LANL CST-7 TWCP Project

Steve Z. 5/14/97

TWCP Messaging Security

An analysis of issues related to electronic message security and authentication

John T. Zoltai, CSP
LANL CIC-12
TWCP Project Software Architect
zsys@lanl.gov (505) 665-0974

1

Overview

The Problem

Background

The Los Alamos National Laboratory (LANL) Trans-uranic Waste Certification Project (TWCP) is tasked with managing the process of validating trans-uranic waste and transporting it to the Waste Isolation Pilot Plant (WIPP). To accomplish this, a formal workflow process has been defined, involving multiple personnel at LANL, WIPP, the Department of Energy (DOE), and other organizations.

The normal technique of creating, copying, transporting and storing paper forms and authorization documents will impose a significant cost load on the entire project, and insert substantial delays into every phase of the workflow process. Use of electronic messaging systems and multi-user databases will minimize these costs. WIPP currently requires electronic database communication between the TWCP database and the WIPP Waste Information System (WIPP) for waste stream, container, and payload authorization requests, and it is anticipated that electronic messaging will be used for acceptance and rejection messages related to these requests.

The purpose of this document is to describe the issues associated with the transmission of electronic messages containing sensitive unclassified information over the Internet. Currently, there are no DOE or LANL standards or guidelines established for this type of communication.

In addition, this document addresses the issues of authenticating the author of an electronic message, or the user of a multi-user information system, where the information system itself processes sensitive unclassified information.

Contents

Chapter 2 describes the problems inherent in transmission of sensitive messages across a non-secure network, as well as descriptions of the terms and methodologies for digital signatures and document encryption.

Chapter 3 describes the methods used to provide user authentication and security in multi-user databases.

Chapter 4 compares and contrasts paper-based messaging and electronic messaging.

Chapter 5 presents requirements and recommendations for implementing secure transmission of electronic messages.

2

Securing Electronic Messages

Security requirements and solutions

Security Requirements

The following are five central security requirements associated with sensitive unclassified electronic messaging:

Confidentiality

Confidentiality refers to ensuring that data is not disclosed to unauthorized persons. A very common network security attack consists of a software program that monitors the data stream across the network, looking for messages addressed to a specific destination. These messages are then “copied” on the fly, without disturbing the flow of network traffic. The message proceeds to the recipient, who is unaware that some “opened the envelope and peeked” at the message.

Access Control

Access Control refers to ensuring that only those who are authorized to view or modify data can access that data. In some cases, sensitive information is intended to be viewed by a single, specific recipient. A method needs to be in place to restrict access to just that single person.

Integrity

Integrity refers to ensuring that the data has not been altered since it was originally created. There are numerous situations in which integrity of data is critical; for example, a "hacker" could potentially tamper with an electronic message enroute, unknown to either the sender or recipient.

Data Origin Authentication

Data Origin Authentication refers to providing proof of the source of data. For example, it is possible to generate messages that appear to be from a specific sender without the sender's knowledge. In the TWCP system, this opens up the possibilities of third parties generating falsified certification and authorization messages to or from WIPP.

Non-repudiation

When someone repudiates involvement in a situation under dispute, they deny having any involvement in the problematic situation. Non-repudiation in the context of electronic messaging means someone cannot deny the authorship of a specific message.

Solutions

Encryption and digital signatures offer solutions to the five fundamental network security requirements described above. Two approaches are used:

Encryption

Encryption addresses the confidentiality and access control requirements. Encryption can be used to make a file private so that only authorized personnel can decrypt the file to read the information.

Digital Signatures

A Digital Signature addresses the integrity, authentication, and non-repudiation requirements. A digital signature is analogous to a handwritten signature in that a digital signature can be used to assure a reader of the authenticated source of the information (authentication, non-repudiation). In addition, a digital signature can ensure that any unauthorized changes to the data will be detected (integrity).

3

Database Security

Traffic security and user authentication

Security Requirements

Like electronic messages, multi-user databases often make use of non-secure networks to maintain the communications pathway between the end users and the central database. As a result, all of the security issues described for messaging apply to database security, but the approaches are not identical.

Traffic Security

In a database, both the client software and the server software are prescribed. When security is required, client and server software is selected that provides automatic encryption of all traffic in a manner that is transparent to the end user. In a messaging system, the sender needs to specify whether the message is to be encrypted or not, depending on the level of security of the message and the capabilities of the recipient.

WIPP requires the use of Oracle Secure Network Services (SNS) to transfer data to the WWIS database. Accordingly, TWCP will use an Oracle server with SNS to store and forward the appropriate data to WWIS. The main TWCP database will use 4th Dimension, an integrated client/server database that automatically provides encryption between clients and the server.

Therefore, database traffic security issues are not a concern at this time.

User Authentication

An end user can generate a large number of transactions in a database, whether it is entering new records, updating existing records, or initiating automated tasks or reports. Since a large amount of data can be effected very quickly, it is important to insure that the end user associated with a specific transaction is in fact the correct person (authentication, non-repudiation).

Since the database handles the traffic security requirements, and the number of "messages" generated during a typical session may be quite large, it is impractical for a user to apply a digital signature to each action taken. Typically, the application of a digital signature is manually initiated when the user finishes composing a message. To force each user to initiate a signature action with each database transaction would quickly lead to rejection of the system.

However, the database cannot make the mistake of assuming the user that logged on at 8 AM and is still connected six hours later is the same person. The probability of a client workstation being left unattended over that time frame is very high. To mitigate this, LANL has implemented a user authentication system using SecurID cards (smartcards) and a central smartcard verification server.

A smartcard requires the entry of a secret Personal Identification Number (PIN), and presents a passcode that changes once a minute for three minutes. After that, the smartcard presents a series of random, non-valid passcodes. A smartcard is permanently signed out to a single user. Typically, the user keeps the smartcard on their person at all times. Since a passcode is only good for one minute, it's non-encrypted presence on the network does not present a security threat, especially since the database software can prevent simultaneous logons by the same user.

During the logon process, the database application requests users to enter their smartcard passcode along with their employee ID number. The passcode is validated against the SecurID server, and if valid, a timer is set to monitor inactivity. If the client application sees no transaction actions for more than pre-determined time period, the timer expires, while the application remains available in its present state. When the user commits the next transaction, the smartcard passcode is requested and re-validated. This allows users to continue long sessions of work without constantly re-authenticating themselves, and provides a higher degree of authentication than a one-time password entry at logon.

4

Paper-based vs. Electronic Messaging

A comparison and contrast

Paper-based Messaging

Organizations treat paper-based messages as very formal documents, usually requiring a formal letterhead or memorandum format. This is usually accomplished by direct retrieval of stationery from a central storage device. Actual composition of the message takes approximately twice as long as an electronic message, because the background and reason for the message need to be described in order to establish the proper context, before the actual heart of the message can be written. Total effort so far: 20 minutes.

After the message is composed, formal messages require some sort of tracking number. This is usually accomplished by looking up the number from a list, or requesting it via phone from a person responsible for issuing numbers. Total effort so far: 25 minutes.

After the number is assigned and the message is printed, the paper is initialed or signed by the sender. The message is then placed in an envelope and sent off in the normal daily mail. Total effort so far: 30 minutes.

Mail transportation delays of one to ten days are then incurred, after which the recipient receives the message, tags it with a receiving identification number, makes a copy, and files the original. Total effort so far: 40 minutes (not counting transportation effort).

Electronic Messaging

The sender, when responding to a message, simply hits the Reply button in the email software, and a new message, quoting the original message, is created. The context of the message is immediately established, reducing the total composition time to 10 minutes.

The sender then hits a button to have the message sent. The software, if necessary, automatically attaches the sender's digital signature to the message and sends it off to the mail server. Total effort so far: 10 minutes.

The mail server transfers the message to the recipient's mail server. Typical transportation delay is 10 to 30 minutes, depending on the configuration of the servers and the network.

The message arrives at the recipients' system, and is presented the next time the recipient checks in with their email software. The software retrieves the message, automatically validates the digital signature, and if set up properly, automatically files the message in the appropriate subject area. Total effort so far: 10 minutes.

Comparison

The additional costs imposed by a paper system consist of additional staff load for message generation, logging, transportation, receiving, and filing appropriately

The electronic message is approximately four times more efficient in the scenario described above, discounting transportation costs. Circumstances may vary, but in no case is a paper-based system faster, more convenient, or more secure than an electronic messaging system. This is why the use of electronic messaging has revolutionized the way organizations communicate, and why congress is now under pressure to establish a formal mechanism whereby digital signatures carry the same legal weight as a physical signature. We just don't have the time or money to do it the old way anymore.

5

Recommendations

Implementing secure electronic messaging

Requirements

The requirements for secure electronic messaging depend on the sensitivity of the content of the message body. The greatest majority of electronic messages are non-sensitive in nature, leaving a few remaining messages that contain sensitive information.

Non-secure messaging

For non-secure messages, full encryption is not required. A digital signature should be attached to validate the identity of the sender, but that is all. Non-sensitive messages can be broadcast to multiple parties, and those parties are free to re-broadcast those messages without regard to controlling their distribution.

Secure messaging

Messages containing sensitive information require full encryption to protect them during transmission. In addition, the issue of multiple-party broadcasting and re-broadcasting must be addressed. With public/private key cryptography, a message is encrypted by the sender using the public key of the intended recipient. This insures confidentiality of the document in transmission, as well as allowing only the intended recipient to decrypt the document with their personal secret key.

This approach restricts multiple-party broadcasts. The sender must encrypt a separate copy of the message with the public key of each intended recipient and transmit it separately. While this does add some overhead to the process, the additional security provided eliminates any possibility of the message being inadvertently sent to the wrong person, or to a list of people not under the direct control of the sender.

Recommendations

Current software exists to allow public/private key digital signatures and message encryption in combination with current electronic mail software. Some encryption software packages support one range of e-mail products, other packages support other e-mail products. At LANL, the e-mail standard is Eudora for both Mac and PC. At WIPP, the standard is ********. The standards for all involved parties need to be determined. At that point, the encryption software that supports the greatest majority of e-mail packages should be selected for implementation.

Post-it® Fax Note 7671	Date 5-8-97	# of pages ▶ 3
To CRAIG	From J.R.	
Co./Dept.	Co.	
Phone # 7452	Phone # 8256	
Fax # 7430	Fax #	

CHAPTER 14

Records, Legal Notices and Oaths

Art.
15. Electronic Authentication of Documents, 14-15-1 to 14-15-6.

ARTICLE 3

Public Records

14-3-1. Short title.

Cross references. — For the Electronic Authentication of Documents Act, see Chapter 14, Article 15 NMSA 1978.

14-3-15.2. Electronic authentication; substitution for signature.

Cross references. — For the Electronic Authentication of Documents Act, see Chapter 14, Article 15 NMSA 1978.

ARTICLE 9

Records Affecting Real Property

14-9-1. Instruments affecting real estate; recording.

Verbal consent to assignment. — A party's verbal consent to an assignment of an interest in a real estate contract is not a substitute for perfection of that interest by recording. Mazer v. Jones, 184 Bankr. 377 (D.N.M. 1995).

14-9-3. Unrecorded instruments; effect.

Verbal consent to assignment. — A party's verbal consent to an assignment of an interest in a real estate contract is not a substitute for perfection of that interest by recording. Mazer v. Jones, 184 Bankr. 377 (D.N.M. 1995).

ARTICLE 15

Electronic Authentication of Documents

14-15-1. Short title.

This act [14-15-1 to 14-15-6 NMSA 1978] may be cited as the "Electronic Authentication of Documents Act".

History: Laws 1996, ch. 11, § 1.

Cross references. — For electronic authentication as substitution for a signature on any document, see 14-3-15.2 NMSA 1978.

Effective dates. — Laws 1996, ch. 11, § 8, makes the Electronic Authentication of Documents Act effective July 1, 1996.

14-15-2. Purpose.

The purpose of the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978] is to:

A. provide a centralized, public, electronic registry for authenticating electronic documents by means of a public and private key system;

B. promote commerce; and

C. facilitate electronic information and document transactions.

History: Laws 1996, ch. 11, § 2.

Effective dates. — Laws 1996, ch. 11, § 8, makes the Electronic Authentication of Documents Act effective July 1, 1996.

14-15-3. Definitions.

As used in the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978]:

A. "archival listing" means entries in the register that show public keys that are no longer current;

B. "authenticate" means to ascertain the identity of the originator, verify the integrity of the electronic data and establish a link between the data and the originator;

C. "document" means any identifiable collection of words, letters or graphical knowledge representations, regardless of the mode of representation. "Document" includes correspondence, agreements, invoices, reports, certifications, maps drawings and images in both electronic and hard copy formats;

D. "electronic authentication" means the electronic signing of a document that establishes a verifiable link between the originator of a document and the document by means of a public key and private key system;

E. "key pair" means a private key and its corresponding public key that can verify an electronic authentication created by the private key;

F. "office" means the office of electronic documentation;

G. "originator" means the person who signs a document electronically;

H. "person" means any individual or entity, including:

(1) an estate, trust, receiver, cooperative association, club, corporation, company, firm, partnership, joint venture or syndicate; and

(2) any federal, state or local governmental unit or subdivision or any agency, department or instrumentality thereof;

I. "private key" means the code or alphanumeric sequence used to encode an electronic authentication that is known only to its owner and that is the part of a key pair used to create an electronic authentication;

J. "public key" means the code or alphanumeric sequence used to decode an electronic authentication that is the part of a key pair used to verify an electronic authentication;

K. "public and private key system" means the hardware, software and firmware provided by a vendor for the following purposes:

(1) to generate public and private key pairs;

(2) to produce a record abstraction by means of a secure hash code;

(3) to encode a signature block and a record abstraction or an entire document;

(4) to decode a signature block and a record abstraction or an entire document; and

(5) to verify the integrity of a document;

L. "record abstraction" means a condensed representation of a document that is prepared by using a secure hash code;

M. "register" means a database or other electronic structure that binds a person's name or other identity to a public key;

N. "revocation" means the act of notifying the secretary that a public key has ceased or will cease to be effective after a specified time and date;

O. "secretary" means the secretary of state;

P. "secure hash code" means a mathematical algorithm that, when applied to an electronic version of a document, creates a condensed version of the document that makes it computationally impossible to identify or re-create the document without essential knowledge of that document; and

Q. "sign" or "signing" means the execution or adoption of any symbol by a person with the intention to establish the authenticity of a document as his own.

History: **Laws 1996, ch. 11, § 3.**
Effective dates. — Laws 1996, ch. 11, § 8, makes the Electronic Authentication of Documents Act effective July 1, 1996.

14-15-4. Office of electronic documentation; powers and duties.

The "office of electronic documentation" is established under the secretary of state. The office shall maintain a register of public keys for electronic authentications made in accordance with standards adopted pursuant to the provisions of Section 14-3-15.2 NMSA 1978. The office shall register public keys for public officials, persons who wish to transact business with the state and any other person when registration will promote the purposes of the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978]. The register shall include both current listings and archival listings.

History: **Laws 1996, ch. 11, § 4.**
Effective dates. — Laws 1996, ch. 11, § 8, makes the Electronic Authentication of Documents Act effective July 1, 1996.

14-15-5. Regulations.

A. The secretary shall adopt regulations to accomplish the purposes of the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978].

B. The regulations shall address the following matters:

(1) registration of public keys;

(2) revocation of public keys; and

(3) reasonable public access to the public keys maintained by the office.

C. The regulations may address the following matters:

(1) circumstances under which the office may reject an application for registration of a public key;

(2) circumstances under which the office may cancel the listing of a public key; and

(3) circumstances under which the office may reject an attempt to revoke registration of a public key.

History: **Laws 1996, ch. 11, § 5.**
Effective dates. — Laws 1996, ch. 11, § 8, makes the Electronic Authentication of Documents Act effective July 1, 1996.

14-15-6. Contracting services.

The secretary may contract with a private, public or quasi-public organization for the provision of services under the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978]. A contract for services shall comply with regulations adopted pursuant to the Electronic Authentication of Documents Act and the provisions of the Public Records Act [Chapter 14, Article 3 NMSA 1978] and the Procurement Code.

History: **Laws 1996, ch. 11, § 6.**
Effective dates. — Laws 1996, ch. 11, § 8, makes the Electronic Authentication of Documents Act effective July 1, 1996.

Procurement Code. — See 13-1-28 NMSA and notes thereto.

New Mexico took a California style approach with a minimum statute, and the Public Records Commission issued standards. The Secretary of State is authorized to establish a registration (not certification) system, and was going to set up a server this fiscal year but the $70,000 appropriation was vetoed, by the same governor who stated that this was one of the important initiatives of his administration.

The basic statute in New Mexico is:

In the Public Records Commission statutes:

Section 14-3-15.2. Electronic authentication; substitution for signature.

Whenever there is a requirement for a signature on any document, electronic authentication that meets the standards promulgated by the commission may be substituted.

END STATUTE

The standards promulgated by the Public Records Commission and issued as regulations effective July 1, 1996 are not yet in the Michie compilation. I need to check and see why.

The Secretary of State provisions are: Chapter 14 Article 15 ELECTRONIC AUTHENTICATION OF DOCUMENTS

14-15-1. Short title.

This act [14-15-1 to 14-15-6 NMSA 1978] may be cited as the "Electronic Authentication of Documents Act".

14-15-2. Purpose.

The purpose of the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978] is to:

A. provide a centralized, public, electronic registry for authenticating electronic documents by means of a public and private key system;

B. promote commerce; and

C. facilitate electronic information and document transactions.

14-15-3. Definitions.

As used in the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978]:

A. "archival listing" means entries in the register that show public keys that are no longer current;

B. "authenticate" means to ascertain the identity of the originator, verify the integrity of the electronic data and establish a link between the data and the originator;

C. "document" means any identifiable collection of words, letters or graphical knowledge representations, regardless of the mode of representation. "Document" includes correspondence, agreements, invoices, reports, certifications, maps, drawings and images in both electronic and hard copy formats;

D. "electronic authentication" means the electronic signing of a document that establishes a verifiable link between the originator of a document and the document by means of a public key and private key system;

E. "key pair" means a private key and its corresponding public key that can verify an electronic authentication created by the private key;

F. "office" means the office of electronic documentation;

G. "originator" means the person who signs a document electronically;

H. "person" means any individual or entity, including:

(1) an estate, trust, receiver, cooperative association, club, corporation, company, firm, partnership, joint venture or syndicate; and

(2) any federal, state or local governmental unit or subdivision or any agency, department or instrumentality thereof;

I. "private key" means the code or alphanumeric sequence used to encode an electronic authentication that is known only to its owner and that is the part of a key pair used to create an electronic authentication;

J. "public key" means the code or alphanumeric sequence used to decode an electronic authentication that is the part of a key pair used to verify an electronic authentication;

K. "public and private key system" means the hardware, software and firmware provided by a vendor for the following purposes:

(1) to generate public and private key pairs;

(2) to produce a record abstraction by means of a secure hash code;

(3) to encode a signature block and a record abstraction or an entire document;

(4) to decode a signature block and a record abstraction or an entire document; and

(5) to verify the integrity of a document;

L. "record abstraction" means a condensed representation of a document that is prepared by using a secure hash code;

M. "register" means a database or other electronic structure that binds a person's name or other identity to a public key;

N. "revocation" means the act of notifying the secretary that a public key has ceased or will cease to be effective after a specified time and date;

O. "secretary" means the secretary of state;

P. "secure hash code" means a mathematical algorithm that, when applied to an electronic version of a document, creates a condensed version of the document that makes it computationally impossible to identify or re-create the document without essential knowledge of that document; and

Q. "sign" or "signing" means the execution or adoption of any symbol by a person with the intention to establish the authenticity of a document as his own.

14-15-4. Office of electronic documentation; powers and duties.

The "office of electronic documentation" is established under the secretary of state. The office shall maintain a register of public keys for electronic authentications made in accordance with standards adopted pursuant to the provisions of Section 14-3-15.2 NMSA 1978. The office shall register public keys for public officials, persons who wish to transact business with the state and any other person when registration will promote the purposes of the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978]. The register shall include both current listings and archival listings.

14-15-5. Regulations.

A. The secretary shall adopt regulations to accomplish the purposes of the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978].

B. The regulations shall address the following matters:

(1) registration of public keys;

(2) revocation of public keys; and

(3) reasonable public access to the public keys maintained by the office.

C. The regulations may address the following matters:

(1) circumstances under which the office may reject an application for registration of a public key;

(2) circumstances under which the office may cancel the listing of a public key; and

(3) circumstances under which the office may reject an attempt to revoke registration of a public key.

14-15-6. Contracting services.

The secretary may contract with a private, public or quasi-public organization for the provision of services under the Electronic Authentication of Documents Act [14-15-1 to 14-15-6 NMSA 1978]. A contract for services shall comply with regulations adopted pursuant to the Electronic Authentication of Documents Act and the provisions of the Public Records Act [Chapter 14, Article 3 NMSA 1978] and the Procurement Code.

END STATUTE

The Secretary of State has not issued regulations, primarily because of the vetoed appropriation.

The New Mexico statutes and regs just went up on the net. They are at:
http://www.michie.com/Code/NM/NM.html

Michie's NM Internet Resources New Mexico Statutes New Mexico Administrative Code

There was an ABA discussion group in 1994, but I have no archives nor pointer. My own view and that of the New Mexico Advisory Committee was that the ABA/Utah approach was totally wrongheaded by getting involved with certification and the liability issues that go along with it. We perferred to believe that the commercial community would accept the _procedural_ safeguards build into the Secretary of State's system. Especially since state Government would be accepting those safeguards as adequate. But I guess we won't know until next year.

The feds have some interesting technical stuff on the net, NIST is at http://www.nist.gov/welcome.html The FIPS from NIST are available electronically from Computer Security Resource Clearinghouse (CSRC) at: http://csrc.nist.gov A couple titles are:

FIPS 186, Digital Signature Standard (DSS), U.S. DOC/NIST, May 19, 1994.

FIPS 180-1, Secure Hash Standard (SHS), U.S. DOC/NIST, April 17, 1995.

We used them in defining New Mexico's standards, but sparingly.

The CSL Bulletrins also make interesting reading:
http://cdrom.com/pub/security/coast/mirrors/csrc.ncsl.nist.gov/nistbul/ presumedly also:
http://csrc.ncsl.nist.gov/nistbul/

There are often interesting discussions on the USENET groups sci.crypt and comp.security.pgp.tech

I hope some of this helps.

--

Thaddeus P. Bejnar

<!-- Author: Wisconsin Department Of Health and Social Services -->
<!-- Date: 2/27/97 -->
<!-- File Path: /dhfs/pubs/html/22096.html -->
<!-- SourceFile: /usr/httpd/test/genweb/dhfs/pubs/litehtmls/22096.txt -->
<!-- Description: 2/12/96, First in the Nation -- DHSS Using Electronic Signature Tech to Speed Social Security Disability Applications -->

<TITLE>2/12/96, First in the Nation -- DHSS Using Electronic Signature Tech to Speed Social Security Disability Applications</TITLE>

<dt>CONTACTS:
Jim Malone, (608) 266-1683<br>
William Shelton, (608) 266-1981

(MADISON, February 12, 1996)--Applicants for Social Security disability benefits will have a shorter wait for their eligibility determination, thanks to a Department of Health and Social Services technology initiative that's the first in the country.

DHSS Secretary Joe Leean announced today that his department has hired the Wisconsin Health Information Network to provide network connectivity and electronic signature technology to help speed communications between physicians and DHSS in determining applicants' medical eligibility.

"We've seen time savings of up to two-thirds in the pilot project," said DHSS Secretary Joe Leean. "Bringing up this leading edge technology statewide will help us serve our customers better by speeding up the application process."

Leean said the pilot project involved three health care professionals who tested the system last year.

As part of the disability determination process, the department's Disability Determination Bureau contracts with physicians to obtain physical or psychological exams in about 25 percent of the 60,000 claims filed each year. Previously, reports were typed and mailed to the physicians, who reviewed, signed and returned them to the bureau.

By transmitting reports directly from the physician's computer, WHIN helps eliminate paper work and saves time.

"It cuts out all the mailing time and it's more convenient for the physicians," said Bureau Director William Shelton. "Also, if a physician needs to make changes to a report before approving it, he or she can easily do it right on the computer screen, instead of marking up a hard copy and returning it for correction."

WHIN is the nation's first fully functional health information network. It electronically connects physicians, clinics, hospitals and other health care organizations. WHIN membership currently includes 14 hospitals and more than 1,300 physicians, as well as seven insurance organizations.