

Memo of Meeting

Date: April 19, 2002

Location: 1350 Piccard Drive, Rockville, Maryland 20850

Representing Vector Intelligence, Inc.
2200 Benjamin Franklin Parkway, Suite 514-South
Philadelphia, PA 19130

John C. Gregory, Interim CEO
Eric Rugart, Acting Chief Technology Officer

Representing FDA:

Charles Snipes, Compliance Officer, Center for Drug Evaluation and Research
Allen Wynn, Consumer Safety Officer, (detailed to Office of Enforcement from)
Center For Devices and Radiological Health
Scott MacIntire, Director, Division of Compliance Information and Quality
Assurance, Office of Enforcement
Tom Chin, Consumer Safety Officer, Office of Enforcement
Paul J. Motise, Consumer Safety Officer, Office of Enforcement

The meeting was held at the request of the Vector Intelligence representatives, to discuss their biometric based electronic signature software, BioSig™, in the context of 21 CFR Part 11. The firm promotes its product as enabling their users to meet requirements of part 11 and the Health Insurance Portability and Accountability Act. At the start of the meeting we explained that FDA does not formally review, approve or disapprove of products or services that enable people to comply with FDA regulations. We advised that the meeting would be an information exchange and that our comments should not be taken as formal FDA positions.

At the start of the meeting we also asked the representatives to tell us if they considered any information, including the contents of several publications they gave us, to be confidential, trade secret or otherwise of a nature that they would not want included in a publicly available memo of our meeting. The publications are attached.

The Vector Intelligence representatives explained that their company produces biometric electronic signature software that is intended to be used with digitizers that can provide x,y, and t coordinates where x and y are positions on the digitizer and t is time. The software measures 23 biometric vectors (parameters) including speed, stroke direction, and order associated with writing one's signature. The representatives explained that their software is capable of

measuring stylus pressure, as well, but that this feature is disabled due to background “noise”. The software uses technology developed by Bell Labs and patented by Lucent Technologies. The software is portable to Windows CE devices, the E-Pad and other PC based pad devices, but not to Palm platform devices.

The representatives explained that they developed their product primarily for use by healthcare/pharmacy companies that track drug samples.

During the meeting we discussed the firm’s validation efforts. The representatives said they would welcome customer audits of their software development activities. The firm will also provide software functional specifications and test scripts.

During the meeting we discussed the system’s false acceptance and false rejection rates. The representatives explained that the system has an error rate of about 1.2%. The software permits system administrators, but not end users, to configure and adjust the system’s sensitivity on a scale of 1 to 6 and the system accuracy on a scale of 1 to 200.

Biometric templates, against which a person’s signing action would be compared for authentication purposes, reside on either a remote server or the local computer. The representatives said they anticipated expanding to the use of smart cards that would hold the user’s template. The template takes 100 bytes of storage without a graphical image and 3K to 5K of storage with a graphical image of the signature.

We asked if the system was designed to adjust to changes in the biometric traits that may occur over time. We commented that such a feature was not a requirement of part 11 but that we had seen some systems that automatically adjusted to such changes. The representatives said that the system does not make such automatic changes and that over a period of time end users may need to be re-enrolled to account for the natural changes in how they execute a handwritten signature.

The representatives also explained that the system does not have a back-up identification code/password feature, (e.g., should an end user be injured or otherwise unable to execute a manual signature).

With respect to the manifestation of the biometric electronic signature, the representatives explained that the system displays the user’s printed name, date and time of signing and the purpose of the signature.

The meeting lasted about two hours.

cc:
FDA Attendees
HFA-224
Part 11 Guidance Dockets

Doc ID VectorIntelligenceMemoOfMeeting041902.doc
P. Motise 05/15/02

The BioSig™ Revolution

**“A lie can travel half way around the world while the truth is putting on its shoes.”
– Mark Twain**

Our dependence upon electronic techniques for creating and distributing documents, and conducting transactions of all types, is immense—and growing. We send and receive more information via email than we do through the postal service. We order billions of dollars of goods and services online. And we are under increased pressure, both financial and regulatory, to convert paper-based processes to electronic ones.

But how safe are our electronic transactions? When you transmit a confidential bid, can you be sure that it won't be intercepted? When you receive an emailed document, can you be sure that it was actually sent by the person on the “From” line? How can you be confident that the timesheet your employee filed electronically was never altered? We could keep asking questions like these, but we'd rather talk about the answer.

For Superior Data Security, Just Sign Here: with BioSig™

BioSig™ is a remarkable technology capable of addressing some of today's most serious information security and integrity issues. BioSig™ is an authenticating technology, a tool for positively determining whether a person is—or is not—who he or she claims to be. It has applications across a wide range of industries, and can be used in a multitude of different ways. BioSig™ works with inexpensive, off-the-shelf hardware to compare a person's signature with a

“Unlike fingerprints, retinal or DNA patterns which remain constant over time, the execution of a person's signature will be unique and individual at that particular moment. Handwriting remains one of the most powerful human identifiers that exist today.”

**-Marc Gaudreau, Forensic Sciences
Laboratory Manager, Canada
Customs and Revenue Agency**

reference file (or “model”). The process is fast, reliable, and exceptionally simple. There is nothing for the user to remember: they simply sign their own name on an electronic pad, on paper with an electronic pen, or on a handheld computer screen, and BioSig™ does the rest.

The software is exceptionally sophisticated. Developed originally by Bell Labs for Lucent Technologies, BioSig™ is true biometric security. It does not work by comparing the appearance of a signature with the model; a modestly-talented forger could easily defeat such a system. Instead, it takes dozens of different measurements of the

way in which the signature is entered to generate a file which is unique to the user. This makes BioSig™ a true behavioral biometric: there may be thousands of “John Smiths” in the world, but no two of them sign their name the same way.

“Cracking” biometric security measures is the stuff of movies: we've seen our heroes fool retinal scanners with clever contact lenses, or fingerprint readers with molds taken from other peoples' fingers. But there is no obvious way to fool BioSig™. A signature file cannot be intercepted and re-used, because the software knows that nobody signs their name quite the same way every

time—a perfect duplicate of a previously submitted signature is always rejected. The signature file includes an embedded time stamp, so that suspiciously old signatures can also be rejected. And since the file is utterly unintelligible if intercepted (it cannot be used to infer what the signature looked like, nor can it be modified in a way that evades the “no duplicates” rule), it can even be used safely in settings where transmission of the signature file is not entirely secure.

As with all biometrics, users need to be enrolled in the system to generate a signature model. This can be accomplished either through a dedicated enrollment (or “training”) session, where the user signs three to six times in succession (depending on the level of accuracy required by the application), or on a rolling basis—as the user signs their name in the ordinary course of business, a model is generated from the series of signatures. The model can be set to adapt over time to the almost imperceptible changes we make to our signatures.

BioSig™ has many applications. It can be used across a range of industries for access control (in lieu of a password or code number, for restricting access to networks or even buildings); to “lock down” documents and records, and prevent them from being altered (the digital signature can be “bound” to the document, so that the document carries its own proof of authorship and cannot be modified); and to meet “electronic signature” requirements under numerous state and federal laws and regulations while meeting real-world requirements for reliable, low-cost, user-friendly data security.

The Benefits of BioSig™

BioSig™ has numerous advantages over other approaches to signature verification, and other forms of data security, in many applications.

Market-Based Advantages

- **Low hardware costs and flexible hardware requirements:** BioSig™ works well with many different kinds of devices already in widespread use, including notebook computer touch pads, handheld computers, the tablet-based computers, and point-of-sale signature capture pads. It could also be used with stylus-enabled cell phones or other “convergence devices.”
- **Low administrative costs:** Signatures are not forgotten as passwords and PINs are, nor do they need to be changed routinely to thwart detection. Business costs for users may also be reduced, not only through fraud reduction, but also by replacing time-consuming visual signature comparison with automated verification in applications such as point-of-sale check cashing.
- **Durability:** Digital pads are rugged and virtually indestructible when compared to the cameras and sensors that enable other biometric technologies.

“I would say today that the weakest link in security management is that passwords are used to identify who is running the system.”

-Bill Gates

Technological Advantages

- **High Security:** BioSig™ technology consistently and accurately distinguishes authentic signatures from forgeries. It is highly reliable and offers enhanced security in many situations where none currently exists.
- **Robustness:** BioSig™ captures information about the process of signing a name, rather than the appearance of the signature, making it all but impossible to trick the system through forgery. The model signature used by BioSig™ for reference (and the file

transmitted during verification) contains no information about the appearance of the signature, or other intelligible information. And unlike an ID card or other “token,” a signature is not a physical object that can be stolen or left at home by its owner.

- **Portability:** The model file is exceptionally small, and can be located in a central database, a portable or handheld computer, or embedded in a smart card or magnetic stripe card (such as a credit card stripe). The attachment of a signature to a document (“signature binding”) works with any type or file format of document, and adds almost nothing to the size of the document.
- **Flexibility and Customization:** This technology can be used to verify a signature, initials, or even a password selected by the user. Risk tolerance can readily be adjusted, to minimize either false positives or false negatives, as business requirements dictate.

Behavioral Advantages

- **User-friendliness:** Unlike most other biometrics (such as fingerprint, hand, iris, or facial scanning), BioSig™ requires no change to user behavior, and is not seen as intrusive—many of the leading applications for BioSig™ are those where the user is already signing their name, and the only change is the use of a stylus instead of a pen.

Legal Advantages

- **Enforceability:** BioSig™ can be readily incorporated into applications that meet the requirements of numerous statutes and regulations, including the Electronic Signatures in Global and National Commerce Act (E-SIGN), Uniform Electronic Transaction Act (UETA), Health Insurance Portability and Accountability Act (HIPAA), 21 CFR Part 11, and others. Indeed, an application incorporating BioSig™ can generate such strong evidence of authorship, intent to be bound, and document integrity, as to lower the risk of dispute and the cost of dispute resolution. BioSig™ is also an outstanding tool for generating an enforceable audit trail for protecting intellectual property (e.g., when used for signing electronic lab notebooks in which patentable discoveries are described).

The advantages can be summarized as follows:

	BioSig	Finger Scanning/ Other Biometrics	Password	Card or “Token”
Low hardware costs	★	☒	★	☒
Versatile hardware (used for other purposes)	★	☒	★	☒
Multiple hardware vendors	★	☒	★	☒
Durable hardware	★	☒	★	★
Low administrative costs	★	(varies)	☒	☒
Hard to crack	★	★	☒	★
Can’t be lost or stolen	★	★	☒	☒
Can’t be forgotten	★	★	☒	☒
User-friendly	★	(varies)	☒	☒
Consistent with existing business practices	★	☒	★	☒

About The Technology

The core of BioSig™ is a set of patented, complex algorithms created by Bell Labs for Lucent Technologies. The major patents in the package are:

US 5,828,772: Method and apparatus for parametric signature verification using global features and stroke-direction codes

Signature verification techniques developed by other companies make use of so-called “global” features describing general characteristic of a signature, such as total time to sign. This patent secures the use of a combination of both “global” features of a signature, and “local” signature curve matching, to verify the authenticity of the signer. This technique provides for higher verification accuracy than reliance on global features alone.

US 5,898,156: Validation stamps for electronic signatures

This patent allows VII to engage not only in any signature verification business (as per patent 5,828,772), but also in the business of verifying the authenticity of electronic documents. The combination of these two technologies is critical for any document-oriented applications. Patent 5,898,156 describes a method of verifying that a given handwritten electronic signature was intended for the given electronic document. The technology covered in the patent prevents such forms of deception as the attachment of an authentic signature from one document to a different document. The patent also thwarts any attempt to fraudulently re-generate a handwritten signature and attach it to another document by re-constructing the timing information in a signature from its geometric shape as sampled by a tablet digitizer. It is oftentimes important to display a signature shape on an unencrypted portion of a document to visually present the signature to a user. However, such an image can present a security threat. The patent covers the entire concept of modifying the geometric characteristics of a signature to hide the signature stroke pattern and speed while preserving the shape of the signature.

Contact Us

The BioSig™ technology package is available for license, to be incorporated into your applications. Call us to see a demo, and to discuss pricing and other terms.

Joel E. Simkins
Chief Marketing Officer
Vector Intelligence, Inc.
604 S. Washington Sq. #1003
Philadelphia, PA 19106

(215) 923-5942
jsimkins99@earthlink.net

VECTOR INTELLIGENCE, INC.

On-line Handwritten Signature Verification A White Paper from Vector Intelligence, Inc.: January, 2002

History

The core of BioSig™, the On-line Handwritten Signature Verification system marketed by Vector Intelligence, Inc. (VII) was developed by Lucent Technologies' Bell Labs. The Bell Labs' project took more than five years of extensive research and development. The size of the research group varied at times from one to four researchers. The effort resulted in several patents, as well as in a highly tested and tuned verification engine code.

VII holds exclusive licenses from Lucent to the signature verification technology, plus a non-exclusive license to technology that provides for secure attachment of handwritten electronic signatures to electronic documents. VII also holds an exclusive license to the signature verification engine's source code developed by Bell Labs.

Patents

The two critical signature verification patents are licensed exclusively to VII.

US 5,828,772: Method and apparatus for parametric signature verification using global features and stroke-direction codes

Signature verification techniques developed by other companies make use of so-called "global" features describing general characteristic of a signature, such as total time to sign. This patent secures the use of a combination of both "global" features of a signature, and "local" signature curve matching, to verify the authenticity of the signer. This technique provides for higher verification accuracy than reliance on global features alone. The local component is described below under "Sophisticated Curve Matching Techniques."

US 5,745,592: Method for detecting forgery in a traced signature by measuring an amount of jitter

This is the second patent controlled exclusively by VII, and focuses on a critical element of forgery detection in handwritten signatures—a forgery created by tracing a signature has much more "jitter" than the original. Jitter is caused by microvibrations of the muscles in the fingers which control the process of handwriting. When a person signs their own signature, these muscles are coordinated and operate fluidly. What Lucent found was that when a forger attempts to copy another's signature, these same finger muscles operate less fluidly and cause the phenomenon of jitter, which can be accurately measured by this patented technology.

US 5,898,156: Validation stamps for electronic signatures

The final patent licensed from Lucent allows VII to engage not only in any signature verification business (as per patent 5,828,772), but also in the business of verifying the authenticity of electronic documents. The combination of these two technologies is critical for any document-oriented applications.

This patent describes a method of verifying that a given handwritten electronic signature was intended for the given electronic document. The technology covered in the patent prevents such forms of deception as the attachment of an authentic signature from one document to a different document.

The patent also thwarts any attempt to fraudulently re-generate a handwritten signature and attach it to another document by re-constructing the timing information in a signature from its geometric shape as sampled by a tablet digitizer. It is oftentimes important to display a signature shape on an unencrypted portion of a document to visually present the signature to a user. However, such an image can present a security threat. The patent covers the entire concept of modifying the geometric characteristics of a signature to hide the signature stroke pattern and speed while preserving the shape of the signature.

Sophisticated Curve Matching Techniques

While the patents cover the key technological bases, a working system requires further perfection of the methodologies described in patents. In particular, very sophisticated curve matching algorithms were developed by Bell Labs to build upon the idea patented in US 5,828,772. As human signatures display a certain amount of variability, it was considered technically challenging to reliably match the proper signature curves. The technical team at Bell Labs experimented with several approaches to curve matching and settled on one which VII believes to be the first curve matching technique reliable enough for commercial deployment.

This new technique, embodied in BioSig™, solves the challenge by generating a “stroke direction code” (or “SDC”) from a signature. It does so by subdividing the signature into a sequence of line segments, which Lucent refers to as links, between discrete points along the signature. These links are ordered according to the time-sequence in which the corresponding portions of the signature were made. Each link is assigned a stroke-direction value that depends upon the orientation of that link. The SDC of a signature is the resulting sequence of stroke-direction values.

Sample Signatures Acquisition - Training Process

BioSig™ requires several signature samples from a person to build a signature model for that person. After a sample has been acquired, the system runs several algorithms to extract parameters for the signature model as well as a model of the curve. The process is called training, or enrollment.

Creation of a model is a very fast process and takes well under a second on current generation PCs in single-user mode. Memory requirements are easily within the capabilities of all currently used PC configurations.

On a UNIX platform, “training” speed depends on the hardware configuration of the system as well as on the number of processes competing for system resources. The training process is CPU-intensive. On a UNIX platform the software is implemented as MT-safe library to allow for multiple training requests to be processed simultaneously. VII does not foresee any system degradation in a UNIX environment as the training process happens in realtime, not batch mode, so that computing demands will not typically be concentrated within a specific period of time.

For optimal performance, BioSig™ should be set to generate a model from six signatures. A model may be built from a smaller sample, but verification accuracy may suffer. A sample of more than six signatures usually provides for little improvement over a sample of six.

The software is very robust as to the natural variations in human signatures. However, if a person consistently uses two or more quite different signatures, for example, one with a middle initial and one without, or one with a maiden name and another without one, separate parameter sets (virtual “signature cards”) should be created for each one. The training process will reject signatures if they are too dissimilar.

The software is very robust as to the skew of a signing line.

Verification Process

The Verification Process compares a newly submitted signature to the model. A verification score is calculated to determine how closely a newly submitted signature matches the signature description stored in a reference database.*

Depending on the business need or on the amount of money involved in a transaction, the system can be tuned as to false acceptance / false rejection ratio. Although the tradeoff between false acceptance and false rejection is not linear and has a point of overall best performance, certain business conditions may dictate an emphasis on one aspect over the other.

Slightly higher accuracy can be achieved if two signatures are required for verification.

Verification can be accomplished either on the front-end machine or on a central server. Due to security concerns, the front-end verification methodology is better suited to relatively secure environments such as in-store POS terminals.

Like the training process, the verification process is very fast and takes a fraction of a second on current PCs in single-user mode. On a UNIX platform, verification is implemented as MT-safe library.

* Verifying a trial signature involves comparing its feature values to the reference feature values. This comparison is conveniently carried out by computing a total global feature error. This error is obtained by combining (in an appropriate norm) the individual discrepancies between each trial-signature feature value and the corresponding reference value. The total error is compared to a threshold, which is usefully established with reference to deviation measures, such as the standard deviations, of the global features over the group of reference signatures. That is, a larger total error should be tolerated if the global features exhibit a high degree of scatter, than if they show a low degree of scatter.

For verification purposes, an SDC error (which can be combined with the total global feature error) is readily computed by comparing the SDC of a trial signature with an average or representative SDC derived from the reference signatures. We refer to this average or representative SDC as the SDC template.

Verification Accuracy

BioSig™ demonstrates a very high degree of accuracy. It also proves to be very robust in taking into account variance in human handwritten signatures while still distinguishing true signatures from forgeries.

The current version of the software provides for 1% of false rejection rate with 1.3% false acceptance rate with two verification signatures.* For comparison, the best human signature expert has about 33% false acceptance / false rejection rate.

System Requirements - Input Devices

The technology is a software solution, and works with any digitizing tablet that can provide (x,y,t) coordinates where x and y are position coordinates on the digitizer, and t is time. Time does not have to be real time, but should only provide for a consistent presentation of the speed of a pen on the tablet. Substantially all digitizing tablets manufactured today conform to these requirements. These tablets can be either full scale graphics tablets, or other devices such as PDAs (Palm or Pocket PC) or even the small touch pads replicating mouse operations found on most notebook computers.

The technology can also make use of the pressure component of a signature if supported by underlying hardware. However, extensive tests conducted at Bell Labs showed that addition of pressure to the model is more likely to simply increase the noise factor and hence adversely affect the overall false acceptance / false rejection ratio. This is due to the fact that pressure ordinarily varies considerably depending on the posture of the signer, weight of the pen, and other factors unrelated to the identity of the signer.

For a MS Windows-based system front end, VII created a driver that converts input from any Wintab-compatible digitizer into the format required by the system for signature training and verification. Wintab is the current industry standard, and practically all tablets manufactured to work under MS Windows support it.

System Requirements - Storage

The system creates a model of a handwritten signature as a set of parameters extracted from signature shapes and speeds in a training sample. The size of the parameter set can be reduced to 100 bytes.

Models of the signatures can be stored either centrally in any conventional database, or on any other device that has 100 bytes available storage per model, such as a "smart card." A signature model can even fit into the available free storage on a conventional credit card's magnetic strip.

Due to the small size of the parameter set, there should be very little impact on network traffic or on server load in sending a signature over a network for any modern network configurations or server platforms.

* Based on tests run against the Lucent Technologies signature database containing 550 genuine signatures and 325 forgeries from 58 subjects. Tests with similar results were also conducted on NCR databases containing 1772 genuine signatures and 825 forgeries from 145 subjects. However, the NCR database was not available for testing of the latest version of the software.

If graphical representation of a signature is required for some business purposes, that graphical representation usually takes an additional 3K to 5K of storage space. VII also offers "SMP" technology, which stores information about graphical input to a pen or stylus-based computer in a highly-compressed, vector-based format, as a space-saving alternative to bitmapped graphics. Call or write VII for additional information about SMP.

Security

It is not possible to re-create a signature from its model. Thus, storing only models of the signatures is usually advantageous from a security point of view. However, if a graphical representation of a signature is required by business considerations, this representation can be stored together with the model.

Patent US 5,898,156 described above provides a security mechanism to prevent the reconstruction of signature model from a visual representation of a signature.

Standard database security mechanisms provided by every major database vendor, plus properly implemented operations procedures, create additional levels of security for the stored signatures.

Copyright 1999-2002, OpenSociety Technologies and Vector Intelligence, Inc.
Proprietary and Confidential

Signature Verification in Health Care

The health care industry today is under ever-increasing pressure to conduct more and more of its business electronically:

- Market forces require firms to drive cost and inefficiency from their outmoded paper-based processes, and to make more information available to consumers and business partners online.
- Litigation risks compel firms to devote more attention to data integrity and to the adoption of practices which ensure accountability of those who create and access data.
- Regulations increasingly permit or even require firms to create and maintain records electronically, while adopting stringent measures to protect that information from unauthorized access or alteration.

Biometric signature verification technology from Vector Intelligence, Inc. can play a major role in meeting both the business and regulatory needs of the health care industry for enhanced data security.

Electronic Signatures in FDA-Regulated Industries

FDA regulations at 21 CFR Part 11, enacted in 1997, permit and encourage the use of electronic signatures and recordkeeping in the industries it regulates (human and veterinary pharmaceuticals, personal care products, medical devices, food and beverages). While the FDA does not mandate the use of electronic processes, firms adopting electronic recordkeeping must do so in a manner that satisfies the agency's requirements, including those for an electronic signature.

The agency has been enforcing Part 11 aggressively since January, 2000. The FDA notes that packaged software should be designed with Part 11 in mind, and should have built-in tools for capturing electronic signatures and creating secure electronic records. The FDA does not regard ordinary UserID/Password log-ins as compliant, because there is no assurance that the person performing or verifying an operation subject to Part 11 is in fact the same person who logged in.

The Prescription Drug Marketing Act

In 1999, the FDA promulgated 21 CFR Part 203 to implement the requirements of the Prescription Drug Marketing Act of 1987. The regulations require that certain prescription drug wholesalers provide a "pedigree" to purchasers identifying each prior sale of a drug. Like Part 11, Part 203 creates opportunities for providers of products and services that would generate an irrefutable electronic pedigree for drug distributors; such a solution will obviously need to include user authentication and data integrity measures.

The HIPAA Challenge

The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates new security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. HIPAA also mandates that a new electronic signature standard be used where an electronic signature is employed in the transmission of a HIPAA standard transaction. Although final rules have not yet been adopted, the security and electronic signature standards proposed at 45 CFR Part 142 are likely to be adopted without substantial modification, and to become effective in 2002. The new standards are intended to protect the confidentiality, integrity, and availability of individual health information. The electronic signature standard in particular is intended to provide a reliable method of assuring message integrity, user authentication, and non-repudiation.*

The importance of reaching HIPAA compliance quickly and completely is difficult to overstate. As a Gartner Group Analyst observed, "When provisions of HIPAA take effect in October 2002, the fine for improper handling of patient data will rise to a maximum of \$50,000 per incident, which can go higher if done under false pretenses or done with the intent to sell, transfer, or use the information. For a provider with thousands of patient records, the cost of even a minor slipup could quickly reach millions of dollars."

Biometric Signature Verification: An Important Part of Your Compliance Program

Signature verification technology from VII can play an important role in meeting these and other compliance challenges. Although BioSig can be deployed in many ways, depending on the requirements of the application or organization, at its core it is an authentication technology: it accurately confirms a user's identity by comparing a reference file, typically generated when the user enrolls in the system, with a signature file that must be created anew each time authentication is required. The reference file (and, theoretically, the verification engine) can be stored remotely in a secure server, or locally on a handheld computer, PC or smart card, as needs dictate. The signature file created at the point of authentication contains time stamp data, and like the reference file, is stored in an encrypted form that contains no useful or intelligible information about the appearance of the signature or any of its characteristics. Verification can be performed over a network (open or closed) or on the same device used to capture the signature file.

Successful user authentication can trigger a range of possible consequences, such as granting access to data (or even to physical facilities), or embedding a signature (with or without its visual counterpart) in an electronic document, thereby creating virtually incontestable evidence of when and by whom the document was signed, and preventing that document from being further edited. BioSig is an excellent supplement to or substitute for alphanumeric passwords (the most problematic form of authentication today), including those employed in Public Key cryptography. Since the final rules under HIPAA are likely to mandate adoption of PKI and digital signatures,

* Electronic signature is defined as "the attribute affixed to an electronic document to bind it to a particular entity. An electronic signature secures the user authentication (proof of claimed identity) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven); supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability of data, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer." 45 CFR § 142.310.

institutions and application developers pursuing HIPAA compliance should give strong consideration to technologies that can improve upon PKI's traditional, but problematic, dependence on passwords, and biometric signature verification is, in many settings, the least expensive, least intrusive, and most administratively practical choice among all the options.

Applications have already been developed incorporating BioSig to meet the same demands imposed by HIPAA and the other regulations facing the health care industry today. The Galactic Access service, from InterNetEx, employs BioSig to authenticate and lock electronic documents. Documents signed within Galactic Access are—among other features and characteristics—authenticated, encrypted, unalterable, time-stamped, and subject to non-repudiation.

The Business Case for Electronic Recordkeeping in Health Care

The use of paper-intensive procedures within the health care industry today is pervasive, but imposes staggering costs while generating errors that cause delay, expense, and in some cases, actual physical harm to patients. For many mission-critical applications within the industry (e.g., writing prescriptions, entering treatment orders at a hospital, and patient discharge and bill review, to name a few), electronic recordkeeping, supported by biometric signature verification, should be carefully considered because it can help to meet patient care objectives in a way that is cost-effective, promotes best practices, and is acceptable to health care providers, insurers and patients alike.

The cost savings from adoption of electronic processes can be impressive. On average, paper-based insurance claims take 60 days until receipt of payment at a cost of about \$5 per claim; payment for a clean electronic claim only takes 14 days at about \$.25 to \$.30 per claim. The Department of Health and Human Services predicts that the savings gained through transaction standardization could be as high as \$29.9 billion over 10 years.

But the benefits of electronic transactions extend well beyond mere cost savings. Consider the problem of patient care order entry in hospitals. Typically today, a nurse or physician leaves the patient's location and orders additional treatment at a potentially distant location. While the procedure is automated, it is also problematic: the practitioner may be distracted or delayed on the way to the terminal, or may make data entry errors (in an extreme case, even designating the wrong patient). By contrast, a practitioner equipped with a handheld computer, operated at the bedside, can ensure that the patient is not left alone during order entry, that the order is entered within moments of the practitioner's decision, and that it is entered for the correct patient (thanks to an identifying bar code on the bedside or even the patient's ID tag). In this setting, signature verification requires no additional hardware (all handheld and tablet computers can deploy BioSig), making it the most natural form of security to employ.

Similarly, consider the patient discharge and bill review scenario. Today's bill review/discharge process is long and drawn-out. Before charges can be submitted to the insurer, the patient must review and approve a lengthy chart of treatments, examinations and prescriptions. Poor recordkeeping results in insurance disputes and delays, and drives up the hospital's administrative costs. Insurance-related disputes and delays can even force patients to delay follow-up care. But presenting bills to the patient in electronic form, and collecting the patient's signature electronically, not only speeds the process, it generates a virtual "paper trail" that can reduce disputes with the hospital or insurer, and their attendant costs and delays.

The drug prescription system is also ripe for change. Today, over two billion prescriptions are written each year, the majority in handwriting, on a prescription pad by a doctor within the

confines of his office. Not only does this system require accurate interpretation by the pharmacist, but it requires multiple data entry points if the additional drug is to become a part of the patient's permanent health record. The Business Roundtable Health and Retirement Taskforce estimates that 500,000 serious medication mistakes could be avoided each year through automated prescription systems, which would remove the difficulties of reading doctor handwriting, warn against contraindications for specific drug treatments—and, incidentally, largely eliminate the trade in illicit drugs linked to stolen (paper) prescription pads. Clearly, electronic prescriptions offer tremendous advantages over their paper counterparts, but only if protected by strong authentication measures; and what could be more simple and natural than preserving the signature process, but simply substituting one surface (an electronic pad) for another (paper)?

Contact Us

Call today to learn more about the role that biometric signature verification can play in your own applications or business processes.

Joel E. Simkins
Chief Marketing Officer
Vector Intelligence, Inc.
604 S. Washington Sq. #1003
Philadelphia, PA 19106

(215) 923-5942
jsimkins99@earthlink.net