Electronic Signature and Secure Forms in the Insurance Industry: Taking the P&C Pen to the Web

Analyst Author:

Karen Pauli

Senior Analyst, Insurance

Oct 2007

Reference # V53:05IG

TowerGroup Take-Aways

- Insurance carriers continue to hold on to traditional paper-based, wet-signature contract execution even though the legal barriers to electronic documents and electronic signature have been eliminated.
- Other segments of financial services have adopted electronic signature technology, and consumers are expecting all their financial transactions to be supported in an electronic environment.
- New forces for globalizing insurance and the demand for environmentally friendly companies combined with the pervasive need to prevent fraud and comply with regulations make use of secure documents and electronic signature imperative for carriers.
- Document security issues are complex, and many insurance carriers would be well served to partner with technology vendors that have deep financial services expertise with electronic signatures.
- Initiatives for using secure documents and electronic signature must be an enterprise decision not only to determine business value and total cost of ownership but also to effect the culture change necessary for success.

Two Charles River Place
63 Kendrick Street
Needham, MA 02494
United States

T +1.781.292.5200
F +1.781.449.6982
towergroup.com

Report Coverage

In 2000, US legislation was passed that made electronic documents and electronic signatures (e-signatures) equal, under the law, to their paper-based versions. After the legislation passed, many segments of financial services quickly commenced electronic commerce initiatives, including electronic signature and secure documents. With reports that processing time decreased about 50% and transactional costs declined up to 75%, it defies logic that the insurance industry has not adopted technology to support e-signature. However, the property and casualty (P&C) insurance industry has been slow to follow its counterparts in the rest of financial services. The experts TowerGroup interviewed in the field of e-signature indicate that the continuing siloed nature of P&C insurance is, arguably, the largest barrier to adoption of the technology. This TowerGroup Research Note explores the numerous opportunities for insurance carriers to improve operations by implementing electronic signature and secure documents technology.

Background

The US Federal Government passed the Electronic Signatures in Global and National Commerce Act (ESIGN) in 2000. The state-level version, Uniform Electronic Transactions Act (UETA), aligned the federal legalities with state governance. This step was critical because the insurance industry is regulated at a state level. UETA or a comparable set of regulations is in place in all 50 states as well as in Washington, DC, and the US Virgin Islands. Even though the legal barriers for e-

commerce were largely eliminated, the property and casualty insurance industry has made little progress in transitioning from a paper environment to an electronic world for conducting business. The industry's use of old, inflexible legacy systems, incapable of accepting any additional functionality has been a significant factor.

An additional barrier to rapid adoption has been a lengthy history of failed technology installations, many of them utilizing leading-edge products, causing many insurance executives to be understandably wary. The process of filling out an application for insurance, gathering information, and successfully concluding that transaction by executing a contract with a signature has remained a highly paper-based process. The fax machine has eliminated some mail time, but paper still has to travel between individuals, sometimes several individuals, and the carrier. These multiple hand-offs take time and delay the issuance of coverage. The longer it takes to generate a policy, the more expensive the transaction.

Many insurance agents and insurance carriers are holding on to the tradition of a pen on paper and a wet signature out of fear stemming from a lack of deep case law on the issue of electronic signature. The insurance industry as a whole frequently stays rooted in archaic practices and procedures because of the comfort of case law. The notion of having to spend unknown sums of money to defend a case that has not been previously adjudicated frequently proves to be overwhelming and suppresses action. However, the time has come to take counsel and comfort from the experience and successful legal proceedings in other segments of financial services and move forward with electronic signature and secure documents.

For purposes of this Research Note, secure documents are associated with signature authorization. However, not all secure documents require a signature. This point of clarification is important because carriers want the documents they distribute electronically to be secure, and many have applied software to ensure that they are. A secure document initiative has one level of complexity, and an e-signature initiative has a whole other level. Securing documents does not necessarily require all the encryption and authorization that an e-signature systems does. It can be done through access rights management. Carriers should not be dissuaded from implementing security for electronic documents simply because they are not yet ready to adopt e-signature capabilities. In fact, a secure documents project can be an excellent first step toward a robust e-signature capability.

Electronic Signature Terms and Principles

When new technology arrives on the scene, some confusion about associated terms and functionality is common. Electronic signature technology is no exception. Compounding the "newness" factor is the relatively rapid development of the various types of signature capabilities, the terms for which are frequently incorrectly interchanged in the marketplace. Unlike many other technology innovations, e-signature technology is based on a set of legal principles. Institutions must understand the legal parameters before they undertake any e-signature initiative. The following sections give an overview of related words, terms, and principles discussed in this Research Note. Rather than provide an exhaustive review, they offer a framework for TowerGroup's strategic view of the way secure documents and e-signatures fit into insurance operations. It is imperative that carriers seek legal counsel on all phases of a secure document and e-signature initiative before they use the technology. It is likewise critical that the legal department be part of the team assessing and implementing a secure document and e-signature project.

Words and Terms Related to Electronic Signatures

The following are explanations of the words and terms used in this TowerGroup Note.

Authentication. A process that verifies that either data contained in a document has not been changed or individuals responsible for executing the document are who they say they are.

Biometrics. Type of authentication that relies on physical attributes such as DNA, iris scans, fingerprints, or speech.

Digital Certificate. An attachment to an electronic document that indicates that the individual is who he or she claims to be. Certificates can be self-issued by the individual or they can be issued by a Certificate Authority. Certificates are driven by keys.

Digital Signature. A code used to authenticate that the person related to a document is who he or she claims to be. A digital signature validates the origin of a document. In actuality, it is not a signature at all; rather, it is based on keys, one public and one private.

Digitized Signature. An image of a person's handwritten signature that is saved in an electronic file. Most frequently, a digitized signature comes from an electronic signature pad or is scanned from a paper document. Digitized signatures are not considered be secure because they can be copied and pasted into other documents.

Electronic Signature. According to the UETA, "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." In its most robust form, it incorporates digital signature technology but also captures the signer's intent for the document and additionally authenticates the data contained in the document. The electronic signature authenticates the user by linking the digital certificate to the signature file. Electronic signature is a legal concept.

Hash. A number generated by a string of text that finitely and discretely identifies text. In practical application, the originator of the document generates a hash of the message, encrypts it, and sends it with the document. Individuals receiving the document decrypt both the text and the hash, produce another hash from the text they got, and compare the two hashes. If they match exactly, it is highly probable that the document was not tampered with.

Public Key Infrastructure (PKI). A security system that issues and manages digital certificates.

Legal Principles Applicable to E-Signature

For ESIGN and UETA, the following principles govern a successful e-signature implementation:

- The document and signature must be under the exclusive control of the individual.
- The signature must be verifiable as belonging to that person.
- The signature must be unique to the individual.
- It must be confirmed that the individual wishes to be bound by the document.
- It must be highly evident whether the signature and document content have been tampered with.
- Revisions to the document must be identified as authorized or not authorized.
- Copies of the document must be identified as such and can be made only with the approval of the person in control.
- An audit trail must exist for the original and copy that specifies the last person to receive the document.

Clearly, many new terms and legal principles are inherent in e-signature requirements. Exhibit 1 is one illustration of how security requirements and methods relate to each other.

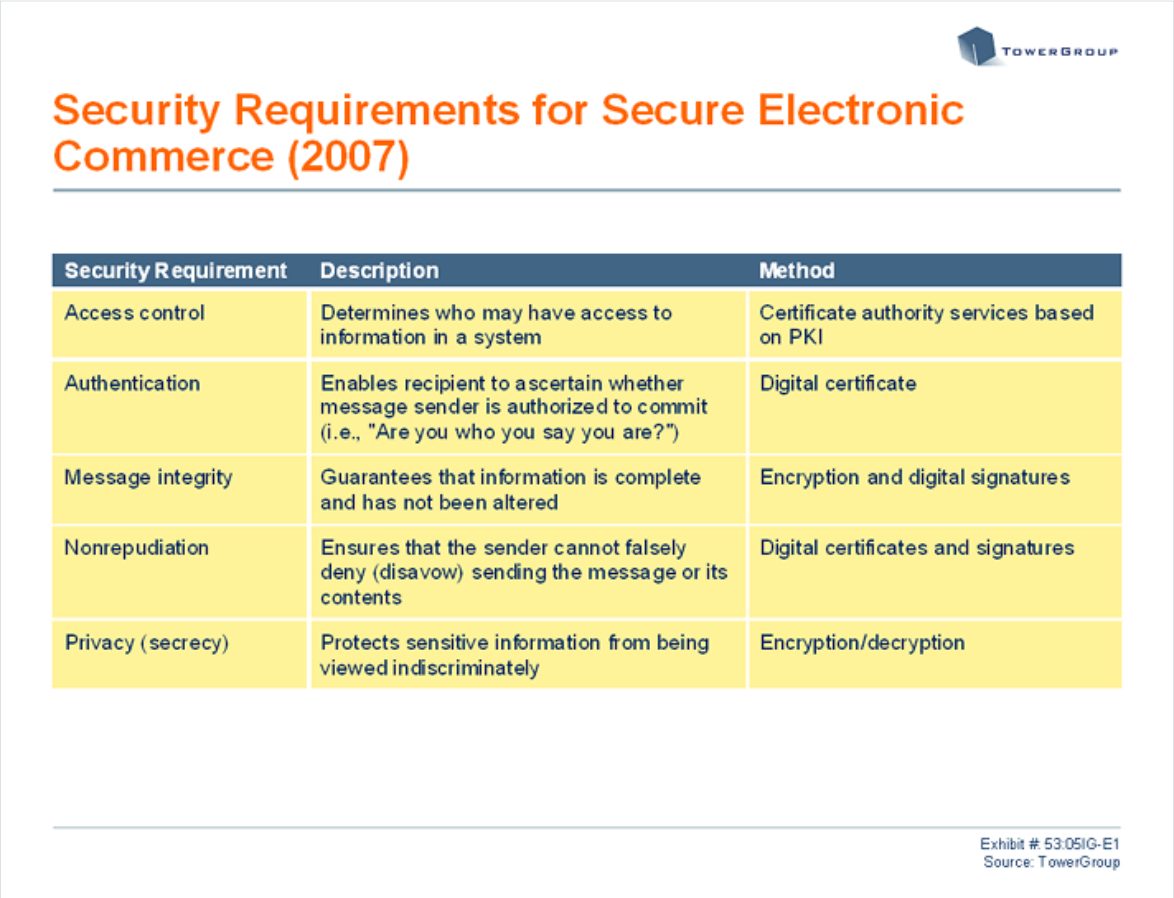

Exhibit 1
Security Requirements for Secure Electronic Commerce (2007)
Source: TowerGroup

The terms and legal ramifications of electronic signature are complex. The whole subject of information security is complex. Because of these complexities, it is critical that carriers work with experts in the field or create internal expertise that is deep and highly informed.

Forces Demanding Change

At this time, many property and casualty carriers are awash in technology initiatives. Those that are not awash can be immersed, and sometimes paralyzed, in determining what to do and where to allocate business and IT resources. A large number of carriers are in the process of replacing legacy systems. In interviews with carriers, TowerGroup finds that document projects are very high on the list of initiatives in progress. Frequently, carriers undertake document initiatives in tandem with replacement of operational systems such as claims administration systems or policy administration systems. There are many compelling reasons to convert document projects into secure document initiatives and to add electronic signature to the design for replacing an administration system.

Customer Expectations

People execute contracts online, via the Web, every day. Some of the contracts, such as those for a credit card, are relatively simple. At the end of the application process, the applicant must agree to the terms the grantor establishes by clicking on an "I Agree" button. eBay, UPS, online catalog companies by the thousands, and a plethora of other consumer transactions all require execution of a contract. These take place online with use of digital signatures and are supported by many of the

legal concepts represented by electronic signatures. More and more, customers are expecting all the contractual relationships that affect their lives to be conducted over the Web. The insurance industry is slow to recognize that consumers' experiences with other businesses shape their expectations for interactions with carriers, agents, and brokers. One could argue that most eBay, UPS, and Eddie Bauer contractual interactions are not as complex as an insurance contract. The risk that a customer will not pay for a ski jacket certainly does not compare to the risk a carrier bears in a deal for a $750,000 (USD) house or a $10 million commercial structure. However, consumers are executing loans and securities transactions via the Web using electronic signature and secure document technology. Those events do stand up, in risk, to an insurance transaction, and carriers need to respond to consumers' experiences with other financial transactions or risk losing their business to financial services organizations that have adopted leading-edge technology for contract execution.

Globalization of Insurance

A rapidly increasing pressure for adoption of electronic signature and secure documents is the growth of the global insurance market. Global business is conducted via the Web, and carriers must match those business practices. When executing an insurance transaction with a business, executive decision makers will not look favorably on a carrier or agent who takes them out of their normal e-commerce environment and involves them in paper-and-pen transactions. The type of technology used particularly impacts carriers that write midsize to jumbo commercial lines and have books of business with multiple locations across the United States and throughout the world. Insurance trade journals are headlining the increase in competition in the commercial lines segment. TowerGroup's interviews with carriers and insurance agents reveal that competition for commercial lines of business has been escalating as each month passes. Justifiable concern about competitive position exists throughout the insurance industry. Carriers that lengthen the new business application process by two, three, or even four weeks while contracts requiring signature are mailed around the world, passing through multiple hand-offs at each location, are at severe risk of allowing a competitor to offer a better deal and losing the business. Use of e-signature and secure electronic documents eliminates this service risk.

It is important to know that the European Union, the United Nations Commission on International Trade Law, and other international governing bodies have enacted laws that regulate and facilitate the use of electronic signature. This is truly an international capability.

Competitive Advantage

The flip side to the threat of loss of business due to customers' poor experience is the competitive advantage that e-signature and secure documents brings to carriers that conduct business this way. In addition to the speed at which a transaction can be concluded via electronic signature functionality, carriers bring value to themselves, their agents and brokers, and consumers when they make contracts available in an electronic form. As time passes, paper-based documents can get lost and be misplaced. Use of electronic documents overcomes this danger. While imaging technology allows electronic access to forms, imaged contracts do not hold the same legal position as e-signature documents. Storing contracts in a secure e-signature environment ensures that legal challenges are met and access to documents is within leading-edge capability. Carriers with these service and access capabilities will have a competitive edge over carriers that are still bound to paper or less secure processes.

Methods for Combating Fraud

E-signature and secure documents play a huge role in combating fraud. A well-executed e-signature and secure document initiative causes the following to happen:

- The signer is discretely and uniquely identified.
- The document content is locked through encryption technology and cannot be altered without being identified.

- The document is electronically stamped with the time and date through all steps in the process.
- The document is stored for access without threat of being misplaced or its existence being denied entirely.

Because these outcomes are generated by e-signature technology, the potential for fraud is reduced. In the legal profession, denying that something is true or has happened is called repudiation. People frequently perpetrate fraud by:

- Denying that a document was signed
- Asserting that the content of the document was different
- Submitting claims for a loss that happened within a time frame that differs from what the carrier can prove

E-signature and secure document technology establishes a transactional and factual environment where repudiation and thus many types of fraud cannot successfully exist.

Compliance

Clearly, carriers can make great strides in the area of compliance by putting e-signature and secure document technologies in place. The ability to meet requirements related to state insurance department audits, the Gramm-Leach-Bliley (GLB) Act, and the Health Insurance Portability and Accountability Act (HIPAA) is significantly facilitated by e-signature technology. Not only do the technologies make documents tamper proof and error proof, but they address data security issues as well. The audit trail provided by e-signature software will grow in importance as regulators focus more and more on where personal information goes in an electronic world.

Cost Savings

E-signature and secure document technology allows carriers to save money on postage and specialty mail-handling costs. Additionally, cost savings emanate from decreased clerical handling of paper. Data rekeying and manual data verification are also reduced, and paper document storage costs can be decreased. Given that applications and contracts for insurance coverage must be kept for a minimum of seven years, those savings can translate into a meaningful amount of money.

The Greening of the Insurance Industry

A growing focus is on businesses and transactions that are environmentally friendly. Many consumers make positive buying decisions when organizations are conscientious about their use of resources that impact the environment. Organizations recognize this trend and now advertise that their business processes do not adversely affect the environment. The insurance industry's reliance on paper is fairly well established. As time goes on and the "green-ness" of companies becomes more of a reputation issue, carriers must make their own claims about being environmentally conscientious. E-signature and secure electronic documents can play a large role in making this happen.

Opportunities for Enterprise Adoption

Carriers must make development decisions on an enterprise basis. IT budgets are stretched thin relative to the demand for new functionality. Exhibit 2 illustrates that the funds for true new development are generally less than 10% of the overall budget.

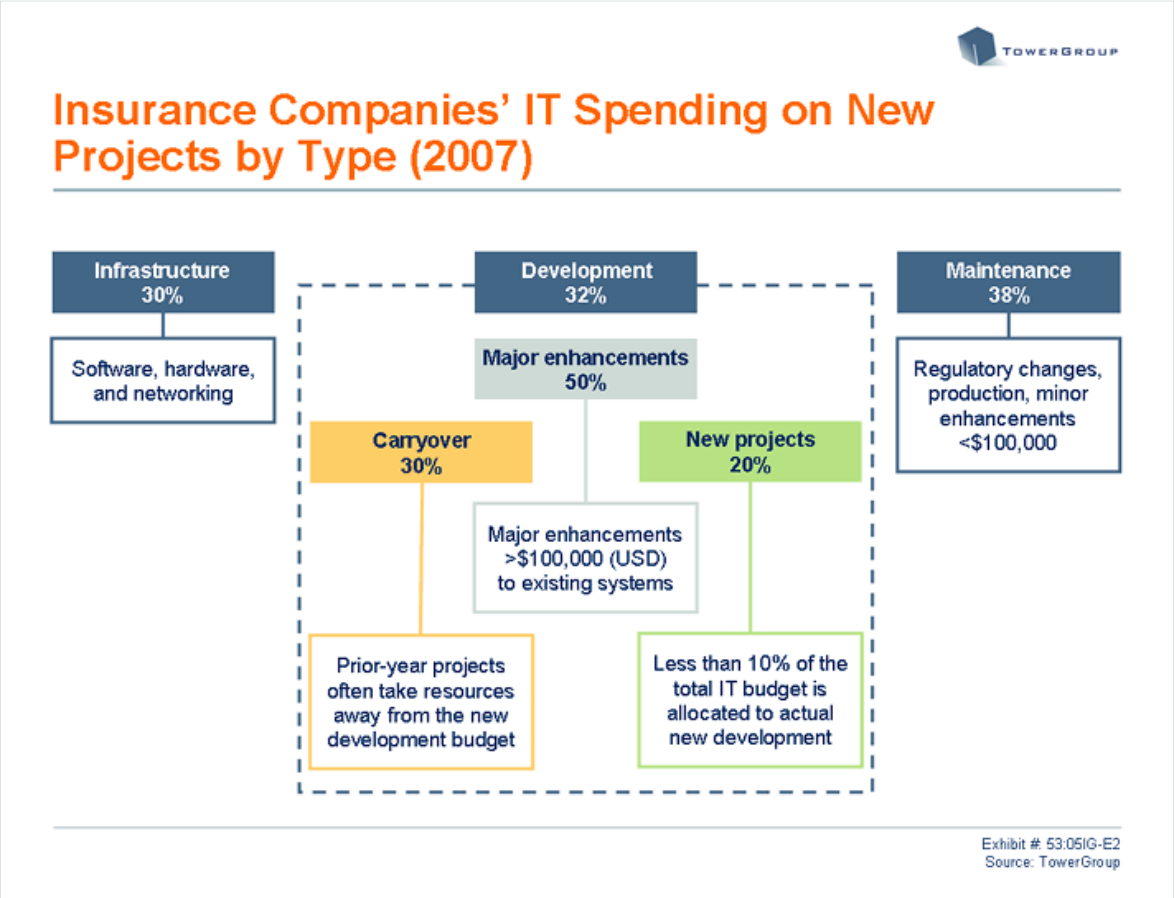

Exhibit 2
Insurance Companies' IT Spending on New Projects by Type (2007)
Source: TowerGroup

E-signature and secure document software can definitely benefit many areas of a carrier's operations, thus lowering total cost of ownership.

Personal Lines and Commercial Lines Underwriting

Nothing happens in an underwriting department until someone fills out an application for insurance. The signature on an application is vital because it indicates that the information provided is factual and true. Any attempt on the part of a carrier to deny a claim based on incorrect information on an application will most likely not succeed if there is no signature. The need for e-signatures and secure documents to facilitate the acquisition of business in the quickest, most cost-effective, and most legal manner is critical. Additionally, for high-valued and complex risks, specifically in midsize to jumbo commercial lines, many documents, not just the primary application, require signatures. As indicated earlier, the people who need to review and sign documents can be spread across numerous locations and continents. The necessity to send legal documents and acquire signatures can continue throughout the policy life cycle, so the requirement definitely is not a one-time mandate for new business only.

Claims

The claims settlement process is document intensive. Many of the documents used by claims adjusters require signatures. The need to send a document to the customer and then wait for it to be signed and returned adds time onto an already long process. In claims, time is always of the essence, and a carrier's ability to accelerate processes, such as for medical release forms, makes a major difference in cycle time. This time saving is especially critical in worker compensation

claims because injuries can worsen, and prompt gathering of information is imperative. Although some forms that require signatures can be faxed, carriers must remember that faxed documents are not secure because a signature can be cut and pasted. Carriers take many steps to ensure that they will not find themselves in court over claim handling. Relying on a faxed signature in a court of law is not prudent. The legality and security of an e-signature transaction is the direction that carriers should be taking for documents that are legally pivotal to the adjusting process.

In addition to executing a transaction with the consumer on their own computers or laptops, carriers should strongly consider extending e-signature capability to applications that are used with mobile technology. An adjuster who is meeting with a customer can, potentially, wrap up a claim during a face-to-face meeting if the adjuster is equipped to acquire the signature. Exhibit 3 illustrates where mobile solutions enhance outcomes in the claims settlement process. The stages outlined in red are areas of opportunity for mobility.

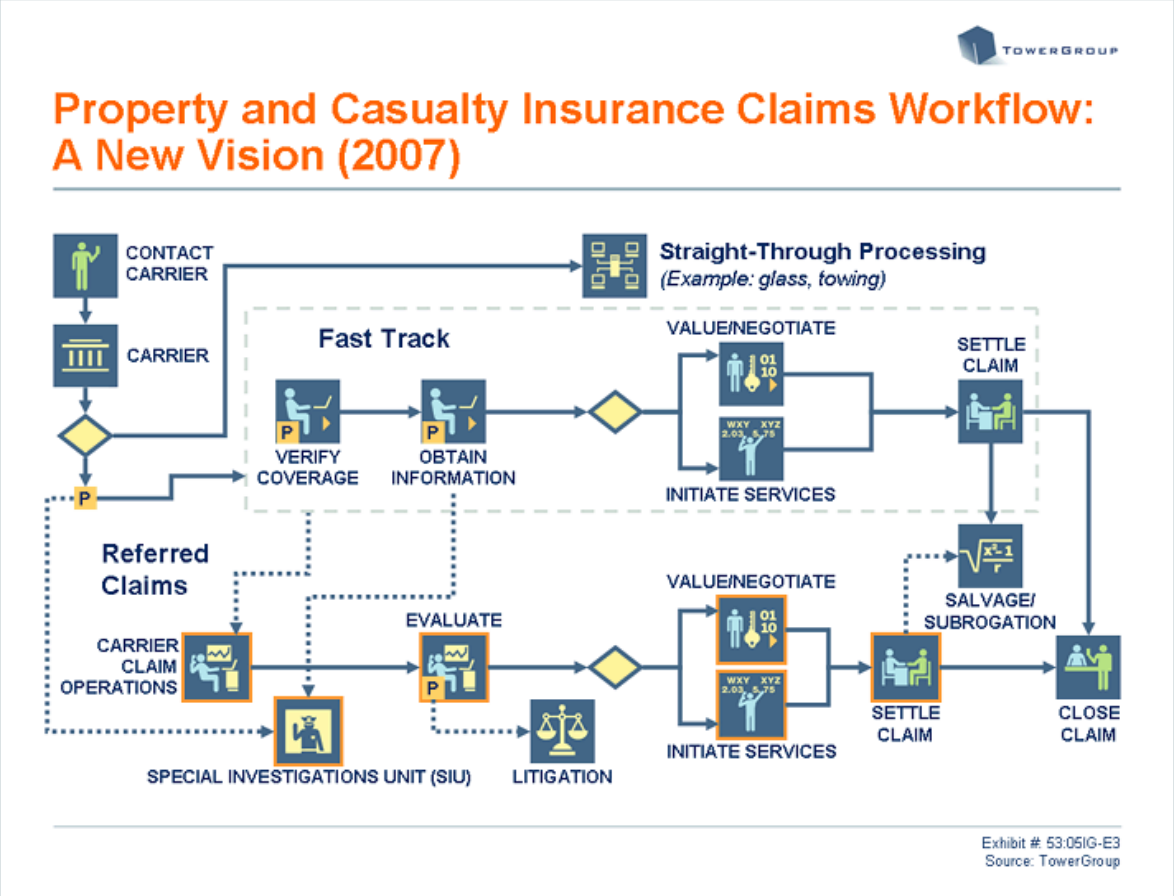

Exhibit 3
Property and Casualty Insurance Claims Workflow: A New Vision (2007)
Source: TowerGroup

Carriers also need to consider the type of signature capture relative to the legal requirements of the document. A signature pad attached to the adjuster's tablet or ultramobile PC is, in all probability, the most practical way to capture a signature and brings competitive advantage as well as cost savings. However, carriers must determine if some documents require more sophisticated signature capture methodologies and do not qualify for signature pad authorization in connection with a mobile device. These transactions can then be routed to the consumer through higher-security e-signature methods.

Human Resources

An initiative to use e-signatures and secure documents can have considerable internal benefits. Human resources (HR) departments have benefit forms and other legal documents that require signatures from employees. Multiple office locations and the ever-expanding existence of remote workers make e-signature capability a plus for carrier HR departments. Not only can these transactions happen faster, but the storage of these legal documents can be taken out of file cabinets and held in secure electronic form. Since some documents HR receives must go on to third parties, e-signature technology ensures that these transactions are routed in a secure environment and personal information of workers is not exposed.

Legal Department

Another internal use for e-signature is in the legal department. Many carriers have their own internal legal counsels, for whom contract execution can be a large part of their responsibilities. An enterprise e-signature and secure document system will not only reduce the time to complete these transactions but also ensure enforceability and defensibility.

Adoption of e-signatures at the enterprise level is important to decrease total cost of ownership as well as to ensure adoption in all business units. As stated early in this Research Note, industry experts indicate that one of the primary barriers to more rapid and pervasive use of e-signature technology is that adoption decisions are discretely made for one business unit at a carrier. Carriers persist in making technology decisions on a siloed basis. A single business unit choosing to implement a new business process that is radically different from the time-honored, traditional incumbent process is not likely to succeed, as many carriers have discovered. Changing the culture is critical for adoption success of e-signature functionality, and an enterprise initiative is the way to facilitate that.

Keys to a Successful E-Signature Implementation

Carriers must take several steps before they can implement e-signature and secure documents successfully. TowerGroup interviewed business people and vendors that have implemented e-signature functionality and learned that, although e-signature initiatives are spotty in the P&C insurance industry, best practices are starting to emerge. These best practices dovetail with successful implementations in other segments of financial services.

Create a Project Task Force

An e-signature initiative is not just another IT project. It is critical that all interested and impacted parties commit to and participate in the project development. Above all, senior executives must be committed to its success; otherwise, adoption will be imperiled. Because leaving pen and paper behind leads to serious cultural change, old processes could easily remain in place without executive-level commitment and enforcement. All affected business units must be represented on the task force, including business units that may be late users of the technology. Their initial participation in the project will negate having to potentially rework parts of the process. Representatives from the legal, marketing, field operations, sales, and IT units must also have a voice in the project, as should individuals responsible for training internal and external users. E-signature will require carriers to develop new processes and workflows, preferably with the input of all impacted parties, including the distribution force.

Decide Whether to Buy or Build a Solution

E-signature and secure documents are heavily laden with security issues. It is critical that carriers make a realistic assessment of their own capabilities and determine if they will build or buy a solution. Several good vendor-provided e-signature and secure document products are available in the marketplace. Examples of vendors that provide these products are Adobe Systems, Communication Intelligence Corporation (CIC), DocuSign, and Silanis Technology. Working with a vendor that has deep expertise and installation experience enables carriers to bridge the practical knowledge gap.

An additional consideration is whether the solution should be supported internally or hosted by a vendor. This avenue is worth exploring if a carrier finds that developing some of the components costs too much or takes too much time or simply chooses not to add to core capabilities. E-signature initiatives require very deep security expertise. TowerGroup finds that, increasingly, carriers are seeking vendors that have focused and detailed expertise in security related to specific applications and are partnering with them rather than doing internal development.

Choose the Appropriate Signature Process

Carriers can implement an electronic signature capability in a number of ways, but not all signature methodologies are right for all processes. Before determining which signature type to implement, carriers must assess business processes and determine how much complexity the process warrants, legally, and how much complexity it can tolerate from a practical standpoint. This is likely to be a balancing act with some trade-offs. Exhibit 4 assesses the business complexity and risk of five signature types.

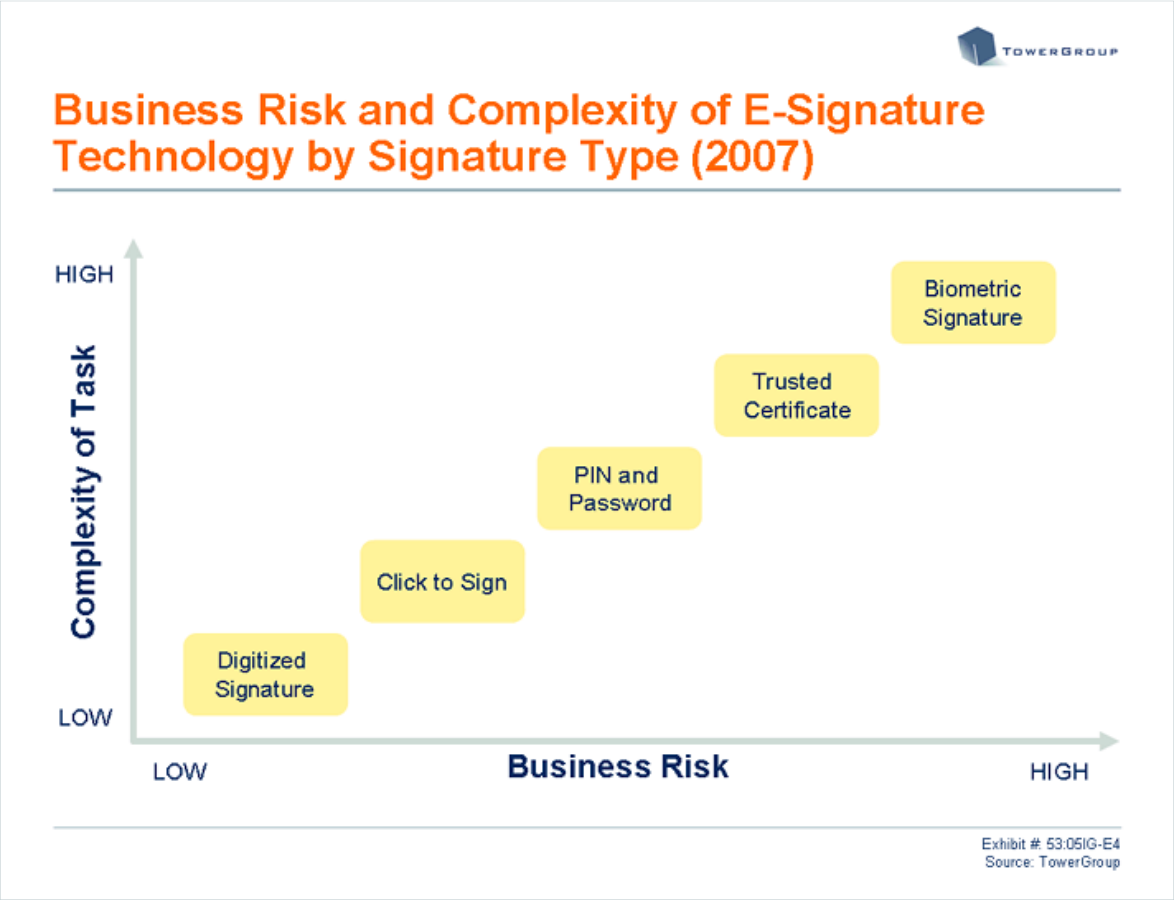

Exhibit 4
Business Risk and Complexity of E-Signature Technology by Signature Type (2007)
Source: TowerGroup

In all probability, a carrier will need several signature capture capabilities. Less risky transactions may be well suited to a digitized signature from a signature pad. However, some business processes that could generate serious business risk if not handled with the utmost security may require electronic certificates or even biometric signature. Collaboration among the business people who understand processes and results, legal counsel who can interpret the law, and seasoned and experienced e-signature experts is absolutely imperative. It bears repeating that they need to collaborate before the project begins. Backtracking if results are not as expected is a waste of time

and money and can permanently jeopardize adoption.

Put Straight-Through Processing in Place

A number of processes must be in place for an e-signature implementation to be successful. In P&C insurance, the term "straight-through processing" (STP) is frequently connected to the processing of new business, endorsements, or claims with no manual intervention. STP in these scenarios involves automating several processes utilizing a number of technologies. For purposes of e-signature, STP is a subset of the larger initiative. While e-signature and secure documents can play a critical role in a robust STP capability, the elements that must be in place to facilitate e-signature are:

- Real-time data integration into documents
- Secure document capabilities
- Storage for the signed documents
- Archiving and retrieval capabilities

Some business people TowerGroup interviewed found that the front-end issues, real-time data integration, and document preparation were the tasks that garnered all the attention. When carriers seriously considered the back-end storage and retrieval issues, they were deep into the project and thus delayed the implementation. Making certain that all segments are scoped out and well accounted for is critical to success.

Summary

Electronic commerce is no longer a "nice-to-have" capability. A more global business model demands that carriers adopt capabilities for moving documents electronically. Consumers are becoming less tolerant of paper-based transactions because of both the time and volume required. Insurance business processes are bound by many legal requirements, and fulfilling those requirements in a cost-effective and documented way is a critical concern for the insurance industry. The ever-increasing demand to establish competitive advantage and deal with pervasive problems related to fraud and compliance requires new and creative solutions. Electronic signature technology has enterprise applicability to address all these issues.

Insurance carriers must transition away from traditional paper-based, wet-signature processes and adopt secure document and electronic signature technology. The technical complexity may appear daunting, but technology solutions providers and experts in the marketplace can partner with carriers to overcome this hurdle. The legal barriers have been eliminated by ESIGN and UETA enactment. The pen is now on the Web, and the time is right for carriers to reach out and grab it.