

# On-line Paperless Insurance Applications

— by Jothy Rosenberg, CTO & Co-founder

*The Insurance industry's need for on-line paperless applications is great. Successfully deploying such systems will mean lower costs, higher revenues from newly served markets and improved business processes that will be more efficient. The need has always been great but many insurmountable barriers have precluded the creation of real solutions in the past. These barriers have been hurdled. Real paperless insurance application solutions can be deployed now. The benefits of deploying such a solution are significant. They include:*

- *Reaching un- and under-served markets for new revenue streams;*
- *Decreased consumer abandonment;*
- *Eliminating the high paper costs per application;*
- *Solving process problems and gaining much faster time-to-money.*

## **The insurance drive to paperless**

The insurance industry will be a strong force in delivering the first on-line paperless transactions to consumers. This is because the 6,000 global insurance companies who collectively receive over \$435B in life insurance premiums have still seen a steady decline in the number of life policies written over the last 10 years. The reasons for this sound like the mantra for paperless *everything* that we have been promised for the past 20 years: a high industry cost structure, the new revenue streams accessible only when using on-line media, process problems that make individual application costs prohibitively high, and a very high rate of abandonment when consumers are faced with lengthy delays at multiple steps of the application process.

## ***High cost structure***

The insurance carrier's agent network is expensive and so is moving "up stream" to the million dollar policies to justify their high costs. Carriers incur paper-based costs of \$150 per insurance application for printing, scanning, faxing, copying, mailing, and the staff to handle all the incoming paper. These costs alone are driving all carriers to look carefully at ways to completely restructure the application process. The revenue side of the equation is even more compelling.

## ***Reaching un- and under-served markets***

In the US, the large middle-aged population bubble is aging and has the resources to buy insurance but has little access to insurance agents or insurance education necessary to compel these baby boomers to buy. The Web is the perfect vehicle to solve this problem and reach this under-served market for \$250,000 to \$500,000 policies especially term life where the complexity of the products is lower and self-education is more practical. But besides high costs and the desire to open up new uncharted revenue streams, the insurance application process is fraught with problems that can only be solved by going to an entirely paperless process.

## ***Process problems***

The process problems include limited reach, a long time to money, a high rate of abandonment, and too high a dependency on the para-med process.

First, limited reach. Customers must have contact with an insurance agent or they must know to call customer service to acquire an application by mail. Right away, the carriers are severely limited in their reach to a market they desperately need to serve.

Second, time-to-money. The typical 60-day application process creates a very costly delay in the carrier's "time to money". There is a built-in minimum of about 15 days for underwriting plus medical scheduling but the front-end 45 days can be all but eliminated if the entire process from qualification through initial premium payment is done in one 30-minute sitting. Improved time to money has in practice been shortened from 60 days down to 15.

Third, high abandonment. Abandonment is a major issue because each lengthy delay from initial inquiry to receipt of application and final submission of completed application causes either "buyers remorse" or just loss of focus and interest on the part of the consumer. If qualification is performed well, abandonment can be dramatically reduced through an on-line process with no built-in delays.

Fourth and finally, para-med dependency and cost. Para-meds increasingly are depended upon while in the physical presence of the consumer doing the medical exam, to get missing elements of paper applications filled in and for doing identification confirmation. Para-meds push back on these tasks and are left unpaid if the customer ends up failing to meet identity requirements or loses interest later in the process.

## **Barriers to Paperless Insurance**

A paperless insurance application requires

- (a) a consumer-facing Web-delivered application,
- (b) a process to authoritatively validate an on-line consumer's identity,
- (c) an electronic signature process that is legal and binding, and
- (d) ways to defend against challenges to the identification process (non-repudiation).

A concerted effort to move to offer paperless on-line insurance applications has previously been blocked by insurmountable barriers, some technical, some regulatory, and some legislative. All of these barriers have now been hurdled or are in the process of being hurdled easing the transition to full paperless processes.

## ***Regulatory problems***

Regulatory problems have by no means evaporated because the nature of insurance requires state-by-state insurance regulator approval. The GeoTrust implementation has been approved in Illinois, Missouri and 5 other states at this time. After a few bellwether states, the remainder tend to follow along quickly.

## ***PKI maturity***

PKI or Public Key Infrastructure, as its name implies, requires complex deployments of infrastructure with associated very high costs. PKI is the basic technology needed to bind a validated identity to an electronically transportable form and to use that form to encrypt and sign digital data for confidentiality and integrity. PKI has a "black eye" because there have been a dearth of ready, enabled security applications; it has been a technology in search of solutions. However, along the way PKI has matured to the point where it now can be provided to insurance carriers not as infrastructure they install and hire specialized security IT personnel to maintain, but instead as an outsourced service managed by specialized organizations called Certificate Authorities. GeoTrust is such a Certificate Authority and is the only one currently offering a totally outsourced managed solution to the insurance industry.

## ***Consumer identity, authentication and non-repudiation***

A digital signature depends entirely for its veracity on being bound to a strongly established identity. The Web is anonymous and so a huge barrier to even taking the first step to on-line insurance applications has been this identity gap. One way identity can be established is through a set of shared secrets that you have and the unidentified person should know if they are who they say they are. Consumer credit files provide such a set of shared secrets if used correctly. Once identity is established this fact is bound to a transportable piece of data – a digital certificate. If the consumer is to re-use this electronic identity over and over, a process of authentication is required that re-establishes the binding between their identity and the digital embodiment of that identity. The binding must be very strong and persistent over

time in case of a challenge (“it was not really me”, “I never said that”) where the carrier has identity proof that is non-repudiatable by the individual.

**The US E-SIGN law**

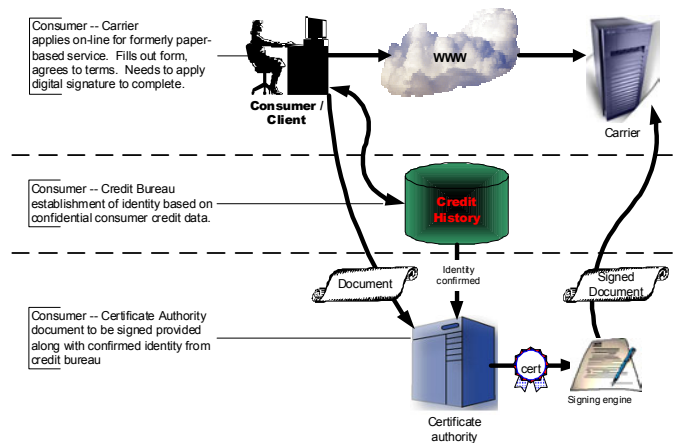
The Legality and acceptance of electronic signatures has not been fully tested. However, the support for and strength of E-SIGN is strong and growing stronger. E-SIGN is the Electronic Signatures in Global and National Commerce Act.

E-SIGN legally validates contracts and signatures made in electronic format so long as the contracting parties have agreed to utilize electronic media. E-SIGN supersedes all Federal, state and local laws containing paper-based requirements that may otherwise deny effect to electronic contracts, signatures or records. Recognized methods of electronically signing a document include “digital signatures” created through encryption software and validated by recognized third-parties (Certificate Authorities). The interpretation of this act, according to the state of Oregon – a leader in electronic transaction legislation – is very clear:

- (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- (c) If a law requires a record to be in writing, an electronic record satisfies the law.
- (d) If a law requires a signature, an electronic signature satisfies the law.

**The Paperless Insurance Application**

A diagram of a paperless insurance solution forms a useful reference point for the remainder of our discussion.



**On-line Web-based application**

Through some marketing or promotional means, a consumer is brought to the carrier’s Web site, is provided qualifying questions and information and begins the application process. Some carriers opt to take an even smaller baby step and have the consumer interact with a customer service representative who in turn deals with the on-line application forms. These forms may be either HTML or fillable form input. HTML is more flexible and works in a familiar Web browser fashion. Fillable forms provide an exact replica of paper-based forms, sophisticated help and guidance ala Turbo Tax, and create a clean encapsulation of the form and the responses in one digital package.

**Automated, on-line consumer identification and authentication**

The second step in the process involves validating the consumer’s identity in an otherwise anonymous medium. To accomplish this the consumer first enters data that could be found in one’s wallet. This includes name, address, home phone number, driver’s license and issuing state, social security number and date of birth.

The phone number is checked with the phone company database against the reported home address. The driver's license is checked with the state DMV with the home address and the birth date provided. The social security number is checked against being from a deceased person, against the reported birth date and for further address confirmation. At this point a significant portion of attempted fraud is blocked from any further time wasting.

The purported identity is hereby established and this individual's credit file is pulled with their explicit permission using a "soft hit" for the next step in identity verification.

Four questions are constructed from the credit file data that are not easy to ascertain even if someone committing fraud were to attempt to access this credit file through the normal public mechanisms. An example might be "which of the following possible vendors supplied you in around 1997 with a student loan?" The result of the answers to these four questions is a score that is compared to the carrier's pre-established business rules for acceptable fraud risk. If the score does not meet the standard, a human customer service representative is handed the task of determining what further action can be taken with this individual.

Under the FCRA, the set of questions and the responses to these questions must not be maintained except by the sanctioned credit bureau. This is done using a "knapsack" which is a digital package encrypted using the public key of the credit bureau. Only the credit bureau's private key maintained exclusively by them will decrypt the knapsack to get at its contents. This makes it safe for the certificate authority and the carrier to maintain this knapsack with the individual's application data.

Telephonic authentication is an option that is available to carriers once identity verification has met the carrier's business rule threshold. GeoTrust employs a process of "out-of-band" verification to the already validated phone number to prove that the individual is indeed physically at that phone number. It requires the individual to enter a random security code into the phone keypad that is generated by their browser on a secure connection. Further, a voice recording is taken of the individual

that can later be used in a non-repudiation challenge should the issue arise.

### ***Fully managed and outsourced digital signature and encryption***

Carriers need not install any hardware or software for public key certificates. Only HTML links from the appropriate consumer-facing Web pages to the designated GeoTrust pages need be built<sup>†</sup>. Upon completion of the identity verification process and with the knapsack from the credit bureau in hand as the manifestation of this individual's identity, the public/private key pair is generated. This key generation can be done either on one of the certificate authority's secure servers or on the individual's desktop using the cryptographic software built into all browsers. The decision about where to do the key generation is a tradeoff between tighter security if the private key never leaves the control of the individual and greater ease of use if the individual never even knows what a digital certificate is and no special client software download is ever needed.

In either case, the digital signature is performed by using the individual's private key to encrypt a small digest of the entire application dataset that is then appended to the application data. It is optional whether the entire application is also itself encrypted since its transmission is already being done over secure encrypted transmission channels. Normally, the private key is used only once for a digital signature and is promptly destroyed. The public key residing inside the digital certificate created by the certificate authority is also appended to the application dataset. The entire dataset is forwarded to the carrier to begin the underwriting process.

### ***Mature payment solutions***

On-line payment solutions make it very easy to get initial premium payment as part of the initial application process. Systems are sophisticated enough to support all credit cards as well as ACH payments directly from bank accounts. They are easy and friendly so as not to create confusion or other reasons for abandonment. And they allow for

---

<sup>†</sup> For the first two systems put into production, the actual time from contract signing to a fully operational system was under four weeks.

an initial check of identity (further creating confidence in the identity verification process) as well as a credit card hold on funds but no debit until the underwriting process concludes.

### ***Non-repudiation and legal challenges***

Challenges are very infrequent but steps need to be taken to handle this eventuality. The entire

package of data for an application including the knapsack, the application and the individual's public key must be retained in case of a challenge. GeoTrust offers the option to the carrier of maintaining this data and provides an interface for a trusted carrier administrator to access this data in the event of a non-repudiation challenge.

### **Conclusion**

On-line paperless insurance applications are no longer theoretical. Several are in production today and many more will appear over the next year. The reasons to deploy are compelling and the barriers preventing deployment have all but been eliminated. The technical barriers presented by the Web medium have been addressed by using fully managed public key infrastructures provided by trusted certificate authorities like GeoTrust. Because these portions of the solution are fully managed, up front costs and delays are minimal. Further, GeoTrust's highly flexible solution allows carriers to configure all aspects of the solution to match their business and underwriting processes. Consumers accept this approach and once qualified, complete the process as predicted delivering real benefits to carriers of reaching this under-served market while delivering real benefits to consumers of insurance solutions they so badly require.