

*Draft*



**Building an Industry-Standard for an Electronic Signature  
Associated with Straight through Processing of Annuities**

**Recommendation of the NAVA E-Signature Working Group**

**November 15, 2003**

*Draft*



**Copyright © 2003- 2004 by the National Association for Variable Annuities except as otherwise indicated. All rights reserved.**

The contents of this publication are copyrighted by the National Association for Variable Annuities. Copyright is not claimed as to information excerpted from the SPeRS Version 1.0 publication. All rights are reserved by NAVA, and content may not be reproduced, disseminated, published, or transferred in any form or by any means, except with the prior written permission of NAVA.

The NAVA logo is a registered mark of NAVA.

This publication is provided with the understanding that neither NAVA, its directors, officers or staff members, or other persons contributing to this publication are engaged in rendering financial, accounting, or legal advice, nor do they assume legal responsibility for the completeness or accuracy of the contents of this publication. The text is based on information available at the time of publication.

*Draft*

## Table of Contents

Executive Summary.....	1
Background on Initiative.....	3
Acknowledgement of Participants.....	4
Findings of the Technology Task Force.....	5
Findings of the Legislative Task Force.....	8
Operational Benefits of E-Signature.....	10
SPeRS Methodology .....	15
Findings of the Working Group.....	17

### Appendices:

Technology Report.....	A
Legislative White Paper.....	B
Operational Flows.....	C
Results of Decision Criteria Survey .....	D
Summary of SPeRS.....	E

*Draft*

## **Executive Summary**

In the telecommunications industry, stringing the “last mile” of fiber-optic cable is always the most costly and presents the toughest engineering challenges.

With respect to straight through processing of annuities, elimination of a “wet signature” is our “last mile,” along with its costs and complexities. While we have made good progress as an industry in reducing paper flow (first electronic data exchange, then introduction of business rules, and now forms standardization) we need to dispense with a wet signature to achieve true end-to-end processing and realize all the benefits of automating the process. The elimination of this wet signature could come in the form of an electronic one, an abdication of the signature requirement to the broker/dealer or the elimination of the signature requirement. While the latter two scenarios will be reviewed by this working group in the next cycle, the subject of this white paper is the electronic signature.

Outside of a vertically integrated arrangement where product manufacturer and distributor are the same, the hard economic benefits of moving to an electronic signature are likely not galvanizing for carriers or distributors by themselves. Both groups have finely honed the signature follow-up process such that the costs of pursuit are not easily outweighed by the investment in technology needed to adopt electronic signature processing.

Only by coupling an electronic signature process with electronic document delivery can our industry see its return on investment meet an acceptable hurdle rate. Additionally to which, the lack of human intervention will mean higher percentage of in-good-order business. And with the increased ease of selling and processing one would hope to see increased product sales.

Here’s the good news:

- Our customers are ready for this, as electronic signature becomes standard practice in other transactions inside and outside of the financial services industry.
- The technology used to implement electronic signature processing is fairly mature
- ESIGN and UETA (if not case law) provide a solid legal and regulatory foundation to establish the signing processes and meet associated requirements.

The E-Signature Working Group recommends that we initiate a pilot and develop an implementation plan for both electronic signature and electronic document delivery early in the first quarter of 2004.

## **Background**

### ***NAVA Technology Committee***

In June of 2001, NAVA created the Technology Committee to identify, research, endorse, and communicate technological directions for the benefit of the annuity and life insurance industry. This was a spin off of the NAVA Operations Committee. The Technology Committee views its charter as defining the industry architecture and setting priorities in the development of open industry standards for annuities. The actual development of those standards is handled within the framework of an ACORD process – with participation of as many business experts within the annuity industry as possible. Many of the Committee initiatives require the participation of NAVA’s Operations and Regulatory Affairs committees.

### ***Electronic Signature Initiative***

An E-Signature Working Group was formed in 2002 to address electronic signatures (“E-Signatures”) as part of the industry initiative of straight through processing. That working group formed several task forces to assist them in their deliberations. *The working group’s scope was defined to include E-Signatures that would bind an electronic annuity application (“E-App”), but with a solution that could be used for in force electronic transactions as well.*

The Technology Task Force was created to prepare a Technology Report that identifies the electronic signature technologies and the vendors who provide them, and the Legislative Task Force was created to analyze the federal and state legal issues arising from use of those technologies in the account opening processes described in the Technology Report.

By mid-2003, with the findings of these two task forces complete, the working group began its deliberations, analyzing the findings and made its recommendation to the Technology and Operations committees in the fall of 2003. The Regulatory Affairs Committee has begun its work in parallel to formulate an approach on getting consolidated, industry state approvals.

# *Draft*

## **Acknowledgements**

### ***Industry Participants***

The E-Signatures working group has participants representing the legal/compliance, operational and/or technical sides of the business from the following member companies: ACORD; AEGON; AIG/SunAmerica/Valic; Allianz Life; Allstate; American Express; American Skandia/Prudential; Banc One; Blazzard, Grodd & Hasenauer; Blue Frog Solutions; Chase Insurance; DALBAR; eAgency; Edward Jones; Fidelity Investments; Foley & Lardner; GE Financial; Goodwin Procter; Hartford Life; ING US; Integrity Life; Jordan Burt; Lincoln National; McCarthy Fingar Donovan; Merrill Lynch Insurance; MetLife; Morgan Stanley; Nationwide Financial; New York Life; NewRiver; Pacific Life; Phoenix; Prudential Financial; RBC Liberty Insurance; SAFECO; SOLCORP; Sutherland Asbill & Brennan; Tactegy Consulting; TIAA-CREF; Transamerica Life; VeraVest; Wells Fargo; and Zurich Life.

In particular, we would like to recognize the following individuals who contributed to the drafting of this report:

Frank Spencer, Nationwide Financial, **Co-chair**  
Alex Varghese, Merrill Lynch Insurance Group, **Co-chair**  
Deborah Alexander, Transamerica  
Pamela Burnham, Hartford Life  
Tom Conner, Sutherland Asbill & Brennan  
George Dobbs, Phoenix  
Jan Gaby, Nationwide Financial  
Judith Hasenauer, Blazzard, Grodd & Hasenauer  
Bob Kiggins, McCarthy Fingar Donovan Drazen & Smith  
Brian Mannion, Nationwide Financial  
Eric Miller, Highpoint Partners  
Paula Minella, Fidelity Investments Life Insurance  
Lynn Peterson, American Express Financial Group  
Linda Samay, Fidelity Investments Life Insurance  
Jeff Stein, Nationwide Financial  
Deb Tucker, NAVA  
David Whitaker, Goodwin, Procter & Hoar

## Findings of the Technology Task Force

### Goal

The goal of the Technology Task Force was to identify the technologies used to facilitate E-Signature and the vendors who provided them. Their findings are covered in a report entitled “Technology Report – E-Sign Technologies and Vendors”. As part of their analysis, the Task Force documented four process flows in the account opening/application process and provided guidance on risk assessment analysis that should be considered by the E-Signatures Working Group in selecting the appropriate technologies. The Report contains a vendor matrix. The findings of this Task Force are contained in Appendix A.

### Technical Options

Type	Description
Clickwrap	Clickwrap signatures offer a flexible, inexpensive signature solution for organizations that require neither the full-strength security of PKI encryption nor the identity verification by a Certificate Authority. Clickwrap signatures have dozens of applications, including internal company documents, online software licensing agreements, online business-to-consumer purchasing agreements, and contracts between known business partners. The ‘signature’ or ‘acceptance’ can be saved as a part of the business transaction record.
Fingerprints	Provides an electronic method of identification through an individual’s fingerprint. There are two methodologies associated with fingerprint biometrics. Each methodology requires an initial capture of a print and a capture of a print to authenticate the user.
Voice Signature	The stored electronic representation of the speaker’s voice is rich enough to allow the reconstruction of the original speech utterance for audition and identity judgment by other listeners and/or devices. The electronic representation must be associated with an identity credential such as a name, member ID, etc. The electronic representation must be transmitted over secure channels, encrypted before storage and transmission, and accessible only to authorized individuals and/or organizations.
Handwritten Signature Capture	Biometric signature capture digitally records the image of a handwritten signature and its dynamics. Although an individual never signs his or her name exactly the same way twice, one’s handwritten signature does conform to certain boundaries which are unique to that person.
Digital Signature	Requires that each signing individual be registered with a certificate authority. Direct application to new customers is not workable since they can not be expected to possess the needed certificate. However a scenario that is based on a much smaller set of people holding the required certificates is feasible. If broker who is closing the sale were properly equipped, that person could verify the identity of the purchaser(s) by inspecting their government documents, thus registering the new customer to allow for the signature.

### Account Opening Scenarios

The Working Group had identified four typical account opening/application scenarios. The Task Force documented these with four process flows:

- Rep or broker/dealer working with a customer in a face-to-face situation
- Rep working with a customer on the phone
- Customer working alone, online
- 1035 transfer

## *Draft*

The report looks at a series of workflow scenarios and makes an initial assessment of which type of technology would be a potential fit for that workflow.

### ***Risk Assessment***

There are two aspects to the risk: one is with respect to the identity of the signer; the other is with respect to the possible financial loss associated with the transaction in question. By understanding the risks associated with each type of E-Signature and its intended application, a proper enrollment procedure can be created. The Technology Report adopts the framework of the National Electronic Commerce Coordinating Council, which established a four level categorization of the risk of loss: Rudimentary; Basic, Medium and High. The report further suggests types of verification that might be required by an institution for each of the four levels.

### ***Verification of Identity***

The report explores strategies for the verification of a person's identity and stresses the importance of enrollment procedures so that credentials can be validated. Certain technologies have the identification built into to the signature process; others require a separate signature authentication.

### ***Trust between Entities***

The report focuses on technical solutions. The report does not focus on the business and technical frameworks that would be needed to establish end-to-end scenarios including multiple business partners, such as broker/dealers and carriers. The Task Force noted in their report the correlation between strength of the "trust level" and the various technologies used.

### **Conclusion**

The Technology Task Force made initial recommendations on which of the various technologies would be best suited for the various levels of risk and the different type of workflows. The team eliminated some forms of biometric signatures that it found too invasive. Except for Clickwrap, all the scenarios have a need for a registration database. For companies that don't need to share these signatures across company boundaries that can be easily done. However, all the participants saw the need to create ways for the signatures to be shared between and verified by multiple entities. This creates a need for interoperability between the carriers and broker/dealers (and others) that will need to be addressed during the pilot phase.

# *Draft*

## **Findings of the Legislative Task Force**

### **Goal**

The Legislative Task Force reviewed the state of the law relating to e-commerce and case law regarding the validity of E-Signature methodologies as outlined in the Technology Report. Their findings are covered in a white paper entitled "Building an Industry-Standard for an Electronic Signature Associated with Straight Through Processing of Annuities: A Discussion of Legal Issues Involved". As part of their analysis, the Task Force also reviewed the impact on electronic processing of other federal requirements such as the Gramm-Leach-Bliley Act, USA PATRIOT Act, federal securities laws and regulations promulgated by the Securities and Exchange Commission (SEC). Finally, the Task Force reviewed the industry's experience to date with state insurance departments. The findings of this Task Force are contained in Appendix B.

### **Summary of the Law**

Under E-SIGN (the Electronic Signature in Global and National Commerce Act) and UETA (the Uniform Electronic Transactions Act), a record or signature may not be denied legal effect or enforceability solely because it is in electronic form, and if a law requires a record or signature, an electronic record or signature may satisfy the law. The white paper outlines the requirements of what is needed to formulate a signature in good order under E-SIGN and UETA.

Under E-SIGN and UETA, an electronic signature may be created in a number of ways and will be valid so long as it is attached to, or logically associated with, a record, created, or adopted, by the signer, with the intent to sign the record. Other requirements relating to authentication, document integrity, non-repudiation, consumer notice, and record retention must also be met.

An electronic transaction may, depending on the circumstances, also need to satisfy the requirements of one or more of the other federal laws and regulations noted above. These involve privacy laws, anti-money laundering, prospectus delivery, and retention of electronic records:

#### ***Privacy Laws***

- Under the SEC's Regulation S-P, a privacy notice must be delivered to applicants but this may be done electronically.
- Consumer information provided electronically, including an electronic signature, must be safeguarded so as to be secure and confidential and protected against unauthorized use.

#### ***USA PATRIOT Act***

- Anti-money laundering, customer identification, and suspicious transaction reporting programs must address electronic transactions.
- Non-documentary methods to verify customer identity must be employed when applications and other transactions are conducted electronically.

#### ***Prospectus Delivery***

- SEC rules require notice, access and evidence of delivery.

## *Draft*

- ESIGN requires consent and consumer demonstration that the consumer can navigate the means of electronic communication that is used to deliver the prospectus.

### ***Document Retention***

- Regardless of the electronic signature methodology used, the document must be unalterable after signature.
- Customer information maintained electronically must meet the requirements of SEC Rule 17a-4(f).

While there was an initial perception that state insurance departments would question whether the use of electronic signatures in the E-App process met applicable regulatory goals, the Task Force could not find any published regulatory guidance or specific examples to justify this concern.

### **Conclusion**

The Task Force did not identify specific legal or regulatory impediments to industry adoption of the use of E-Signature in annuity processing as outlined here. The Task Force cautions member companies that:

- ESIGN and UETA are relatively new statutes and there is little case law interpreting them.
- Electronic processing must be set up so as to comply with the requirements of other federal and state laws applicable to the sale of annuities.
- The lack of state regulatory uniformity regarding electronic commerce makes it unclear how individual state insurance departments will react to electronic processing of annuities.

- 

The Regulatory Affairs Committee has begun its work to formulate an approach on getting consolidated, industry state approvals for electronic signature filing on behalf of the industry.

## **Operational Benefits of E-Signature**

This section is intended to provide a high level framework to understand:

- What kinds of benefits could reasonably be expected
- The rationale for investment in this technology
- Benefits to the annuity business as a whole
- Possible barriers to success as an investment

### **Purpose of Electronic Signature Capture Initiative**

Capturing signatures electronically (vs. “wet signatures” on paper) is not an end unto itself. It must be viewed as a piece of a whole continuum of business choices to enable the annuity industry to be “easy to do business with” for agents and end consumers in a cost effective way. E-Signatures will enable end-to-end electronic processing that includes electronic document delivery when client-consent is obtained at point of application. Once E-Signatures are a reality, it streamlines the process, eliminates one more reason for an agent or consumer not to purchase an annuity (as opposed to a mutual fund or CD) and gets the operations area one step closer to true straight through processing that will allow us to spend our people resources on truly value added interactions with our agents and consumers.

E-Signatures, in conjunction with other NAVA initiatives (standardizing transfer data, ACATS, forms etc) dramatically improve the “Ease of Doing Business” quotient for agents and consumers. Without electronic signatures, there will continue to be gaps in the efficient and seamless business flow.

### ***Consumer & Advisor Experience***

The world has changed, and with it, agents and consumers expect to be able to do business differently than 10-20 years ago. Their daily lives are full of electronic, “real time” data exchange. For certain pieces of the annuity application and service life cycle, this is now a reality. For other pieces, there are discordant manual interruptions in the end-to-end process. The annuity business is not just competing with itself for agent and consumer loyalty. It is fighting for the “share of wallet” of all other choices for the consumer and agent’s discretionary time and money. Annuities are perceived as complex and time consuming. These interruptions in business flow reinforce this perception that is bigger than the reality. Perception becomes reality, preventing the annuity marketplace from growing to its full potential.

# *Draft*

## ***Current Practices***

Many carriers and distributors have enabled online application processing and data exchange, either through industry vendors or proprietary applications. These online applications collect data that is driven by business rules for the product that then “populates” the appropriate paperwork. This allows business to be “in good order” before it is sent. Other businesses have web-enabled direct business with consumers or accept data over the phone for the agent to enter.

The agents’ electronic identifier has been accepted as their “signature” if security processes for workstation and application access are in place. However, in order to get the client’s signature, this seamless electronic process is broken in several ways:

- The agent must print the electronic output, have the client sign the forms, and mail it to the manufacturer to match the signature with the contract data they already have received over the feed, or
- The manufacturer will need to produce an “application” or “owner acknowledgement” page and request the client’s signature by mail at time of contract delivery (with follow up if not received)

If the new business is an exchange, the need for a “wet signature” by the replaced carrier drives overnight mail costs and frustrating delays for the agent and the consumer.

Many manufacturers have modified their initial processes to limit the amount of follow up when signatures are not received, preferring instead to obtain the pending signatures when a client requests any change on their account (monetary or non-monetary). There is a business risk assumed in this modification of process. E-Signatures would close that risk, but may replace it with different risks. In addition, many manufacturers no longer file the “owner acknowledgement” forms with the states, thus there is little “hard save” in not needing that form any longer.

## **What Benefits Are Included/Excluded**

Benefits specific to the change between obtaining a “wet signature” and an “electronic signature” are:

### ***Cost Reductions***

- Printing costs
- Postage costs involved in sending the paper (needed for wet signature) to the carrier for cash and exchange business
- FAX costs
- Owner acknowledgement and follow up letter programming/maintenance costs
- Incremental “people time” for handling the following up process (mail desk, workflow processes, etc)
- Phone volumes from consumers/agents about the status of the signature

### ***Opportunity Costs***

- Exchange business asset booking “time”

## *Draft*

- Agent productivity (printing paper at point of sale, etc)
- RR efficiencies - frees up more time for agent for interpersonal activities
- Back office efficiencies - reduction in time spent on matching paper and electronic documents.

### ***Regulatory and Consumer Complaints/Risks***

- When signature is not obtained

Benefits excluded as they are not directly a result of the electronic signature capture (though signature capture may enhance usage of tools that directly enable these benefits) are:

- Business in Good order increase
- Driving business to the Web for self service
- Consumer selection of total electronic statement delivery

### **Business Risks**

The industry must be able to demonstrate that the use of E-Signatures reduces annuity costs, completes transactions more quickly, ensures legal enforcement, and provides technical security. This goal will only be achieved if the transaction is as convenient for the customer as providing a handwritten signature today.

Similar to other groundbreaking business opportunities, the use of E-Signatures to complete annuity product transactions involves many business risks. The predominant research and development expense involves developing a cost-effective and enforceable electronic signature technology. The technology must be adaptable and scalable. The solution might change depending upon the level of risk inherent in a contemplated annuity transaction.

In addition to the cost of development, early adopters will need to develop and implement a technology that satisfies the business requirements of each party involved in an annuity transaction. The lack of standard protocols regarding the use of E-Signatures and the technology associated with E-Signatures further complicates this emerging field.

### **Scenario Building & Payback/Benefit Projections**

Because processes have been modified by many carriers over the last few years to reduce the costs involved in collecting signatures “on the back end” as SNAP tickets and online application methods have become more common, the hard costs for collecting signatures are relatively small, as measured as a percentage of overall new business and service costs.

We believe the operational benefits are primarily in the following areas:

- Firms which are both the manufacturer and broker/dealer (captive sales force). These firms can control the methods of the sales process and will save much in agent productivity. Historically, they have not done the “signature later” approach as they understand the burden on the manufacturer - as they are the same entity.
- Broker/dealers whose internal practices require them to obtain signatures even when doing business electronically. By changing to an E-Signature

## *Draft*

- process, they avoid printing the electronic annuity application output and their back office personnel avoid a lot of manual process and costs associated with either imaging/sending or copying/ mailing the paperwork and sending to the manufacturer. The Broker/dealers who have been using the "signature later" approach will be difficult to convert. The carriers have made it easy for the Broker/dealers to avoid dealing with the signature.
- The manufacturer saves time and money by not having to match the electronically transmitted new business with the later arriving paper (either image or hard copy) with the signature.
  - All Firms - whether broker/dealer or manufacturer would avoid cost and delays by accepting the E-Signature. This benefit would be compounded by the adoption of the other work going on in standardization of forms/data exchange. By leveraging that, along with the electronic annuity application capabilities, the exchange process would be dramatically transformed in end-to-end process speed and cost.
  - Direct Business Online would benefit by avoiding the "hard copy" follow up processes involved.

### **Requirements for Success**

- Processes must be designed based on agent and consumer needs and desires that then are analyzed to determine how to make them efficient/cost effective - not the other way around. The industry web experience has taught us that if "we build it" based on our internal cost needs and efficiencies they won't necessarily use it. However, if a process can speak to their need or want, they will use a new process.
- In order to change behavior, it must not only address an agent or consumer need, it must be "standard" for the vast majority of their business. If it is perceived as "one off", or only applicable to a niche portion of their overall processes, behaviors will not change.
- Training and education will need to be a continual process to drive perceived value and behavior.
- Avoid tools that will only address niche portions of the business or drive the need for multiple tools. This addresses not only requirements for changing agent and consumer behavior, but the cost of the tools and the need for volume.
- Businesses must still be able to accept "wet signatures" in cases of system failures, consumer disabilities, or consumer preference.
- Processes must be designed and tools selected that will not drive a different follow-up process for the E-Signature. (Example: if business can come in without the electronic signature and we must call or write the consumer to request that they "click" or "call" to collect the signature.
- Maintenance and upgrade costs must be minimal or the payback period will never be met.
- The industry adoption must be broad and deep to get the most benefit. For example, if exchange business uses electronic signatures, but many manufacturers do not have the tools to "read" or the processes to accept, then even adopter manufacturers will have to send "wet" signatures.
- Other processes must be examined for leverage points and opportunities.

## *Draft*

- Regulatory risk must be kept at least even with the current risk profile.
- Proliferation of multiple tools among distributors and manufacturers must be kept to a minimum to avoid needing many different tools to send and receive signatures to do business.

## *Draft*

### **Recommendation for Use of SPeRS Methodology**

New eCommerce laws and regulations make possible the widespread replacement of paper documents with electronic records. While the new eCommerce laws and regulations permit the use of electronic records and signatures, they also require that electronic systems and processes meet standards for:

- ***Consent and Disclosures***

Informing users about what they are “signing” online and about their rights and responsibilities under consumer protection laws

- ***Identity, Security, Privacy***

Establishing the identity of users, and employing procedures that limit exposure to identity theft, fraud, money laundering, etc

- ***Signature***

Establishing intent to “sign” a transaction, such as by a two-step process that confirms intent and avoid the “slipped finger” syndrome

- ***Agreements and Notices***

Making documents accessible online and providing required notices electronically, such as by hyperlink to a designated site

- ***Record Retention***

Adopting standards for storing records that need to be reviewed or referred to later, making records available for printing, and protecting the integrity of records

Failure to meet those standards may impair the enforceability of electronic records. To address this, industry leaders have undertaken a cross-industry initiative to establish commonly understood “rules of the road” available to all parties seeking to take advantage of the powers conferred by ESIGN and UETA. The product of this initiative is Standards and Procedures for Electronic Records and Signatures (SPeRS).

Creation of such Standards and Procedures will:

- Permit businesses to establish a common understanding with vendors concerning design parameters for routine functions, without having to develop detailed custom specifications,
- Assist in establishing industry standards for commercially reasonable, enforceable structures and processes,
- Provide the customer with a “common experience” across various online transactions, increasing the customer’s comfort level with the transactions.

The SPeRS effort is an important initiative which is not being addressed in any other forum. NAVA and other trade groups such as ACORD, ABA, AFSA MBA, and the ACLI have agreed to recommend to its members the adoption of the standards as set forth in the “SPeRS Version 1.0” that was published in November 2003. A copy may be ordered from their website [www.spers.org](http://www.spers.org). See Appendix E for a summary of the material.

## Findings of the E-Signatures Working Group

### Basic Assumptions

- E-Signature solutions include Clickwrap, Voice, & Signature Pads
- Sales processes include face-to-face, telephone, direct and transfer business
- The same E-Signature solutions would be used for in-force document signature requirements
- E-Signature solutions will need to work with multiple platforms (DTCC, AnnuityNet, ACORD NBfA, Proprietary, etc.)
- E-Signature processes and procedures are as outlined in the flow process diagrams in Appendix C

### Risk Assessment

The Working Group surveyed its participants on the various forms that accompany an application to determine which forms are filed and what the perceived levels of risk are attendant to the signatures on those forms. The following summarizes the findings of that survey.

#### Current Forms: Risk Assessment Map

*Risk evaluated from perspective of importance to attach verified signature*

<b>MED-High Risk</b>	<b>HIGH Risk</b>
<i>form normally filed signature normally required</i>	<i>form filed signature normally required prior processing</i>
Application Application Acknowledgement / eTicket	NAIC forms Replacement paperwork Transfer-of-Asset form
<b>MED-Low Risk</b>	<b>LOW Risk</b>
<i>form not normally filed signature normally required</i>	<i>form not normally filed signature not normally required new biz</i>
Beneficiary Instructions*** eDelivery Consent Investment Options Supplement*** Qual Plan: Market Conduct Quests/Discl	DCA Instructions Direct Deposit Durable Power of Attorney forms/pwork Portfolio Rebalancing Request Qualified Plan Documentation Telephone Authorization form

\*\*\*include in this category because data content generally confirmed in app-later package which is signed (eSign validation desired but s/b part app acknowledgement)

# Draft

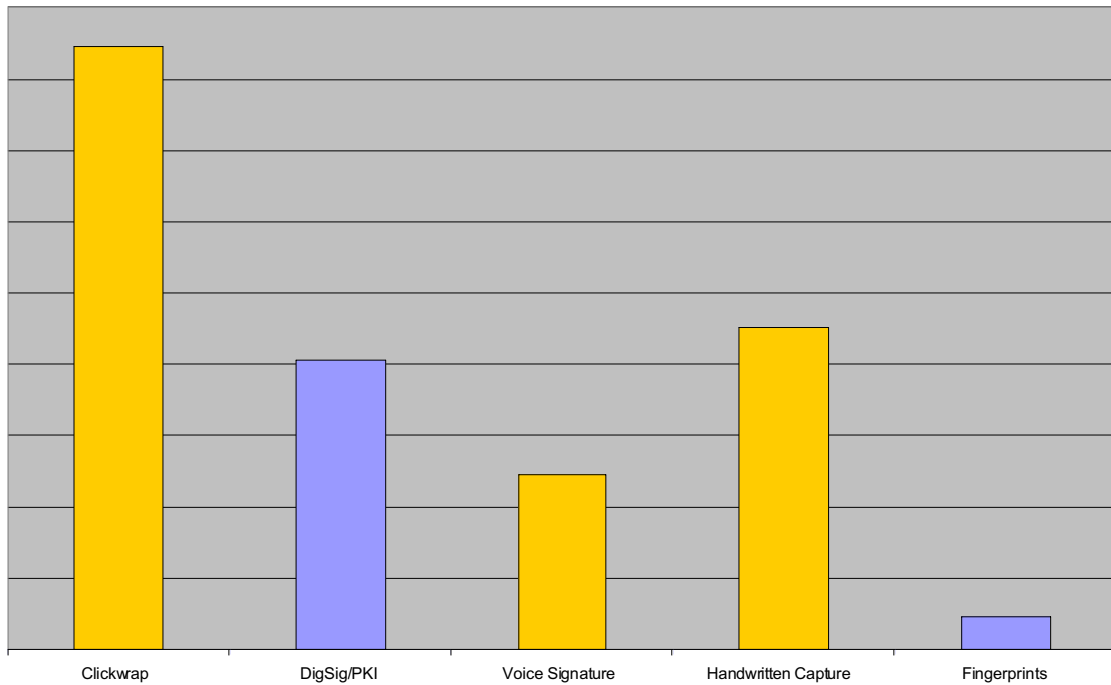
## Technologies Chosen

The Working Group reviewed the findings of the Technology Report. They felt it was important to down-select to two or three technology types. They used a decision criteria survey that ranked them for the following. A copy of the survey is included in Appendix E:

- Ease of Doing Business - Enhances Customer Experience
- Ease of Business - Enhances Ease of Operations/
- Shareholder Return
- Leveragable Solution
- Business Risk
- Sustainability/Life Cycle Expectations

The consolidated ratings are represented below. The working group then decided that it would make recommendations for Clickwrap, Voice and signature pad.

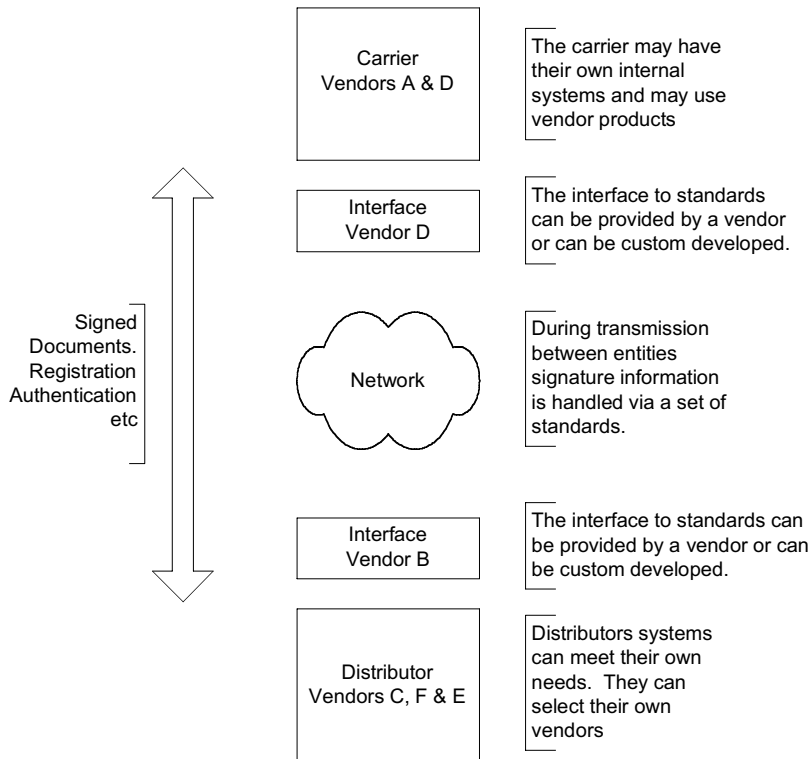
Cumulative Ranking



# Draft

## Interoperability

In an effort to get wide spread adoption for E-Signatures, interoperability is an important alternative to mandating a solution. A concept of utilizing standards for communication between entities but maintaining neutrality at the end points has been proposed. The networking industry has a long experience in dealing with interoperability issues and has frequently employed vendor neutral standards to allow the market to create innovation while at the same time allowing participants to effectively communicate with each other.



# *Draft*

## **Challenges**

### ***Ease of Use for the Registered Representative (RR):***

- It will be challenging to get the RRs to modify their sales process to support capturing the E-Signature.
- The RRs must be connected to the web tools for the electronic capture and signature process to work efficiently.
- The RRs must be trained and feel comfortable explaining the electronic signature process.
- Many RRs conduct multiple interview sales, with the final decision being initiated over the telephone and the data entry being conducted by clerical staff.

### ***E-signatures for 1035 Exchanges:***

An industry-wide agreement would be necessary to accept E-Signatures and a common form to surrender a contract as the replaced carrier on a 1035 Exchange.

### ***Authentication of signatory:***

An authentication solution will need developed that can support both face-to-face sales and sales-over-the-telephone. Additionally, such a solution will need to support in force transactions (post sale) as well.

### ***Non-Repudiation:***

ESIGN and UETA are generally silent regarding the issue of connecting the signature to the person responsible for the obligations in the contract. This connection is important because it assures the contract will not be disputed based on this fact alone. In electronic commerce terms, this is generally referred to as non-repudiation. All parties to the contract must be able to rely upon the E-Signatures of the other parties. Protections must be integrated into the technology solution to connect the E-Signature back to the owner of the signature.

For click-wrap specifically, non-repudiation is a concern. A process will need to be developed to ensure the signer cannot deny that they attached their signature on all appropriate documents.

### ***Document Integrity:***

To ensure document integrity, all electronic forms will need to be locked down and not be modified in any way after the signature is affixed. This will put extreme pressure on all electronic application platforms to keep all products and features current on the platform as newly added (but not supported) features will not be able to be added once the carrier receives the application. This will potentially slow down time to market new products and features.

### ***Cost Benefit:***

Carriers and distributors will be challenged initially to identify a cost benefit with E-Signatures as they will need to continue supporting processes for wet signatures and application-later. This is due to the fact that not all firms will utilize E-Signatures and for the ones that do, every new customer will be given

## *Draft*

the opportunity to choose “electronic or app-later” on an individual basis. The infrastructure will need to support both processes.

### ***Record Retention:***

In today’s electronic new business world, electronic data (not electronic forms) is transmitted for new business. A process will need developed to ensure the electronic signature is affixed to a non-modifiable form and this form is retrievable for future reference at the broker/dealer firm and the insurance carrier.

### ***Ongoing Maintenance of Solutions:***

An industry-wide process will need developed to keep all electronic new business processes utilizing electronic signatures compatible. Over time software solutions will be modified and signature pads will be upgraded and for the industry to obtain benefits from the processes they must remain compatible at all times.

### **Conclusion**

Capturing signatures electronically (vs. “wet signatures” on paper) is not an end unto itself. It must be viewed as a piece of a whole continuum of business choices to enable the annuity industry to be “easy to do business with” for agents and end consumers in a cost effective way. E-Signatures will enable end-to-end electronic processing that includes electronic document delivery when client-consent is obtained at point of application. Once E-Signatures are a reality, it streamlines the process, eliminates one more reason for an agent or consumer not to purchase an annuity (as opposed to a mutual fund or CD) and gets the operations area one step closer to true straight through processing that will allow us to spend our people resources on truly value added interactions with our agents and consumers.

*Draft*

## **Appendix A**

### Technology Report



## **Technology Report**

e-sign Technologies and Vendors

NAVA Technology Task Force  
May 2003

# Technology Report

## Contributors

- Linda Samay, Chair, Fidelity Investments Life Insurance Co.
- Deborah Alexander, Transamerica
- Pamela Burnham, Hartford Life
- Daniel Davis, Nationwide Financial
- Kathy Dermer, Wells Fargo
- George Dobbs, Phoenix Life Insurance Co.
- Adam Ducorsky, Morgan Stanley Investment Management
- Keith Joseph, Wells Fargo
- Tim Mead, GE Financial Assurance
- Brian Phillips, Merrill Lynch Insurance Group
- David Piereth, Morgan Stanley Investment Management
- Kimberly Smithson, Merrill Lynch Insurance Group

## Important Notice

**The information contained in this report is being provided to illustrate the various eSignatures technologies and vendors that are available – and should not be considered a comprehensive listing of what is available in the market. Much of the material was created by companies or organizations that are independent of NAVA.**

While NAVA and its committee members make every effort to present accurate and reliable information, we do not endorse, approve, or certify this information, and we do not guarantee the accuracy, completeness, efficacy, timeliness, or correct sequencing of such information. Your use of such information is voluntary, and you should rely on it only after an independent review of its accuracy, completeness, efficacy, and timeliness. If any specific commercial product, process, or service is referred to in such information by trade name, trademark, service mark, manufacturer, or otherwise, that reference does not constitute or imply endorsement, recommendation, or favoring by NAVA.

# Contents

<b><u>BACKGROUND</u></b>	<b>4</b>
<b><u>GOAL OF THE TECHNOLOGY TASK FORCE</u></b>	<b>4</b>
<b><u>E-SIGNATURE TECHNOLOGIES</u></b>	<b>5</b>
<b><u>ENROLLMENT AND RISK</u></b>	<b>6</b>
<b><u>VERIFICATION OF IDENTITY</u></b>	<b>6</b>
<b><u>VERIFICATION IDENTIFICATION METHODS</u></b>	<b>7</b>
<b><u>RISK ASSESSMENT</u></b>	<b>8</b>
<b><u>RISK ASSESSMENT PROCESS FLOW</u></b>	<b>9</b>
<b><u>TRUST AND VERIFICATION</u></b>	<b>10</b>
<b><u>ACCOUNT OPENING SCENARIOS</u></b>	<b>11</b>
<b><u>PROCESS FLOW: REP OR BROKER / DEALER AND CUSTOMER FACE-TO-FACE</u></b>	<b>11</b>
<b><u>PROCESS FLOW: REP AND CUSTOMER ON THE PHONE</u></b>	<b>12</b>
<b><u>PROCESS FLOW: CUSTOMER ONLINE</u></b>	<b>13</b>
<b><u>PROCESS FLOW: 1035 TRANSFER</u></b>	<b>14</b>
<b><u>TECHNOLOGY EVALUATIONS</u></b>	<b>15</b>
<b><u>EVALUATION:CLICKWRAP</u></b>	<b>15</b>
<b><u>EVALUATION: FINGERPRINTS</u></b>	<b>17</b>
<b><u>EVALUATION: VOICE SIGNATURE</u></b>	<b>19</b>
<b><u>EVALUATION: HANDWRITTEN SIGNATURE CAPTURE</u></b>	<b>22</b>
<b><u>EVALUATION: DIGITAL SIGNATURE (PKI)</u></b>	<b>23</b>
<b><u>APPENDIX: VRU PROCESS FLOW</u></b>	<b>25</b>
<b><u>VENDOR LIST</u></b>	<b>26</b>

## Background

### NAVA Technology Committee

In June of 2001, The National Association for Variable Annuities (NAVA) created the NAVA Technology Committee to identify, research, endorse, and communicate technological directions for the benefit of the annuity and life insurance industry. This was a spin off of the NAVA Operations Committee.

### Intent of the Committee

The NAVA Technology Committee views its charter as defining the industry architecture and setting priorities in the development of open industry standards for annuities. The actual development of those standards is handled within the framework of an ACORD process – with the participation of as many business experts within the annuity industry as possible.

### Subcommittees

The four current Subcommittees are:

1. *Digital Sales Process (DSP)* –This Subcommittee will deal with pre-sale issues.
2. *In Force Support (IFS)* –This Subcommittee will deal with post-sale issues.
3. *Vendor Advisory* –This Subcommittee will work with both the DSP and IFS Subcommittees in providing technical advice and support.
4. *Legal Advisory* –This Subcommittee will work on projects that require legal or regulatory advice or support.

An eSignature working group was formed to address electronic signatures, and the Technology Task Force was created to research e-signature technologies.

## Goal of the Technology Task Force

The goal of this task force is to prepare a Technology Report that identifies the technologies used to facilitate electronic signatures and the vendors who provide them. The focus of the team is on the account opening process.

## E-signature Technologies

The task force has identified and evaluated the following e-signature technologies. The evaluation of biometric methods was limited to the non-invasive types, such as fingerprints, voice, and handwriting.

### **Clickwrap**

The familiar "I accept" button used in e-commerce to confirm an online purchase or agreement to a contract. Typically secured only by means of secure sockets layer (SSL) technology.

### **Digital Signature**

A piece of encrypted data used to verify that a digitally encoded message originated with a specific individual and that the message was not altered after being sent.

### **Public Key Infrastructure (PKI)**

A system where two numeric keys, one private and one public, are used to encrypt and decrypt electronic messages. The public key is circulated to anyone with whom the user wishes to engage in secure communications. The private key is contained in the user's digital certificate. PKI software verifies the integrity of the messages and their authors.

*Source: Celent Communications*

### **Biometrics**

Automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions.

*Source: Biometrics Consortium*

#### **Biometric: Voice Signature Capture**

An electronic representation of an individual's utterances. Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text.

#### **Biometric: Handwriting**

Biometric signature capture digitally records the image of a handwritten signature and its dynamics.

#### **Biometric: Fingerprints**

Provides an electronic method of identification through an individual's fingerprint. Methodology requires an initial capture of a print and a capture of a print to authenticate the user.

## Enrollment and Risk

Customer identity verification during account origination is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when new customers are accepted through the Internet or other electronic channels, because of the absence of the physical cues traditionally used to identify individuals. The acceptance of new customers is usually considered as high risk, but the level of risk should be determined based on the nature of the business in which the customer is being accepted.

There are various forms of electronic signatures and each one provides a different degree of certainty in the validity that the user is who she or he purports to be and that the electronic signature being applied is appropriate to insure the integrity of the signed document. Only via appropriate enrollment procedures can valid signatures be created and maintained.

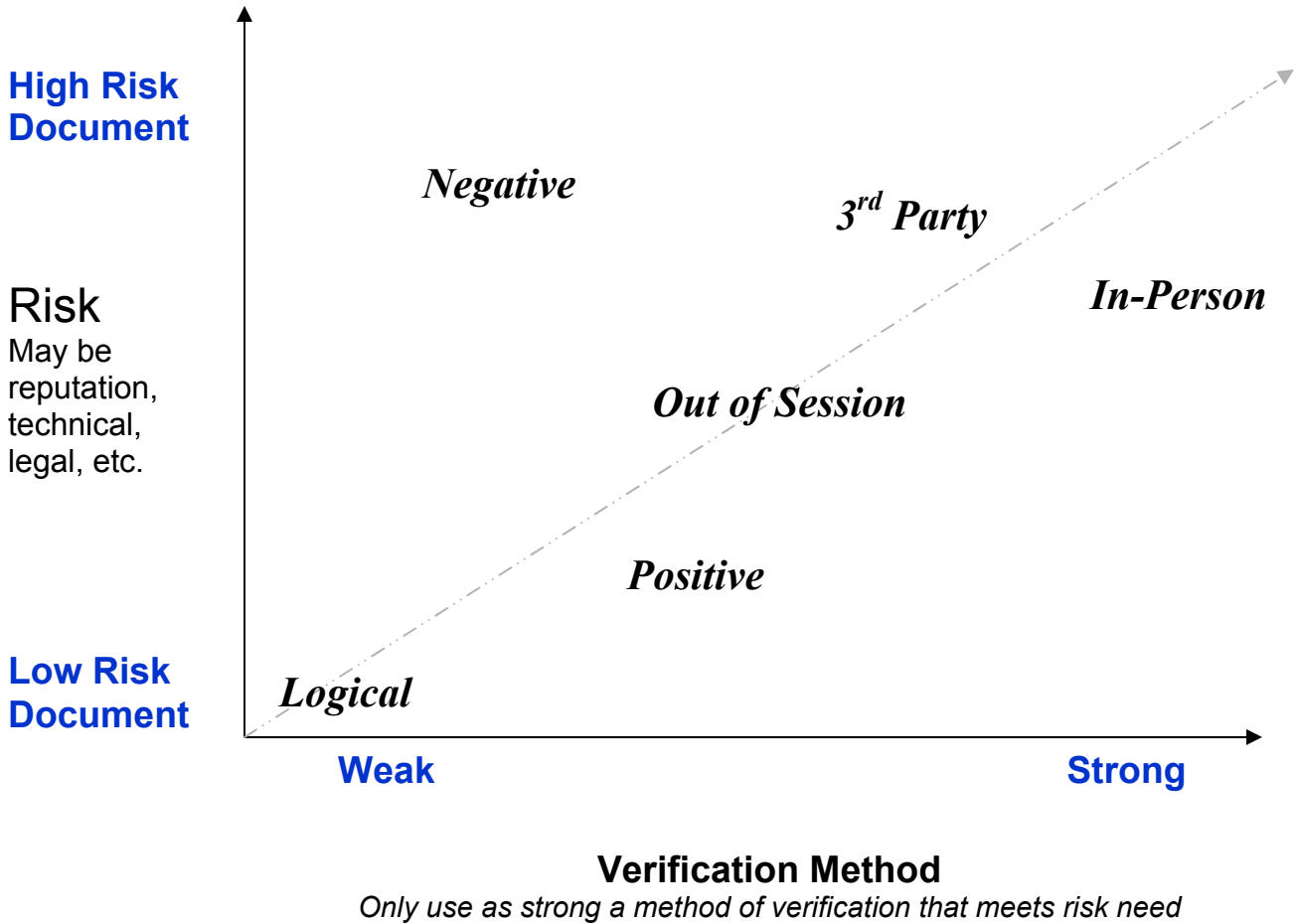
By understanding the risks associated with each type of electronic signature and its intended application, a proper enrollment procedure can be created. For instance, a password and username may be appropriate to sign certain electronic documents, but is not appropriate for others.

## Verification of Identity

Customer identity verification during enrollment is integral to the electronic signature process. Electronic identity can be established, with varying degrees of risk associated with it, via:

1. **Logical Verification**  
Verification via address, phone, zip code, etc.
2. **Positive Verification**  
Identity of customer can be established via a set of questions. The more specific the questions, the more likely the verification.
3. **Negative Verification**  
Verification against fraud databases.
4. **Out of Session Verification**  
Establish identity via a financial institution representative looking up information of the customer and contacting the customer.
5. **Third-Party Verification**  
Other source, such as a credit bureau or other trusted institution establishes identity. Credential acceptance is pre-established.

**Verification Identification Methods**



## Risk Assessment

Risks should be identified and evaluated for all aspects of the electronic signature process being considered. After evaluating the risks, the controls that need to be established to mitigate those risks must be determined and based on a number of factors. Controls take the following forms:

1. Evaluation and application of known risks to types of enrollment procedure used to create a trusted digital signature
2. Evaluation and application of trusted electronic signature to type of electronic document being signed
3. Evaluation and application of risk mitigation controls for technology, and processes including authentication.

[\*The Framework for Electronic Signature Reciprocity\*](#) suggests that there are four levels of risk and accompanying trust in the identity of the individual:

### 1. Rudimentary

Provides for the lowest level of trust concerning the identity of the individual and reflects a situation where there is negligible risk. Usually used for data integrity; for instance, the data being signed is correct. User cannot be strongly authenticated. Not intended for interstate transactions.

- **Example Electronic Signature:** User clicks on 'I accept button' after filling in name, address and phone number (logical verification).

### 2. Basic

Used where there may be risks and consequences of data being compromised, for instance, personal information, but not considered of major significance. Malicious intent or access is considered low.

- **Example Electronic Signature:** User creates a new account based on previously established account numbers, name and address. Only after establishment of identity of user is document available for signature via click through. (Positive Verification)

### 3. Medium

Moderate risks and consequence of data being compromised. May include some transactions of value or private information. Malicious intent or access may be high.

- **Example Electronic Signature:** User enrolls via a formal process with enough valid information such as date of birth, account numbers, and pin number to receive a digital certificate that can be used to sign electronic documents. (Positive Verification)
- **Example Electronic Signature:** User enrolls via a formal process with enough information for financial institution to check user against credit report agency lists; determines eligibility to sign electronic document. (Positive and/or Negative Verification)

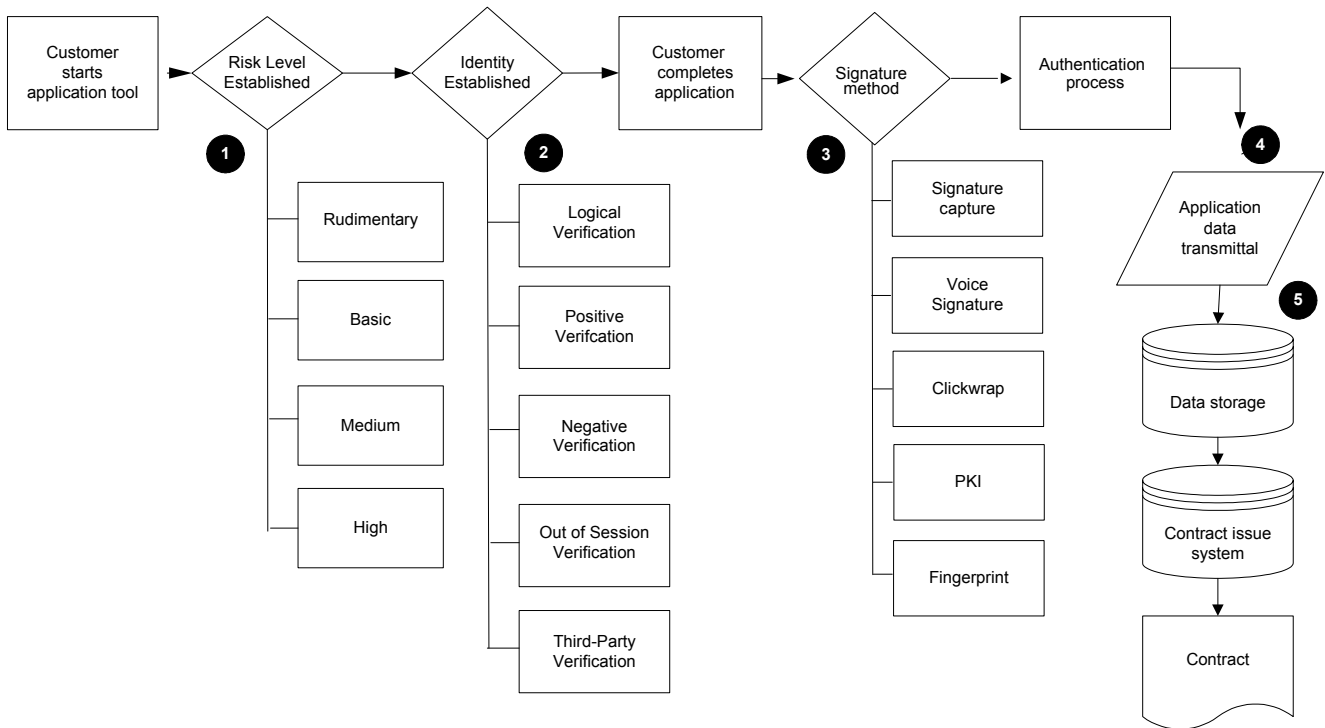
### 4. High

Used where threats to data are high or consequences of failure of security services are high. May include high value transaction levels or high levels of fraud risk.

- **Example Electronic Signature:** User pre-enrolls in-person at a financial institution branch and uses an electronic signature pad to establish a digital signature. Signature is emailed to customer for further use. Electronic documents can then signed with electronic signature and accompanying password. (Positive Verification after enrollment)

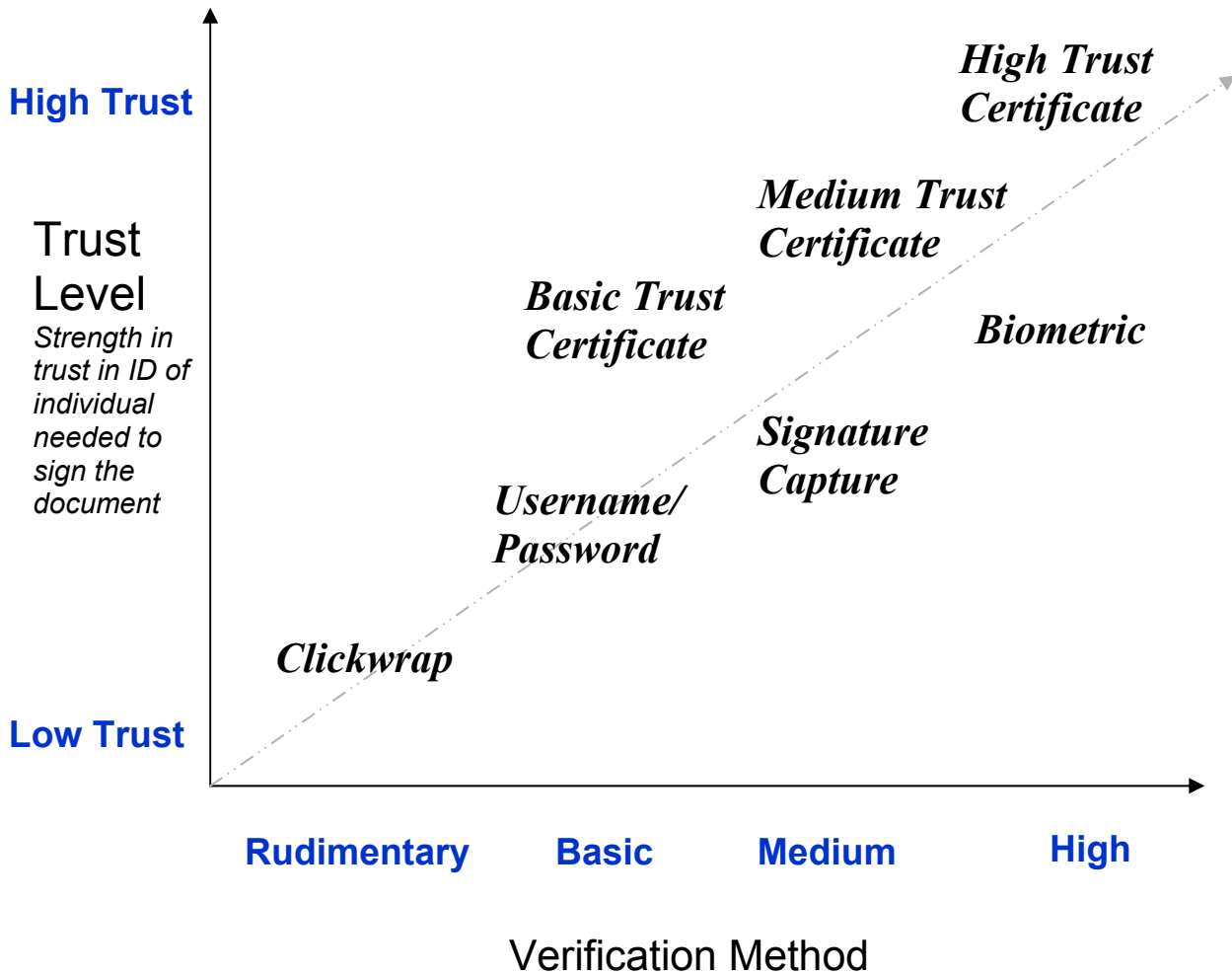
*Continued on next page*

**Risk Assessment Process Flow**



1. Risk level established for document.
2. Identity established based on risk level.
3. Signature method applied based on risk level.
4. Following successful authentication, the application data is transmitted to the carrier.
5. The data is then stored and available for processing.

**Trust and Verification**



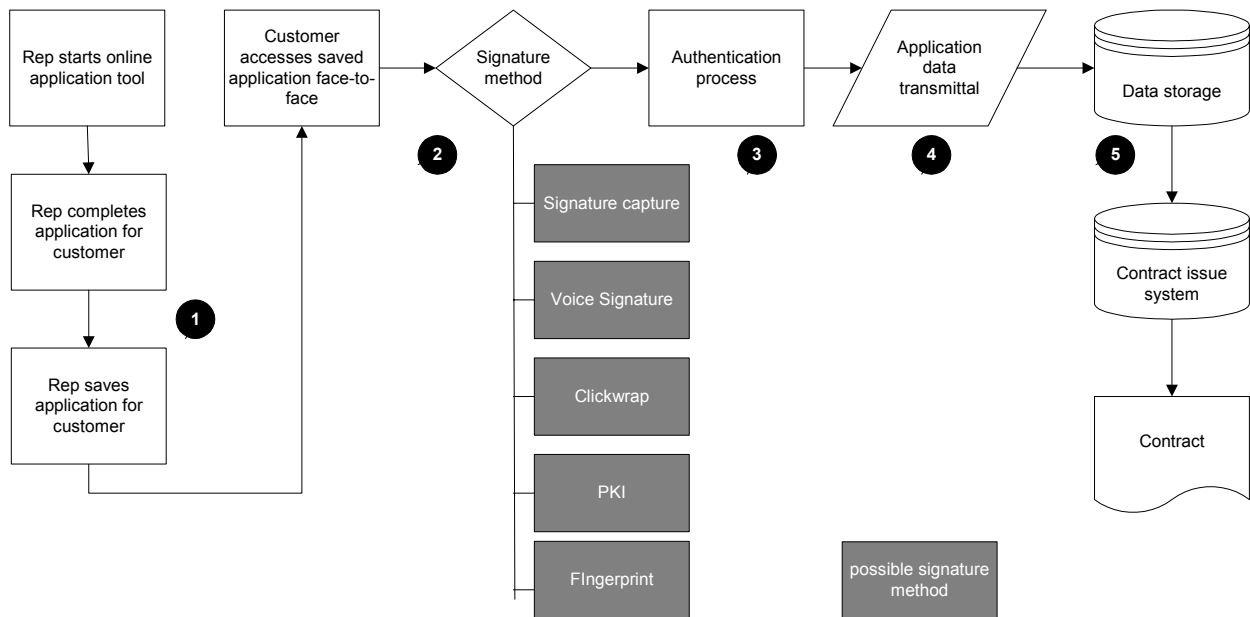
*If it's not a strong enough level of verification, identification may be deemed untrustworthy.*

## Account Opening Scenarios

Following are process flows for these account opening scenarios:

1. Rep or broker/dealer working with a customer in a face-to-face situation
2. Rep working with a customer on the phone
3. Customer working alone, online
4. 1035 Transfer

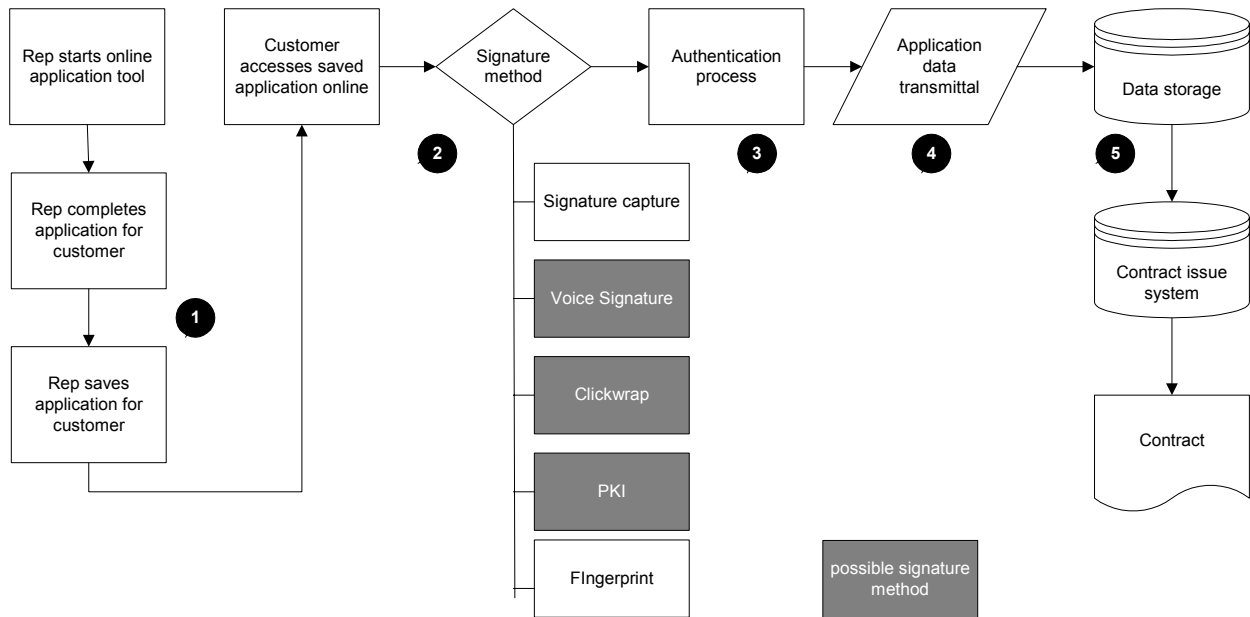
### Process flow: Rep or Broker / Dealer and customer face-to-face



1. A representative or broker/dealer begins an online application for a customer.
2. The customer accesses the application and chooses an electronic signature method. In this scenario, the possible methods include signature capture, voice signature, clickwrap, PKI<sup>1</sup>, or fingerprint.
3. If not part of the signature method, the signature is then authenticated.
4. Following successful authentication, the application data is transmitted to the carrier.
5. The data is then stored and available for processing.

<sup>1</sup> Deemed possible but not practical

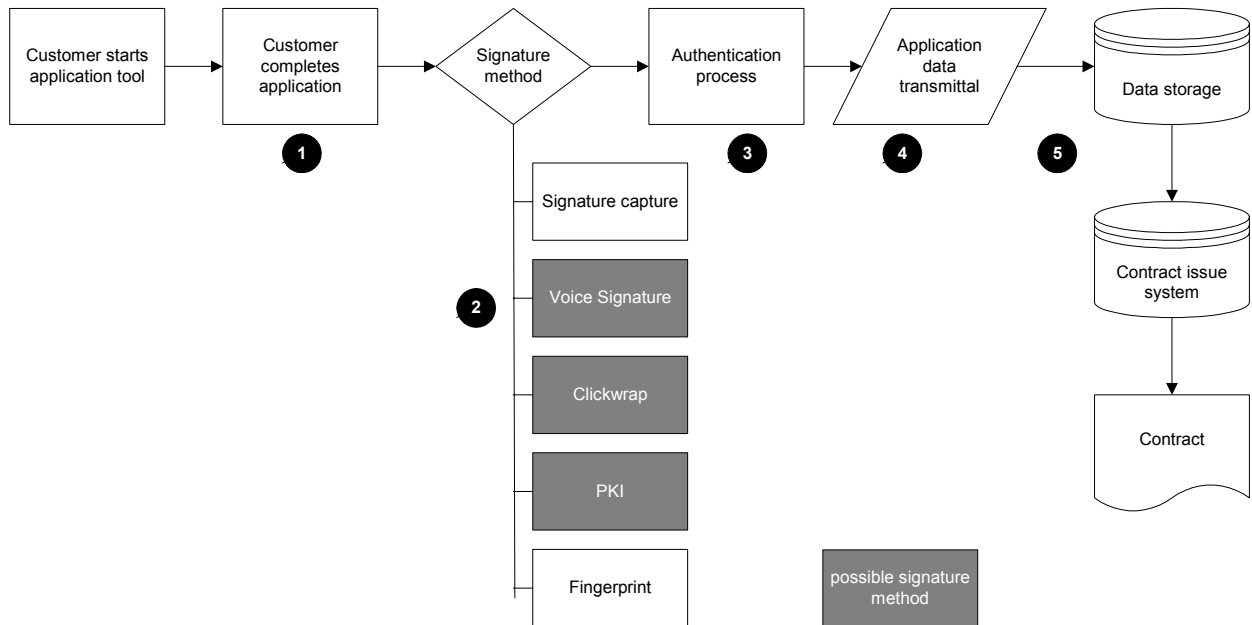
**Process flow: Rep and customer on the phone**



1. A representative begins an online application for a customer.
2. The customer accesses the application online and chooses an electronic signature method. In this scenario, the possible methods include voice signature, clickwrap, or PKI<sup>2</sup>.
3. If not part of the signature method, the signature is then authenticated.
4. Following successful authentication, the application data is transmitted to the carrier.
5. The data is then stored and available for processing.

<sup>2</sup> Deemed possible but not practical.

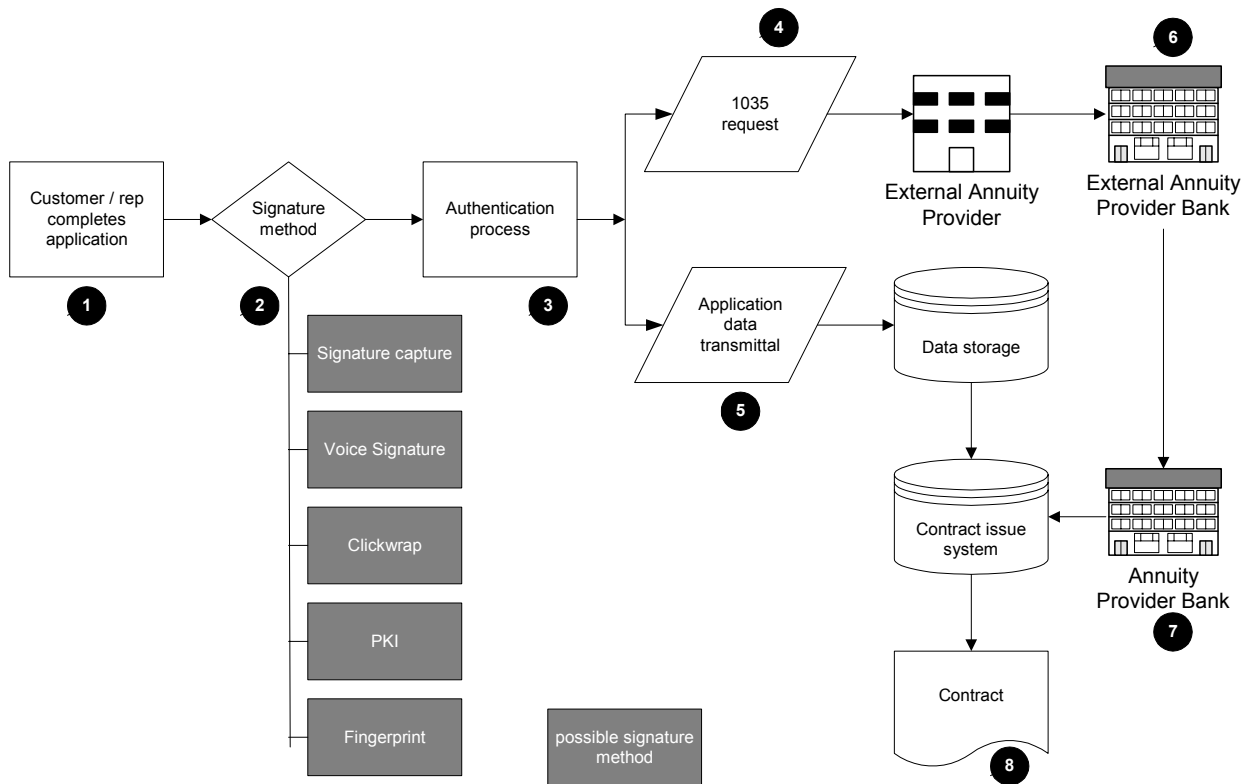
**Process flow: Customer online**



1. A customer begins an online application.
2. The customer chooses an electronic signature method. In this scenario, the possible methods include voice signature, clickwrap, or PKI<sup>3</sup>.
3. If not part of the signature method, the signature is then authenticated.
4. Following successful authentication, the application data is transmitted to the carrier.
5. The data is then stored and available for processing.

<sup>3</sup> Deemed possible but not practical.

**Process flow: 1035 Transfer**



1. A customer or rep completes an application either in the branch or on the web. The chosen funding method is via 1035.
2. The customer chooses an electronic signature method. In this scenario, the possible methods include signature capture pad, voice signature, clickwrap, fingerprint, or PKI<sup>4</sup>.
3. If not part of the signature method, the signature is then authenticated.
4. Following successful authentication, the 1035 request is transmitted to the external annuity provider.
5. The application data is transmitted to the carrier.
6. The external annuity provider sends the request to its bank and the external annuity provider's bank sends the funding to the annuity provider's bank.
7. The funding data is received and transmitted to the contract issue system.
8. The contract is issued.

<sup>4</sup> Deemed possible but not practical.

## Technology Evaluations

Following are descriptions of each e-sign technology, as well as a vendor listing. Vendor overviews are provided in separate documents. Note that the list of vendors is not comprehensive, but merely a representative sampling.

1. ClickWrap
2. Biometric: Fingerprints
3. Biometric: Voice Signature
4. Biometric: Handwritten Signature Capture
5. Digital Signature (PKI)

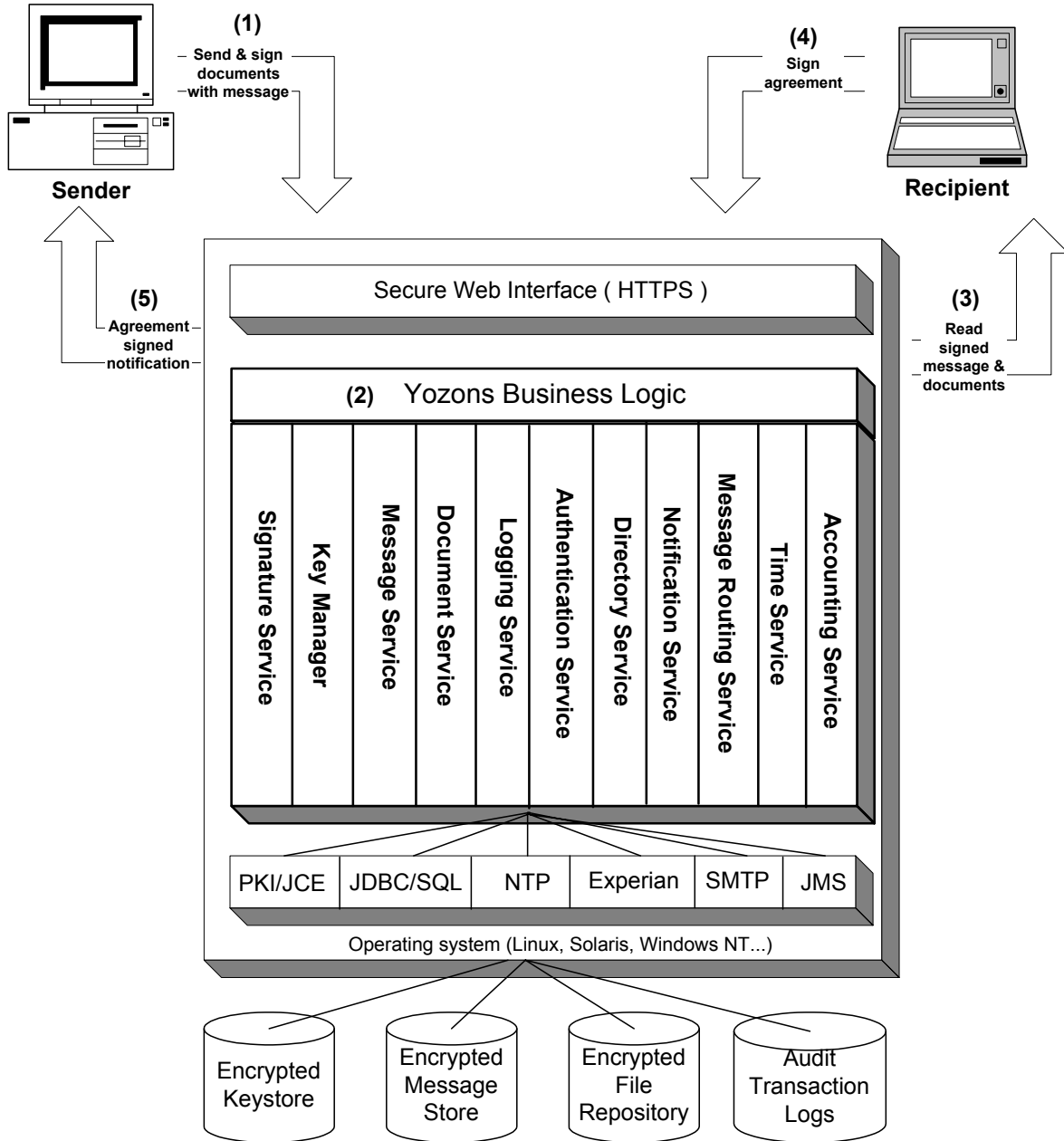
### Evaluation:ClickWrap

<p><b>Description</b></p>	<p>Click-wrap signatures offer a sophisticated, inexpensive signature solution for organizations that require neither the full-strength security of PKI encryption nor the identity verification by a Certificate Authority. Click-wrap signatures have dozens of applications, including internal company documents, online software licensing agreements, online business-to-consumer purchasing agreements, and contracts between known business partners. The ‘signature’ or ‘acceptance’ can be saved as a part of the business transaction record.</p>
<p><b>Vendors</b></p>	<p>PureEdge; Yozons; some back office business system ISVs such as EAI Systems can provide this functionality.</p> <p><a href="http://www.pureedge.com/e-forms/products/signatures/clickwrap.htm">http://www.pureedge.com/e-forms/products/signatures/clickwrap.htm</a></p> <p><a href="https://www.yozons.com/pub/features/signatures.jsp">https://www.yozons.com/pub/features/signatures.jsp</a></p>
<p><b>How it works</b></p>	<p>An on-line user is presented with a screen that contains the various terms and conditions of the transaction. The user is deemed to have agreed to the terms and conditions of the agreement simply by clicking on part of the screen, such as clicking on the “I Agree” button.</p> <p>Greater sophistication can be factored into the process by introducing any one or number of personal information attributes; such as last 4 digits of SSN, Mother’s Maiden Name, Birth City, Drivers License Number, Credit Card Number, etc. This information can be validated against a number of third party verification/authentication services.</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Click-Wrap Agreement Held Enforceable</a></li> <li>▪ <a href="#">Electronic Contracts: Evidence and CyberNotaries</a></li> <li>▪ <a href="#">Click-Wrap Agreements - Enforceable Contracts or Wasted Words?</a></li> <li>▪ <a href="#">Shrink-wrap / Click-wrap Licensing Under UCITA</a></li> <li>▪ <a href="http://www.murdoch.edu.au/elaw/issues/v9n3/kunke193_text.html">http://www.murdoch.edu.au/elaw/issues/v9n3/kunke193_text.html</a></li> <li>▪ <a href="http://online.securityfocus.com/infocus/1602">http://online.securityfocus.com/infocus/1602</a></li> <li>▪ <a href="http://online.securityfocus.com/infocus/1636">http://online.securityfocus.com/infocus/1636</a></li> </ul>

*Continued on next page*

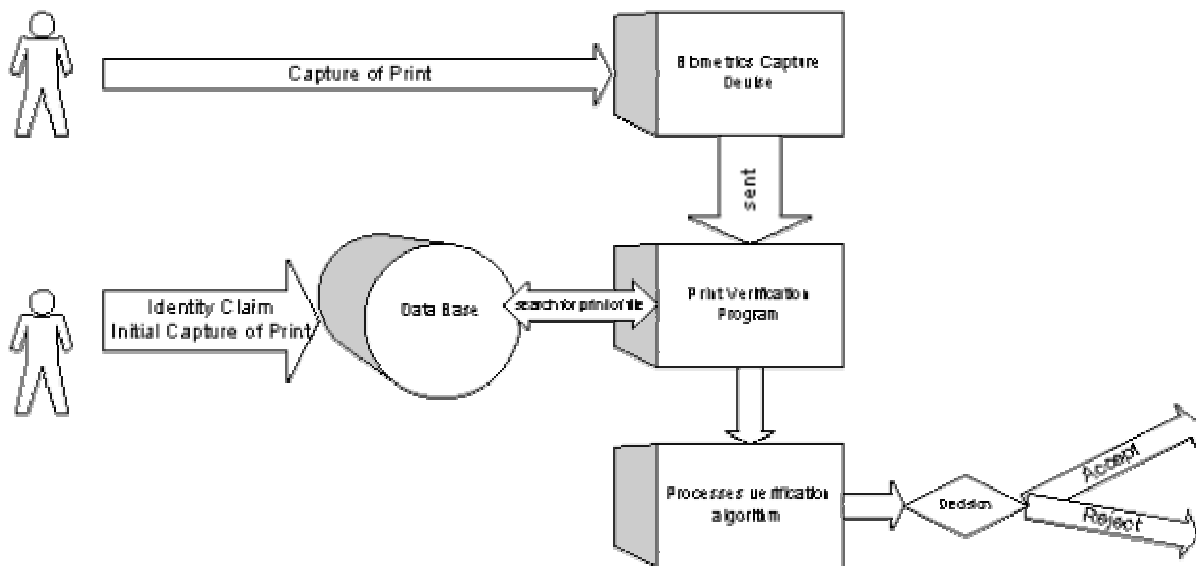
**Clickwrap, continued**

# Yozons High-level Services



**Evaluation: Fingerprints**

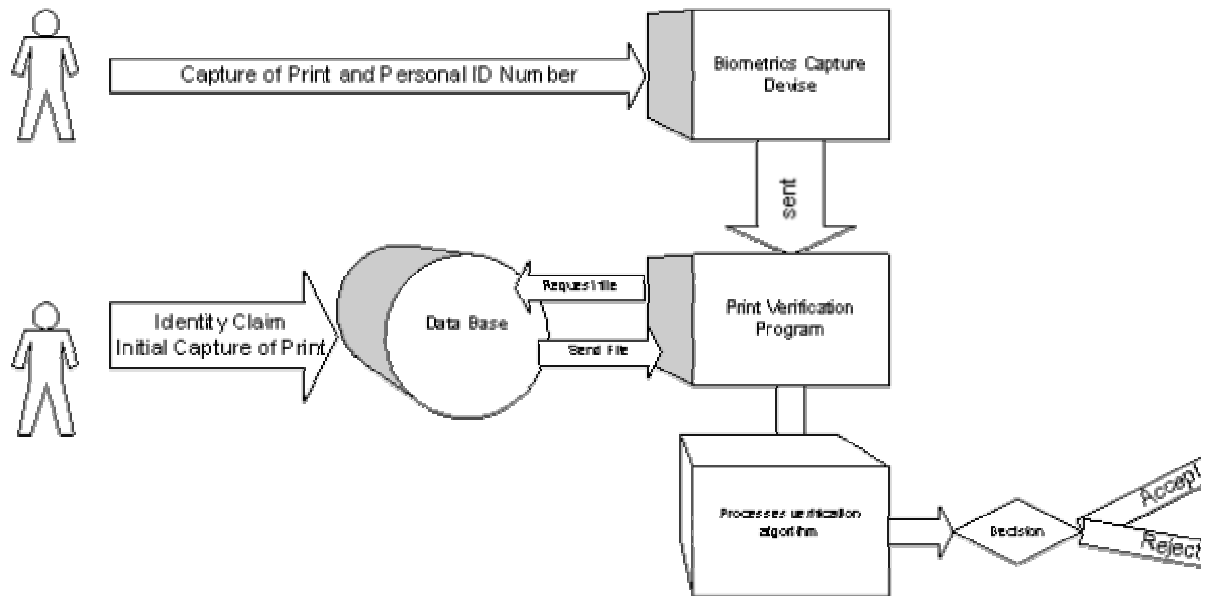
<p><b>Description</b></p>	<p>Provides an electronic method of identification through an individual's fingerprint. All fingerprints differ from one another and are classified by the following 3 groups:</p> <ol style="list-style-type: none"> <li>1. Loop – Most common pattern, which accounts for 65% of all prints.</li> <li>2. Arch – More of an open curve than a loop.</li> <li>3. Whorl – Pattern that occurs in 30% of all prints and are defined by at least 1 ridge that makes a complete circle.</li> </ol>
<p><b>Vendors</b></p>	<p>DigitalPersona, Inc.; International Biometric Group; Veridicom</p>
<p><b>How it works</b></p>	<p>There are two methodologies associated with fingerprint biometrics. Each methodology requires an initial capture of a print and a capture of a print to authenticate the user. I have also included a process flow diagram for each description.</p> <p><b>Identification</b>                  A user captures both his/her thumb prints into the system. Both hands are required to prevent false negatives when there is an injury to a hand, scarring or a skin condition on the thumb. The image is stored and warehoused on a server for later authentication. When a user is required to authenticate, a new image is captured from the user and cross referenced to the database. The database process an algorithm search to see if there is a match. With numerous Financial Advisors with numbers Clients with 2 prints each; the database becomes very large. This will make the search very cumbersome and lengthy.</p>



*Continued on next page*

**Fingerprints, continued**

<p><b>Verification</b></p>	<p>Verification is very similar to Identification in the capturing process, but differs in the authentication process. When a user's prints are captured they associate a pin/id number (could be soc/sec) to the print. When the user's print is captured for a transaction, the user also gives his/her identification number. The identification number pulls the record of the original print and then begins to cross reference the new print with the print on file. This methodology prevents a computer from executing an exhaustive search to locate a print, and speeds up the verification process.</p>
----------------------------	--



**Evaluation: Voice Signature**

<p><b>Description</b></p>	<p>An electronic representation of an individual's utterances, with the following properties:</p> <p><b>Reconstructable</b> - The stored electronic representation of the speaker's voice is rich enough to allow the reconstruction of the original speech utterance for audition and identity judgment by other listeners and/or devices.</p> <p><b>Identity Labeled</b> - The electronic representation must be associated with an identity claim such as a name, member ID, etc.</p> <p><b>Protected</b> - The electronic representation must be transmitted over secure channels, encrypted before storage and transmission, and accessible only to authorized individuals and/or organizations.</p> <p>Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware; most PCs already contain a microphone.</p> <p>However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly.</p> <p>Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.</p>
<p><b>Benefits</b></p>	<ul style="list-style-type: none"> <li>▪ Voice is intuitive – people are accustomed to recognizing other people by their voice.</li> <li>▪ Voice is portable – your voice is always with you.</li> <li>▪ Voice is non-threatening – unlike retina or iris scans.</li> <li>▪ Voice does not have a forensic connotation – most people associate fingerprints with crime.</li> <li>▪ Voice authentication is the only biometric that can be used remotely.</li> <li>▪ Voice biometrics is non-obtrusive: non-invasive and easy to use.</li> <li>▪ Ubiquitous: access from any telephone, anywhere; no need for special devices.</li> <li>▪ More secure and convenient than PIN/password based security measures.</li> <li>▪ Eliminate the need and the cost of PIN/password resets.</li> <li>▪ Robust for cellular/wireless and “hands free” phones.</li> <li>▪ Ensures high security with high performance with the least amount of application downtime.</li> <li>▪ Proven in mission critical applications.</li> <li>▪ Allows additional security through additional knowledge verification: “Who you are” + “What you know”.</li> <li>▪ Allows random knowledge verification questions.</li> <li>▪ Allows user to be verified by simply saying their name.</li> <li>▪ Can allow DTMF for additional/backup input verification.</li> <li>▪ Compliant with HIPAA legislation.</li> <li>▪ Multilingual capabilities.</li> <li>▪ The lowest cost biometric in terms of implementation, use and maintenance.</li> </ul>

*Continued on next page*

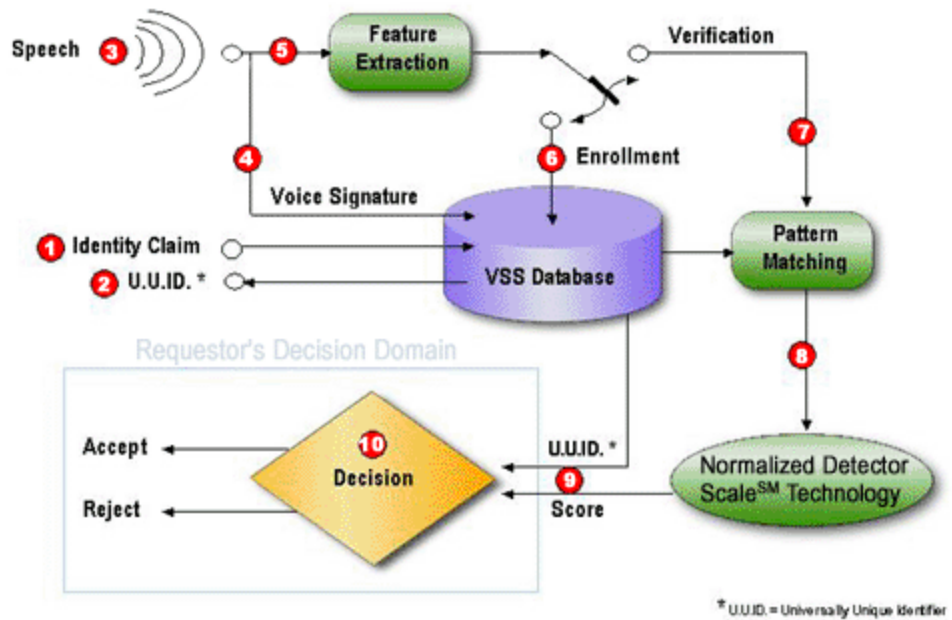
**Voice signature, continued**

<b>Vendors</b>	<p>Diaphonics <a href="http://www.diaphonics.com">www.diaphonics.com</a>          Nuance <a href="http://www.nuance.com">www.nuance.com</a>          TradeHarbor <a href="http://www.tradeharbor.com">www.tradeharbor.com</a>          Vocent, Inc. <a href="http://www.vocent.com">www.vocent.com</a></p>
<b>How it works</b>	<p>To better understand how biometrics works, a general description of the process will be explained in the steps below.</p> <p><b>Capture</b>          A raw biometric (e.g., fingerprint, voice, etc.) is captured by a sensing device, such as a fingerprint scanner, video camera or telephone.</p> <p><b>Process</b>          The distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (sometimes called biometric sample).</p> <p><b>Enrollment</b>          The processed “template” (a mathematical representation of the biometric sample now converted into a digital format – not the original biometric sample) is registered (with user identifiers and other relative reference information) and stored in a (secured) storage medium for a later comparison during an authentication. The original or “raw” biometric sample cannot be reconstructed from this template identifier. In many applications, storing the original biometric sample is neither needed nor desirable. An option of the enrollment process can allow the processed biometric sample (or digital copy of it) to be stored in a portable token such as a SmartCard.</p> <p><b>Verification</b>          A verification (i.e., “1 to 1 matching” or 1:1) process implies matching the enrolled biometric sample against a single record. If the biometric-based recognition system requires that an individual present a claim of identity, for example, by entering a user name or user identification number, a password or presenting a token (i.e., SmartCard), the individual is “recognized” through biometrics in a “verification” mode.</p> <p>In this mode, a newly captured/processed biometric sample is (or can be) taken during, for example a login, and is compared against a previously enrolled sample (i.e., “template”) to determine whether the person is who they claim to be. It addresses the question “Are you who you claim to be?” If there is a 1:1 matching, the person is deemed “authenticated” and is granted permission/access to continue to the next task or required action.</p> <p>Different biometric systems may allow for a specific discrimination percentage in the 1:1 matching process such as dirty fingers, background noise, etc.; the lower the tolerance, the more accurate the authentication.</p> <p>Additionally, should the subject fail to provide a biometric sample that falls within the acceptable authentication range, some systems may ask or require an additional session sample for the verification process and then conduct an “averaging” and/or “weighing” of the samples’ scores for authentication considerations.</p>

*Continued on next page*

**Voice signature, continued**

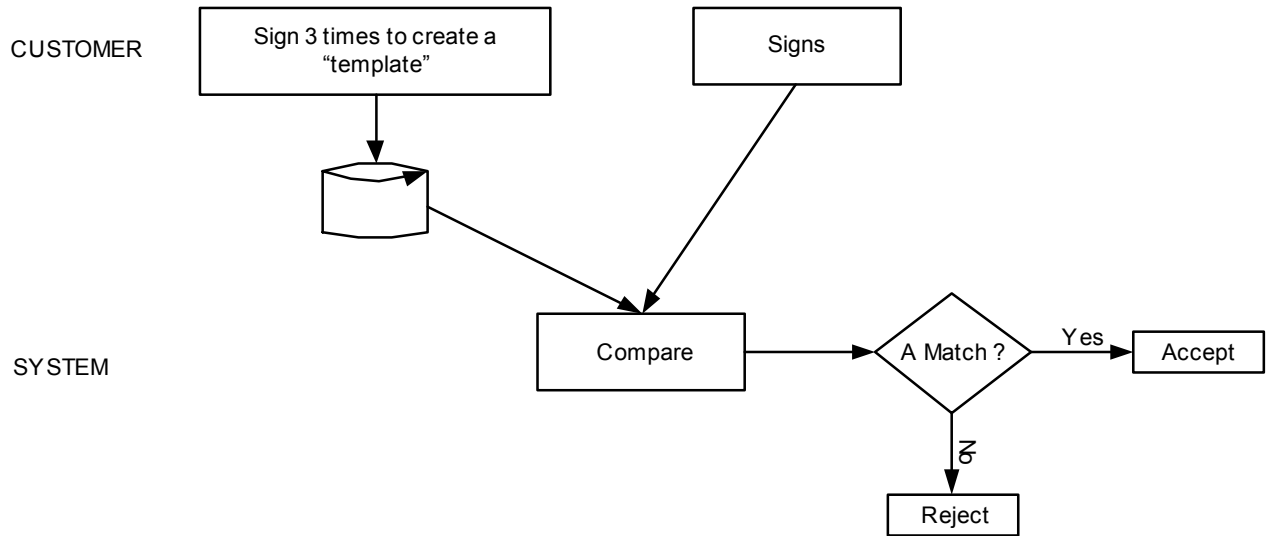
The Voice Signature Service<sup>SM</sup> Bureau Process



©TradeHarbor

**Evaluation: Handwritten signature capture**

<b>Description</b>	Biometric signature capture digitally records the image of a handwritten signature and its dynamics. Although an individual never signs his or her name exactly the same way twice, one’s handwritten signature does conform to certain boundaries which are unique to that person.
<b>Vendors</b>	Communications Intelligence Corp. (CIC) dominates this space (software). MotionTouch, Interlink, Wacom and Topaz are hardware vendors. Orion Sytems and Valyd are smaller (software) competitors to CIC. Other vendors such as Silanis, PureEdge, eOriginal, and iLumin offer the technology as part of a larger solution by OEMing third part products such as CIC’s.
<b>How it works</b>	Biometric signature capture records the signer's handwritten signature on an input device called a signature pad. The software records the image of the signature and also the behavioral properties such as the order of the strokes, pressure, pen-up and pen-down, speed, acceleration and aspect ratio.

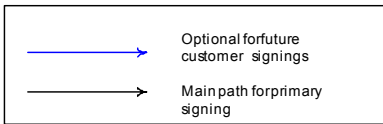
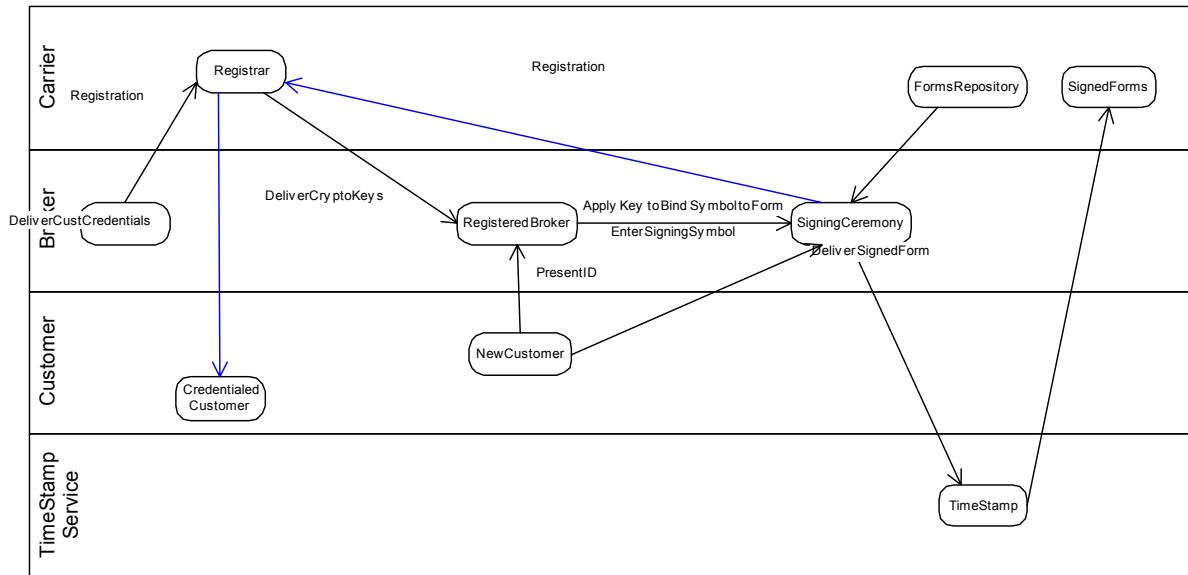


**Evaluation: Digital Signature (PKI)**

<b>Technology type</b>	Digital Signatures (based on Digital Certificates and public key infrastructure – i.e., PKI)
<b>Description</b>	<p>Of greatest interest is the sales application process, which requires a signature from the end customer. However, the technology requires that each signing individual be registered with a certificate authority.</p> <p>Since new customers are not typically expected to possess the needed certificate, we deem a direct approach using this technology to be untenable.</p> <p>However, it may be possible to create a scenario that is based on a much smaller set of people that would have the required certificates. If the broker or broker who is closing the sale were properly equipped, that person could verify the identity of the purchaser(s), who could then sign the documents.</p>
<b>Vendors</b>	Baltimore Technologies; Entrust; NxLight; PureEdge Solutions; Verisign; Yozons Technology
<b>How it works</b>	<ol style="list-style-type: none"> <li>1. Carrier registers broker and delivers private keys to broker. (Alternatively, the carrier and the broker/dealer could have a common PKI root certificate and the broker/dealer could register the broker.</li> <li>2. Customer shows identification to the broker.</li> <li>3. Broker and customer complete the application.</li> <li>4. Customer signs (types name, clicks submit etc)</li> <li>5. Broker releases his private key to the system by entering his passphrase.</li> <li>6. System binds document to the customer signature using cryptographic hash derived from the document and the broker's private key</li> <li>7. The signed document is bound to a time stamp using a time stamp service.</li> <li>8. The signed document is delivered to the carrier.             <ul style="list-style-type: none"> <li>o Optionally, the signing ceremony initiates a customer registration with the carrier. This would cause customer credentials to be created and delivered to the customer. This would most likely be a PIN or password.</li> </ul> </li> <li>9. Further signings could then occur without the presence of the broker.             <ul style="list-style-type: none"> <li>▪ Note, this is similar to a click wrap scenario, with two differences:                 <ul style="list-style-type: none"> <li>o Broker acts as authenticator</li> <li>o The broker's private key is used to create the binding hash.</li> </ul> </li> </ul> </li> </ol>

*Continued on next page*

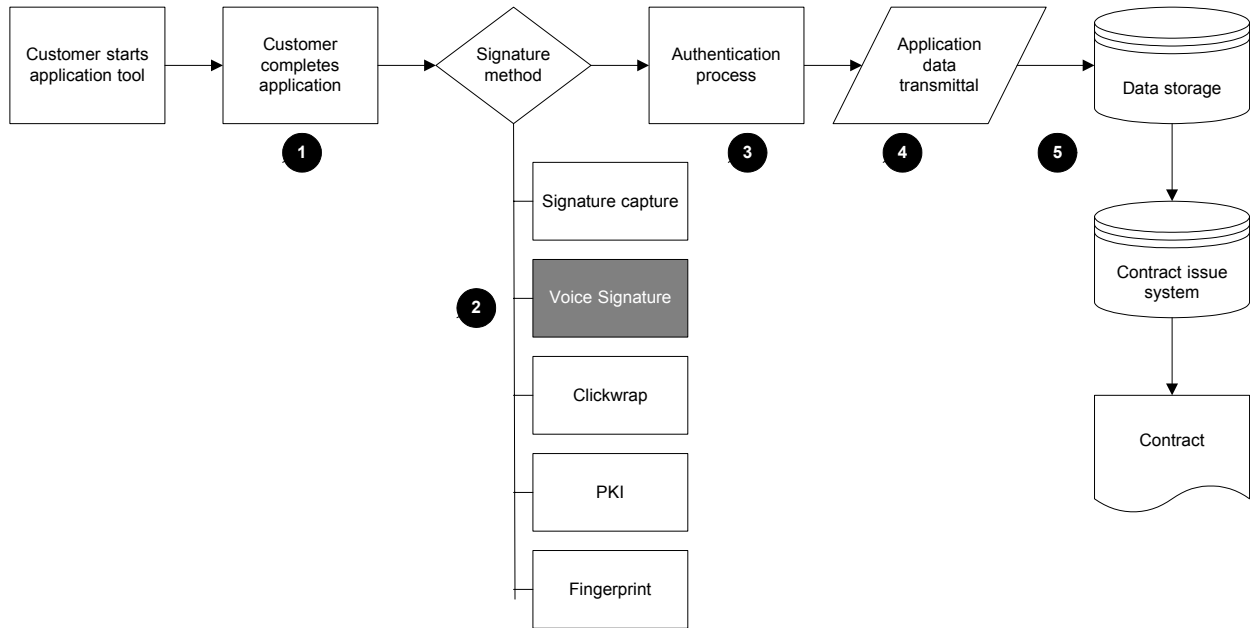
**Digital Signature (PKI), continued**



### Agent Assisted Customer Registration

**Appendix: VRU process flow**

Electronic application over a voice response unit was discussed by the Technology Task Force. We deemed this method as out of scope, since we focused on e-sign technologies utilizing a personal computer.



1. A customer begins an electronic application over the phone (VRU).
2. The customer chooses an electronic signature method. In this scenario, the method is voice signature.
3. If not part of the signature method, the signature is then authenticated.
4. Following successful authentication, the application data is transmitted to the carrier.
5. The data is then stored and available for processing

**Vendor List**

The information contained in this report is being provided to illustrate the various eSignatures technologies and vendors that are available – and should not be considered a comprehensive listing of what is available in the market. Much of the material was created by companies or organizations that are independent of NAVA.

While NAVA and its committee members make every effort to present accurate and reliable information, we do not endorse, approve, or certify this information, and we do not guarantee the accuracy, completeness, efficacy, timeliness, or correct sequencing of such information. Your use of such information is voluntary, and you should rely on it only after an independent review of its accuracy, completeness, efficacy, and timeliness. If any specific commercial product, process, or service is referred to in such information by trade name, trademark, service mark, manufacturer, or otherwise, that reference does not constitute or imply endorsement, recommendation, or favoring by NAVA.

Name / Company	e-mail	Web	Phone	Product
<b>PKI Vendors</b>				
<b>Baltimore Technologies</b>		<a href="http://www.baltimore.com/">www.baltimore.com/</a>	781-455-3333 781-455-4005 (Fax)	UniCert
<b>Entrust</b>	<a href="mailto:entrust@entrust.com">entrust@entrust.com</a>	<a href="http://www.entrust.com">www.entrust.com</a>	888-690-2424	
Ken Sapp, Managing Director Insurance Market, <b>NxLight</b>	<a href="mailto:ksapp@nxlight.com">ksapp@nxlight.com</a>	<a href="http://www.nxlight.com/">www.nxlight.com/</a>	817-427-5666	Tablet PC; voice signature collection
<b>PureEdge Solutions</b>	<a href="mailto:info@PureEdge.com">info@PureEdge.com</a>	<a href="http://www.pureedge.com/">www.pureedge.com/</a>	888-517-2675 888-438-8495 (Fax)	PKI-based Signature Authenticated ClickWrap
<b>Verisign</b>		<a href="http://www.verisign.com">www.verisign.com</a>	650-961-7500 650-961-7300 (fax)	
<b>Yozons Technology</b>	<a href="mailto:sales@yozons.com">sales@yozons.com</a>	<a href="http://www.yozons.com/">www.yozons.com/</a>	425-822-4465	Signed & Secured
<b>Fingerprint Vendors</b>				
<b>DigitalPersona, Inc.</b>	<a href="mailto:sales@digitalpersona.com">sales@digitalpersona.com</a>	<a href="http://www.digitalpersona.com">www.digitalpersona.com</a>	650-261-6070 650-261-6079 (fax)	U are U
<b>International Biometric Group</b>	<a href="mailto:contact@biometricgroup.com">contact@biometricgroup.com</a>	<a href="http://www.biometricgroup.com">www.biometricgroup.com</a>	888-IBG-8-IBG 212-809-6197 (fax)	
<b>Veridicom</b>	<a href="mailto:info@veridicom.com">info@veridicom.com</a>	<a href="http://www.veridicom.com">www.veridicom.com</a>	408-543-4200 408 734-0308 (fax)	

Name / Company	e-mail	Web	Phone	Product
<b>Voice Signature Vendors</b>				
Diaphonics, Inc.	<a href="mailto:info@diaphonics.com">info@diaphonics.com</a>	<a href="http://www.diaphonics.com">www.diaphonics.com</a>	902-446-3680 902-446-3662 (fax)	
Nuance		<a href="http://www.nuance.com">www.nuance.com</a>	650-847-0000	
TradeHarbor	<a href="mailto:pheirendt@tradeharbor.com">pheirendt@tradeharbor.com</a>	<a href="http://www.tradeharbor.com">www.tradeharbor.com</a>	314-878-1200 314-878-1225 (fax)	
Vocent, Inc.	<a href="mailto:info@voцент.com">info@voцент.com</a>	<a href="http://www.voцент.com">www.voцент.com</a>	650-316-3001	
<b>Signature Capture Vendors: Software</b>				
Communications Intelligence Corporation	<a href="http://www.cic.com/enterprise/inquiry">www.cic.com/enterprise/inquiry</a>	<a href="http://www.cic.com/">www.cic.com/</a>	650-802-7888 650-802-7777 (Fax)	Handwritten Biometric Electronic Signature
Valyd	<a href="mailto:sales@valyd.com">sales@valyd.com</a>	<a href="http://www.valyd.com">www.valyd.com</a>	408-436-1000 408-904-7444 (fax)	
<b>Signature Capture Vendors: Hardware</b>				
Motion Touch	<a href="mailto:info@motiontouch.com">info@motiontouch.com</a>	<a href="http://www.motiontouch.com">www.motiontouch.com</a>	+44 1932 854721 +44 1932 854940 (fax)	Signature Capture hardware vendor
Tom Fischer, Sales Director, Interlink Electronics		<a href="http://www.interlinkelectronics.com">www.interlinkelectronics.com</a>	805-484-1356 x 420	Signature capture pads
Lew Levey, President Topaz Systems	<a href="mailto:Lew@Ctstl.com">Lew@Ctstl.com</a>	<a href="http://www.topazsystems.com/">www.topazsystems.com/</a>	800-423-8826 314-428-0314 (Fax)	Signature capture tablets
<b>Signature Capture Vendors: OEM</b>				
Silanis Technology	<a href="mailto:Andrea_Simmons@silanis.com">Andrea_Simmons@silanis.com</a>	<a href="http://www.silanis.com/">www.silanis.com/</a>	514- 337-5255 ext. 1152	Approvelt web server
eOriginal	<a href="mailto:Contact@eoriginal.com">Contact@eoriginal.com</a>	<a href="http://www.eoriginal.com">www.eoriginal.com</a>	410-659-9796 410-659-9799(fax)	Core Business Suite
iLumin	<a href="mailto:info@iLumin.com">info@iLumin.com</a>	<a href="http://www.ilumin.com">www.ilumin.com</a>	703-481-8627 703-481-8672 (fax)	Digital Handshake
PureEdge Solutions	<a href="mailto:info@PureEdge.com">info@PureEdge.com</a>	<a href="http://www.pureedge.com/">www.pureedge.com/</a>	888-517-2675 888-438-8495 (Fax)	PKI-based Signature Authenticated ClickWrap

*Draft*

**Appendix B**

Legislative White Paper



**NAVA Legislative Task Force of the eSignature Working Group**

**Building an “Industry-Standard” for an Electronic Signature  
Associated with Straight Through Processing of Annuities:  
A Discussion of Legal Issues Involved**

**DRAFT OF SEPTEMBER 25, 2003  
THIS DRAFT TO BE CIRCULATED TO THE TECHNOLOGY TASK FORCE, LEGAL  
ADVISORY SUBCOMMITTEE AND NAVA’S REGULATORY AFFAIRS  
COMMITTEE FOR REVIEW AND ADDITIONAL INPUT**



**Copyright © 2003 by the National Association for Variable Annuities except as otherwise indicated. All rights reserved.**

The contents of this publication are copyrighted by the National Association for Variable Annuities. Copyright is not claimed as to information excerpted from the SPeRS Version 1.0 publication. All rights are reserved by NAVA, and content may not be reproduced, disseminated, published, or transferred in any form or by any means, except with the prior written permission of NAVA.

The NAVA logo is a registered mark of NAVA.

This publication is provided with the understanding that neither NAVA, its directors, officers or staff members, or other persons contributing to this publication are engaged in rendering financial, accounting, or legal advice, nor do they assume legal responsibility for the completeness or accuracy of the contents of this publication. The text is based on information available at the time of publication.

## TABLE OF CONTENTS

<b>Contributors</b> .....	4
<b>SECTION 1 – Executive Summary</b> .....	5
<b>SECTION 2 – Introduction</b> .....	7
Mission Statement.....	7
General Rules.....	7
Summary of Four Application Process Flows Involved.....	7
<b>SECTION 3 – Regulatory Requirements for Valid E-Signatures</b> .....	9
<b>SECTION 4 – Detailed Discussion</b> .....	10
The Legal Essentials for Valid E-Signatures.....	10
UETA.....	10
ESIGN.....	12
The Industry’s Current Experience with State Insurance Departments.....	13
Legal Implications of E-Signature Methodologies.....	16
Privacy Regulations – How they apply to E-Apps.....	20
Effect of USA PATRIOT Act Regulations.....	22
Prospectus Delivery Rules – Interplay with ESIGN, UETA and SEC Guidelines.....	27
Issues Related to Retention of Electronic Records of Insurance Companies.....	30

## CONTRIBUTORS

### *Legislative Task Force:*

Tom Conner, Chair, Sutherland Asbill & Brennan LLP  
Carrie Bekker, AEGON Insurance Group  
Judith Hasenauer, Blazzard, Grodd & Hasenhauer, P.C.  
Paula Minella, Fidelity Investments Life Insurance Company  
Richard Choi, Foley & Lardner  
Sandra Downes, Hartford Life  
Ann Furman, Jordan Burt LLP  
Bradley Skarie, Lincoln National Life Insurance Co.  
Robert Kiggins, McCarthy Fingar Donovan Drazen & Smith  
Brian Buckley, Merrill Lynch Insurance Group  
Alex Varghese, Merrill Lynch Insurance Group  
Myra Saul, MetLife  
Brian Mannion, Nationwide Financial  
Frank Spencer, Nationwide Financial  
Deborah Tucker, NAVA  
Michael DeGeorge, NAVA  
Karen Alvarado, Pacific Life Insurance Co.  
Deborah Alexander, Transamerica/AEGON Insurance Group

## SECTION 1 – Executive Summary

### Background

#### *NAVA Technology Committee*

In June of 2001, NAVA created the Technology Committee to identify, research, endorse, and communicate technological directions for the benefit of the annuity and life insurance industry. This was a spin off of the NAVA Operations Committee. The Technology Committee views its charter as defining the industry architecture and setting priorities in the development of open industry standards for annuities. The actual development of those standards is handled within the framework of an ACORD process – with participation of as many business experts within the annuity industry as possible. Many of the Committee initiatives require the participation of NAVA’s Operations and Regulatory Affairs committees.

#### *Electronic Signature Initiative*

An eSignatures working group was formed in 2002 to address electronic signatures (“E-Signatures”) as part of the industry initiative of straight through processing. That working group formed several task forces to assist them in their deliberations. *The working group’s scope was defined to include E-Signatures that would bind an electronic annuity application (“E-App”), but with a solution that could be used for in force electronic transactions as well.* The Technology Task Force was created to prepare a Technology Report that identifies the electronic signature technologies and the vendors who provide them, and the Legislative Task Force was created to analyze the federal and state legal issues arising from use of those technologies in the account opening processes described in the Technology Report.

### Findings of the Legislative Task Force

#### *Summary of the Law*

As described within this white paper, the Legislative Task Force reviewed the state of the law relating to e-commerce and case law regarding the validity of eSignature methodologies. It also reviewed the impact on electronic processing of other federal requirements such as the Gramm-Leach-Bliley Act, USA PATRIOT Act, federal securities laws and regulations promulgated by the Securities and Exchange Commission. Finally, the Task Force reviewed the industry’s experience to date with state insurance departments.

Under ESIGN (the Electronic Signature in Global and National Commerce Act) and UETA (the Uniform Electronic Transactions Act), a record or signature may not be denied legal effect or enforceability solely because it is in electronic form, and if a law requires a record or signature, an electronic record or signature may satisfy the law. This white paper outlines the requirements of what is needed to formulate a signature in good order under ESIGN and UETA.

Under ESIGN and UETA, an electronic signature may be created in a number of ways and will be valid so long as it is attached to, or logically associated with, a record, created, or adopted, by the signer, with the intent to sign the record. Other requirements relating to authentication, document integrity, non-repudiation, consumer notice, and record retention must also be met.

An electronic transaction may, depending on the circumstances, also need to satisfy the requirements of one or more of the other federal laws and regulations noted above. These involve privacy laws, anti-money laundering, prospectus delivery, and retention of electronic records:

#### Privacy laws

- Under the SEC's Regulation S-P, a privacy notice must be delivered to applicants but this may be done electronically.
- Consumer information provided electronically, including an electronic signature, must be safeguarded so as to be secure and confidential and protected against unauthorized use.

#### USA PATRIOT Act

- Anti-money laundering, customer identification, and suspicious transaction reporting programs must address electronic transactions.
- Non-documentary methods to verify customer identity must be employed when applications and other transactions are conducted electronically.

#### Prospectus delivery

- SEC rules require notice, access and evidence of delivery.
- ESIGN requires consent and consumer demonstration that he/she can navigate the means of electronic communication that is used to deliver the prospectus.

#### Document retention

- Regardless of the electronic signature methodology used, the document must be unalterable after signature.
- Customer information maintained electronically must meet the requirements of SEC Rule 17a-4(f).

While there was an initial perception that state insurance departments would question whether the use of electronic signatures in the E-App process met applicable regulatory goals, the Task Force could not find any published regulatory guidance or specific examples to justify this concern.

#### ***Conclusion***

The Task Force did not identify specific legal or regulatory impediments to the eSignatures Working Group proceeding with its initiative with the following caveats:

- ESIGN and UETA are relatively new statutes and there is little case law interpreting them.
- Electronic processing must be set up so as to comply with the requirements of other federal and state laws applicable to the sale of annuities.
- The lack of state regulatory uniformity regarding electronic commerce makes it unclear how individual state insurance departments will react to electronic processing of annuities.

## **Next Steps**

Once the eSignatures Working Group has completed its findings relative to determining the technologies and process procedures for industry adoption, a task force of the Regulatory Affairs Committee will document that process and file notification of intended E-App electronic signature methodology on behalf of the industry in all 50 states.

## SECTION 2 – Introduction

### Mission Statement

NAVA’s eSignature Legal Task Force (the “Legal Task Force”) has been asked by the NAVA eSignature Working Group to draft a “white paper” analyzing the federal and state legal issues arising out of four proposed electronic processing systems as described in the “Technology Report” of the NAVA Technology Task Force (May 2003). These four application processes (the “NAVA Application Processes”) represent the sales processes anticipated to become the most common within the annuity industry.

This white paper has two related purposes. With respect to the current state of the law relating to e-commerce generally, the white paper refers readers to other articles and papers, including the “SPeRS Version 1.0,” that provide analysis and guidance.<sup>1</sup> With respect to the federal and state legal issues that arise specifically from the NAVA Application Processes, this white paper provides an analysis and, in some cases, recommendations for further analysis and information-gathering by NAVA and its members.

### General Rules

The following general rules apply to specific factual circumstances.

- The Task Force did not focus on the issues that would arise out of traditional paper processes.
- Facsimile methods are not within the white paper’s scope.
- Fixed and variable annuities are in the white paper’s scope.

### Summary of Four Application Process Flows Involved

The following are the process flows for the account opening scenarios that are outlined the Technology Report of the NAVA Technology Task Force:

#### *Scenario 1 -- Registered Representative (“RR”) meeting customer face-to-face*

- RR starts online application tool
- RR completes application for customer
- RR saves application for customer
- Customer accesses saved application
- Signature method (face-to-face) via signature capture, voice, click wrap, or fingerprint
- Authentication process
- Application data transmittal
- Data storage
- Contract Issue System

---

<sup>1</sup> It is important to note that the Legislative Task Force has not independently verified and does not endorse the legal analyses or conclusions of SPeRS or any other individual or organization.

- Contract

***Scenario 2 -- RR and Customer complete application over the phone***

- RR starts online application tool
- RR completes application for customer
- RR saves application for customer
- Customer accesses saved application online
- Signature method (customer when RR not present) via voice or click wrap
- Authentication process
- Application data transmittal
- Data storage
- Contract Issue System
- Contract

***Scenario 3 -- Customer Direct Model***

- No RR in transaction
- Customer completes application online
- Customer completes application
- Customer e-signs application via voice or click wrap
- Authentication process
- Application data transmittal
- Data storage
- Contract Issue System
- Contract

***Scenario 4 -- Variation of 1, 2 or 3 - Chosen Method of Funding is a 1035-Transfer***

- Customer or RR completes application either in branch or on the Web which is 1035 funded
- Signature method election via signature capture, voice, click wrap or fingerprint
- Authentication
- 1035 request to the ceding company
- Application date transmittal to new carrier
- Ceding company requests funding from its bank
- Ceding company's bank sends funding to new carrier's bank
- Contract Issue System
- Contract

## SECTION 3 – Regulatory Requirements for Valid E-Signatures

New eCommerce laws and regulations make possible the widespread replacement of paper documents with electronic records. While the new eCommerce laws and regulations permit the use of electronic records and signatures, they also require that electronic systems and processes meet standards for:

- ***Consent and Disclosures***

Informing users about what they are “signing” online and about their rights and responsibilities under consumer protection laws

- ***Identity, Security, Privacy***

Establishing the identity of users, and employing procedures that limit exposure to identity theft, fraud, money laundering, etc

- ***Signature***

Establishing intent to “sign” a transaction, such as by a two-step process that confirms intent and avoid the “slipped finger” syndrome

- ***Agreements and Notices***

Making documents accessible online and providing required notices electronically, such as by hyperlink to a designated site

- ***Record Retention***

Adopting standards for storing records that need to be reviewed or referred to later, making records available for printing, and protecting the integrity of records

Failure to meet those standards may impair the enforceability of electronic records. To address this, industry leaders have undertaken a cross-industry initiative to establish commonly understood “rules of the road” available to all parties seeking to take advantage of the powers conferred by E-SIGN and UETA (see page 10). The product of this initiative is the Standards and Procedures for Electronic Records and Signatures (“SPeRS”).

NAVA and other trade groups such as ACORD and the ACLI have agreed to recommend to its members the adoption of the standards as set forth in the “SPeRS Version 1.0” that will be published in November 2003. A copy may be ordered from their website [www.spers.org](http://www.spers.org).

## SECTION 4 – DETAILED DISCUSSION

### THE LEGAL ESSENTIALS FOR VALID E-SIGNATURES

#### Governing Statutes

E-Signatures and E-Apps are generally governed by two statutes: (i) UETA (the Uniform Electronic Transactions Act) and (ii) ESIGN (Electronic Signature in Global and National Commerce Act (Public Law 106-229, and U.S. Senate Bill 761)).<sup>2</sup> The discussion is not intended to be an exhaustive comparison of the particulars of each law, but instead, provide a general background for the discussion of using electronic signatures and contracts for the sale and service of variable annuities.

UETA and ESIGN are two separate and distinct laws, comprising state and federal laws, respectively, addressing the use of electronic signatures and electronic contracts. Their intent is to provide some assurance that contracts entered into electronically, whether they are online or through a digitizer used in the presence of an agent, will not be invalidated solely because they occur in an electronic environment. Neither UETA nor ESIGN assume that electronic contracts and/or signatures are valid, but instead, place such contracts on equal footing as their hard copy counterparts, so long as the provisions of UETA/ESIGN are followed. Both UETA and ESIGN are intended to eliminate doubts surrounding the use of online contracting and, among other things, prevent someone from arguing that a signature or contract is invalid and cannot be enforced solely because it is electronic. Electronic signatures and records, like their hard copy counterparts, remain subject to the types of legal challenges that may be brought against insurance contracts generally, such as evidentiary challenges regarding the underlying authenticity of the signature or contract, questions as to a party's intent to sign the electronic document, attribution of the signature, and non-repudiation.

ESIGN explicitly and UETA implicitly also recognize the validity of storing documents electronically. Additionally, both acts have exclusions relating to transactions involving wills and trusts, family law, and UCC Article 2 and 2A transactions.

#### UETA

##### *Introduction to UETA*

UETA was developed by the National Council of Commissioners for Uniform State Law (NCCUSL). This organization drafts the various model laws that states enact, such as the Uniform Transfers to Minors Act, the Uniform Commercial Code, the Uniform Probate Code and the like. UETA, as drafted, is not intended to change substantive law – instead, it is intended to remove legal barriers to online contracting. UETA only becomes effective when it is adopted by a state. To date, almost all of the states have adopted some form of UETA (some with

---

<sup>2</sup> Bob's discussion re: applicability of UCC?

deviations from the standard format that as discussed below raise the issue of federal preemption under ESIGN).

UETA applies to both electronic records and electronic signatures. An electronic record means a record created, generated, sent, communicated, received or stored by electronic means, whether it be electrical, digital, magnetic, wireless, optical, or other means. An electronic signature can be 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. UETA is a technologically neutral statute, and does not place any signature or electronic record technology over another.

### ***Requirements of UETA***

UETA states that the following requirements must be met in order to benefit from its provisions:

- 1. Freedom of Choice.** Doing business electronically must be the choice of the contracting party – a party to a transaction cannot require that business be done electronically.
- 2. Consent.** The parties must affirmatively consent to conduct transactions electronically.
- 3. Ability to Revoke Consent.** A party may, after initially consenting, refuse to continue conducting transactions electronically. If such occurs, the parties must revert to a paper format.
- 4. Retention of Record.** The electronic record or signature must be capable of being retained by the recipient. Thus, it must be able to be recalled and retrieved if asked for.
- 5. Document Integrity.** In order to ensure that no doubt exists about a document's integrity after a signature is captured, once the signature is captured, the document must be, in effect, frozen, so that there cannot be a change to the electronic document or record post-signature. A document's integrity and the ability to demonstrate that what every system adopted for electronic signatures and contracts does not permit modifications post-signature, is paramount in addressing concerns of non-repudiation. In order to assert non-repudiation, the integrity of the document once signed should be beyond challenge. Otherwise, the party signing can claim that the document presented does not in fact reflect the electronic document actually signed.
- 6. Authentication.** The electronic record and/or signature must be authenticated by and attributable to the person signing – there must be some sort of validation or verification of the signer's identity. Authentication and attribution may be demonstrated through the methods adopted to confirm that the identity of the person signing electronically is in fact the person represented as signing.
- 7. Consumer Protection.** In addition to the above, many states adopting UETA have also added specific consumer protection language that appears in ESIGN.

## ESIGN

### *Introduction*

Like UETA, ESIGN provides that no contract, signature or other record can be denied legal effect solely because it is in an electronic form. ESIGN contains definitions for electronic signatures and records similar to UETA and, like UETA, is technologically neutral. UETA also has similar requirements on what needs to surround an electronic signature in order for it to come under ESIGN's rules.

### *Requirements of ESIGN*

ESIGN limits its protection to transactions that otherwise meet the standard requirements for a valid signature or contract, such as:

1. **Authentication** – verification of the sender, typically through a verification of a certificate identifying the sender;
2. **Document Integrity** – confirmation that the message has not been modified in any way since the signature was attached – once a document is electronically signed it must be locked so that it cannot be later modified by a third party; and
3. **Non-Repudiation** – confirmation that the sender or signer cannot deny that the message or signature was sent or attached the document signed.
4. **Consumer Notices** – Under ESIGN, where a disclosure is required under consumer protection laws, such as in a replacement notice or an illustration, the electronic means used for the consumer disclosure must, prior to capturing the signature, inform the consumer of:
  - The right to request a hard copy of any document, and the cost, if any, of doing so;
  - The right to use a paper format instead of electronic communications;
  - The scope of consent granted related to the electronic transactions – specially, what kinds of transactions the consent applies to;
  - The right to withdraw consent to continuing electronic transactions, and how to withdraw such consent; and
  - The hardware and software technical requirements for both completing on-line transactions and accessing any related records. The consumer must be able to confirm that he or she can in fact access the information that is the subject of the consent electronically. This is an ongoing requirement, and, upon updating its hardware and software, must be reconfirmed by the company with the consumer.

It is important to note that many states adopting UETA have included consumer disclosure provisions similar to those contained in ESIGN.

5. **Record Retention** – ESIGN specifically authorizes electronic record retention, so long as the record remains accessible to all persons legally entitled to access them “in a form that

is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.”

### ***Additional ESIGN Considerations***

- 1. Applies to Insurance Transactions** – ESIGN specifically states that it applies to insurance transactions, but specifically excludes termination notices for life insurance (but not annuities).
- 2. Specifically Authorizes Digital Signatures** – While not requiring a specific form of electronic signatures, ESIGN does specifically recognize digital signatures as a permissible form of electronic signatures.
- 3. UETA does not have specific ESIGN Consumer Protections** – ESIGN also contains some specific consumer protections that do not appear in standard UETA language adopted by NCCUSAL.
- 4. Preemption** – ESIGN preempts state laws on digital or electronic signatures, except if a state has adopted the uniform version of UETA (the addition of consumer protection provisions offered under ESIGN would not cause federal preemption). UETA, unlike ESIGN, specifically provides that electronic records are not to be denied admissibility into evidence solely because they are in an electronic format – no such provision exists in ESIGN. Presently, approximately 46 states have adopted some form of UETA. There are a few states, such as California, Hawaii, Louisiana and Maryland that have adopted UETA with specific exclusions that pertain to life and health insurance. These exclusions could result in federal preemption of the limiting provisions. Preemption by ESIGN could occur, if a state adopts a form of UETA that deviates from its NCCUSL Model and is inconsistent with the provisions of ESIGN.

## **THE INDUSTRY’S CURRENT EXPERIENCE WITH STATE INSURANCE DEPARTMENTS**

According to an article published recently in *Best’s Review*, research indicates that only about 5% of U.S. insurers are using e-signatures despite the fact that federal and state governments, along with many state insurance departments, have given the green light for insurers to use e-signatures.<sup>3</sup> The article cites the lack of case law and uncertainty about compliance as key reasons why insurers have not yet begun to rely on e-signatures.

Since annuities are insurance contracts, the NAVA Application Processes may be subject to review and approval by the insurance departments of the 50 states and the District of Columbia. The Legal Task Force understands that state insurance department approval is perceived to be the most important and potentially limiting regulatory dimension of the NAVA Application Processes. However, as of the date of this draft of the white paper it is unclear how much of this

---

<sup>3</sup> “E-SIGN Here,” *Best’s Review* (March 2003), citing the “E-Signatures and U.S. Insurance” report by the research and advisory firm, Celent Communications.

perception is simply lingering concern because of the issues raised by the National Association of Insurance Commissioners (the “NAIC”) in its 1997 “Marketing of Insurance Over the Internet,” and how much is reflective of continuing problems NAVA members are experiencing in obtaining state insurance department approval of their E-Apps.

**The Legal Task Force is in this draft of the white paper asking for input from NAVA members as to their current actual experience with state insurance departments.<sup>4</sup> To assist in eliciting such information, the following section discusses several of the perceived legal issues that have been identified in various articles and studies.**

### **Remaining Legal and Regulatory Uncertainties**

Despite the protections provided by UETA and ESIGN, businesses subject to independent state regulation, like insurance companies, have been slow to embrace the electronic commerce business model. In part, this reluctance can be traced to lack of case law and precedent regarding the interpretation of when ESIGN preempts inconsistent provisions in UETA. Moreover, the federal preemption issue raised by ESIGN has not been addressed, leaving it unclear what portions of a non-complying state UETA statute will be held preempted by state law. For example, does ESIGN preempt the entire state statute, or just inconsistent provisions? Finally, the unique nature of state insurance departments and their role in regulating the sale of insurance has further discouraged insurance companies from jumping into electronic commerce and electronic sales without hesitation.

### **Lack of State Regulatory Uniformity**

Some states, such as California, have adopted rules and regulations requiring both insurance companies and agents to provide information on their web sites that list the statutory companies, where they are authorized to sell insurance and any applicable NAIC Code or license number. This information must be clear and conspicuous on the web site, and easily accessible by site visitors. These types of regulations are directed toward consumer protection rather than addressing the core need of insurance companies – how to use the Internet to maximize customer service and potential savings while coordinating with regulatory authorities.

In the past few years, the NAIC attempted, through its E-Commerce Working Group, to clarify many of the issues related to the effect of electronic commerce on the insurance industry. To that end, the NAIC adopted a model bulletin on E-Commerce entitled “Regulatory Issues Associated with the Provision of Insurance.” Unfortunately, this model bulletin has not been adopted by many states. If widely adopted, the model bulletin could provide clarity and uniformity on the issue of electronic signatures and contracts. The lack of wide acceptance of the Bulletin may necessitate individual insurance e-commerce coordination with DOIs in 50 states, DC and the territories, each potentially taking a slightly different tack on the issues.

The model bulletin, in a nutshell, provides the following guidelines relating to electronic commerce and insurance transactions:

---

<sup>4</sup> Some carriers have, for example, reported approval difficulties from New York.

- Affirms the validity of electronic signatures, records and record retention;
- States that the mere operation of a web site available to consumer in a state that contains insurance advertising, does not, by itself, constitute the transaction of insurance (provided that the operator does not otherwise solicit, sell or negotiate insurance with consumers in that state);
- States that advertising on a web site is generally considered subject to the same rules as advertising in any other media;
- Treats such issues as formatting, paper size, and font requirements originally established for printed documents as being satisfied for electronically transmitted or displayed records if the electronic record/document uses characteristics that are designed to meet the same regulatory objectives. (It is unclear, however, if this would mean that an insurer would have to re-file or do an informational filing for an approved hard copy contract/advertisement/form if it is intended to be displayed electronically);
- Recognizes electronic record retention so long as an insurer can reassemble the original information upon request;
- Recognizes the validity of electronic delivery of documents where the parties have agreed to such means of delivery; and
- States that privacy laws are equally applicable to all forms of media, including electronic media/web sites. As a note, the issue of privacy and electronic commerce play hand in hand with each other. As the NAIC creates privacy regulations, it is important that business look to both the paper and electronic processes in order to protect the interests and privacy of their customers.

### **Lack of Legal Authority in the Form of Case Law**

ESIGN and UETA are relatively new statutory laws. Electronic signature methodologies are also relatively new.

This means that very little case law exists to interpret the statutes. For example, both ESIGN and UETA require that the parties consent to the use of electronic signatures. However, the fact patterns in which consent will be deemed to have been sufficiently manifested in the context of electronic signatures is not well developed, including for the electronic signature methodologies discussed in this paper. Some case law is discussed in the following section of this paper. The lack of legal interpretation in the form of case law for both ESIGN and UETA could allow the DOIs to take at least colorably meritorious positions that under the facts of a given case E-Signatures are not permissible.

As has already been noted, there is very little if any case law regarding the precise fact patterns in which ESIGN will pre-empt contrary provisions of state UETA laws.

## **NAVA Could Clarify Treatment of E-Apps by State Insurance Departments**

It is not clear whether the failure of various state insurance departments to adopt the NAIC model bulletin reflects continuing concern by such departments with respect to electronic contracts and signatures in the insurance industry. Notwithstanding the guidelines provided by ESIGN and UETA, it has been observed that state insurance departments, with a few exceptions, have been slow to comment on or embrace electronic signatures in the consumer marketplace. The Legal Task Force understands that some in the industry believe it is the better practice not to assume that an approved paper form will be deemed approved in an electronic format. An informational filing may therefore be advisable if a company wants to use electronic media to display an already approved paper form. If the electronic media deviates in any material way from the content of the approved paper form, then it can be re-filed. Moreover, it is not clear whether or not any given electronic signature methodology would be accepted by all state DOI's.

In light of this state of affairs, NAVA is considering notice filings on behalf of the industry with state DOIs for E-Signature/E-App process. This issue will be addressed once the eSignatures working group has completed its deliberations and decided on standard processes and procedures.

## **LEGAL IMPLICATIONS OF E- SIGNATURE METHODOLOGIES**

A core issue facing insurance companies is what kind of electronic signatures and electronic records are legally sufficient for the electronic sale of insurance and annuities. For variable annuities, a primary issue is how an insurance company can validate the identity of the applicant. This question has different answers depending on whether an application is signed electronically, in the presence of an agent, or, if they are signed electronically via an Internet application, without the benefit of an agent's presence.

### **E-Signature Methodologies**

The term "electronic signature" is a generic one that encompasses various forms of technology and various types of signatures. Common types of electronic signatures include:

***Clickwrap Acceptance Signature or an Email Signature*** – An email with the "signatory's" name attached, clicking on an "I Accept" button on a web site licensing agreement, or confirming an order on Amazon.com are all considered forms of electronic signatures. Since an imposter can easily click "I Accept," clickwrap requires extra care with authentication of the signatory. Commonly, in order to verify the identity of the signatory, credentialing methods, either internal, such as a user name and password, or external, such as asking the signatory to furnish externally verifiable data that would not be likely to be known to an imposter (e.g., drivers license number, bank account information, etc.), are employed. (As to identity verification, see "Digital Certificate" below). Also since an argument can be made that an "I Accept" box was inadvertently checked (e.g., "my finger slipped") by the signatory, added design elements to prove intent to sign may be needed with clickwrap.

***Biometric: Handwriting (Point of Sale POS)*** – This form of signature uses a stylus to actually record the act of signing – such as signing for a Federal Express package, or, a credit card charge with a plastic stylus capturing the act of signing and displaying it on a screen. A digitized signature can also use biometrics. One common form of biometrics captures the unique elements of that signature, such as such as the signer’s pressure points when actually signing the document, and compares them to a signature on file. Biometrics is most commonly used where there is an existing and ongoing business relationship. Currently, digitized signatures are most commonly used in the insurance sales process when there is an electronic application, such as one contained in a laptop computer of a company agent. After viewing any sales presentation and filling out the application, the applicant then signs the electronic application via a digitized signature in the presence of an agent.

***Biometric: Voice Signature Capture*** – Currently, many insurance companies’ customer service departments use recorded lines to capture the consent of contract owners for various annuity transactions. Once an individual is validated as an owner, whether it be through providing a unique set of identifiers such as an address, date of birth, contract number and the like, or using a PIN number assigned by the company, the call is recorded as evidence of the owner’s consent. Voice can also include a biometric authentication of the signer.

***Digital Signatures*** – A digital signature validates and authenticates both the originator of the information and the integrity of the document sent. A digital signature consists of an encrypted or mathematically scrambled document that appears as a string of characters appended to a message – often called a hash mark. This string of characters serves to identify the sender of the document and establish the integrity of the document via a unique set of keys. Digital signatures typically use a combination of a public and private “key” to validate the signature, the document and its integrity. The private key is kept confidential, and used to encode the document it is appended to. This key is part of the digital signature. The public key is made available to those who need to decode transmissions sent by the private key holder. The public key can only open documents if the proper private key accompanies them. If an electronic document is changed in any way during transmissions, then the hash mark is changed, and the document cannot be opened by the public key – thus insuring both the integrity of the document and the identify of its sender.

Unfortunately, while digital signatures are the most secure and most attractive for purposes related to Internet applications, they have not been widely embraced by the consumer marketplace. There is no centralized repository of digital signatures that any one institution can look to for validation purposes, which limits the value of such signatures on the new-business sales front.

***Digital Certificate*** – Digital certificates involve retaining a third-party vendor to assist in the validation/authentication process. Generally, a company or group, such as the combined efforts of Equifax and GeoTrust, would ask the signor a series of questions that only he/she could know. The answers to these questions are then compared to the information on file for the signor. If the third-party vendor is comfortable that the person answering the questions was actually the individual identified, then a certificate would be issued validating/authentication the identity of the signor. The questions asked would be in addition

to any contained in the application, and there would have to be clear and conspicuous consent to use this methodology to confirm the signor's identity.

### **Statutory Law Regarding Use of Methodologies**

Both UETA and ESIGN are intended to eliminate doubts surrounding the use of online contracting and, among other things, prevent someone from arguing that a signature or contract is invalid and cannot be enforced solely because it is electronic. However, under both UETA and ESIGN, electronic signatures and records, like their hard copy counterparts, are subject to evidentiary challenges regarding the underlying authenticity of the signature or contract, including facing such questions as the intent to sign the electronic document, attribution of the signature, and non-repudiation.

UETA and ESIGN provide that no contract, signature or other record can be denied legal effect solely because it is in an electronic form. Both UETA and ESIGN contain similar definitions for electronic signatures and records and are technologically neutral. UETA and ESIGN also have similar requirements on what needs to surround an electronic signature for such signature to have legal effect.

Because the statutory law is technologically neutral all of the e-signature methodologies outlined above are theoretically legally usable under UETA or ESIGN.

### **Case Law Regarding Validity of E-Signature Methodologies**

There is some federal case law which we have located which has a bearing on the validity of e-signatures. The earliest relevant case law goes back to the traditional "shrink-wrap" software where the software came with a hard copy "take it or leave it" user license.

Initial case law in the late 80's and early 90's found shrink wrap licenses legally unenforceable for lack of user assent.<sup>5</sup> However, later case law found assent to shrink-wrap licenses where (i) the software automatically splashed the license on the user's computer screen and (ii) would not run unless the user affirmatively indicated acceptance of the license.<sup>6</sup>

Later cases have found that the legal principles involved in the shrink wrap cases have important implications in assessing the validity of online agreements. In one case involving Netscape<sup>7</sup> ("*Netscape Communications*"), users downloading software off the Internet were not deemed to have assented to the terms of a license for the software where (i) the only reference to the software license appeared via a link which read "Please review and agree to the terms of the ... software license agreement," (ii) the link was not even visible unless the user scrolled down to the bottom of the webpage from which the downloading took place, and (iii) the user was allowed to proceed to use the software without affirmatively consenting to the terms of the license.

---

<sup>5</sup> See, for example, *Step-Saver Data Systems v. Wyse Technology*, 939 F. 2d 91 (Third Cir., 1991)

<sup>6</sup> *ProCD Inc v. Zeidenberg*, 86 F. 3rd 1447 (7th Cir, 1996)

<sup>7</sup> *Sprecht v. Netscape Communications Corp*, 150 F. Supp 2d 585 (S.D.N.Y., 2001)

The court in *Netscape Communications* held that Netscape failed to provide sufficient notice of its license and consequently did not assent to the “browsewrap” license involved. The court stressed that “the mere act of downloading . . . was hardly an unambiguous indication of assent; the primary purpose of downloading was to obtain a product, not to assent to an agreement. However, the court found, by contrast, that clicking an “I Accept” box at the end of a license – or what we have referred to in this paper as “clickwrap”- would have “no meaning or purpose other than to indicate assent” to its terms.

In another case (“*Register.com*”) involving a “who is”<sup>8</sup> inquiry made through one of the internet domain name registry firms, assent to an on-line license was found, even where the user did not check a box or click an icon to indicate acceptance.<sup>9</sup> The *Netscape Communications* court would have found the on-line “who is” use license an invalid “browsewrap” procedure but the court in *Register.com* upheld the license; the license was upheld because the vendor automatically presented the license terms in clear view and in close proximity to its “who is” service where a user would readily notice them. Also, there was a paragraph next to the “who is” inquiry which read “by submitting this query, you agree to abide by these terms.”

This case law indicates that clickwrap (i.e., clicking “I accept”) can be sufficient proof of consent if all the terms of what the consumer is assenting to are automatically presented to the consumer. In fact, in the proper circumstances, assent will be proven by browsewrap provided that the terms being assented to are automatically presented to the consumer and that unambiguous and clear notice is given to the consumer that by proceeding he agrees to those terms.

Based on the foregoing cases, an online clickwrap signed annuity application stands the best chance of being deemed of indicating the required assent if all the terms of the annuity are automatically splashed to the purchaser and must be, for example, at least scrolled through to proceed with the application. However, this is impractical given the voluminous amount of verbiage involved in an annuity contract.

The question then becomes whether the application can merely provide links to additional documents which will form the annuity agreement. In one case, *Pollstar*,<sup>10</sup> a vendor stated that its services were “subject to the license agreement.” This language served as a hyperlink to the actual license agreement. This hyperlink was in small gray print on a gray background and the vendor failed to underline the text. In addition, the court pointed out that some blue colored links on the site were not working properly which might have caused a consumer to think that all colored links were not working. Under these circumstances, the court held that the website did not sufficiently put the visitors on notice for there to be sufficient assent to the license. The license was held unenforceable.

Despite *Pollstar*, scholarly opinion on the issue seems to be that hyperlinks will be legally sufficient if other design elements on a website or in an electronic document put the consumer on

---

<sup>8</sup> This is an inquiry to find the registered owner of an Internet domain name.

<sup>9</sup> *Register.com v. Verio*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000)

<sup>10</sup> *Pollstar v Gigmania*, 170 F. Supp.2d 974 (E.D. Cal. 2000)

requisite notice. If so, then an e-annuity application which creates a prominent link to, for example, a prospectus and places the link directly adjacent to an “I have read and accept” check box will likely be treated by a court as providing an acceptable level of notice. Certainly, courts can be expected to consider whether or not the link is underlined or otherwise highlighted, or in a readily distinguishable color, or if conditional language of a “no consent - no deal” type occupies the text of the link. A prominent, colorful link, next to an “I have read and accept” box should be sufficient for a court to find consumer assent.

No case law has been found on digitized signatures or voice methods.

## **PRIVACY REGULATIONS – HOW THEY APPLY TO E-APPS**

The assumption is that an E-Signature will only be used with electronic documents -- in particular the E-App. As such, the Legislative Task Force reviewed the regulations associated with the E-App.

### **Introduction**

The Gramm-Leach-Bliley Act (“GLBA”) was enacted on November 12, 1999 to reform the financial services industry and to address concerns relating to financial privacy. The Securities and Exchange Commission (“SEC”) privacy regulation is known as Regulation S-P and applies to variable annuities. Additionally, the National Association of Insurance Commissioners (“NAIC”) issued a model privacy regulation in late 2000. This regulation is directly applicable to fixed and variable annuities. These two regulations set forth the requirements for protecting the financial privacy of customers as well as setting forth limitations on the use of customer data by financial institutions.<sup>11</sup>

### **Regulation S-P Requirements**

The application of Regulation S-P to each of the four process flows is fundamentally the same. In each instance, an applicant for an annuity product is providing information to a financial institution. The collection of financial information, known as nonpublic personal information (“NPI”), triggers many protections under Regulation S-P. For purposes of this document, there are two primary concerns:

- Privacy statement delivery; and
- Security requirements for NPI.

### ***Privacy Statement Delivery***

The information being sent to the financial institution is more than likely nonpublic personal information (“NPI”). Regulation S-P defines NPI to include “personally identifiable financial

---

<sup>11</sup> The FTC has been assigned the responsibility of enforcing GLBA when another regulator does not exist and has promulgated the Rule and Standards for Safeguarding Customer Information. Readers should review this document as well.

information.” Both the annuity issuer and a broker/dealer must provide a privacy statement to the applicant. The statement may be the same, but generally each financial institution involved in the financial transaction will provide its own privacy statement to the applicant. The rules for when delivery of the privacy statement must occur depend upon whether the applicant is a customer or a consumer. The timing also depends upon the application of some exceptions to the general rule.

The public policy for delivery is to provide persons providing NPI to financial institutions with an understanding of how the financial institution will use this information. For a customer, Regulation S-P requires the delivery of an initial notice that clearly and conspicuously states privacy practices when the relationship is established. For consumers, a financial institution must deliver an initial notice that clearly and conspicuously states the financial institution’s privacy practices before disclosure of NPI to a non-affiliated third party. Broker/dealers and annuity issuers may establish this relationship at different times in each of the four process flows. Each financial institution must perform an analysis of whether the applicant is a customer or a consumer depending upon the type of financial institution involved in the transaction, the product offered, the information collected, and the use for the collected information.

Once the timing for delivery is determined, Regulation S-P sets forth specific requirements for actual delivery of the privacy statement. Actual delivery of the initial privacy notice may be achieved electronically if:

- the privacy notice is posted on a web site<sup>12</sup>;
- the applicant agrees to receiving the privacy notice electronically;
- the applicant acknowledges receipt of the notice; and
- compliance procedures are designed to evidence the above requirements.

In conclusion, an electronic application should include a process to provide the privacy notice to the applicant in a meaningful, clear and conspicuous manner; the applicant’s permission to receive the notice electronically must be collected; and the applicant must acknowledge actual receipt of the privacy statement by reviewing the privacy notice on the financial institution’s web site.

### ***Information Security Requirements***

The security of NPI is specifically required by Regulation S-P. Section 248.30 requires all broker/dealers to adopt procedures and policies to ensure the physical safeguards of NPI. The rule requires NPI be secure and confidential, protected against anticipated threats or hazards, and protected against unauthorized use. The electronic application and the electronic signature must comply with this requirement.

---

<sup>12</sup> Regulation S-P sets forth specific requirements regarding the definition of clear and conspicuous within the context of a web site. See 17 CFR 248.3(c)(2)(iii).

## **NAIC Model Regulation and State Privacy Regulations**

The NAIC has also issued a model privacy regulation to ensure compliance with GLBA. Versions of the model regulation have been implemented in many states. It is important for all entities subject to state insurance law to comply with the state version of the NAIC model regulation. The NAIC model regulation is nothing more than guidance. The actual state regulation or law must be analyzed.

For the most part, the NAIC model regulation and the actual state regulations implementing the NAIC model regulation closely follow Regulation S-P. So, each of the requirements discussed above also apply to the NAIC model regulation. There are some significant differences in the treatment of participants to certain types of plans in the NAIC model regulation. This may impact when the notice must be provided to the applicant.

### **State Law Implications**

The federal and state laws associated with financial privacy are still evolving. The GLBA specifically permits states to implement more stringent privacy obligations. A thorough review of applicable state laws must be completed to ensure the delivery requirements and information security obligations are consistent with Regulation S-P and the NAIC model regulation.

Regarding information safeguarding obligations, the states have been implementing such rules. While the theory of protecting NPI is similar in both Regulation S-P and state privacy regulations, the state regulations tend to be more specific than Regulation S-P. A review of each applicable state regulation is necessary.

## **EFFECT OF USA PATRIOT ACT REGULATIONS**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 (Public Law 107-56) was signed into law on October 26, 2001. The Act makes a number of amendments to the anti-money laundering provisions of the Bank Secrecy Act which are intended to make it easier to prevent, detect, and prosecute international money laundering and the financing of terrorism.

### **Anti-Money Laundering Programs**

Section 352(a) of the PATRIOT Act requires every financial institution to establish an anti-money laundering program that includes, at a minimum, (i) the development of internal policies, procedures, and controls; (ii) the designation of a compliance officer; (iii) an ongoing employee training program; and (iv) an independent audit function to test programs. Section 352(c) of the Act directs the Department of Treasury to prescribe regulations for anti-money laundering programs that are commensurate with the size, location, and activities of the financial institutions to which such regulations apply.

**Broker/dealer AML Programs** – Broker/dealers are subject to AML regulations issued by the NASD in Rule 3011. These regulations require each member broker-dealer to develop and

implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the Bank Secrecy Act and the implementing regulations promulgated there under by the Department of the Treasury.

***Insurance Company AML Programs*** – A proposed rule for anti-money laundering programs for insurance companies was issued by Treasury on September 26, 2002.<sup>13</sup> To date, a final rule has not been issued. Under the proposed rule, each insurance company would be required to develop and implement a written anti-money laundering program reasonably designed to prevent the insurance company from being used to facilitate money laundering or the financing of terrorist activities.

### **Customer Identification Programs**

Section 326 of the USA PATRIOT Act requires Treasury to prescribe regulations "setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution."

***Broker/dealer CIP*** – On April 29, 2003, Treasury and the SEC issued a joint final rule for customer identification programs for broker-dealers.<sup>14</sup> Broker-dealers must comply with the rule by October 1, 2003.

The rule requires a broker-dealer to establish, document, and maintain a written Customer Identification Program appropriate for its size and business. The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable and must enable the broker-dealer to form a reasonable belief that it knows the true identity of each customer. The procedures must be based on the broker-dealer's assessment of the relevant risks, including the various methods of opening accounts provided by the broker-dealer.

Prior to opening an account, the broker-dealer must obtain the following customer information: name, date of birth, address, and identification number. For a U.S. citizen, this is a taxpayer identification number. For a non-U.S. citizen, it may be a taxpayer identification number, passport number, alien identification card number, or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

The CIP must contain risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The rule permits customer verification to be performed through both a review of documents and non-documentary methods, such as contacting a customer, independently verifying identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source, checking references with other financial institutions, or obtaining a financial report.

---

<sup>13</sup> Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Insurance Companies, 67 Fed. Reg. 60625 (September 26, 2002).

<sup>14</sup> Securities and Exchange Commission, Department of Treasury; Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25113 (May 9, 2003).

The rule also requires that a record be made and maintained containing the customer identification information, a description of any document that was relied on to verify identity, a description of any non-documentary methods used to verify identity, and a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained.

**Insurance Company CIP** – Regulations for insurance company CIP have not yet been proposed.

### **Suspicious Transactions Reporting**

**Broker-dealer Reporting of Suspicious Transactions** – on July 1, 2002, Treasury issued a final rule requiring the filing of a Suspicious Activity Report-Brokers or Dealers in Securities ("SAR-BD")<sup>15</sup>:

- If a transaction is conducted or attempted by, at, or through a broker-dealer involving or aggregating funds or other assets of at least \$5,000, and
- The broker-dealer knows, suspects or has reason to suspect that the transaction:
  - Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity;
  - Is designed to evade any requirements of this or any other regulation;
  - Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or involves use of the broker-dealer to facilitate criminal activity.

**Insurance Company Reporting of Suspicious Transactions** – a proposed rule requiring insurance companies to file suspicious activity reports was issued by Treasury on October 17, 2002.<sup>16</sup> To date, a final rule has not been issued. The proposed rule would impose a reporting requirement under the same conditions as described above for broker-dealer reporting.

---

<sup>15</sup> Financial Crimes Enforcement Network; Amendments to the Bank Secrecy Act Regulations - Requirement that Brokers or Dealers in Securities Report Suspicious Transactions, 67 Fed. Reg. 44048 (July 1, 2002).

<sup>16</sup> Financial Crimes Enforcement Network; Amendments to the Bank Secrecy Act Regulations - Requirement that Insurance Companies Report Suspicious Transactions, 67 Fed. Reg. 64067 (October 17, 2002).

## **USA PATRIOT Act Issues Arising out of the Electronic Sales Process for Variable Annuities**

The May 2003 Technology Report of the NAVA Technology Task Force identified four types of electronic application process flows: registered representative (RR) and customer face-to-face; RR and customer on the phone; customer working alone; and 1035 transfer. All result in an electronic application being completed and an electronic signature by the customer. Different electronic signature methods are available for the different flows, including signature capture, voice, click wrap, and fingerprint.

Transactions that are processed electronically are subject to the requirements of regulations issued under the USA PATRIOT Act.

### ***AML***

As described above, the AML programs of broker-dealers (and insurance companies when a final rule is issued) must be reasonably designed to detect and prevent money laundering or the financing of terrorist activities. These programs must include E-App processes. Regardless of the electronic application process employed, the selling broker-dealer and the insurance company issuing the variable contract must have procedures in place that will enable them to discern "red flags" or other indications of suspicious activities and take appropriate action. Broker-dealers and insurance companies should review their AML programs to ensure that their procedures will be effective for electronic applications.

The NASD has issued guidance in the form of a Notice to Members to assist member firms in developing AML programs.<sup>17</sup> The Notice states that broker-dealers should perform additional due diligence when opening an account, depending on the nature of the account, and to the extent reasonable and practicable. This should include inquiring about the source of the customer's assets and income, gaining an understanding of what the customer's likely trading patterns will be, maintaining records that identify the owners of accounts and their citizenship, requiring customers to provide street addresses to open an account, periodically contacting businesses to verify the accuracy of addresses, places of business, telephone numbers, and other identifying information, and conducting credit history and criminal background checks. The RR should perform this additional diligence when interacting with the customer, either face-to-face or over the telephone, in application processes 1, 2, and 4.

NTM 02-21 specifically addresses online brokers who generally do not meet or speak directly to their prospective or existing customers (*i.e.*, application process 3). The NASD states that the online broker must still acquire information about customers and make maximum use of other means of verifying customer identity, such as electronic databases. The NASD also recommends that online firms should consider conducting computerized surveillance of account activity to detect suspicious transactions and activity. Given the global nature of online brokerage activity, AML programs must provide for procedures to confirm the customer data and review the OFAC

---

<sup>17</sup> NASD Notice to Members 02-21, NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Programs Required by Federal Law (April 2002).

List to ensure that customers are not prohibited persons or entities and are not from embargoed countries or regions.

### ***CIP***

The CIP rule for broker/dealers requires that two things be done prior to or within a reasonable time after the opening of an account: the broker-dealer must verify the identity of the customer and the broker-dealer must obtain certain specified customer information.

Verification of identity through documents is only available in a face-to-face sale since part of the verification process involves looking at the photograph on the document to confirm that it is the photograph of the customer. Therefore, in the setting of an electronic application, verification of identity through documents can only be used in application process 1, RR meeting customer face-to-face, and application process 4, involving a 1035 exchange completed in the branch.

Application processes 2 and 3, and process 4 where the application is completed on the Web, would require the broker-dealer to verify the identity of the customer through non-documentary methods. The CIP rule for broker-dealers provides that non-documentary methods are to be employed in situations including, *inter alia*, when "the customer opens the account without appearing in person at the broker-dealer." In non face-to-face processes special care should be taken to make up for the lack of "gut reaction" sensory input and impressions humans get about one another in a face to face encounter. For example, exceptional nervous on the part of a customer might be apparent in a face to face encounter but not in a non face-to-face process. As noted earlier, the NASD recommends that online brokers consider conducting computerized surveillance of account activity.

Company procedures for electronic processing must ensure that the required customer information is obtained. As described above, the CIP rule for broker-dealers also requires that a record be made and maintained containing the customer identification information, and a description of the documents and/or non-documentary methods relied on to verify the identity of the customer. The section-by-section analysis of the rule states: "nothing in the rule modifies, limits, or supercedes Section 101 of the Electronic Signatures in Global and National Commerce Act. A broker-dealer may use electronic records to satisfy the requirements of this final rule, in accordance with guidance that the [Securities and] Commission has issued." This guidance requires that records made and maintained electronically must satisfy the requirements of Rule 17a-4(f).

### ***SARs***

It does not appear that the suspicious transactions reporting rules raise any special issues in regard to electronic processing of applications. Regardless of whether the application is prepared electronically or by paper, a SAR-BD will have to be filed by the broker-dealer if the transaction meets the reporting requirements set out in the rule. This will likely also be the case for insurance companies once a final rule is issued.

## **PROSPECTUS DELIVERY RULES – INTERPLAY OF ESIGN, UETA AND SEC GUIDANCE**

The following discussion applies to variable annuities, fixed annuity products are not securities and, therefore, are not required to be sold pursuant to a prospectus.

### **Federal Securities Law Prospectus Delivery Requirements**

Variable annuity contracts (either the contract itself or interests in the contract (hereinafter, the “contract”)) have been held to be securities under the federal securities laws. For purpose of the following discussion, it is assumed that there is no available exemption from registration available, and, therefore, the contract must be registered under the federal securities laws in order to be offered and sold.

Variable annuities are issued through a life insurance company’s “separate accounts,” which are registered as investment companies under the federal securities laws (specifically, the Investment Company Act of 1940). In fact, variable annuities are typically issued and funded through a two tiered structure: the separate account is registered as a unit investment trust with the Securities and Exchange Commission (the “SEC”) and the underlying investment vehicles are registered “mutual funds” which are dedicated to receive assets from various variable annuity and variable life contracts. Thus, there are at least two, sometimes more, prospectuses that must be distributed in connection with the purchase of a variable annuity: a contract prospectus and one or more mutual fund prospectuses.

Section 5 of the Securities Act of 1933 (“Securities Act”) prohibits the delivery after sale of a registered security unless the security is accompanied or preceded by a prospectus that meets the requirements of Section 10(a) under the Securities Act.

Based upon this prohibition, at the latest, the variable annuity contract prospectus must be delivered at the time the contract is delivered. In addition, Section 5 generally prohibits the use of contract applications without accompanying prospectuses, since applications may constitute “supplemental sales literature” that must be preceded or accompanied by a prospectus. Therefore, the delivery of an application for a variable contract may also require a prospectus. As discussed below, some broker-dealers do not deliver underlying fund prospectuses with the contract prospectus at the time an application is solicited. Instead, they deliver the fund prospectuses at the time the confirmation of the sale is delivered. Others deliver both the contract and fund prospectuses at the time the application is solicited.

Rule 482 under the Securities Act permits the use of certain types of advertisements without being accompanied by prospectuses, but Rule 482 generally prohibits an advertisement from containing or being accompanied by a purchase application.<sup>18</sup> Rule 482(a)(5)(i) does permit an application for a variable insurance contract (which discusses the funds) to accompany the

---

<sup>18</sup> A Rule 482 advertisement is an advertisement that contains the “substance of” information in the prospectus in the advertisement. At the time this draft of the paper was being finalized, the SEC was about to consider amending Rule 482 to among other things, eliminate the “substance of” requirement.

contract prospectus, even though the contract prospectus is not accompanied by prospectuses for the underlying funds. However, many broker-dealers and insurance companies do not rely upon this rule because the effect of this rule has not been entirely clear and is now currently under review by the SEC staff.

### **Electronic Delivery of Required Documents and the Customer “I Can Do It” Demonstration – The Interplay Between SEC Rules and ESIGN**

In connection with electronic commerce, prior to the enactment of ESIGN, the SEC promulgated both rules and advice to regulated entities regarding electronic delivery of documents and the conduct of electronic offerings. (See, SEC Releases Nos. 33-7233 (October 6, 1995); 33-7288 (May 15, 1996); 33-7289 (May 15, 1996) and 33-7856 (May 4, 2000).) Effective delivery of electronic documents was deemed to occur if three requirements were met: notice, access and evidence of delivery. With respect to evidence of delivery, the SEC staff indicated that prior consent was one way to evidence such delivery.

ESIGN legislation passed into law after the SEC issued its guidelines establishing different requirements for valid delivery. These requirements include consent as well as evidence provided electronically by the user of the user’s ability to use the specified electronic means of communication, e.g., the client can use a computer and e-mail features or knows how to load or unload a CD-ROM, etc. ESIGN consent must also be obtained prior to delivery.

Since ESIGN does not on its face overrule SEC rules, many issuers have determined, unless the SEC makes a contrary pronouncement, to conform their electronic delivery process to both ESIGN and SEC pronouncements, since E-Sign is relevant to the delivery of “required documents” to conduct a commercial transaction and a prospectus is a required document as disclosed above.<sup>19</sup>

### **Discussion of the four Application Process Flows based upon general guidelines stated above:**

#### ***Scenario 1 – RR Meets the Customer Face to Face***

In this scenario, since an application is provided to the customer, arguably under the federal securities laws the client must also be provided with a prospectus. If the prospectus is delivered by electronic means, a consent to such delivery would have to be obtained prior to the sales presentation and completion of the application. Arguably, to fulfill ESIGN requirements, the customer himself or herself would have to input the computer directions to “Agree” to electronic delivery in a manner that reasonably demonstrates that the customer can access the prospectus in the means it is electronically delivered. Although consent to the delivery of the prospectus does not require that the client open the prospectus document, practically speaking, because the computer is the representative’s, some selling firms may download and print the document for

---

<sup>19</sup> While as discussed above many states have adopted a version of VETA, ESIGN governs the federally-mandated delivery of prospectuses in connection with the offer and sale of registered securities such as variable annuity contracts.

the client. Since the contract prospectus is itself usually 30-60 pages in length, this may be difficult. If the fund prospectuses were also downloaded, the document could be over 200 pages in length. In addition, the client may have no means at hand to know if he or she can in fact electronically navigate the document, as required.

To avoid the issue of paper download, it has been suggested that the broker-dealer deliver a CD-ROM of the prospectuses to the client. However, it is not clear how the client could demonstrate the knowledge of the use of the CD-ROM to satisfy ESIGN requirements and the SEC has given no guidance on this point. It would seem here that the client would have to input the CD-ROM to demonstrate his/her familiarity with it. This could be an awkward procedure.

### ***Scenario 2 – RR and Customer Complete Application over the Phone***

Regarding prospectus delivery, the selling firm must deliver it to the client. If the client wants paper delivery, that request would have to be made prior to the telephone conversation.

If the client desired electronic delivery, the representative would have had to obtain consent prior to the application input. However, in this scenarios, since the client is presumably working from a computer the client can do this online him or herself.

Regarding the form of electronic delivery, the prospectus must be delivered in such a way that satisfies SEC and ESIGN requirements. This could be in an e-mail from the broker-dealer to the client or sent in a link to a download (where there is some evidence message back to the broker that the client clicked on the link).

Regarding the CD-ROM, it would have to be delivered to the client prior to the sales discussion. Again, there would have to be a mechanism in place for the broker-dealer to confirm that the client had the “know-how” to use the CD-ROM. There is no successful legal model as yet for CD-ROM delivery.

### ***Scenario 3 – Customer Direct***

Scenario 3 is similar to Scenario 2 from a prospectus delivery point of view. The only difference is that the representative is not inputting application information for the client and cannot mail the prospectus to the client. Instead, the client is fending for him/herself. In terms of prospectus delivery, the client must input his/her consent online. The prior discussion in Scenario 2 is equally valid here once the client has consented.

### ***Scenario 4 - Replacement***

This scenario, depending on the format, could mimic scenarios 1, 2, or 3, which have already been discussed. The most significant difference is that the transaction deals with a replacement of a variable annuity from one carrier for a variable annuity of another, which triggers the need for the client and representative to complete various state replacement forms and, perhaps, internal forms of the new carrier, the old carrier or both. Thus, the electronic consent would have to be broad enough to encompass these forms, as well as other information that the new carrier

would need to complete the transaction. These replacement forms are governed by state insurance law and arguably could require “wet” signatures of the representative and client.

## **ISSUES RELATED TO RETENTION OF ELECTRONIC RECORDS OF INSURANCE COMPANIES**

One technological factor that must be kept in mind for all signature methodologies is the need for “non-repudiation”. For “non-repudiation” there can be no doubt about the document’s integrity after the signature is captured: once a signature is captured, the document must be, in effect, frozen, so that there cannot be a change to the electronic document or record post signature. A document’s integrity and the ability to demonstrate that every system adopted for electronic signatures and contracts does not permit modifications post-signature, is paramount in addressing concerns of non-repudiation. In order to assert non-repudiation, the integrity of the document once signed must be beyond challenge. Otherwise, the party signing can claim that the document presented does not in fact reflect the electronic document actually signed.

Section 101 of ESIGN provides that the legal validity of a signature, contract or other record may not be denied solely because it is in electronic form. It also encourages electronic record storage by providing that any statute, regulation, or other law that requires the retention of contracts or other records relating to transactions in or affecting interstate commerce may, with certain exceptions, be complied with by storing the documents electronically. Section 104 preserves the ability of regulatory agencies to interpret the requirements for electronically stored documents with respect to statutes under which such agencies have rulemaking authority.

The guidance refers to SEC Release No. 34-44238, Commission Guidance to Broker/Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with respect to Rule 17a-4(f).<sup>20</sup> In the Release, the SEC found that the electronic storage requirements set out in Rule 17a-4(f) under the Securities Exchange Act of 1934 meet, and are consistent with, the accuracy, accessibility, and accurate reproduction requirements of Section 101(d)(1) of the Electronic Signatures Act.

Therefore, the records required to be made and maintained by the CIP rule may be done so electronically if the requirements for electronic storage media set out in Rule 17a-4(f) are satisfied. Rule 17a-4(f) specifies:

"The records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.

- For purposes of this section:

---

<sup>20</sup> Exchange Act Release No. 44238 (May 1, 2001), 66 Fed. Reg. 22916 (May 7, 2001).

- The term micrographic media means microfilm or microfiche, or any similar medium; and
- The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and (f)(1)(ii) of this section, that meets the applicable conditions set forth in this paragraph (f).
- If electronic storage media is used by a member, broker, or dealer, it shall comply with the following requirements:
  - The member, broker, or dealer must notify its examining authority designated pursuant to section 17(d) of the Act prior to employing electronic storage media. If employing any electronic storage media other than optical disk technology (including CD-ROM), the member, broker, or dealer must notify its designated examining authority at least 90 days prior to employing such storage media. In either case, the member, broker, or dealer must provide its own representation or one from the storage medium vendor or other third party with appropriate expertise that the selected storage media meets the conditions set forth in this paragraph (f)(2).
  - The electronic storage media must:
    - Preserve the records exclusively in a non-rewriteable, non-erasable format;
    - Verify automatically the quality and accuracy of the storage media recording process;
    - Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and
    - Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.
- If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:
  - At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.
  - Be ready at all times to provide, and immediately provide, any facsimile enlargement which the Commission or its representatives may request.

- Store separately from the original, a duplicate copy of the record stored on any medium acceptable under Rule 17a-4 for the time required.
- Organize and index accurately all information maintained on both original and any duplicate storage media.
  - At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
  - Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.
  - Original and duplicate indexes must be preserved for the time required for the indexed records.
- The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.
  - At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the SEC and the self-regulatory organizations of which the broker or dealer is a member.
  - The audit results must be preserved for the time required for the audited records.
- The member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the SEC or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media; or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.
- For every member, broker, or dealer exclusively using electronic storage media for some or all of its record preservation under this section, at least one third party ("the undersigned"), who has access to and the ability to download information from the member's, broker's, or dealer's electronic storage media to any acceptable medium under this section, shall file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records:

The undersigned hereby undertakes to furnish promptly to the U.S. Securities and Exchange Commission

("Commission"), its designees or representatives, upon reasonable request, such information as is deemed necessary by the Commission's or designee's staff to download information kept on the broker's or dealer's electronic storage media to any medium acceptable under Rule 17a-4.

Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to information contained on the broker's or dealer's electronic storage media, including, as appropriate, arrangements for the downloading of any record required to be maintained and preserved by the broker or dealer pursuant to Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 in a format acceptable to the Commission's staff or its designee. Such arrangements will provide specifically that in the event of a failure on the part of a broker or dealer to download the record into a readable format and after reasonable notice to the broker or dealer, upon being provided with the appropriate electronic storage medium, the undersigned will undertake to do so, as the Commission's staff or its designee may request."

Broker/dealers who desire to utilize electronic application processing should review their record storage procedures to make sure that records maintained electronically meet the requirements of Rule 17a-4(f).

There are different retention periods provided for records under insurance laws than under securities laws. The insurance law period (length of the policy plus 7 years) is generally the longer period and the one that will need to be considered by the variable industry. This creates a need for records storage technology that will result in unalterable, fully readable, and readily retrievable documents for a long period. Systems must be capable of very long term storage, impervious to deterioration over time, and provide needed records accessibility despite likely monumental long term changes in technologies.

*Draft*

## **Appendix C**

### Operational Flows Report

## **eSignature: Operational Process Flows**

### **Process Overview:**

This eSignature paper includes two operations process examples: 1. Representative or Broker and Customer face-to-face; and 2. Representative or Broker and Customer via phone. The examples are written within the context of describing business processes for approved technology that could bind new business transactions at solicitation. Technologies approved by the NAVA eSignature Working Group for illustration in these examples include: Click-Wrap, Voice Signature, and Electronic Handwriting. The examples do include all major components of the SPeRS recommendation for “proper” processing of electronic signatures. These key components include:

- Authentication
- Consent to use electronic signature
- Agreements, notices, and disclosures (general principle for presentation & display)
- Electronic signatures – “signing ceremony”
- And Record retention

The examples are organized around the following major sections of the annuity new business transaction:

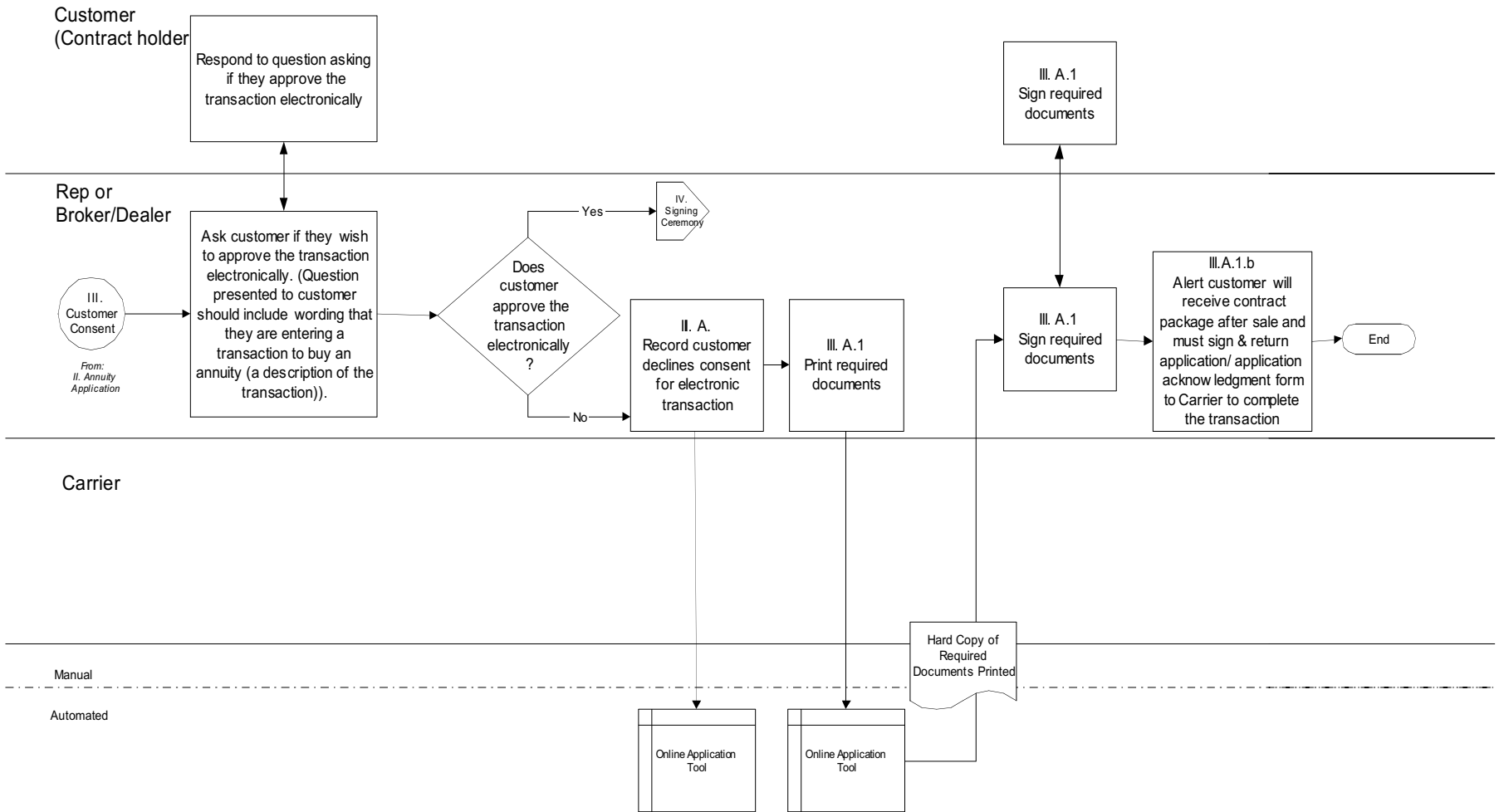
- I. Suitability Review / Purchase Decision
- II. Annuity Application
- III. Customer Consent to Electronic Transaction
- IV. Signing Ceremony
- V. Application and Supplements Data Transmittal / Contract Issuance



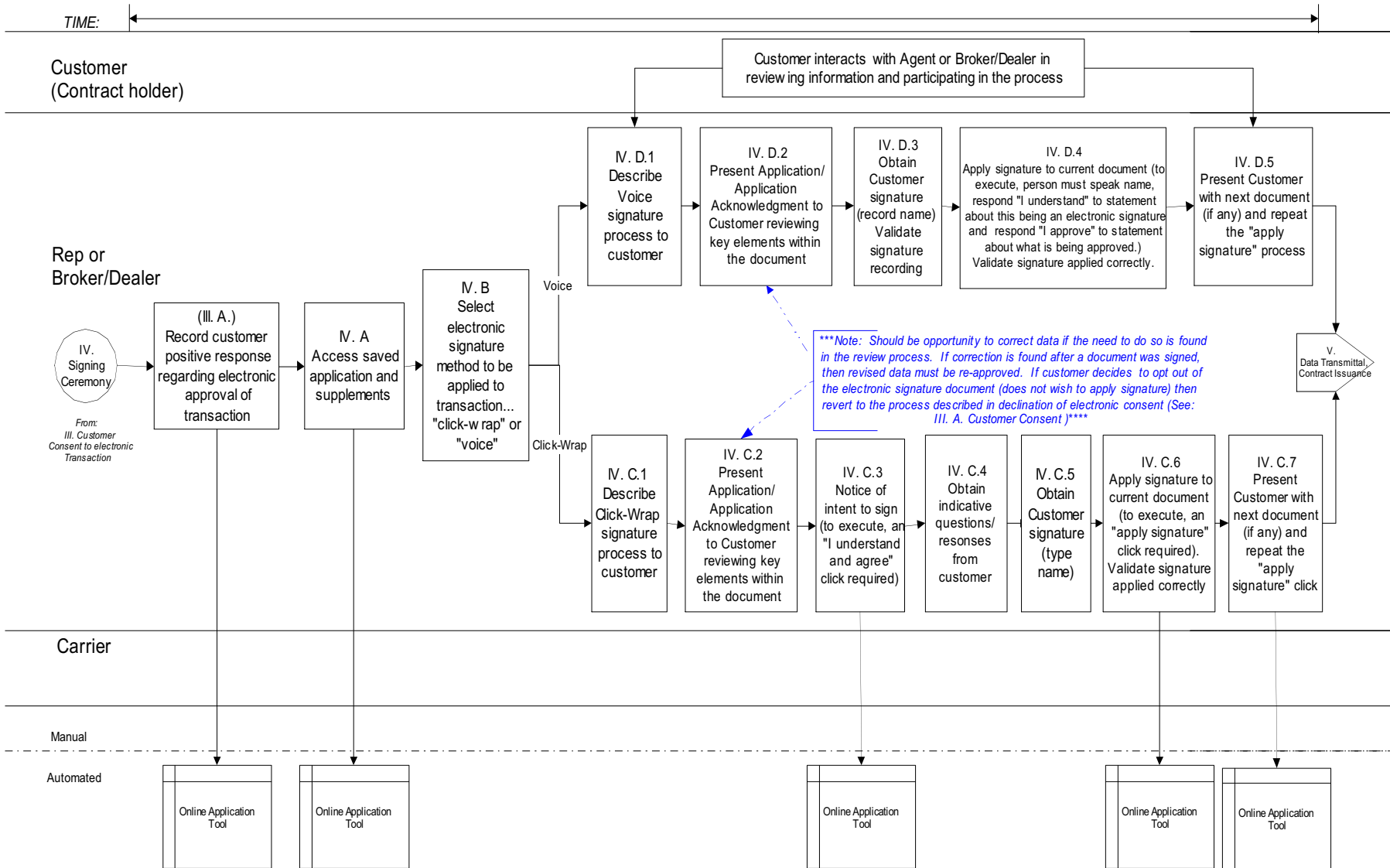


TIME: ←

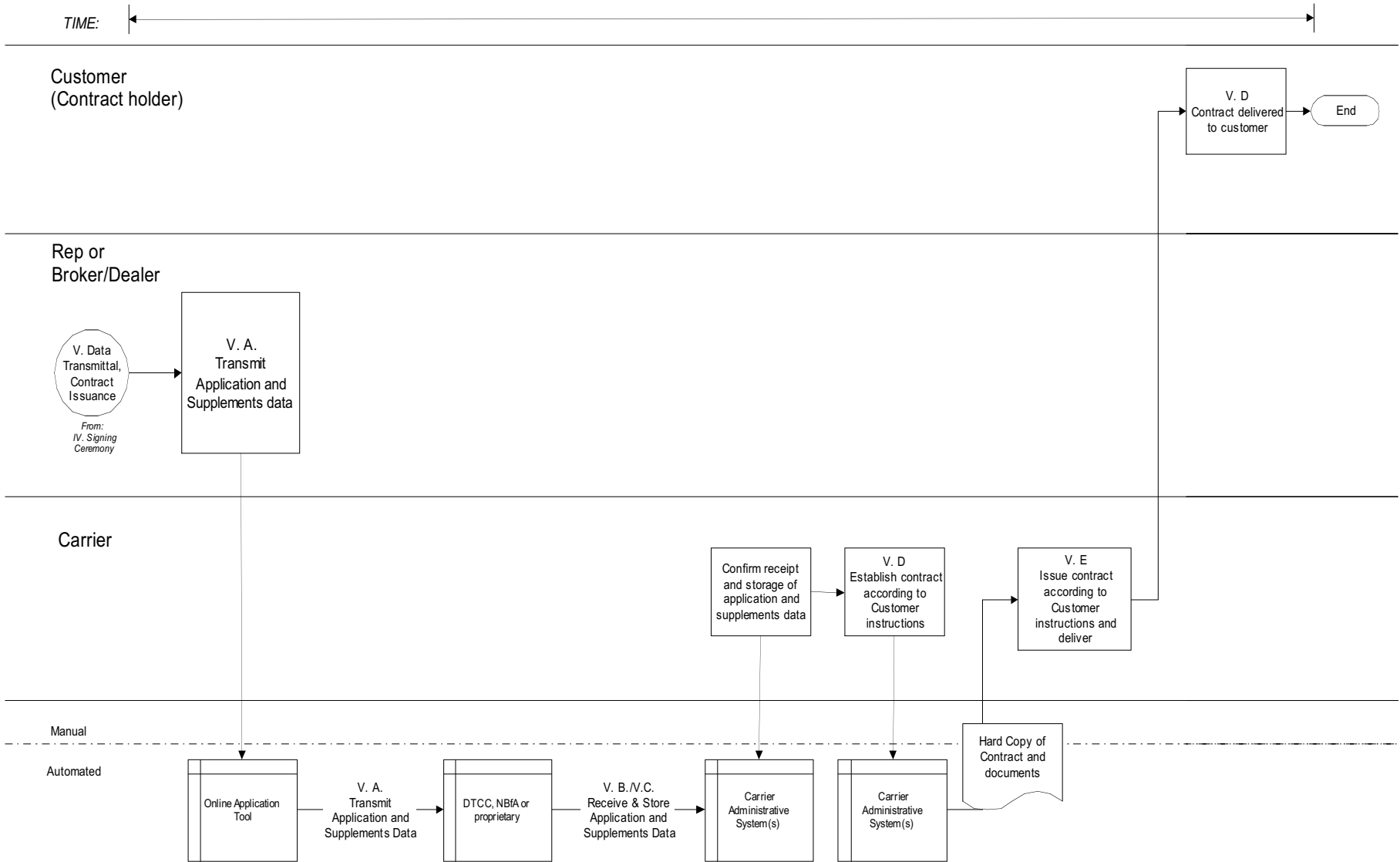
→



### IV. Signing Ceremony



TIME: ←



## eSignature: Operational Process Flows

### Process Flow Example 1: Rep or Broker / Dealer and customer face-to-face

ID	Action	Responsible Party	Remarks
I.	Suitability Review / Purchase Decision		
A.	Identify Customer goals & risk tolerance	Distributor	
B.	Complete know-your-customer / customer identification program / suitability review	Distributor	
C.	Perform illustrations / comparisons as appropriate	Distributor	
D.	Decide on product, carrier, and investment amount	Distributor	
II.	Annuity Application		
A.	Start online application tool	Distributor	
B.	Enter Customer data into tool	Distributor	
1.	Collect Application data (all)	Distributor	Includes Beneficiary instructions, investment instructions, and party information. As well as how the application will be funded.
2.	Collect Application Supplemental data (if applicable)	Distributor	Includes (any applicable): DCA instructions, Direct Deposit instructions, Durable Power of Attorney data, eDelivery Consent, Investment Options supplement, Portfolio Rebalancing request, Qualified Plan documentation, Qualified Plan: Market Conduct Questions/disclosures; and/or Telephone Authorization data
3.	Collect NAIC data (if applicable)	Distributor	Applicable in required states
4.	Collect Replacement data (if applicable)	Distributor	Applicable if a replacement
5.	Collect Transfer-of-Asset data (if applicable)	Distributor	Applicable if a replacement
C.	Save Application & Supplements in tool	Distributor	
III.	Customer Consent to Electronic Transaction		
A.	Record customer response regarding electronic approval of transaction	Distributor	Ask the Customer if they wish to approve the transaction electronically. System should record presenting this question and the response. Question presented to Customer should include wording that they are entering a transaction to buy an annuity (a description of the transaction)
1.	If answer is "no"		
a.	Print and sign all required documents	Distributor	Required documents are those that must be signed at solicitation, if applicable – items like replacement & transfer-of-asset paperwork; NAIC forms; and/or full application if New York.
b.	Alert customer will receive contract package after sale and must sign & return application/application acknowledgement form to Carrier to complete the transaction	Distributor	Unless New York, in which signature @ solicitation is required.
2.	Proceed with this flow if answer is "yes"	Distributor	
IV.	Signing Ceremony		
A.	Access saved Application and Supplements	Distributor	Data should be presented in the tool via a clear and easy to understand format. An electronic display of the forms rendered from data entry is a good selection ... with the forms being reviewed and signed individually
B.	Select electronic signature method to be applied to transaction ...	Distributor	

## eSignature: Operational Process Flows

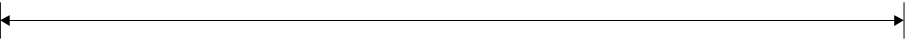
ID	Action	Responsible Party	Remarks
	“click-wrap” or “voice” or “electronic handwriting”		
C.	Sign documents using Click-Wrap		
1.	Describe click-wrap signature process to Customer	Distributor	Involves setting Customer expectations on how the process will work, a verbal overview by the Distributor is all that is expected. Comments along lines of ... that document will be presented, they'll review, identify and adjust if needed, then Customer will need to indicate they understand they are binding the transaction, will be asked to type their name, and then will be asked to apply this approval stamp to each form reviewed.
2.	Present Application/Application Acknowledgement to Customer, reviewing key elements within document.	Distributor	Key elements for review should include items like product, carrier, purchase amount, funds, features/options, death benefit, and applicable state disclosure statement(s)
3.	Notice of intent to sign (to execute, an “I understand and agree” click required)	Distributor	System presents a disclosure along the lines that you are about to sign this document. By signing you are binding this transaction for processing. Customer must click “I understand and agree” to move forward
4.	Obtain indicative questions responses from Customer	Distributor	This assists in the authentication that the person signing is the customer. Examples of indicative questions: mothers maiden name, childhood pet, etc. At least 2 indicative responses should be gathered.
5.	Obtain Customer signature (type name).	Distributor	Customer is asked to type name, instructions alert customer that by typing name and then applying to documents they are signing documents
6.	Apply signature to current document (to execute, an “apply signature” click required). Validate signature applied correctly.	Distributor	Present Customer with question if they wish to apply signature to the current document. This action associates the signature with the record. Customer clicks “apply signature” and the system must bind/lock data – no subsequent changes allowed unless customer re-applies signature. Data that can be rendered into the form reviewed is usually locked with a hash-mark applied behind the scenes that indicates it was signed. This hash mark is what is invalidated if subsequent data changes are made. Should validate signature applied correctly.
7.	Present Customer with next document (if any) and repeat the “apply signature” click	Distributor	Individual documents presented with signature applied similar to how process would work with “wet” signature process. This step repeats until key data included in the application & supplements has been reviewed & authorized (bound/locked with hash-mark indicating approved). Key documents should include application/application acknowledgement, and if applicable: NAIC form, Replacement Form, Transfer of Asset Form.
**Note: should be opportunity to correct data if the need to do so is found in the review process. If correction is found after a document was signed, then revised data must be re-approved. If customer decides to opt out of the electronic signature document (does not wish to apply signature) then revert to the process described in declination of electronic consent.**			
Or D.	Sign documents using Voice		Technology Requirement: PC being used must have a microphone. The standard microphone built into most newer PC's should be sufficient.
1.	Describe voice signature process to Customer	Distributor	Involves setting Customer expectations on how the process will work, a verbal overview by the Distributor is all that is expected. Comments along lines of ... that document will be presented, they'll review, identify and adjust if needed, then Customer “sign” by recording name, and indicating “I understand” that they are binding the transaction and “I approve” to actually approve execution of the document ... that this process will be repeated for all forms required by the transaction.
2.	Present Application/Application Acknowledgement to customer, reviewing key elements within document.	Distributor	Key elements for review should include items like product, carrier, purchase amount, funds, features/options, death benefit, and applicable state disclosure statement(s)

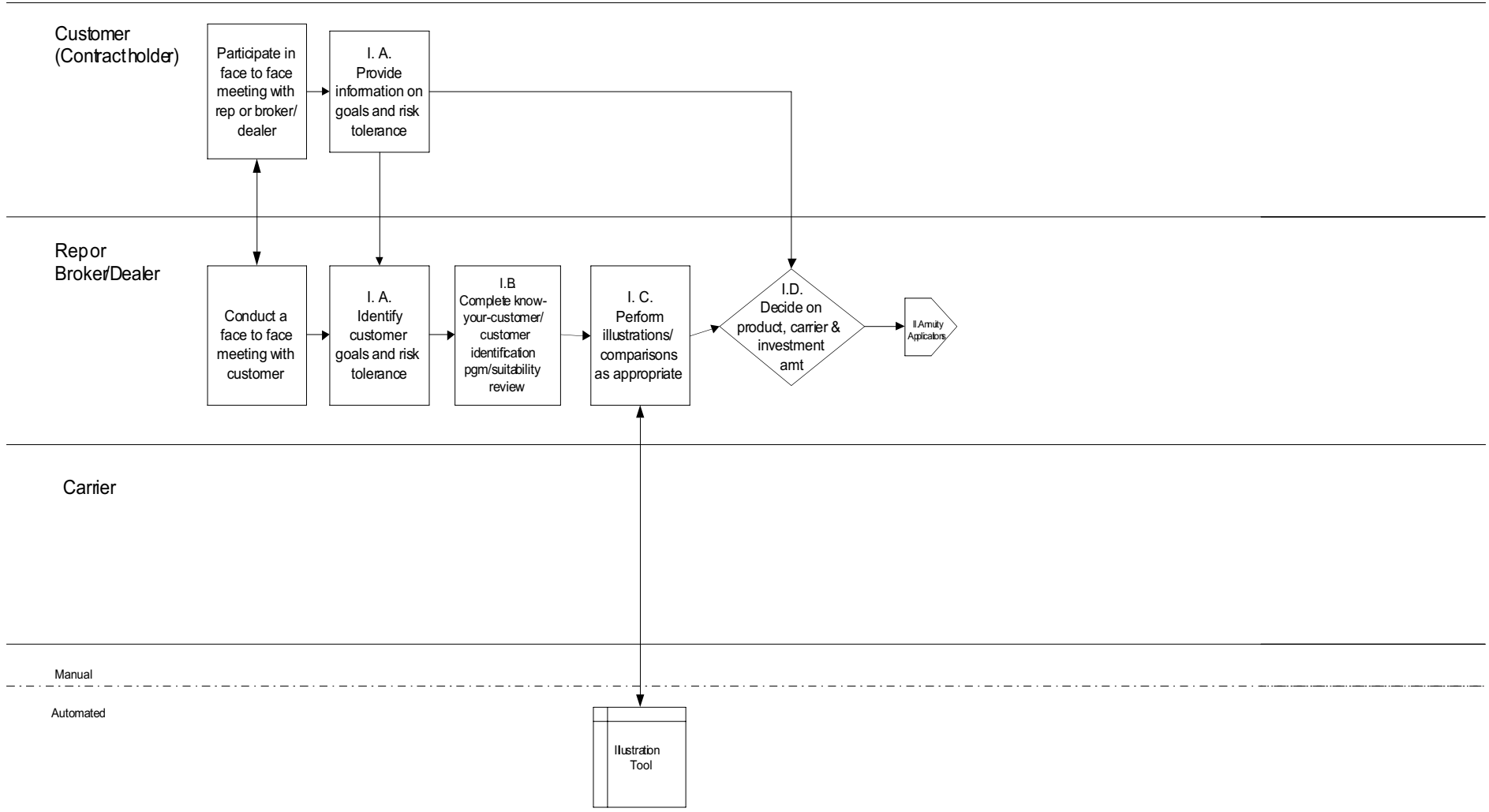
## eSignature: Operational Process Flows

ID	Action	Responsible Party	Remarks
3.	Obtain Customer signature (record name). Validate signature recording.	Distributor	Customer is asked to record name, likely have to speak name twice into a microphone that will establish the voice pattern that becomes their hash-mark signature in documents. Assure voice recorded correctly (requires play-back functionality to check that voice can be heard).
4.	Apply signature to current document (to execute, person must speak name, respond "I understand" to statement about this being an electronic signature, and respond "I approve" to statement about what being approved). Validate signature applied correctly.	Distributor	This action associates the signature with the record. The recording of spoken name, I understand, and I approve "applies signature" and the system must bind/lock data – no subsequent changes allowed unless customer re-applies signature. Data that can be rendered into the form reviewed is usually locked with a hash-mark applied behind the scenes that indicates it was signed. This hash-mark is what is invalidated if subsequent data changes are made. Should validate to assure signature applied correctly.
5.	Present Customer with next document (if any) and repeat the "apply signature" process	Distributor	Individual documents presented with signature applied similar to how process would work with "wet" signature process (record name, I understand, and I approve on each document). This step repeats until key data included in the application & supplements has been reviewed & authorized (bound/locked with hash-mark indicating approved). Key documents should include application/application acknowledgement, and if applicable: NAIC form, Replacement Form, Transfer of Asset Form.
**Note: should be opportunity to correct data if the need to do so is found in the review process. If correction is found after a document was signed, then revised data must be re-approved. If customer decides to opt out of the electronic signature document (does not wish to apply signature) then revert to the process described in declination of electronic consent.**			
Or E.	Sign documents using Electronic Handwriting		Technology Requirement: Must have a biometric signature pad
1.	Describe electronic handwriting signature process to Customer	Distributor	Involves setting Customer expectations on how the process will work, a verbal overview by the Distributor is all that is expected. Comments along lines of ... that document will be presented, they'll review, identify and adjust if needed, then Customer will need to indicate they understand they are binding the transaction, will be asked to sign their name on the signature pad, and then will be asked to apply this approval stamp to each form reviewed.
2.	Present Application/Application Acknowledgement to Customer, reviewing key elements within document.	Distributor	Key elements for review should include items like product, carrier, purchase amount, funds, features/options, death benefit, and applicable state disclosure statement(s)
3.	Notice of intent to sign (to execute, an "I understand and agree" click required)	Distributor	System presents a disclosure along the lines that you are about to sign this document. By signing you are binding this transaction for processing. Customer must click "I understand and agree" to move forward
4.	Obtain Customer signature (sign name on the biometric signature pad).	Distributor	Customer is asked to sign name, instructions alert customer that by handwriting name via the signature pad and then applying to documents they are signing documents
5.	Apply signature to current document (to execute, an "apply signature" click required). Validate signature applied correctly.	Distributor	Present Customer with question if they wish to apply signature to the current document. This action associates the signature with the record. Customer clicks (or taps using the signature wand) "apply signature" and the system must bind/lock data – no subsequent changes allowed unless customer re-applies signature. Data that can be rendered into the form reviewed is usually locked with a hash-mark applied behind the scenes that indicates it was signed. This hash mark is what is invalidated if subsequent data changes are made. Should validate signature applied correctly.
6.	Present Customer with next document (if any) and repeat the	Distributor	Individual documents presented with signature applied similar to how process would work with "wet" signature process. This step repeats until key data

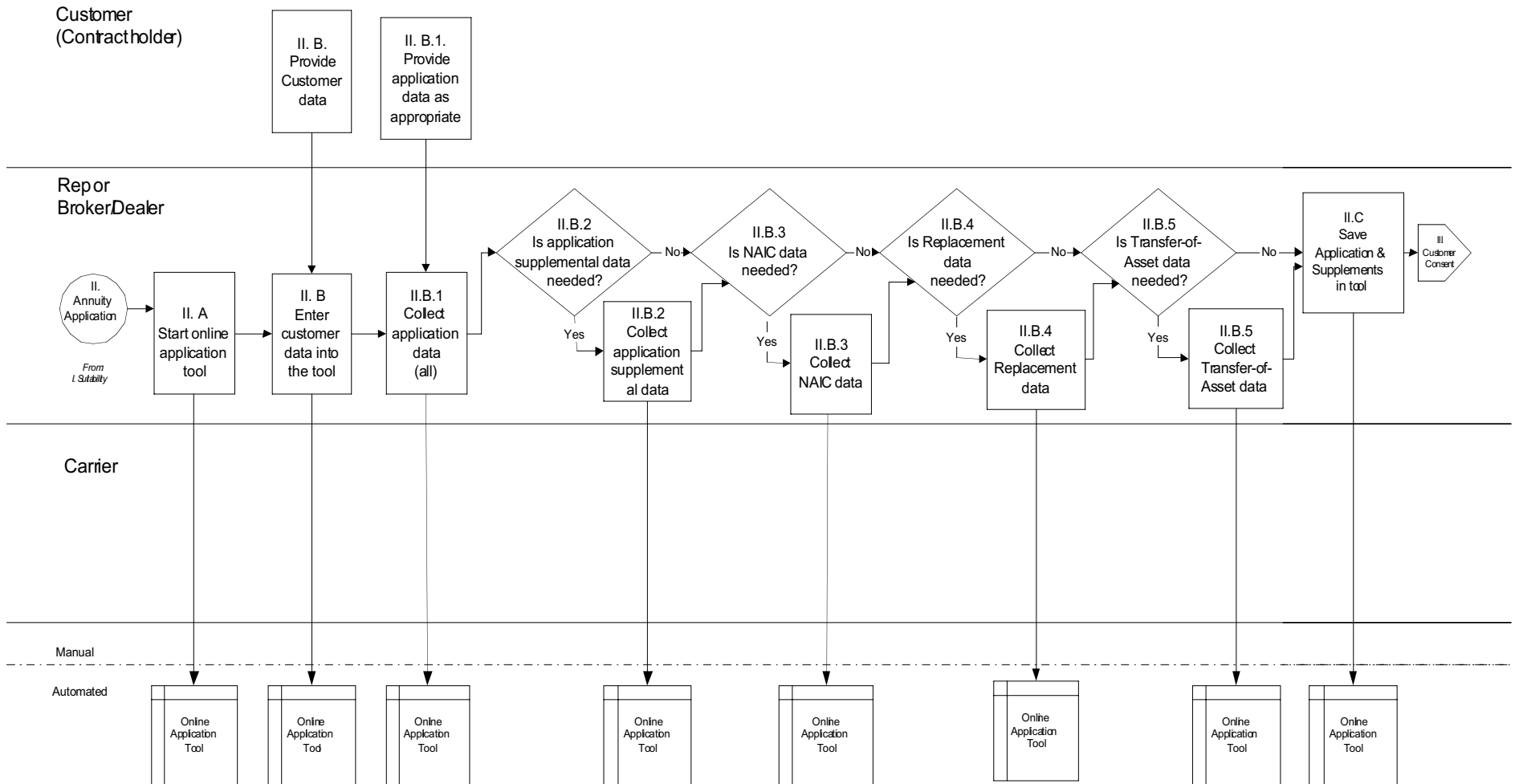
## eSignature: Operational Process Flows

ID	Action	Responsible Party	Remarks
	"apply signature" click		included in the application & supplements has been reviewed & authorized (bound/locked with hash-mark indicating approved). Key documents should include application/application acknowledgement, and if applicable: NAIC form, Replacement Form, Transfer of Asset Form.
**Note: should be opportunity to correct data if the need to do so is found in the review process. If correction is found after a document was signed, then revised data must be re-approved. If customer decides to opt out of the electronic signature document (does not wish to apply signature) then revert to the process described in declination of electronic consent.**			
V.	Application and Supplements Data Transmittal / Contract Issuance		
A.	Transmit Application and Supplements data	Distributor	Distributor/Carrier must have a previous agreement regarding the data format that will be used (like DTCC, NBFA, or proprietary). Distributor/Carrier must also have secured connectivity (like FTP with PGP encryption). The hash-mark should be associated with locked data streams within the transmission (ACORD's "attachment" object allows)
B.	Receive Application and Supplements data	Carrier	Carrier loads administrative system(s) with data received. Carrier should be able to re-render the form approved by applying the form template to the data received (forms themselves are not transmitted). Technology used for applying hash-mark at Distributor should also include a validation function that Carrier can use to prove data stream received has not been modified. <i>This may require same vendor deployment at Distributor and Carrier – unless there is a standard recognized by multiple vendors.</i>
C.	Store Application and Supplements data	Carrier	Carrier must store data stream as received from Distributor. Storage duration must match Carrier's interpretation of record retention rules for paper (i.e. 7 years).
D.	Establish contract according to Customer instructions	Carrier	Using data provided, contract should be established in Carrier's administrative system(s)... this should include any programs for which data is provided (items like DCA program, Portfolio Rebalancing, etc if applicable). If Replacement and Transfer of Asset documentation received with valid electronic approval, then Carrier should re-render applicable forms using data and indicating electronic approval in signature portion. This paper should be used in replacement processing until an electronic method for sharing the appropriate locked data streams is available between carriers. <i>This recommendation assumes Carriers would accept a paper-based process before electronic support is in place. If not supported, then replacement transactions cannot be electronically approved (must print and sign these documents, and mail to carrier)</i>
E.	Issue contract	Carrier	Upon receipt of data and money determined to be "in good order" by the Carrier, a contract package should be created for the Customer. This contract package should include the re-rendered forms of all documents electronically approved by the Customer, along with all other normal elements of a contract package (no change from paper-based contract package). Contract to be mailed using documented instructions between Carrier/Distributor. No change from paper-based process for contract delivery regulations (items like delivery receipt verifications, where required, still apply – as do 10 day free look requirements).
<b>Assumptions:</b>	Desire new business to be bound at solicitation.		

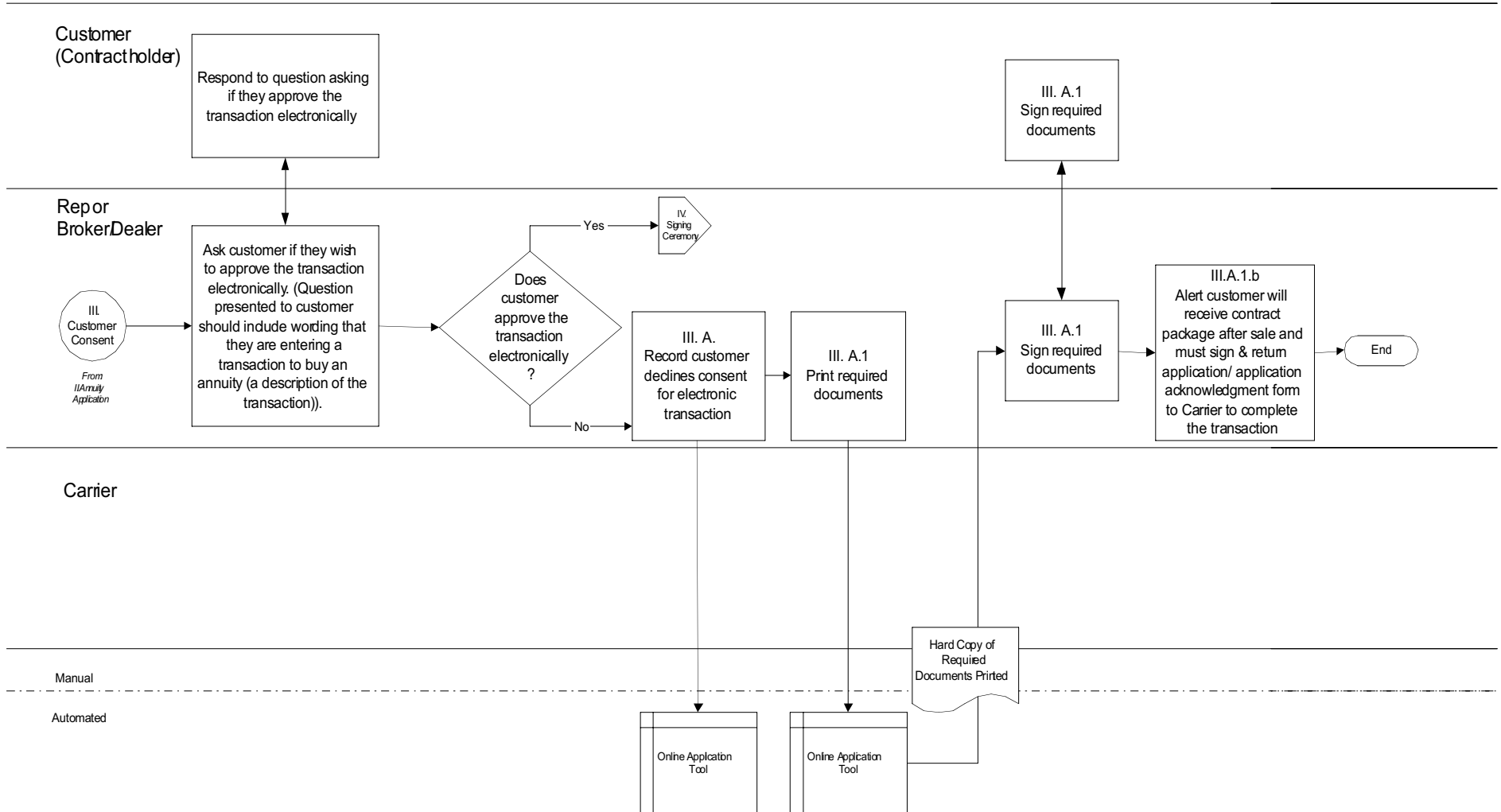
TIME: 



TIME:

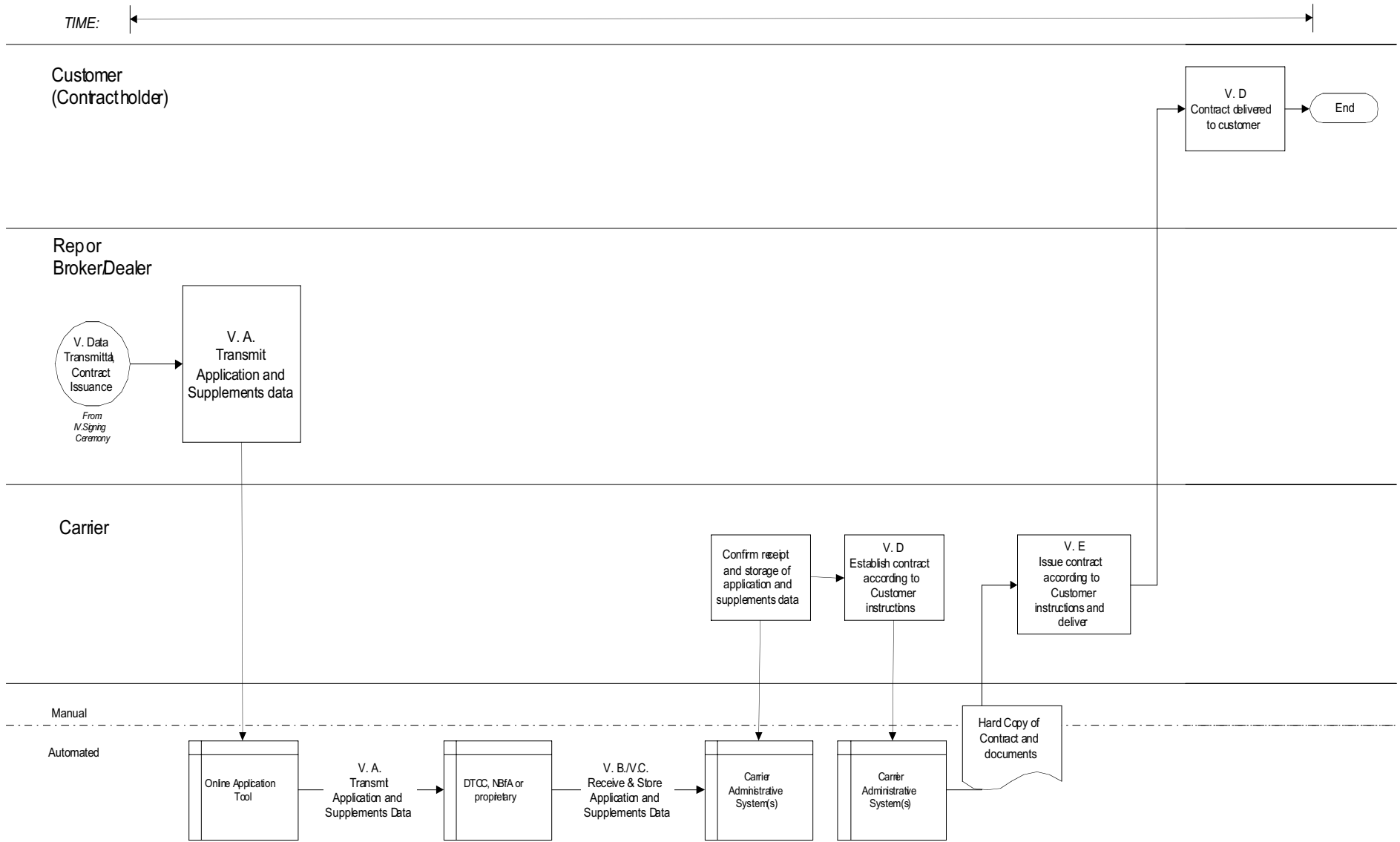


TIME: 





TIME: ←



## eSignature: Operational Process Flows

### Process Flow Example 2: Rep and customer on the phone

ID	Action	Responsible Party	Remarks
I.	Suitability Review / Purchase Decision		This section serves as an "Authentication" process for eSignature in this Operational Process Flow. Is likely broker/dealer and Customer have a previous relationship in which much of this activity would have been performed (using a face-to-face meeting).
A.	Identify Customer goals & risk tolerance	Distributor	
B.	Complete know-your-customer / customer identification program / suitability review	Distributor	
C.	Perform illustrations / comparisons as appropriate	Distributor	
D.	Decide on product, carrier, and investment amount	Distributor	
II.	Annuity Application		
A.	Start online application tool	Distributor	
B.	Enter Customer data into tool	Distributor	
1.	Collect Application data (all)	Distributor	Includes Beneficiary instructions, investment instructions, and party information. As well as how application will be funded.
2.	Collect Application Supplemental data (if applicable)	Distributor	Includes (any applicable): DCA instructions, Direct Deposit instructions, Durable Power of Attorney data, eDelivery Consent, Investment Options supplement, Portfolio Rebalancing request, Qualified Plan documentation, Qualified Plan: Market Conduct Questions/disclosures; and/or Telephone Authorization data
3.	Collect NAIC data (if applicable)	Distributor	Applicable in required states
4.	Collect Replacement data (if applicable)	Distributor	Applicable if a replacement
5.	Collect Transfer-of-Asset data (if applicable)	Distributor	Applicable if a replacement
C.	Save Application & Supplements in tool	Distributor	
III.	Customer Consent to Electronic Transaction		
A.	Record customer response regarding electronic approval of transaction	Distributor	Should ask the Customer if they wish to approve the transaction electronically. System should record presenting this question and the response. Question presented to Customer should include wording that they are entering a transaction to buy an annuity (a description of the transaction)
1.	If answer is "no"		
a.	Print and arrange for signature all required documents	Distributor	Required documents are those that must be signed at solicitation, if applicable – items like replacement & transfer-of-asset paperwork; NAIC forms; full application if New York.
b.	Alert customer will receive contract package after sale and must sign & return application/application acknowledgement form to Carrier to complete the transaction	Distributor	Unless New York, in which signature @ solicitation is required.
2.	Proceed with this flow if answer is "yes"	Distributor	Technology Requirement: customer must have online access to a Distributor site to review completed information. (Other potential option is a webex type presentation controlled by Distributor?)
B.	Select electronic signature method to be applied to transaction ... "click-wrap" or "voice"	Distributor	
1.	Describe click-wrap signature	Distributor	Involves setting Customer expectations on how the process will work, a verbal overview by the Distributor

## eSignature: Operational Process Flows

ID	Action	Responsible Party	Remarks
	process to Customer		is all that is expected. Comments along lines of ... that document will be presented, they'll review, identify and adjust if needed, then Customer will need to indicate they understand they are binding the transaction, will be asked to type their name, and then will be asked to apply this approval stamp to each form reviewed.
2.	Describe voice signature process to Customer	Distributor	Involves setting Customer expectations on how the process will work, a verbal overview by the Distributor is all that is expected. Comments along lines of ... that document will be presented, they'll review, identify and adjust if needed, then Customer "sign" by recording name, and indicating "I understand" that they are binding the transaction and "I approve" to actually approve execution of the document ... that this process will be repeated for all forms required by the transaction. <i>Minimum system requirements for voice must be shared and confirmation that customer system meets must be obtained before can proceed using this signature method.</i>
IV.	Signing Ceremony		
A.	Access saved Application and Supplements	Customer	Data should be presented in the tool via a clear and easy to understand format. An electronic display of the forms rendered from data entry is a good selection ... with the forms being reviewed and signed individually. Customer should have to enter an ID and PIN to access information, which re-Authenticates them for executing this transaction.
B.	Sign documents using Click-Wrap		
1.	Review Application/Application Acknowledgement	Customer	System should present instructions when form brought up that suggest Customer review key elements within the document. Could include specific elements to check, such as: product, carrier, purchase amount, funds, features/options, death benefit, and applicable state disclosure statement(s)
2.	Notice of intent to sign (to execute, an "I understand and agree" click required)	Customer	System presents a disclosure along the lines that you are about to sign this document. By signing you are binding this transaction for processing. Customer must click "I understand and agree" to move forward
3.	Obtain indicative questions responses from Customer	Distributor	This assists in the authentication that the person signing is the customer. Examples of indicative questions could be mother's maiden name, childhood pet, etc. At least 2 indicative responses should be gathered.
4.	Obtain Customer signature (type name)	Customer	Customer is asked to type name, instructions alert customer that by typing name and then applying to documents they are signing documents
5.	Apply signature to current document (to execute, an "apply signature" click required). Validate signature applied correctly.	Customer	Present Customer with question if they wish to apply signature to the current document. This action associates the signature with the record. Customer clicks "apply signature" and the system must bind/lock data – no subsequent changes allowed unless customer re-applies signature. Data that can be rendered into the form reviewed is usually locked with a hash-mark applied behind the scenes that indicates it was signed. This hash mark is what is invalidated if subsequent data changes are made. Should validate signature applied correctly.
6.	Review next document (if any) and repeat the "apply signature" click	Customer	Individual documents presented with signature applied similar to how process would work with "wet" signature process. This step repeats until key data included in the application & supplements has been reviewed & authorized (bound/locked with hash-mark indicating approved). Key documents should include application/application acknowledgement, and if applicable: NAIC form, Replacement Form, Transfer of Asset Form.

## eSignature: Operational Process Flows

ID	Action	Responsible Party	Remarks
<p><b>**Note:</b> should be opportunity to correct data if the need to do so is found in the review process. If correction is found after a document was signed, then revised data must be re-approved. If customer decides to opt out of the electronic signature document (does not wish to apply signature) then revert to the process described in declination of electronic consent.**</p>			
Or D.	Sign documents using Voice		
1.	Review Application/Application Acknowledgement	Customer	System should present instructions when form brought up that suggest Customer review key elements within the document. Could include specific elements to check, such as: product, carrier, purchase amount, funds, features/options, death benefit, and applicable state disclosure statement(s)
2.	Obtain Customer signature (record name). Validate signature recording.	Customer	Customer is asked to record name, likely have to speak name twice into a microphone built into their PC that will establish the voice pattern that becomes their hash-mark signature in documents. Assure voice recorded correctly (requires play-back functionality to check that voice can be heard).
3.	Apply signature to current document (to execute, person must speak name, respond "I understand" to statement about this being an electronic signature, and respond "I approve" to statement about what being approved).	Customer	This action associates the signature with the record. The recording of spoken name, I understand, and I approve "applies signature" and the system must bind/lock data – no subsequent changes allowed unless customer re-applies signature. Data that can be rendered into the form reviewed is usually locked with a hash-mark applied behind the scenes that indicates it was signed. This hash-mark is what is invalidated if subsequent data changes are made.
4.	Review next document (if any) and repeat the "apply signature" process	Customer	Individual documents presented with signature applied similar to how process would work with "wet" signature process (record name, I understand, and I approve on each document). This step repeats until key data included in the application & supplements has been reviewed & authorized (bound/locked with hash-mark indicating approved). Key documents should include application/application acknowledgement, and if applicable: NAIC form, Replacement Form, Transfer of Asset Form.
<p><b>**Note:</b> should be opportunity to correct data if the need to do so is found in the review process. If correction is found after a document was signed, then revised data must be re-approved. If customer decides to opt out of the electronic signature document (does not wish to apply signature) then revert to the process described in declination of electronic consent.**</p>			
V.	Application and Supplements Data Transmittal / Contract Issuance		
A.	Transmit Application and Supplements data	Distributor	Distributor/Carrier must have a previous agreement regarding the data format that will be used (like DTCC, NBFA, or proprietary). Distributor/Carrier must also have secured connectivity (like FTP with PGP encryption). The hash-mark should be associated with data streams within the transmission (ACORD's "attachment" object allows)
B.	Receive Application and Supplements data	Carrier	Carrier loads administrative system(s) with data received. Carrier should be able to re-render the form approved by applying the form template to the data received (forms themselves are not transmitted). Technology used for applying hash-mark at Distributor should also include a validation function that Carrier can use to prove data stream received has not been modified. <i>This may require same vendor deployment at Distributor and Carrier – unless there is a standard recognized by multiple vendors.</i>
C.	Store Application and Supplements data	Carrier	Carrier must store data stream as received from Distributor. Storage duration must match Carrier's interpretation of record retention rules for paper (i.e. 7 years).
D.	Establish contract according to Customer instructions	Carrier	Using data provided, contract should be established in Carrier's administrative system(s)... this should include any programs for which data is provided (items like DCA program, Portfolio Rebalancing, etc if applicable). If Replacement and Transfer of Asset documentation received with valid electronic approval, then Carrier should re-render applicable forms using data and indicating electronic approval in signature

**eSignature: Operational Process Flows**

ID	Action	Responsible Party	Remarks
			<p>portion. This paper should be used in replacement processing until an electronic method for sharing the appropriate locked data streams is available between carriers. <i>This recommendation assumes Carriers would accept a paper-based process before electronic support is in place. If not supported, then replacement transactions cannot be electronically approved (must print and sign these documents, and mail to carrier)</i></p>
E.	Issue contract	Carrier	<p>Upon receipt of data and money determined to be "in good order" by the Carrier, a contract package should be created for the Customer. This contract package should include the re-rendered forms of all documents electronically approved by the Customer, along with all other normal elements of a contract package (no change from paper-based contract package).                      Contract to be mailed using documented instructions between Carrier/Distributor. No change from paper-based process for contract delivery regulations (things like delivery receipt verifications, where required, still apply – as do 10 day free look requirements).</p>
<b>Assumptions:</b>	Desire new business to be bound at solicitation.		

*Draft*

## **Appendix D**

Results of Decision Criteria Survey

## Decision Criteria-Survey E-Signature Tools

Submitted by firm name: \_\_\_\_\_

#	Category	Definitions	Score	Clickwrap	Digital Signature	PKI	Biometric: Voice	Biometric: Handwriting	Biometric: Fingerprints
1	<b>Ease of Doing Business- Enhances Customer Experience</b>								
A		Enables VA market to grow substantially as easier to sell/easier for clients to deal with complicated product	20						
B		Keeps VA market from shrinking due to lack of customer ease of doing business	10						
C		Is easier- but no tie to VA market share of wallet	5						
D		Not sure it is easier	-5						
E		Is somewhat harder to do business for agent/end consumer for some scenarios	-10						
	<b>Comments on Category #1</b>	Fingerprints feel invasive- clients may not like to give them. Question on all: would the technology be used at set up of initial account at b/d or of a brokerage account or only at sale of initial annuity? Would make a difference on ease of use for PKI, handwriting and voice.							
2	<b>Ease of Business- Enhances Ease of Operations/ Shareholder Return</b>								
A		Because ease/efficiency- offers very positive IRR within 18 months of wide/broad adoption. Substantial opportunities for process redesign.	10						

## Decision Criteria-Survey E-Signature Tools

Submitted by firm name: \_\_\_\_\_

#	Category	Definitions	Score	Clickwrap	Digital Signature	PKI	Biometric: Voice	Biometric: Handwriting	Biometric: Fingerprints
B		Because ease/efficiency- is neutral to marginally positive IRR offsetting costs. Some opportunities for process redesign	5						
C		Ease of Doing Business is enhanced for Distributor/Manufacturer- however, IRR is not a positive factor overall /long time horizon to recoup initial costs (due to costs of purchase/maintenance/slow adoption)	3						
D		Not sure it is easier to operate overall- think it may also have a negative return	-5						
	<b>Comments on Category #2</b>	<p>Voice- some concerns that the methods of retrieval/verification for back office/manufacturer might be cumbersome.</p> <p>Signature pad/fingerprint- requires equipment at Point of Sale</p> <p>Click wrap has substantial opportunities for process redesign</p>							
<b>3</b>	<b>Leveragable Solution</b>								
A		Solution is fully leveragable for all types of e-signature business/processes- one solution will fit all processes. Set the stage for future business opportunities	10						
B		Solution is excellent for some types of highest volume/highest priority e-signature needs, and "ok" for others. Sets the stage for some future opportunities.	5						

## Decision Criteria-Survey E-Signature Tools

Submitted by firm name: \_\_\_\_\_

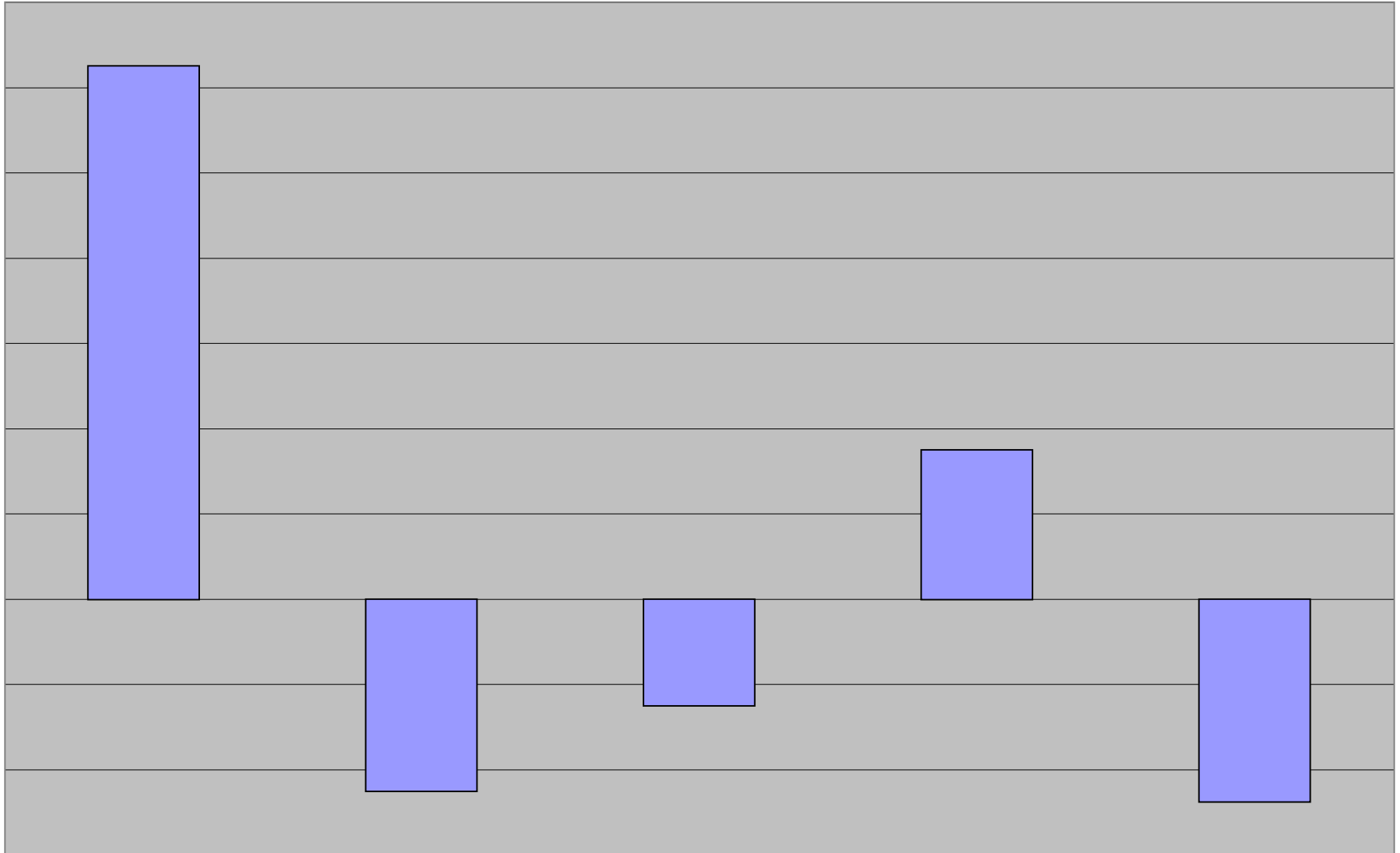
#	Category	Definitions	Score	Clickwrap	Digital Signature	PKI	Biometric: Voice	Biometric: Handwriting	Biometric: Fingerprints
C		Solution meets some needs very well- but not right solution for others. Will need multiple platforms/technologies to be fully "e-signature" enabled for all processes.	3						
D		Solution meets one need only- every major process needs different technology	-5						
	<b>Comments on Category #3</b>	Fingerprints & signatures- won't work from home for consumers.							
<b>4</b>	<b>Business Risk</b>								
A		Does not increase business risk over current processes- may decrease some	20						
B		Some risks go up, some risks go down- overall even risk profile	10						
C		Small increase in business risk overall- but mitigation strategies are achievable without undue burden	5						
D		Business Risks increase and mitigation strategies do not/only partially mitigate	-5						
	<b>Comments on Category #4</b>	Click wrap- concerns about agent behavior. Could mitigate by b/d agreements, supervision, audits- but still a concern.  All forms eliminate the risk of not getting signatures in some of our "app later" processes.							

## Decision Criteria-Survey E-Signature Tools

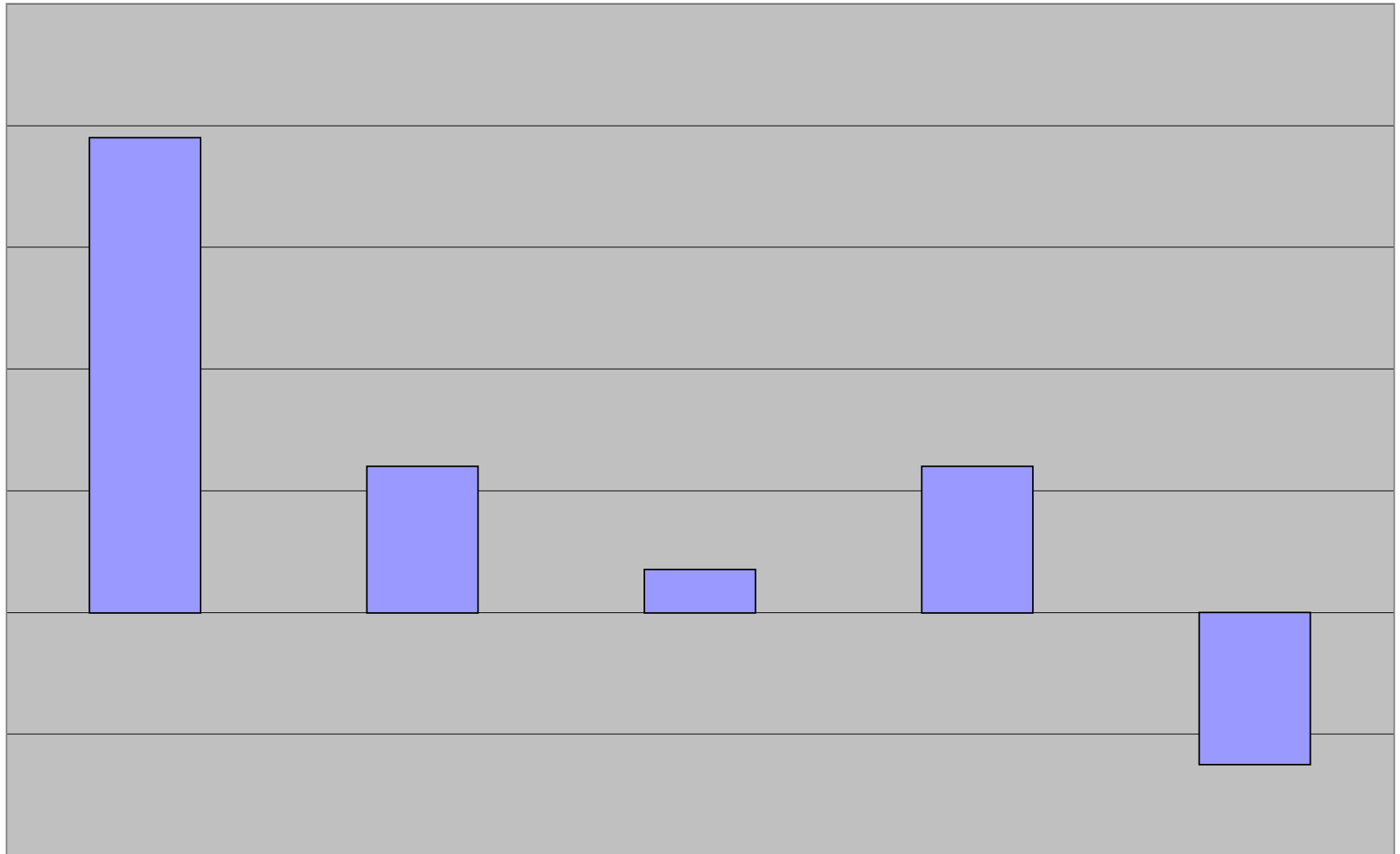
Submitted by firm name: \_\_\_\_\_

#	Category	Definitions	Score	Clickwrap	Digital Signature	PKI	Biometric: Voice	Biometric: Handwriting	Biometric: Fingerprints
5	<b>Sustainability/Life Cycle Expectations</b>								
A		Technology is know commodity (not “blue sky”) , technology will not be “throw away” for at least 10 years, possibilities for pricing to go down is there, need to do substantial infrastructure upgrades very often is minimal	10						
B		Technology is know commodity (not “blue sky”) , technology will not be “throw away” for at least 10 years, Not sure about: possibilities for pricing to go down is there, and how often/how burdensome infrastructure upgrades may be	5						
C		Technology is rapidly changing, possibility of multiple upgrades in next 5-7 years, not sure how expensive/burdensome keeping up with the evolving technology will be. Possibility of some throwaway as adoption grows.	3						
	<b>Comments on Category #5</b>	Not sure how corporations and consumers’ perceptions of security will affect how the tech will need to change. As identify theft becomes even more of a concern- will things like “click wrap” be seen as too risky & need completely overhauled?							

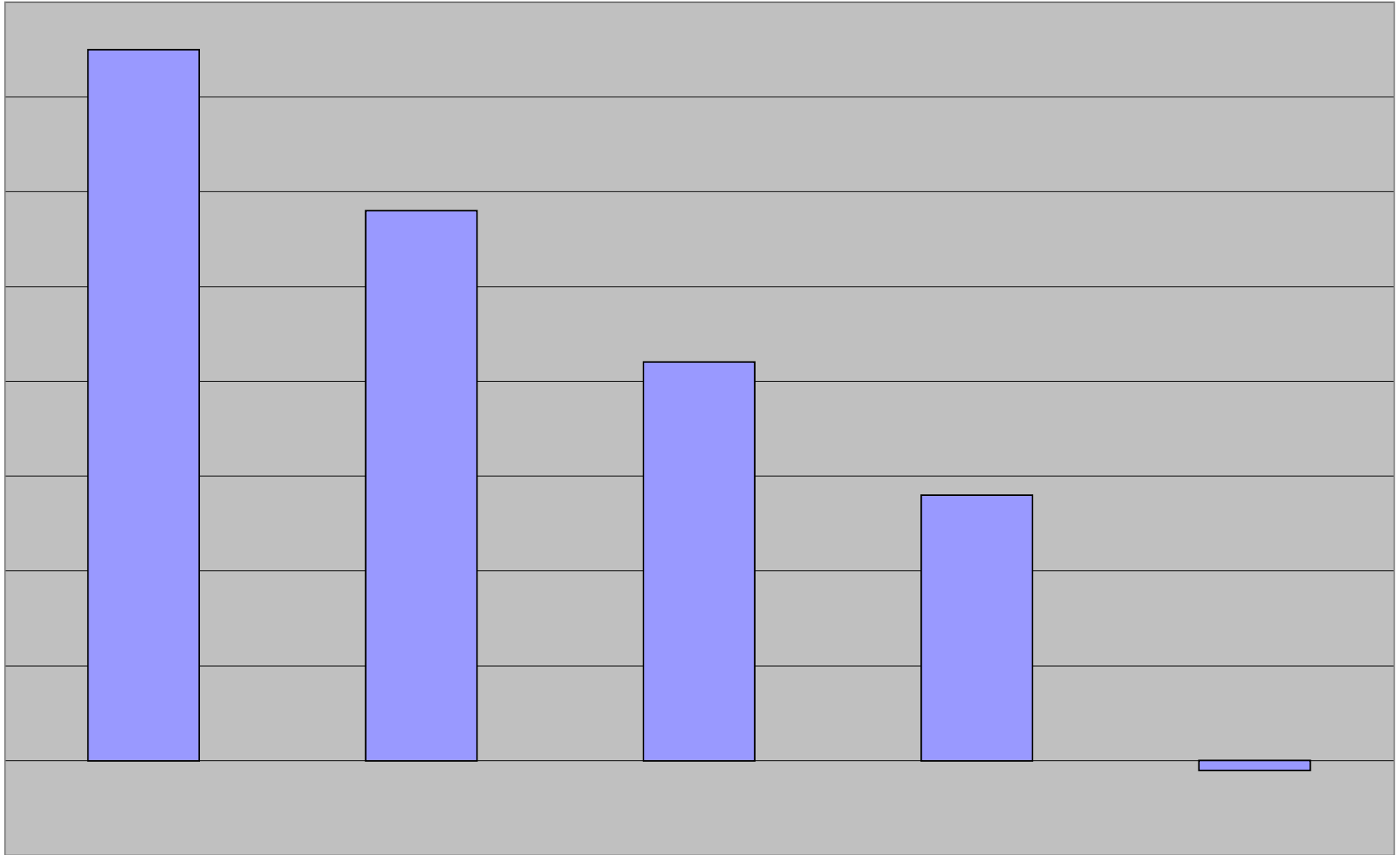
**Cat. #1 - Ease of Doing Business - Enhances Customer Experience**



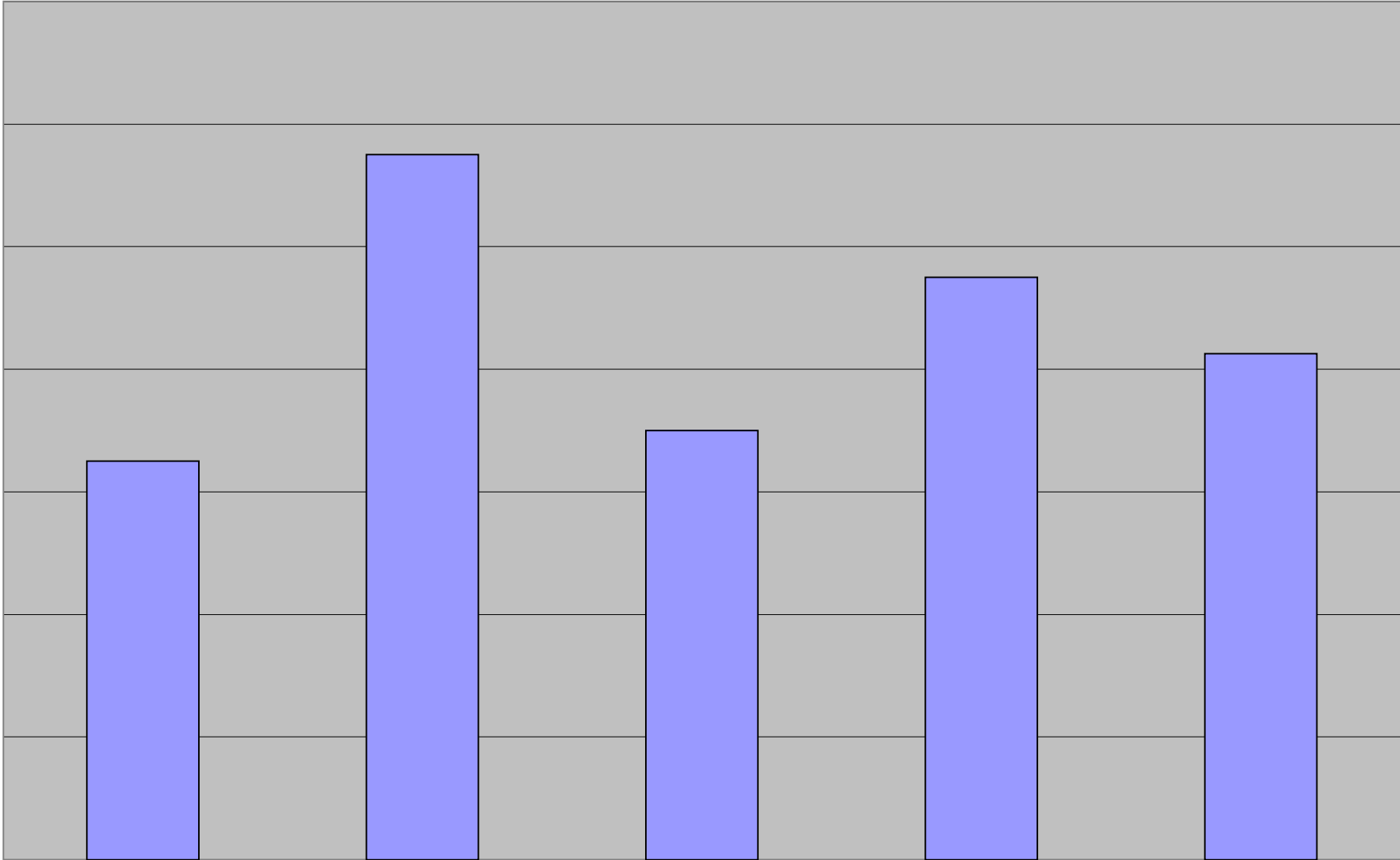
**Cat. #2 - Ease of Business - Ease of Operations/Shareholder Return**



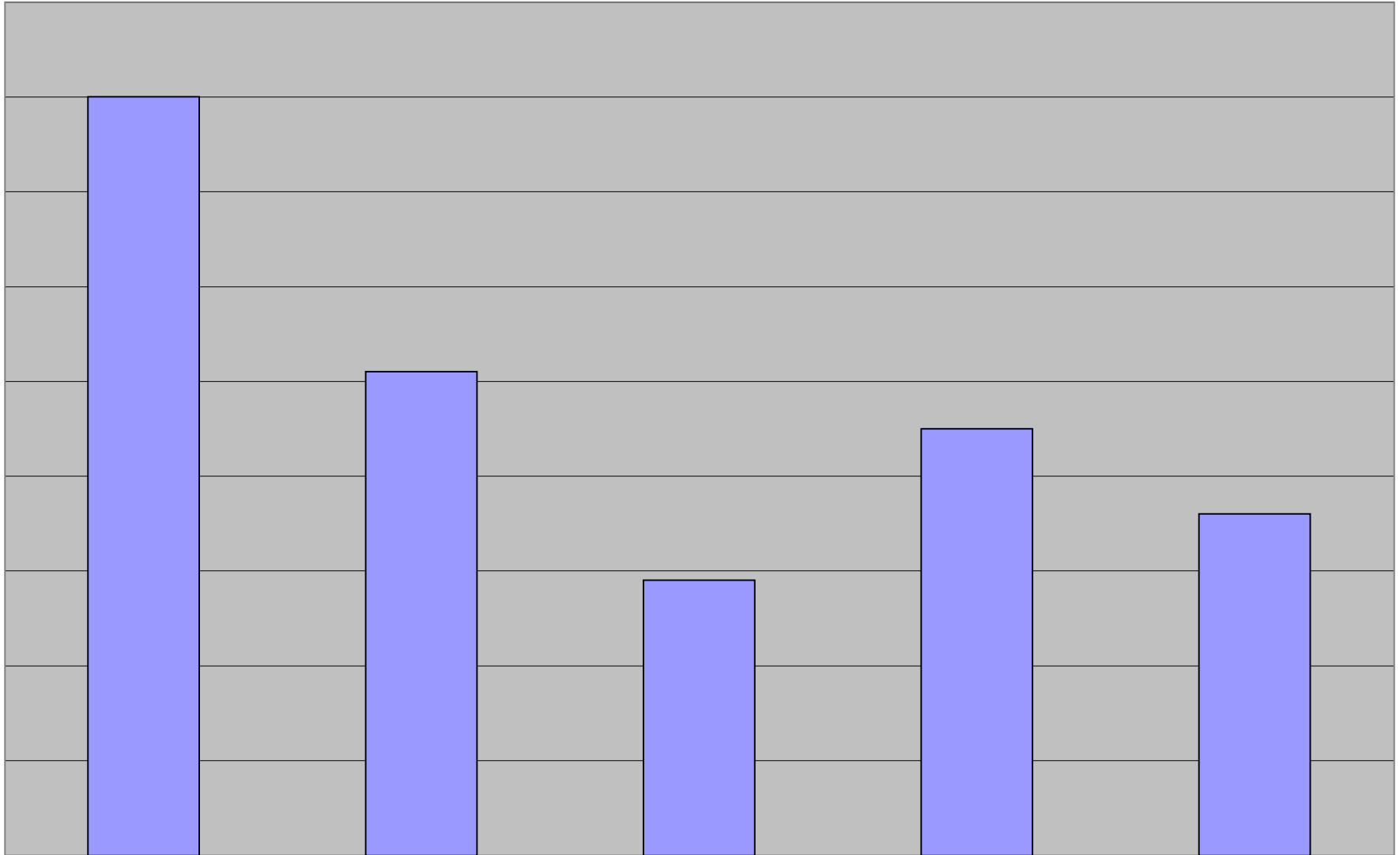
### Cat. #3 - Leveragable Solution



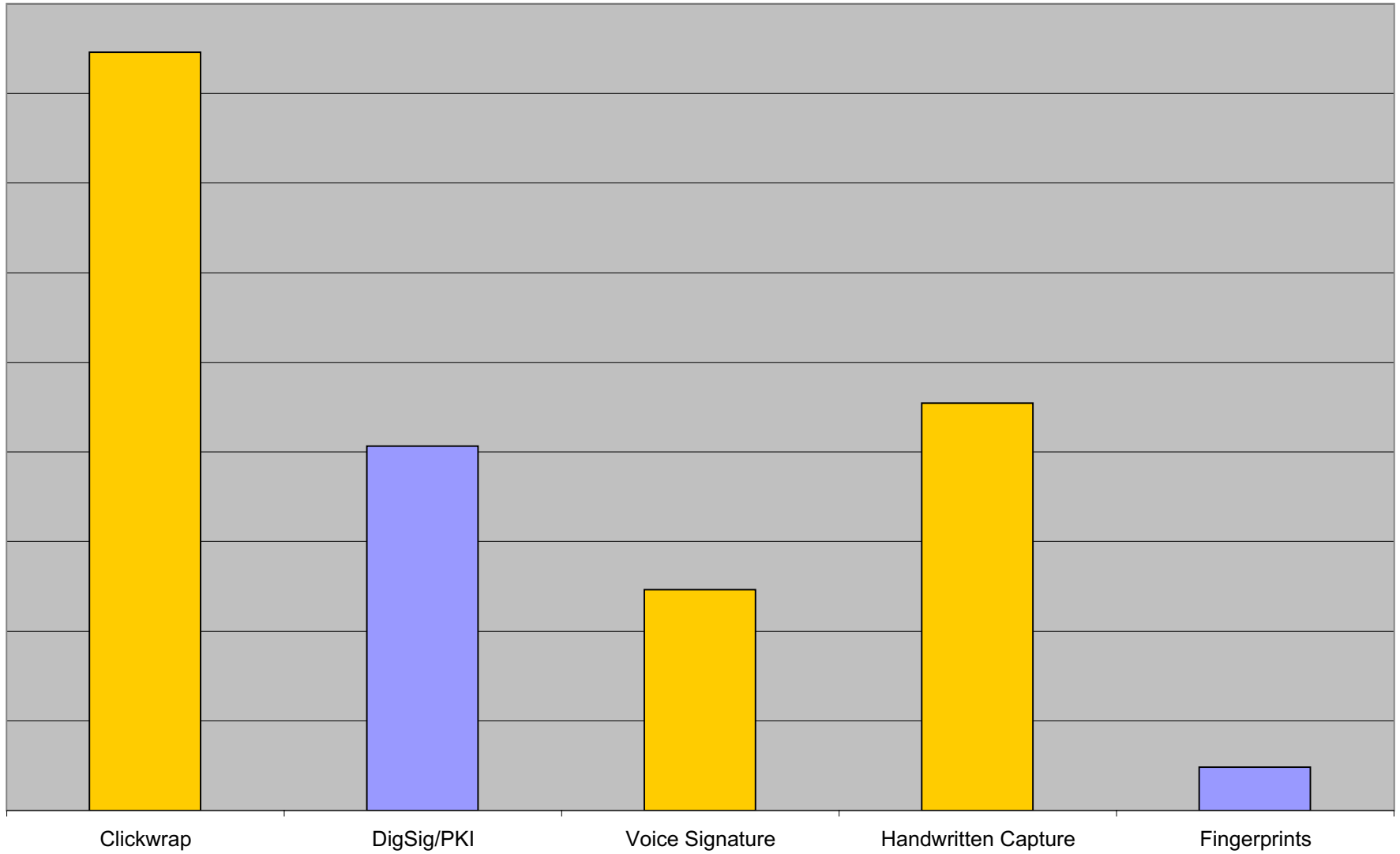
**Cat. #4 - Business Risk**



**Cat. #5 - Sustainability/Life Cycle Expectations**



### Cumulative Ranking



## Comments

### Category #1

#### Ease of doing business - Enhances customer experience

PKI - Producers buying into issuing certificates? ID verification does match new process reqts.

Voice - Registering voice may prove difficult;

Handwriting - Required hardware for distributors that they may not want. NOTE: general perception that due to store usage this would be most commonly accepted by end customers

fingerprint - Feel too invasive for serious consideration

PKI - I think the common person is yet to adopt this, it needs to be made easier

Voice - I am not sure how this will work, is there technology available?

Handwriting - Hard to implement in when the distribution is not in-house

Fingerprints feel invasive- clients may not like to give them.

Question on all: would the technology be used at set up of initial account at b/d or of a brokerage account or only at sale of initial annuity? Would make a difference on ease of use for PKI, handwriting and voice.

Handwriting functionality is becoming so common that it should be easily accepted by all users. The more technical solutions may scare off broker and clients that uncomfortable with technology.

NOTE: not sure current workflows will really gain b/d support since all involve signature at solicitation and seems majority of current ENB implementations involve data-entry AFTER customer sale has been made (by broker assistant or back-office). Believe we do need to consider applying technology to enhance the "signature-later" process since the sales process will not immediately change

"Ease" factor doesn't apply to self-directed customers

Would we verify (for clickwrap) via email address that the client is the one who is making the transaction?

### Category #2

#### Ease of business - Ease of Operations/Shareholder Return

PKI-another password may not be the most user friendly way since everyone is inundated with passwords to remember.

PKI-ROI is not justifiable and technology firms charge way too much to implement this

Voice - I need more information on this one

Voice- some concerns that the methods of retrieval/verification for back office/manufacture might be cumbersome.

Signature pad/fingerprints- requires equipment at Point of Sale

Click wrap has substantial opportunities for process redesign

### Category #3

#### Leveragable Solution

Believe majority of other transactions wish to apply eSign to are customer-initiated (only on custodial biz is broker usually involved). Thereby must have a process that doesn't require b/d. NOTE: currently use a one-time click wrap at internet profile setup that allows customer to process transactions with us directly!

Clickwrap and PKI seem the most versatile – other seem like they would be used for on the spot transactions they would also be good for setups and post transactions.

Fingerprints & signatures- won't work from home for consumers.

### Category #4

#### Business Risk

Concern how "prove" customer is one who clicked (if can make process DOI will support)

Fingerprints & Voice may be almost full proof for verification of client. The others appear to have similar risks to accepting signed applications and EDI transmissions.

PKI - States like New York still require wet signature, what about 1035 exchanges and REG 60 in NY they need wet signatures

Click wrap- concerns about agent behavior. Could mitigate by b/d agreements, supervision, audits- but still a concern.

All forms eliminate the risk of not getting signatures in some of our "app later" processes.

### Category #5

#### Sustainability/Life Cycle Expectations

## Comments

The largest risk for any of these choices is that technology is evolving and we never know what may be coming that would be a better choice.

PKI - I am hoping the next generation of agents will adopt more technology. We have agents who don't use computers at all

Not sure how corporations and consumers' perceptions of security will affect how the tech will need to change. As identify theft becomes even more of a concern- will things like "click wrap" be seen as too risky & need completely overhauled?

*Draft*

**Appendix E**

SPeRS Summary

## **Summary of SPeRS Guidelines still in draft form**

### **I. AUTHENTICATION**

#### **I-1. Selecting an Authentication Process for Establishing a Relationship**

The system design team should determine the appropriate authentication process for establishing a relationship with each party to a transaction. The assessment and selection process should include:

- Assessing the legal liability and transaction risk associated with failing to correctly identify the transaction party,
- Assessing the practical and system considerations that may affect the choice of an authentication process,
- Determining whether the authentication process for the transaction must comply with specific legal or regulatory requirements,
- Selecting an authentication strategy that provides an appropriate level of security and certainty, based on the preceding considerations, and
- Determining what information will be required in order to implement the selected authentication strategy.

When evaluating and selecting potential authentication strategies for a new consumer, the system design team should consider the type of transactions the consumer will be allowed to take once authentication is completed. For instance, the team should consider if the consumer will engage in multiple transactions or will just a single one be associated with the new relationship? If it is anticipated that there could be multiple transactions, the team should consider if a credential would be issued to the consumer.

The design team should also consider the type of information to which the consumer will have access. For instance, will the consumer have access to confidential information only about himself/herself or will the consumer also have access to confidential information about other parties to the transaction (in a multiple transaction scenario).

The design team should also consider if the electronic transaction is susceptible to identity fraud and to what extent. According to the SPeRS document, securities are in a category that has a higher risk of authentication fraud than other categories. The factors likely to lessen the likelihood of attempted authentication fraud include if the transaction is involves delivery of goods to a specific address known to match the transaction party.

The team should also consider whether the information that will need to be collected from the consumer in order to process the transaction would also be enough or appropriate to complete the authentication process.

Also the team should consider whether there are any laws or regulations applicable to the transaction that need to be taken into account when designing the authentication process. Some of the laws and regulations that need to be considered in the annuity context include the USA Patriot Act, the Gramm-Leach-Bliley Act privacy provisions, and the

Insurance Information and Privacy Protection Act (enacted by some states). There are also practical considerations that may impact the selection of an authentication process such as, the cost of designing and implementing the authentication process and the cost of applying the authentication process to the creation of each relationship.

When evaluating and selecting potential methods for authenticating a consumer when creating a new relationship, the system design team should consider whether relationships would be created remotely, as part of a consumer-to-representative transaction, or both.

The SPeRS draft encourages the design team to apply one or more of five authenticating strategies when choosing an authentication method. These five strategies include:

1. Self Authentication: consumer states his/her name
2. Logical Authentication: consumer's phone number area code matches address  
*Team should consider: Whether the use of logical authentication provides meaningful authentication information in the context of the transaction.*
3. Negative Authentication: Transaction Participant checks consumer's information for history of fraud or identity theft.  
*Team should consider: Whether there is sufficient information available, either from the operator of the system or from a 3<sup>rd</sup> party source to provide reliable predictive value.*
4. Positive Authentication: Transaction Participant matches information provided by the consumer on a trusted 3<sup>rd</sup> party source of information (consumer's SS# matches # on credit report)  
*Team should consider: Availability of pre-packaged authentication services from 3<sup>rd</sup> party vendors; the likelihood that the database will contain stale or inaccurate data that will produce false alarms; and whether the consumer's consent is necessary to access the available authentication data.*
5. Third Party Authentication: identity of the consumer is confirmed by a trusted 3<sup>rd</sup> party source. (Consumer's ID confirmed by a digital certificate or 3<sup>rd</sup> party company, like Equifax.)  
*Team should consider: steps taken by 3<sup>rd</sup> party to authenticate the consumer; quality of information sources used by 3<sup>rd</sup> party to validate information provided by consumer; the controls and monitoring process used by the 3<sup>rd</sup> party; if the 3<sup>rd</sup> party will outsource some or most of the work; and the extent to which the 3<sup>rd</sup> party will be providing insurance or indemnification in the event of an improper authentication is made.*

Once the design team has selected the authentication strategy(ies), it should next select a specific method to implement it. In order to determine which option is appropriate, the design team may need to review additional factors. For instance, with the positive authentication, the Transaction Participant will need to consider whether the consumer's

consent is necessary to access the available authentication data or the likelihood that the database will contain inaccurate data that would produce false reports.

The SPeRS draft does not feel that one option is better than another. The effectiveness of any one of these options or a combination of them will depend on the implementation, surrounding circumstances, and appropriateness to the circumstances surrounding the relationship. Note that any of these strategies may be implemented either remotely, as part of an online transaction, or as part of a consumer-to-representative transaction.

**There is also a section that provides examples of application of authentication strategies to specific relationships.**

**There is also a chart that explains and compares the methodologies, strengths, weaknesses and suitability of each of the five authentication options discussed above.**

### **I-2. Selecting Credentials for Authentication**

The system design team should determine the appropriate credential for a party conducting a transaction as part of an established relationship. The process for selecting a credential should include:

- Assessing the risks associated with unauthorized access to conduct the transaction,
- Determining whether there are specific legal or regulatory requirements for a credential associated with the transaction;
- Determining the types of credentials appropriate to the transaction based on the risk assessment and any applicable legal or regulatory requirements,
- Determining the cost of establishing and using a particular credential,
- Assessing the relative speed with which the credential may be established and used,
- Assessing any specific hardware or software requirements to use a particular credential and whether such requirements are appropriate to the transaction, and
- Evaluating the information that needs to be obtained from, and provided to, the transaction party to implement and maintain a particular credential.

A credential in the electronic signature world functions much like a government-issued ID, which substitutes for continually re-proving identity. A credential that is too easy to mimic or steal poses a greater risk of fraud than one that isn't. Alternatively, a credential that is too difficult to remember or burdensome in some other way, may prevent the consumer from going forward with the transaction.

When evaluating and selecting potential credentials, the design team should consider a variety of factors. For instance, the team should consider the type of actions that the consumer will be authorized to enter once authentication is completed. The team should also consider the number of transactions permitted, the potential value of each transaction

or the aggregate number of transactions, and whether there will be some types of limits on the consumer's authority.

Additionally, the types of information the consumer will have access to when using the credential should also be evaluated. (confidential information about the consumer vs. confidential information about other parties).

We should also consider the likelihood of fraudulent activity and if the particular credential selected is sufficiently secure to prevent unauthorized use if properly secure and not so complex to use.

The process for selecting a credential must ensure that the type of credential will balance the cost of designing and implementing the credential, the complexity of using the credential and the risks associated with unauthorized use of the credential.

There are 3 basic elements of a credential:

- 1) something the consumer **knows**,
- 2) something the consumer **possess** or
- 3) something the user **is**.

A credential may consist of just one category, or it can be more than one. The use of more than one is more secure but also more complicated to use.

### **I-3. Providing Information Concerning The Risk of Unauthorized Transactions**

Where appropriate in consumer transactions, the system design team should consider providing a transaction participant with an opportunity to obtain information concerning the risks associated with unauthorized transactions, including:

- The consumer's responsibilities with respect to protecting credentials,
- The potential consequences of unauthorized use of credentials, and
- The procedure for giving notice that a credential has been stolen or compromised.

Such information should make the consumer aware of his/her responsibilities with respect to protecting credentials. It should also make the consumer aware of the potential consequences of unauthorized use of credential and the procedures for giving that a credential has been stolen or comprised.

The need to provide this information will vary considerably depending on the circumstances. For example, in a consumer-to-representative transaction, these issues will usually be addressed in an initial agreement between the parties establishing the relationship, and there will be no reason to repeat the information as part of an electronic transaction. (i.e. When creating a relationship where multiple future transactions are anticipated.)

#### **I-4. Establishing Representative Authority**

Where appropriate, the system design team should consult with legal or compliance personnel to determine whether it is likely that individuals will be representing transaction participants (either individuals or legal entities such as corporations or trusts) other than themselves, and if so:

- Determine whether it is advisable to obtain some representation or evidence of the individual's authority to act as a representative, and
- Establish appropriate methods for obtaining representations or evidence of the representative's authority.

In cases where an individual is acting in a transaction on behalf of another party, the design team should have procedures in place to ensure the individual is authorized to enter the transaction he is engaging. If the representative does not have authority, then the transaction, or some part of it, may not be enforceable against the unauthorized representative.

Various methods are used to establish a representative's authority. The design team should consider the type of transaction and the amount of risk involved in choosing a method.

Additionally, the team should also evaluate whether the relationship will be created remotely or at the branch with a representative, or both.

## **II. AGREEMENT AND CONSENT TO TRANSACT TRANSACTION PARTICIPANT ELECTRONICALLY**

### **II-1 General Agreement to Transact Business Electronically**

Systems should be designed to obtain either:

- The Transaction Parties' express agreement to use electronic records and signatures; or
- The Transaction Parties' implied agreement in a fashion that allows a reasonable inference that Transaction Parties have assented to use electronic records and signatures.

Express agreement may be established by either:

1. presenting the Transaction Party with a pre-transaction notice that electronic records and signatures will be used in the transaction instead of paper documents and handwritten signatures; or
2. obtaining the Transaction party's signature, whether written or electronic, which approves the use of electronic records and signatures instead of paper documents and handwritten signatures.

A pre-transaction notice for obtaining an express agreement or a signed express agreement should include a description of the transaction(s) covered by the agreement and be made available for printing, downloading or retention by Transaction Parties either at the time of review or at a later time in accordance with record retention rules.

## **II-2 Applicability of the ESIGN Consumer Consent Process**

With respect to business to-Consumer Transactions, the system design team should consult with legal counsel or a compliance officer concerning application of the ESIGN Consumer Consent Process. The ESIGN Consumer Consent Process should be used if:

- The Consent Process is required by any rule of law, or
- The system design team determines that its voluntary use would be beneficial and its use will not hamper, confuse or unduly complicate the Transaction.

SPeRS distinguishes between two types of information: information businesses are legally required to provide the customer in writing (“Required Consumer Information”) and information not required to be provided to a consumer in writing. If a business delivers or provides electronically records that it must make available to customers in writing, then according to ESIGN, it must obtain the consumer’s affirmative consent.

When a business electronically delivers information required to be provided in writing to the consumer, the Consumer Consent Process should require the following:

- delivery of a series of required consent disclosures prior to obtaining the consumer’s affirmative consent, covering a variety of issues, such as scope, and equipment needed to participate.
- The business should also obtain either electronic affirmative consent or electronic confirmation of affirmative consent from the consumer.
- It should be provided either as part of obtaining the consumer’s consent or thereafter, a reasonable demonstration of the consumer’s ability to receive electronic records.
- Meet statutory retention requirements.

The ESIGN Consumer Consent Process applies to federal laws, and to the laws of any state that has either incorporated the ESIGN rules into their version of the UETA or has not yet adopted UETA at all. This being the case, any multi-state implementation of a Consumer Transaction using electronic records and signatures is likely to run up against the ESIGN Consumer Consent requirements, unless it either does not involve:

- 1) any written disclosure or notice requirement
- 2) any federal written notice or disclosure requirement can be governed solely by the law of a state that has adopted UETA without incorporating the ESIGN Consumer Consent Process by reference.

## **II-3 The ESIGN Consumer Consent Disclosures.**

When the system design team has determined that the ESIGN Consumer Consent Process should be employed, it should implement the Consent Process:

- In compliance with the requirements of the ESIGN Consumer Consent Disclosures; and
- With the goal of providing the Consumer with information designed to assist the Consumer in making an informed choice with respect to the use of electronic records and signatures.

There are specific disclosures that must be made in order to comply with E-SIGN Consumer Consent Process.

Several issues arising from consent disclosures that should be considered when an online program is developed, including:

- Consumer's right or option to have the Required Consumer Information provided or made available in paper form
- Procedures the consumer must use to withdraw consent
- Procedures the consumer must use to update information needed to the contact the consumer
- Hardware and software requirements for access to and retention of the Required Consumer Information.
- Multiparty consents

#### **II-4. The E-SIGN Consumer Consent Disclosures –Format and Timing**

When presenting the E-SIGN Consumer consent disclosures to the consumer, they must be provided:

- in a clear and conspicuous format,
- during a meaningful part of the transaction and
- prior to the consumer providing his or her affirmative consent.

SPeRS advises to set the consumer's expectation for the transaction as early as possible by giving the consumer notice of key information and a link to the consent disclosures for early review. (i.e. inform consumers they must have email address or certain hardware/software in order to participate electronically)

#### **II-5. Obtaining the Consumer's Affirmative Consent – Methods and Timing**

When employing the Consumer Consent Process systems will need to be designed to obtain the Consumer's affirmative consent to access Required Consumer Information. Providers should obtain the Consumer's affirmative consent either:

- Prior to, or at the time Required Consumer Information is presented, or
- After Required Consumer Information is presented but before the time when the Consumer becomes obligated on the Transaction.

The consumer consent process is not complete until:

- 1) the consent disclosures have provided
- 2) the consumer has provided his or her affirmative consent; and
- 3) the reasonable demonstration requirement is met.

Affirmative consent may be obtained from any location including home, work, library, kiosk and hand-held device.

The giving of affirmative consent may be memorialized by, among other methods, retaining a method of the consent agreement and the consent notice.

When consent is required from multiple consumers who are acting in concert, consent may be obtained from each consumer; or from one consumer who represents that he/she is authorized to consent on behalf of all the consumers acting in concert.

Procedures should be established in the event the consumer does not wish to consent to electronic transactions.

## **II-6 Reasonable Demonstration of Access**

If the ESIGN Consumer Consent Process will be employed, system design teams should create a mechanism, method or process that enables a Consumer's provision of consent to reasonably demonstrate that the Consumer can access the electronic method(s) and format(s) the system will use to provide or make available electronic records such as notices, disclosures, and agreements over the course of the Transaction.

Design team should consider how would the consumer access the Required Consumer Information (i.e. via the Internet, email or other software, or a combination, etc.)

The design team should also consider in what format (html, PDF, word, etc.) will this Required Consumer Information be presented; and

The team should also determine the appropriate mechanism, method of process for obtaining the consumer's consent that reasonably demonstrates that the consumer can access the format of the legally required information.

Once the access mechanism and format have been decided, a strategy for how to meet the reasonable demonstration requirement can be developed.

Lastly, businesses are not required to verify that the customer has received the Required Consumer Information, but if the business has any indication that the consumer is unable to access this information, the business should re-confirm the consumer's ability to access it or send the consumer a paper copy. Business should consider establishing procedures for sending paper copies in the event an email bounces back.

## **III. AGREEMENTS, NOTICES AND DISCLOSURES**

### **III-1. General Principles for Display and Presentation of Information**

The system should be designed to display and present information efficiently and effectively. Absent special circumstances, the system design team should provide a reasonable opportunity to access information, whether it is part of an agreement, notice or disclosure, so that:

- the information is displayed or made available in a manner and/or format that complies with any applicable rule of law.
- The opportunity to access the information occurs:
  - At the point in the transaction required by any applicable rule of law, or

- If there is no applicable rule of law, at or before the point in the transaction where having access to the information is appropriate for the recipient, but not later than the point at which the recipient is asked to indicate agreement with, or acknowledge access to, the information.
- During the course of the transaction, the information may be retained by the recipient, or accessed by the recipient at a later time, consistent with the purpose of the transaction, the nature of the information and applicable law.

In an electronic environment, it is possible for agreements to be manifested in different ways. The election to continue a process or transaction may be enough. Checking a box may also demonstrate agreement. Because there are so many ways the choice to continue with the electronic transaction or the showing of an agreement can be presented, a system design team will need to take into account the need to convincingly demonstrate the indication of agreement as part of the process.

The terms of an agreement or contract should almost always be available for review before the parties are irrevocably bound to its terms.

Other important information, including any required notices and disclosures, should be available at a time and in a manner that preserves the purpose of the notice or disclosure.

When designing a system to present electronic records for review, the system design team should base their assumptions on the sophistication of the potential Transaction Parties; the sophistication of the technology being employed; and the desired level of security and reliability for the system.

With respect to access, display and review, the information should be made available in a manner that makes its general purpose clear and encourages, rather than discourages, review with respect to issues associated with retaining agreements, notices and disclosures (*See* SPeRS Section V).

When designing a system to present information for review, the design team may wish to consider, where appropriate and practicable using hyperlinks, dialog boxes, navigational cues or other strategies to provide the definitions of defined terms, etc. and also offering the recipient the option of increasing the font size or changing the font in which the information is presented to facilitate easier review or reading.

### **III-2. Delivering and Displaying Records and Information**

When developing a process that includes the electronic display and delivery of agreements, notices or disclosures, the system design team should:

- Identify the records and information that will be delivered electronically to each Transaction Party in the course of the Transaction;
- Consult with legal counsel or compliance personnel to determine whether any of the records or information to be provided are subject to any specific delivery requirements under an applicable rule of law;

- Accomplish delivery by providing access or the opportunity to access the record, as applicable;
- Determine the appropriate method(s) for providing access to the records and information, taking into account:
  - The nature of the Transaction and the intended audience,
  - Whether the records and information will be provided or made available as part of an interactive session with the recipient, as part of a unilateral transmission to the recipient, some combination of the two, or through other means,
  - Whether the records and information to be provided or made available include sensitive or confidential information,
  - The time period for which the records and information should remain available for access by the recipient during the course of the transaction, and
  - Whether the recipient should be required to access any of the records and information in order to proceed with the transaction.

### **III-3. Delivering and Displaying Records and Information – Retention of Records by Other Customers**

For electronic records that must be signed, or that contain Required Information, the system design team:

- Should provide the transaction participant signing or accessing an electronic record with:
  - An explanation of the options that the transaction participant will have during the transaction to retain a copy of the record, including any disclosure or explanation required by the E-SIGN Consumer Consent Process (*See* SPeRS Standard II-2), and
  - A reasonable opportunity to retain a copy of the record for later reference.
- May wish to provide the transaction participant with an opportunity to agree to the methods being provided to retain a copy of the record.

### **III-4. Indicating Agreement**

When developing a process that includes the electronic delivery or display of agreements to transaction participants, the system design team should:

- Consult with legal counsel or compliance personnel to determine:
  - Which records or information being delivered or displayed require some indication of agreement by a transaction participant
  - The level of formality or ceremony required for each indication of agreement
  - Implement a process design which, in the context of the transaction and the particular information or record in question:
    - Offers the transaction participant:
      - A clear choice to either agree or decline to agree, and
      - A clear method to express agreement or decline to agree.
    - Provides an explanation of the consequences of assenting or failing to assent except when the consequences are inherently obvious in the context of the transaction, and

- When appropriate, offers the transaction participant an opportunity to correct an election to assent or refuse assent made in error except when impractical or unnecessary.
- Indication of agreement may involve a formal signature process, a less structured explicit agreement by the transaction participant, or an action that implies agreement.
- 
- The appropriate level of formality will often depend on the circumstances of the transaction, the intent of the transaction participants, and the requirements of any applicable rule of law.
- 
- The key element of indicating agreement is to establish that the party whose agreement is sought engaged in a voluntary act knowing, or with the reasonable opportunity to know, that the act would be understood to indicate agreement
- 
- **III-5. Acknowledging Access or Delivery**
- When developing a process that includes the electronic display of and opportunity to access disclosures and notices to Transaction Parties, the system design team should:
  - Consult with legal counsel or compliance personnel to determine:
  - Which records or information being displayed or provided require some acknowledgment of access or opportunity to access by a Transaction Participant, and
  - The level of formality or ceremony required for each acknowledgment of access or opportunity to access.
  - For records that require acknowledgment of access or delivery, implement a process design which, in the context of the Transaction and the particular information or record in question, offers the Transaction Participant a clear method to acknowledge access or opportunity to access.

Acknowledgment of access or opportunity to access an electronic record may sometimes be necessary or desirable.

Acknowledgment may involve a formal signature process, a less structured explicit acknowledgment by the Transaction Party, or an action that implies acknowledgment.

The appropriate level of formality will often depend on the circumstances of the Transaction, the intent of the Transaction Parties, and the requirements of any applicable rule of law.

### **III-6. Conspicuous Disclosure**

When developing a process that includes the electronic display of or access to agreements, notices or disclosures to Transaction Parties, the system design team should:

- Consult with legal counsel or compliance personnel to determine whether any of the records or information to be provided are subject to “conspicuous disclosure” requirements under an applicable rule of law, and
- If “conspicuous disclosure” is required:
- Implement a process design which, in the context of the transaction and the particular information or record in question, delivers the required record or information in a form which is:
  - Reasonably understandable, and
  - Designed to call attention to the information that must be disclosed.
- Employ electronic tools and display techniques so as to effectively convey the information.
- 

### **III-7 Using Hyperlinks and Other Directional Devices**

When displaying information electronically, the system design team should consider using navigational cues in order to better organize, enhance or protect the presentation of information.

When using a navigational cue, the system design team should label or title the navigational cue, or provide explanatory information for use of the navigational cue, reasonably sufficient to permit the transaction party to understand the general nature of the records or information associated with the navigational cue.

## **IV. SIGNATURES**

### **IV-1 Selecting a Signature Process**

The selection of an appropriate signature technology for a particular application should be based on a determination of the relevant factors and circumstances, including:

- Applicable hardware and software requirements (i.e. technical expertise and expense involved in acquiring/installing;
- Any rule of law limiting the type of electronic signature that may be used (e.g. Revised UCC Article 9)
- Characteristics of the signer (i.e. tolerance level of potential signers for any delays or technical issues raised by installation of special hardware/software; the sophistication level;
- Susceptibility of the technology to repudiation (e.g. factors that provide external evidence of authenticity and may lessen the risk of repudiation, i.e., issuance of documents, flow of money into the signer’s account)
- Ability of the signature to protect the record from undetected alteration after signing
- Portability of the signature process (i.e. the importance of the signer being able to use the electronic signature in different locations; or the appropriateness to expect the customer to carry necessary hardware for signature (i.e. smart card for storing digital signature) or memorizing a PIN or password.
- Suitability of the signature for:

- Non-repetitive in-person transactions
- Repetitive in-person transactions
- Non-repetitive remote transactions
- Repetitive remote transactions
- Ease of use for multiple signatures by same signer in one record
- Ease of use for multiple signers in one record
- A variety of symbols, devices and procedures have been recognized as valid signatures.

There are many ways to create electronic signatures (a click-through, PIN, password, etc.). It is not necessary that a signature be created in any particular manner, or using a particular mark or symbol to be valid. “A signature is whatever mark, symbol or device one may choose to employ as representative of himself.”<sup>1</sup> Many cases have held that any symbol, character or mark may be used as a signature, as may a fictitious name, if it is adopted as a substitute for the signer’s name. Even if a person uses his own name as a signature, the person need not use his full name; mere initials can constitute a valid signature. Likewise, a person need not sign his own name to a document in order to create a valid signature; another person can sign for him.

Many of these electronic signature methods involve the use of a credential to authenticate the consumer. A credential can also serve as a signature, if it is the signer’s intent. In this case, however, the credential will not appear printed as the signature, but rather it will be reflected as a recitation or a symbol.

The document suggests that if there are to be a series of remote transactions, then a type of signature easily activated by the use of a PIN, password, or token may be more appropriate. It also may be helpful to combine electronic signature techniques so to demonstrate proper attribution to the signer

Additional factors to consider when determining which type of electronic signature is appropriate:

- will the signers be receiving electronic or paper records to retain for future reference?
- will the signature be expected to authenticate the signer’s identity?
- will the signature be expected to protect the record from alteration?
- how the signature process will be reflected in or displayed.

This section ends with a section known as “Signature Criteria”. It’s about 20 pages and it provides a set of comparative charts that evaluate a number of the most popular electronic signatures. They are offered as an illustration of the kind of analysis a systems design team might go through in selecting an appropriate electronic signature process.

#### **IV-II Providing Information on the Signing Process**

---

<sup>1</sup> *Griffith v. Bonawitz*, 73 Neb. 622, 103 NW 327 (1905).

The execution of an electronic signature should be preceded by an opportunity for the signer to review:

- A description and explanation of the procedure used to create the electronic signature, and
- A description of the sequence of events that will result in the signature becoming final and effective.

Provided, however, that the signature process may be sufficiently familiar or self-explanatory that a description is superfluous or would be repetitive.

Both E-SIGN and UETA require that a signature is only valid if the signer intends to sign something. There are a number of ways signers can provide evidence of their intent to sign (i.e. placement of signature at the end of the document, statements above the signature that declare that the parties are signing the document to demonstrate their agreement to the terms in the document, etc.). The online signing process should include evidence of the consumer's intent to minimize the risk of a later claim that no intent to sign existed.

An electronic signature process should address whether the signature is effective immediately when it is completed or whether additional steps will be necessary. Also, when multiple parties are signing, the parties should be informed of the process for obtaining each signature early in the process.

When designing a signature process, the following should be considered:

- What information about the signature process should be made available
- When it is appropriate time to provide information on the signature process.

The document also provides examples of sample language describing various signature processes. (i.e. click-through, digitized signature, PIN signature process for multiple signers, etc.). SpeRs acknowledges that the type of explanation during the signing ceremony will at some point become unnecessary and even an annoyance as the general public becomes more comfortable with electronic signatures.

### **IV-3 Establishing the Intent to Sign**

The process used to create an electronic signature should be designed so that:

- It is clear that the signer intended to create a signature, and
- When not reasonably apparent under the circumstances, the signer is advised that the signature fulfills one or more purposes:
  - Affirming the accuracy of information in the record
    - Affirming assent or agreement with the information in the record
    - Affirming the signer's opportunity to become familiar with information in the record,
    - Affirming the source of the information in the record, or
    - Other specified purposes.

System designers should create a signature process that minimizes the risk that customers could legitimately claim later that they created an electronic signature without realizing what they have done, or its legal significance. For signature created by click-throughs, Designers should consider the likelihood of a customer raising a “slipped-finger” claim, indicating a lack of intent.

A confirmation process may be particularly useful as a way to avoid disputes over intent.

The system design team should establish the intent to create a signature through a process that forms intent by one of many available mean, including having the signer click on a button that follows ceremonial signing language that states “I agree” or some other expression of contractual assent.

Intent can also be established by a process that allows for reviewing and signing of records to be preceded by an informational description of the signature process and an explanation that it will be legally binding (see IV-2). Another process would allow the creation of the signature to be preceded by a notice that a signature is being created and an explanation that it will be legally binding. Alternatively, the transaction may be structured so that it is readily apparent that a signature is being created and that it will be legally binding (i.e. A note to the customer in a dialog box that reads: “...please sign this agreement to proceed with the transaction...”).

#### **IV-4 Associating a Signature with a Record**

A process for signing records should be designed so that:

- The record is presented for signature before the signature becomes effective, and
- The signature is attached to, or logically associated with, the record presented at the time of signing.

*Ex: Harry Jones fills out an on-line loan application. Harry fills in all the necessary information in the online application form. When Harry is ready to submit his application, he is asked to sign the application by clicking on a button marked “I agree”, and then confirming his signature by clicking on a “Submit” button that formally delivers the application to the potential lender. A final version of the application is generated by the system for Harry to download or print, and for maintenance in the lender’s files, that states in the signature block “Signed and submitted by Harry Jones on June 12, 2002 at 12:45 PM Eastern time.” A record of Harry’s selection of the “I agree” and “Submit” keys is maintained by the system.*

The design team should consider, prior to receiving the consumer’s signature, providing the record to be signed for review and making available to t he signer the opportunity to print or download the record for review according to SpeRs standards stated in Section III-3.

The signature should be attached or associated with the record in a manner that permits a person reviewing a record of the transaction after the transaction to determine clearly that a signature occurred. Methods for attaching or associating the signature include:

- 1) for graphic signatures: such as typed or handwritten names, embedding a graphic representation of the signature in the signed record, and
- 2) for process signatures, such as PIN or click-throughs, the identity of the signer, the fact that the record has been signed, the date, the method used to sign the record; or maintaining a system log or audit trail that reflects the completion of the signature process by the signer.
- 3) For signatures based on cryptographic process, by: associating with the signed record the data necessary to identify the person to whom the encryption key was assigned or for whose use the encryption key as created; or reflecting the completion of the signature process in the signed record itself by stating in the signature block or at the end of the signed record appropriate information concerning the signature; and
- 4) For handwritten or typed signatures on paper to be associated with an electronic record, the paper document bearing the signature should include a description of the electronic record being signed and the date the record was presented to the signer for review; or a statement that the signature is associated with an electronic record.

Timing: The record should be displayed or the opportunity to review the record made available, either immediately before the signature process is initiated by either the system or the signer or as part of the signature process. The signature should be attached to, or associated with, the record at the time of signing.

The Legal Commentary discusses a series of case law that examined the differences between fraud in the factum and fraud in the inducement, but they do not specifically apply to the electronic signature context. The point of the case law discussion is to show the importance of creating a process that reliably and predictably associates the signature with the electronic record presented for signature. These two contract defenses could apply in the electronic signature context.

#### **IV-5 ATTRIBUTING A SIGNATURE**

A process for signing records should be designed so that either:

- The signature itself provides evidence of the signer's identity, or
- The process surrounding creation or affirmation of the signature:
  - Provides evidence of the signer's identity, and
  - Is in some manner preserved, evidenced, or capable of recall or recreation during the life of the transaction.

The System Design team should determine the method or methods that will be used to attribute each signature obtained as part of the transaction. Principal options for establishing attribution include, obtaining the signature at the same time a new relationship is authenticated; use of a credential for either accessing the records to be

signed or creating the signature; eyewitness testimony; circumstantial evidence; or certification of the signature by a trusted third party.

When obtaining a signature at the same time a new relationship is authenticated, the system design team should determine:

1. whether it is appropriate to store the information used to authenticate the signer so that it may be reviewed at any time over the life of the transaction, and
2. whether it is appropriate to store the process used to authenticate the signer and obtain the signature so that it may be demonstrated at any time over the life of the transaction.

When using credentials to establish attribution, the system design team should determine:

1. Whether the credential will be used to access the record for signing, or create the signature;
2. How the credential will be associated with the person holding the credential

#### **IV-6 Signatures and Agreements by Electronic Agents**

A system designed to implement an agreement and signature by an electronic agent:

- Should require a clear and detailed definition of the parameters of the electronic agent's authority to form an agreement and sign on behalf of the represented party, and
- May either reflect the use of an electronic agent in the signature information provided as part of the signed record, or present the signature as the act of the represented party without reference to the use of an electronic agent.

### **V. RECORD RETENTION**

#### **V-1 Accuracy, Accessibility and Retainability in General**

Electronic record retention systems should be designed to ensure that information contained in the electronic records remain:

- Protected from undetected and unauthorized alteration, and
- Accessible to the Record Holder and others entitled by rule of law or agreement to access, or obtain a copy of, the Record Holder's copy of the record.

*See Also* SPeRS Standard 3-3 for the Record Provider's obligation to provide access or copies of records to other transaction participants (e.g. consumers).

#### **VI-2 The Physical and Technical Environment**

As part of the infrastructure necessary to protect the integrity of electronic records, the system design team should establish a commercially reasonable design for:

- The physical environment in which the records are maintained that takes into account:
  - The types of transactions evidenced by the electronic records,
  - The value of the transactions evidenced by the electronic records,
  - The value or confidentiality of the information contained in the electronic records, including whether the record is subject to state or federal privacy laws, and
  - The impact of loss, destruction or theft of the electronic records on the operations of the Record Holder.
- The technical environment in which the records are maintained that takes into account:
  - Network controls,
  - Hardware controls, and
  - Software controls.

### **V-3 Verifying the Consistency and Integrity of Electronic Records**

Where appropriate, the system design team should consider including in the process for creating, delivering and submitting electronic records commercially reasonable checks to confirm that:

- The record:
  - Contains information that is both internally consistent and consistent with other transaction records;
  - For signed electronic records, appears to have been electronically signed by each of the targeted signers before being accepted as final and complete;
  - Has not been altered without authorization once it is effective; and
  - Is retrievable in a form perceivable by an individual.
- Any set of transaction documents intended to be reviewed, completed, and/or signed as a group is complete and that all necessary tasks have been performed before being submitted and/or accepted in final form.
- 

### **V-4 Document Conversion**

System design teams should develop guidelines and procedures for the preservation and conversion of paper to electronic documents to meet the following objectives:

- Promote cost and organizational efficiency;
- Ensure safekeeping of documents;
- Ensure compliance with state and federal requirements regarding record retention, access to records, and document destruction;
- Maintain secure, reliable, long-term access to records; and
- Establish data integrity to satisfy the Rules of Evidence.
- 

### **V-5 Vendor Due Diligence**

When using third party vendors to perform record retention functions, Providers should adopt a risk management process that includes:

- Proper due diligence to identify and select a third-party provider;

- Contracts that outline duties, obligations, and responsibilities of the parties involved; and
- Ongoing oversight of the third parties and third-party activities

#### **V-6 Governmental Regulation of Record Retention**

The system design team should consult with legal counsel or compliance personnel to determine whether there are any state or federal regulatory requirements that may affect the form or methods used to create, file or maintain the records.

#### **V-7 Transferable Records and Electronic Chattel Paper**

If the system is intended to manage the creation, execution, transfer and/or storage of electronic equivalents of negotiable promissory notes, bills of lading, warehouse receipts, retail installment sales contracts, debt obligations secured by personal property, or leases of tangible personal property, the system design team should consult with legal counsel or compliance personnel to determine the special requirements for:

- Controlling the transfer of ownership of the electronic record,
- Storing the electronic record, and
- Protecting the electronic record from unauthorized alteration.