

Ensuring Identification in Web-Based Data Collection – Signature Capture Capability on Handheld Computers

[This is the first of a series of articles that will explore how to ensure traceability of web-based data by including opportunities to identify individuals correctly in end-user applications. This article looks at industry-specific opportunities for including signature capture capability in applications for handheld computers.]

Who is Responsible?

Every day, massive amounts of data are collected and stored. Replacing paper and pencil with computers, databases, scanners, and PDAs may have expanded our capability to collect and organize information, but the transition has weakened the link between the source of that information and its ultimate repository. The Internet has further shredded that link by making it possible for one person to assume another's identity with near-impunity – identity theft has become the crime of the moment. The source and validity of web-based data can be challenged.

Six familiar interrogatory words support every piece of information - **who, what, where, why, when, how**. Today, identifying **who** - the responsible party, the source of information, the receiver of goods - is a more urgent need than ever before.

Regaining Control

While the paperless back office can store electronic records almost indefinitely, the task of identifying who did what yesterday can present problems. Until recently, a delivery could be tracked from warehouse to front porch by virtue of a bar code scanner, but the driver still had to collect the recipient's signature on a piece of paper which would have to take up space in a drawer until long past the time it might be necessary to prove that delivery was successful.

Without a signature, it is nearly impossible to complete any process involving goods or services with confidence. As Federal regulations increasingly demand proof of acknowledgment in medical matters; as corporations strive to increase efficiency and streamline processes; as end users struggle to manage increased workloads; information technology companies race to implement the latest advances in the workplace. Public key infrastructure (PKI), with its complex and expensive layers of certificates and add-on hardware, connects individuals who are still anonymous under those layers. Entering an ID key can still shield the signer behind an assumed mask. Advanced biometrics are costly to implement, especially when the field of possible "signers" is vast and inconsistent.

For many industry applications, mobile and wireless devices equipped with signature-capture capability can secure the link between source and destination.

Electronic Signature Capture

An electronic signature is a signature that has been attached to a document by electronic means. The electronic signature process is accomplished according to system design and software instructions, authenticating the signer's identity, binding the signature to a document, and assuring that the document and signature cannot

be altered after the fact. When captured correctly, an electronic signature has the same legal weight as a signature on a paper document.

Implementation

Responding to security and privacy issues that are now key concerns in every industry, any enterprise can easily incorporate electronic signature capture into applications on handheld terminals and desktop computers. Portable or desktop printers can produce a copy of a document on the spot or a duplicate can be sent to the signer at a later date – electronically or by conventional mail. Records can be retrieved instantaneously for review on the desktop. The goal is to store and retrieve a copy of any signed document, providing security and accountability to all involved parties.

The InVision **iSignIt™** ActiveX control was designed for use on handheld devices with touch-screen displays running Microsoft® Windows® CE. iSignIt can capture a signature entered from any orientation, timestamp it, encrypt it, and then store it as a data or graphic file of as little as 750 bytes. At InVision Software, engineers develop custom solutions for collection and secure storage and retrieval of this vital information.

Whether a device is wired or wireless, adding signature capture capability to your application is a simple way to enhance the security and traceability of your transactions.



The additional savings in time, cost, and efficiency when the management of records of this type becomes digital is a benefit that no business can overlook.

Applications

Proof of Delivery – Shipping manifests – based on date, route, and driver - can be downloaded to PDAs. A driver collects an electronic signature for each delivery right on the terminal, instead of a form that might get lost or damaged. At the end of the day, records and signature files are uploaded to the company network and managed as needed. Customers know they will not be charged for items they did not sign for and there will always be a record of who signed for a package. Customer Service staff can quickly verify delivery status and resolve delivery questions with confidence.

Mobile Sales and Ordering – Vendors who enter orders at store locations can easily validate order forms by collecting a signature on-site, instantly validating orders of any size or value. Store owners can easily trace orders to the managers who approved them.

Warehouse Inventory – When multiple users are receiving or releasing shipments at the loading dock, a signature entered on the handheld terminal covers both ends of the transaction – the driver and the shipping clerk. Uploaded records for all inventories are merged in the database with the confirming signatures available for reference.

Field Service – Dragging a folder of service reports through a day of repair calls is not a technician’s favorite task. A handheld terminal that offers easily completed forms can get a tech out the door faster when the job is done. Add to that a downloadable task list and he is free to concentrate on his customers’ problems instead of pushing papers. Parts orders and reports of service completion can be tied easily into a company’s billing system, with the customer’s and technician’s confirming signature available for every step.

Healthcare – The healthcare industry offers numerous scenarios where the introduction of signature capture technology can support patient safety and privacy and provide accountability. Transitioning from paper forms to electronic records enables patient histories and billing records to be stored, retrieved, and backed-up for safekeeping and permits security in the form of login IDs and passwords as well as more advanced biometric safeguards against unauthorized access. Entering patient data electronically on a handheld terminal eliminates transcription errors. A handheld application that also collects electronic signatures from practitioner and patient makes it possible to offer patient confirmation, practitioner accountability, and accurate history in a secure package.

Enabling signature capture on a medication or treatment order can permit a doctor to place that order remotely – even from home – enabling more responsive patient care.

In August of 2002, the Department of Health and Human Services released its final version of the Health Insurance Portability and Accountability Act (**HIPAA**) privacy rule. Provisions of the rule require that release of patient information by healthcare organizations must be **authorized** by the patient and that patients will usually **sign a receipt** that they have received notification of their health care provider’s privacy practices. Other provisions concern obtaining patient authorization in other areas.

Capturing a patient signature electronically provides a record that the provider has satisfied the HIPAA requirement and eliminates the need to manage paper documents. Since this documentation must be retained and made accessible for up to six years, electronic storage of the patient signature is mandatory for any facility that wants to reduce dependency on paper documents.

By extension, **patient registration** documents can be completed and signed on a handheld terminal, uploaded to a practice’s records system, and then updated or replaced periodically to verify information on insurance provider, dependents, etc. Collecting the patient’s signature directly from the device ensures patient identity and statements regarding insurance coverage and responsibility for payment. The patient signature on **informed consent** forms can also be recorded by this method.

In the case of **in-home care**, clinical data can be transferred from the patient’s home directly to a medical facility, with verifiable identification of the caregiver.

Pharmacy – Current regulations require a customer to sign a receipt for certain classes of medication. Typically, this receipt is only a form on a clipboard, completely handwritten. Each medication is written into the form at time of purchase and the customer signs or initials alongside. Signature capture from a form on a handheld terminal provides a retrievable record for customer and pharmacist alike – without the need for error-prone interim transcription – of prescriptions containing controlled substances. For instance, such traceable information is vital for identifying an individual who acquires a prescription for a home-bound patient.

In healthcare, where every action must be recorded with proper documentation and traceability, the availability of electronic signature capture offers security and reassurance to patient and professional alike.

Summary

For every transaction that requires identification of a responsible party, incorporation of a signature capture control is the enhancement that can bridge the gap between the paperless office and traditional processes that are historically wasteful of paper, personnel, time, and space. The savings in effort, cost, and time cannot be complete without including the security, traceability, and accountability advantages afforded by electronic signature capture.