sense of confidence to those who are involved in this rapidly growing field.

### **Combining PKI with Typical Security**

There are two basic types of users today: those who operate from one location (non-roaming) and those who log on to systems from different locations and equipment (roaming).

#### *Non-roaming Users*

Security for non-roaming users—users who operate from a single location—is less problematic than security for roaming users. Because non-roaming users always use the same computer, secret information (the encryption key) is stored on the user's hard disk, which matches information on the server. Since the encryption key is stored, it can be far more complex than a typical password, making information encoded with impossible for intruders to decode.

#### *Roaming Users*

The basic problem with security for roaming users is giving the user an encryption key that won't fall into the wrong hands, yet will always be readily available. Passwords are limited in their usefulness because the human mind doesn't work well with seemingly random combinations of letters and numbers, particularly those that change regularly. As a result, passwords are typically short and easily memorized. Despite the usual admonitions to mix letters and numbers and upper and lower case, a strong password-cracking program can discover most in a matter of minutes (usually seconds). Many can be guessed. The solution to this is Public Key Infrastructure (PKI).



---

### *What is PKI?*

Public Key Infrastructure (PKI) generally refers to a range of authentication systems that use a “public key” as well as some other “private key” (password or other encoding that may be either of the user’s choosing or may be assigned by a system and stored on disk or card) to authenticate users. The requirement of both keys increases security over simply using a password (which could be guessed). Users are issued tickets, usually referred to as “authentication certificates,” that are stored on the server and act as their gateway to broader communications. When users want to connect to another server, they use their password (over an encrypted communications line) to identify themselves to the server holding their ticket. That server, having authenticated the user, then makes a secure connection with the destination server and uses very strong authentication methods to identify itself and the user to the other server.

Another approach uses Smart Cards that have complex keys stored on them. The user doesn’t have to remember a password. Once the card is plugged in, the user is identified.

### *Weaknesses of Most PKI Systems*

Most PKI systems use the credentials servers described above. While they are fairly robust, they have weaknesses that can allow access by savvy criminals. Weaknesses include an inflated sense of security among users and susceptibility to a number of different kinds of attack, including direct attack, lockout disablement, and insider attack. Let’s have a brief look at each of these weaknesses.

The sense of security that users often have when told they are using “a secure mode of communication” tends to lead them to use easy-to-guess passwords. It’s like having a massive steel lock on your door and keeping the key in the mailbox. Direct attack involves an intruder finding a “back door” into a server. This may not be easy, but it is, unfortunately, accomplished routinely. Once the server has been accessed, the passwords of hundreds or thousands of users can be readily accessible. Even if a would-be intruder cannot gain access to the server’s password list, he or she might disable the lockout mechanism. A lockout mechanism prohibits access to a user after the wrong password has been entered a certain number of times. If this is disabled, the criminal can make as many attempts at guessing a password as he or she wants, usually using programs that systematically generate every possible password at high speeds

While Smart Cards offer a robust solution because the keys stored on them are complex, non-copyable, and unknown to the user, they are somewhat expensive at present and require special readers attached to any device from which the user wants to communicate. These readers, which could easily be available at computers in a healthcare facility, would not be available to users from other locations. While Smart Cards may be an important part of a total internal solution, they probably do not represent the best solution for remote users.



---

## ComTrust™/VeriSign's Approach to PKI

The numerous problems discussed in the previous section are overcome by a unique approach used by ComTrust™ and VeriSign, which involves the use of multiple servers and operators (sometimes in different companies) so that it would be necessary to break into more than one server to undermine security and insider attacks require collusion. *Authentication is only possible when all of the servers work together, and none of the individual servers knows the resulting key.*

### *How It Works*

The method created by ComTrust™ and VeriSign is based on a password-hardening procedure in which multiple servers interact with the client's computer to "harden" (make mathematically complex) the user's password into a strong secret without learning either the user's password or the hardened result. The hardened password is then combined to obtain additional secrets, which none of the servers can determine alone. The value of the method is that the only way to crack the code is to control all of the servers.

The number of possible codes is nearly 1.1 trillion for international clients (limited to this by federal law) or somewhat more than 340 trillion trillion trillion (3.4 followed by 38 zeroes) for U.S. and Canadian clients. These are referred to as 40-bit and 128-bit encryptions, respectively. Note that the latter is 309 septillion times "stronger" than the former.

In addition to the mathematically complex encryptions, the requirement of a number of servers contributing to authentication, and the number of possible codes, there is another basic precaution. The number of times each server contributes to the hardening of a key is recorded. This number is then checked against the number of times successful authentication occurs, giving a result that could be called a failure/success rate. If the rate of failure reaches a suspicious level, it is assumed that this is the result of break-in attempts rather than accidental password typos, and the system locks out further authentication until the situation has been investigated and new keys (referred to as "certificates") have been issued.

While the use of 40- and 128-bit keys and failure-rate certificate revocations described here are widely used in PKI, the important difference to the ComTrust™/VeriSign method is the use of multiple servers with multiple operators for authentication. This makes it impossible for any one machine or person to know the key. The only way authentication takes place is if all of the servers, controlled by different operators and companies, have made their necessary contributions.

### *Closed vs. Open PKI*

One way of classifying PKI is in the distinction between "closed" and "open." "Closed" refers to when a computing architecture (method, program, design) identifies one that is proprietary and not widely shared. "Open" architectures, on the other hand, are available to anyone for inspection so that others can design compatible programs and systems. There are numerous disadvantages



---

to closed PKI and myriad advantages to open PKI. There is really only one aspect of closed PKI that can notably be called an advantage over open PKI: secret code. Because of the ComTrust™/VeriSign approach to PKI, this single issue is, for us, moot. The following paragraphs discuss the value of open over closed PKI.

Closed PKI requires that code is proprietary, so PKI software must be installed on every desktop. Further, applications using the PKI require a proprietary software interface from the PKI vendor. The disadvantages are obvious. With closed PKI, the vendor dictates what desktop software must be used by everyone involved. In addition, all users must assume the burden and cost of installing, updating, and troubleshooting this special software.

#### **True Story:**

Not long ago, a version of a popular Web browser was released by a well-known PKI software vendor. The browser had been customized to interface to that PKI vendor's products using a proprietary interface. When later versions of the browser were produced by the browser's original manufacturer, however, they would not work with the same PKI. As a result, the PKI customers were stuck having to use the obsolete browser.

With open PKI (used by ComTrust™/VeriSign), on the other hand, native applications interface to the PKI using industry-standard interface protocols or tailored interfaces agreed through PKI-application vendor partnerships. The advantages are the converse of closed PKI's disadvantages: no proprietary PKI-software is needed on the desktop, and there are no upgrade burdens to users.

The one major advantage to closed PKI is its very foundation: the secrecy of the PKI code itself. By keeping the programming underlying the PKI a secret, the system can be maintained in a fairly secure state. In addition to those previously mentioned, there may be another significant weakness: it assumes that no one will unravel that code. Given the sophistication of today's e-criminals, that may not be such a safe assumption.

The ComTrust™/VeriSign architecture uses open PKI for all of its advantages without sacrificing the one offered by a closed architecture. The use of multiple servers and operators not only nullifies the need for closed PKI, it offers something more powerful. If someone discovers the coding tricks and keys used in a closed system, it is no longer a closed architecture but an open door. Our technique allows everyone to understand how the lock works, yet denies intruders access by the necessary collaboration of multiple servers. In fact, VeriSign's PKI architecture is recognized by 98% of all of the Web browsers on the market today.

#### *Consistency of Service*

ComTrust and VeriSign can ensure solid, consistent service due to total redundancy. Every server has at least one backup ready to come online immediately should the primary server fail.



---

Similarly, their data storage is fully redundant. In fact, every aspect of the system has a backup, not unlike a modern airliner: Databases, ISPs, telecommunications, and power are all fully backed with additional systems that are regularly tested. Further, VeriSign is prepared seven days a week, 365 days a year for disaster recovery from a geographically removed site in conjunction with ComDisco.

### *Security*

What would a security provider be without good security? No one wants to be guarded by a company that leaves its own doors unlocked at night. ComTrust and VeriSign operate state-of-the-art facilities with several layers of physical security. The personnel are carefully screened and trained, and have individually restricted access to the parts of the system for which they are responsible. They follow strict guidelines as outlined in VeriSign's Certification Practices Statement (CPS). The facility and its personnel are subjected to stringent security audits.

### *Scalability*

No matter the size or the growth potential of a system, ComTrust<sup>TM</sup>/Verisign offer all the support needed. It is a given that current systems often grow exponentially. The ability to deal with changing scales is built into our underlying structure. We use multi-processor servers, high-performance transaction engines, multi-unit cryptographic hardware banks, and scaleable Oracle database technology.

### *Directory/Database Technology*

ComTrust/Verisign can accommodate a variety of directory/database systems with PKI integration, including X.500-technology directories, Web-based LDAP directory servers, traditionally supplied DBMS systems, and a variety of legacy systems.

### **ComTrust<sup>TM</sup>/VeriSign's Leadership in Establishing Certification Authority Standards**

The careful reader may note that this section belongs logically with the earlier discussion of security within ComTrust<sup>TM</sup> and VeriSign. It has been held for last because the security issue is seemingly routine (however important). This is not.

VeriSign's Certification Practices Statement is a carefully developed document that spells out the practices required within its VeriSign Trust Network, of which ComTrust<sup>TM</sup> is a part. It is unusual in that it is considered the most comprehensive document of its type in the world and is emulated by others as a foundation for PKI practices. Its significance is that, by being a leader in establishing international practices, VeriSign also ensures that its practices are stable over time and its profile is high. ComTrust is proud to be a member of that network.

It is VeriSign's specific intent to continue leading the way in authentication technology and practices establishment the world over. ComTrust will be a part of that leadership.



---

## **Summary/Review**

All businesses need to ensure the security, integrity, and “non-repudiability” of communications. This is particularly true of the healthcare industry under HIPAA. PKI is a means to that end.

PKI is a method of verifying the authenticity of electronic communications by using both public and private keys. PKI architectures can be either closed or open. Closed PKI uses proprietary secret software to help ensure security. Open PKI has the advantage of not requiring the user to own software particular to the PKI vendor or to worry about upgrades. The ComTrust™/VeriSign approach to PKI is able to take advantage of open PKI because multiple servers are used. Further, the method is extremely secure because multiple servers must contribute to authentication; the failure of one server to participate leads to failed authentication, and no server ever holds the key.

*For more information about HIPAA, and how your organization can achieve compliance, please see the Superior Consultant Company Web page [www.superiorconsultant.com](http://www.superiorconsultant.com), email us at [HIPAA@superiorconsultant.com](mailto:HIPAA@superiorconsultant.com), or call us at (248) 386-8300.*

*For more information about PKI and ComTrust™, please see the ComTrust™ web page [www.ComTrustTM.com](http://www.ComTrustTM.com), or call us at (248) 226-4005.*