**AlphaTrust® e-Sign**

This white paper is written for senior executives, line of business managers, legal staff, risk management staff, technical managers, and security managers involved in deploying paperwork solutions intended to leverage and comply with the US Federal E-SIGN law as codified in 15 USC 7001 et. seq., the Uniform Electronic Transactions Act at the US State level, the US Sarbanes-Oxley Act, Canadian provincial and Federal legislation, the EU Signature Directive in Europe, EU eIDAS Regulations, EU GDPR Regulations, HIPAA (in the US), as well as other national laws and regulations globally. Industry specific regulatory compliance (in the US) includes Federal Reserve, OTS, Comptroller of the Currency, SEC, NASD, FDA, Dept. of Education, US DoD, and IRS regulations.

Disclaimer: The information in this document is subject to change or update without notice and should not be construed as a commitment by iPipeline. This document is for informational purposes only and does not constitute an offer or commitment to provide AlphaTrust e-Sign to you or any related or associated company, nor shall it constitute technical information. Any such offer, commitment, or presentation of technical information will be made only by means of a mutually agreed upon services agreement with iPipeline.

## CONTENTS


| | |
|---|---|
| Executive Summary | 2 |
| Paperwork Automation | 4 |
| Standard Document Workflow Example (Current State) | 4 |
| Fully Automated Paperwork Flow | 4 |
| Where Does AlphaTrust e-Sign Fit in Business Processes? | 5 |
| Technical Overview | 6 |
| Architecture - AlphaTrust e-Sign Solution | 7 |
| Transactions in AlphaTrust e-Sign | 8 |
| Electronic & Digital Signatures | 9 |
| Dispute Resolution and Admissibility | 10 |
| Document Data Integrity | 10 |
| Client-side Requirements | 10 |
| System Requirements | 11 |
| Getting Up and Going the Easy Way | 11 |
| Summary | 11 |

**Executive Summary:**
Electronic forms, documents, and business records executed with electronic signatures today have the legal and commercial equivalence of paper records with handwritten signatures in most of the developed world. These online processes are decreasing the cost of business, increasing the speed at which business is done, and adding needed security to electronic business transactions. Due to the unique business requirements placed on permanent business records and signatures, business managers find that they must properly marry technology with sound processes and practices to achieve effective results (i.e. to achieve proper "internal controls" for regulatory compliance).

An effective electronic record and signature solution must address these business issues:

1. Does the solution deliver the needed technical security requirements (authentication, data integrity, and technical non-repudiation)?
2. Does the solution address the business requirements for:
    a. Compliance with laws and regulations?
    b. Enforceability of transactions (legal recourse)?
    c. Acceptance by users of the solution?
    d. Using proven technology?
    e. Viability as a long term solution?
3. Does the solution provide for growth/easy scalability as the organization identifies future potential for electronic documents and records?
4. Can the solution integrate and work with existing electronic workflow and security solutions?

This white paper discusses paperwork automation in general, as well as how AlphaTrust® e-Sign offers a superior solution for reducing cost, improving revenue, and decreasing risk exposure, by fully automating paperwork and avoiding physical paper processing.

In the US, major legislation exists at the federal level (the Electronic Signatures in Global and National Commerce Act, or E-SIGN for short) and at the state level (the Uniform Electronic Transactions Act, or UETA, now passed in 47 US states, along with the District of Columbia, and the U.S. Virgin Islands, with equivalent legislation in the other 3 states) that provides for the use of electronic signatures and records in place of paper records and ink signatures. The EU has its similar eIDAS regulations, and most other developed countries have electronic signature enabling legislation. Any solution must meet the baseline requirements set out in these laws and regulations.

In addition to legal and regulatory requirements, it is also important to look at the bigger picture. While you want a solution that meets legal requirements, the introduction of electronic records and signatures introduces a shift in business processes that may affect other business applications. Your solution should not just focus on electronic signature. The entire process of automating paperwork (document creation, document workflow, electronic signature, downstream data, and document processing) must be considered to achieve process success. Additionally, your solution should not merely address the needs of one use case, but be capable of easily extending to other applications and areas to meet the growing needs of your enterprise, supply chain, industry, and governmental requirements.

Many companies think about eliminating manual signatures and therefore look for eSignature vendors to help solve their problem. There are many vendors of e-Signature solutions on the market. AlphaTrust's strength

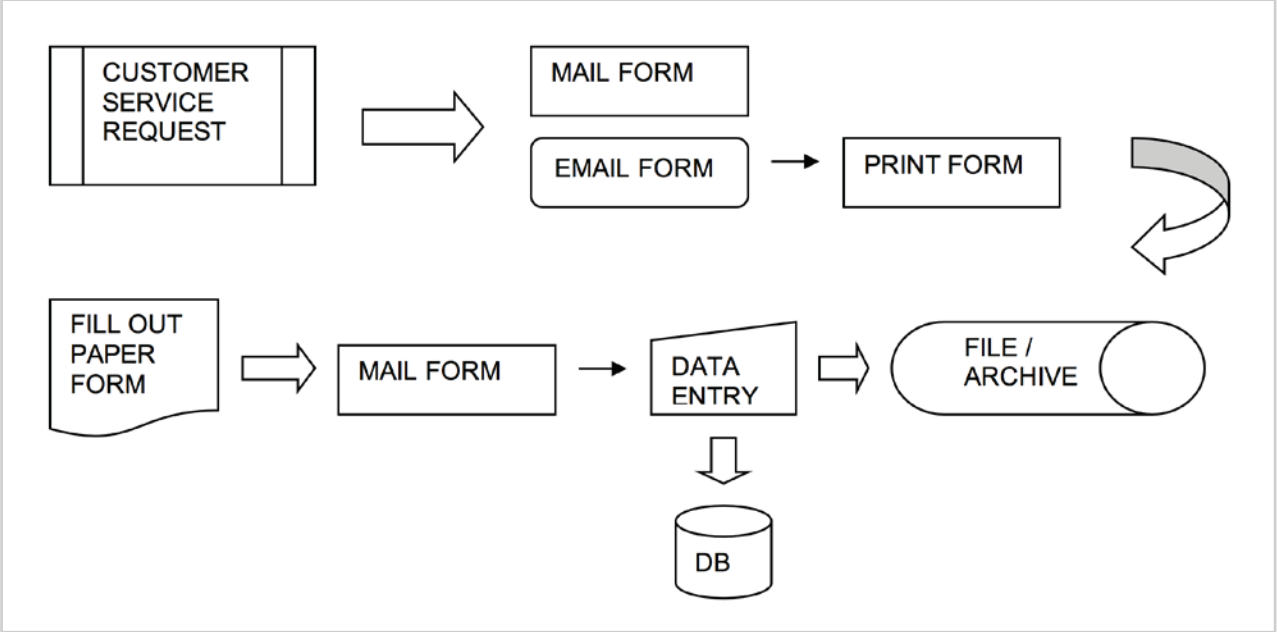
and difference is our focus on the full needs of paperwork automation for the enterprise, not just e-Signature. We offer:

- An enterprise-grade software platform for automating paperwork processes, including robust e-Signature capabilities.
- Deployment flexibility: host the solution internally or use a cloud deployment, fully managed by AlphaTrust with full IT resource and data segregation.
- Fully customizable workflows, language, and user experience to meet your exact needs.
- Management and control of your documents throughout their lifecycle, so you can maintain the all-important “chain of custody” including full audit trail details. It is not enough just to have e-signed document files produced by an eSignature system. You need to be able to prove them up years down the line.
- Ease of integration with other business processes and document management systems.
- Advice, consulting, and best practices as applied to your particular needs.
- A 17-year history of serving diverse needs across many industries serving clients such as: AT&T, ADP, CVS, Dohmen Life Sciences, Elsevier, Fidelity National, General Motors, Gerber Life, HCC Insurance, MetLife, New York Life, Paychex, Pfizer, Reed Elsevier, Thomson Reuters, Vanderbilt University Medical Center, Vantiv, and the US Government.

AlphaTrust e-Sign addresses the full requirements of paperwork automation, creating successful projects. Our software solution has been in production use since 2001 with a wide variety of applications.

**Paperwork Automation:**
Most current paperwork processes are manual or semi-automated, often bouncing back and forth from paper to electronic form (i.e. fax, print, scan, email).

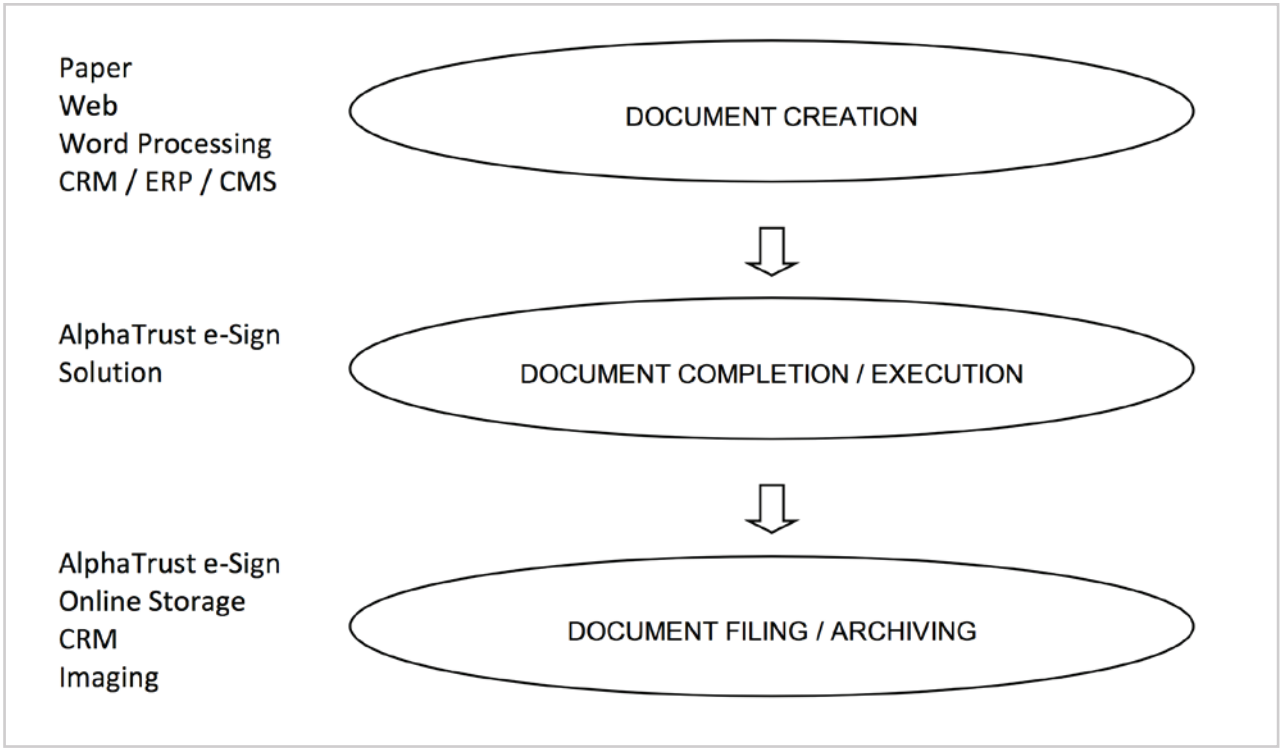
**Standard Document Workflow Example (Current State):**




Whether customer services requests originate from mail, telephone or web inquiry, paper forms are sent to the customer for completion, signature, and return. This process can take seven to fourteen days and have direct costs of $5 to $50. Non-response rates vary with the application but result in lost business.

**Fully Automated Paperwork Flow:**
Using AlphaTrust e-Sign, you can design and integrate a web-based workflow that dynamically creates documents, routes them to appropriate parties, presents them for acceptance, requests additional information or documentation, and allows for approval and/or signature, all while maintaining a full audit trail, central control, and archiving of documents.

**Where Does AlphaTrust e-Sign Fit in Business Process?**



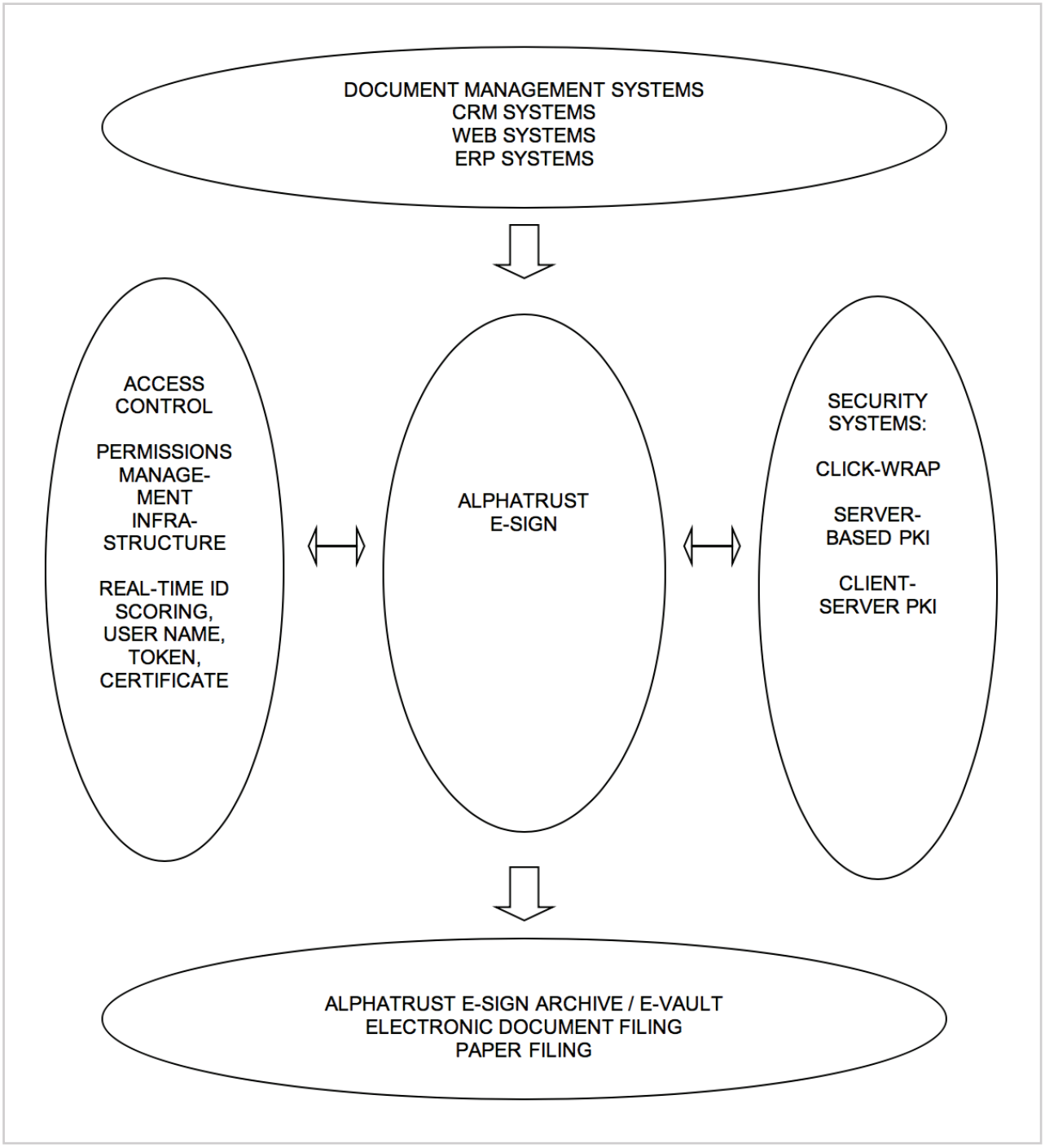

AlphaTrust e-Sign manages the routing, completion, execution, and storage phase of document processes, whether a single document, single-signer transaction, or a complex closing involving multiple documents and multiple signers. AlphaTrust e-Sign uses web and email processes to manage the complete execution cycle for a transaction. The result is a completed document set for the transaction in fully electronic form. Completed documents may be transmitted, filed and archived electronically, or printed for paper filing. AlphaTrust e-Sign archives all completed documents within its database archive.

AlphaTrust e-Sign supports multiple user authentication methods to identify signers and jurisdictional rules management to deal with the various requirements imposed by special regulations or state rules, especially around consumer consent and disclosure.

AlphaTrust e-Sign is an essential part of an e-business infrastructure and can integrate and interoperate with document management systems and security systems (see technical overview).

**Technical Overview:**

Full e-Business Integration Example:



**Architecture - AlphaTrust e-Sign Software Solution:**
AlphaTrust e-Sign is an application server-based transaction system. It is available as a cloud service, or for on-premise installation. AlphaTrust e-Sign is designed to address three important classes of use cases:

1. Straight Through Processing, referred to as "STP" below
2. General Business Process Workflow, referred to as "Workflow" below
3. Ad-hoc or On-Demand work, referred to as "Ad-hoc" below

Straight Through Processing ("STP")
STP use cases have these characteristics:

- Process control is critical
- Focus is on system generated documents
- Direct integration with upstream document generation systems
- Direct integration with downstream operations and archival systems
- Achieves "no touch" end-to-end paperwork automation - STP
- Very high process quality and large reduction in human processing and intervention
- Requires a formal project: analysis, integration, deployment
- Owned by IT or Operations

For STP cases, your applications communicate with AlphaTrust e-Sign via industry standard web services.

General Business Process Workflow
Workflow use cases have these characteristics:

- Process control is important
- Differs from a core process in that it does not justify a formal integration project (needs a "no code" approach)
- May or may not connect to upstream and downstream systems
- May use system generated, process generated, or user generated documents
- Achieves "low touch" end-to-end paperwork automation
- High process quality and good elimination of human processing and intervention
- Typically uses an informal project: analysis, process creation (using tools), deployment to end users
- Implemented typically by a business analyst or process engineer using design tools and configuration

The principal difference between an STP approach and a general Workflow approach is that you do not need integration and developer/IT resources for a Workflow use case. AlphaTrust e-Sign provides the tools, accessed via a web browser, for designing, testing, and publishing workflows for other users to leverage.

Ad-Hoc Work
Ad-Hoc work use cases have these characteristics

- Process control is less important, or managed elsewhere
- User defined and controlled (i.e. send a desktop document for signature)
- Relies on end user to define a template or use a one-off ad hoc approach
- Uses user generated or managed documents

- No or minimal data collection required, no or low data validation, no processing rules
- Not integrated with other systems
- Achieves avoidance of direct handling of paper (fax and mail) but low elimination of human processing and intervention
- Fast to deploy

The Ad-hoc approach is most familiar to the user of e-Signature tools. The approach, typically, is to upload a document you would like to send for signature, tag signature locations, enter recipient names and email address, and send for signature. This approach has its place. It achieves the tactical benefit of getting a document signed faster. However, there is no process control with this approach. The tool user is solely responsible to getting the process right.

The strength of AlphaTrust e-Sign is in the power to address all these use cases along with the flexibility to deploy in house or be consumed as a cloud service.

**Transactions in AlphaTrust e-Sign:**
The basic unit of work for AlphaTrust e-Sign is a transaction. Each transaction is defined as one or more participants that need to perform tasks against one or more documents. These tasks may include receipt of disclosures, review, data addition (form fill or documentation upload), approval without signature, e-Signature (including initials where needed), and secure delivery.

Each participant is authenticated using many access control methods before being allowed to perform tasks. AlphaTrust e-Sign communicates with signers via web and email interactions. AlphaTrust e-Sign users are defined as either registered or unregistered users. Examples of registered users are employees, vendors, and existing customers. Registered users authenticate using single sign on via federated authentication or with a defined username and password. Examples of unregistered users are new customers and one-time transactional users.

Additionally, registered users have a signature profile, may use a registered bitmap image of their handwritten signature, have access to documents they have signed in the AlphaTrust e-Sign archive, and have access to additional features not available to unregistered users. Unregistered users may either be unauthenticated, authenticated with a one-time transactional password, or use challenge-response knowledge-based authentication (KBA) via third party providers.

Documents processed by AlphaTrust e-Sign are typically stored and managed as HTML documents or as PDF documents. Even though some documents may originate in proprietary formats such as Microsoft Word, it is more effective to convert them to a native HTML or PDF format prior to execution, which can be done automatically. Industry groups have studied their long-term requirements and concluded that the open, standard HTML or PDF formatted documents best meet the need for permanent electronic documents. The reasons are many.

Both HTML and PDF:

1. Are open standards
2. Are long-lasting and supported
3. Support data embedding and mining

As an example, the mortgage industry has a 37.5-year archive requirement. There is concern with using proprietary formats such as Word files due to uncertainty around whether old file versions will be supported more than a few years out. Additionally, such formats often use "active content" technologies, meaning the documents are programmable, which can cause them to be unenforceable. AlphaTrust e-Sign natively supports, and is designed with, the requirements of HTML and PDF documents in mind. Furthermore, the trend in government applications, such as online filing, is to accept only open document standards including text, HTML and PDF (including PDF/A). While other document formats are very useful for document creation, they can have serious drawbacks as permanent document formats.

Document Integrity

Once a document is signed, the signer's electronic signature in the form of a signature block is inserted into the document, and the document is "sealed" with a cryptographic digital signature. The digital signature provides evidence of document tampering or alteration after signing. This is an essential security requirement for any enforceable digital document. Digital data can be easily and undetectably changed. Digital data protected with a cryptographic digital signature is often referred to as having a tamper evident seal. If the data is changed after signing, it can be easily detected.

When deployed on customer premises, AlphaTrust e-Sign is provided as server-based software running on Windows Server 2012 R2 or Windows Server 2016. It easily integrates with web processes operating on UNIX, Linux, or mainframe applications using a web services programming interface.

AlphaTrust e-Sign is also available as a cloud service. Customers may use our standard multi-tenant software-as-a-service offering or may subscribe to a custom Dedicated Managed Service (single tenant SaaS). With either cloud service, there is no software to buy. AlphaTrust will manage the entire process. If you choose the dedicated SaaS option, you may migrate from the cloud to your own on-premise deployment when needed.

**Electronic & Digital Signatures:**

Electronic signatures and digital signatures are used interchangeably. In reality, they are very different, and the fact that both terms use the word "signature" has caused confusion.

An electronic signature is a legal concept for using an electronic symbol to represent a person's volitional consent to be bound to the terms of a document. With any business process that requires an enforceable document, it is necessary to obtain a legally-valid electronic signature for that document, using the process processes This is what AlphaTrust e-Sign is designed to do.

A digital signature is a technical security concept for a data integrity process using cryptographic data hashing and encryption. Simply applying a digital signature process to the data of a document will generally not result in an enforceable electronic signature. Digital signatures are a very important security tool and AlphaTrust e-Sign uses digital signature technology in its electronic signature processes.

AlphaTrust e-Sign uses cryptographic security technology. In its standard configuration, AlphaTrust e-Sign uses its own server cryptographic signing keys to apply the required digital signatures ("digital seals") to documents. In this configuration, there is no requirement for a public key infrastructure. AlphaTrust e-Sign may be integrated into a PKI if required. AlphaTrust e-Sign can support both software key sets and hardware key sets. AlphaTrust e-Sign manages all documents securely on the server during the signing process. There is no opportunity for a signer to alter a document presented to them for signature. Once a signer has indicated

their consent to sign, by clicking in appropriate locations in a document, AlphaTrust e-Sign will insert their signature block into the document, seal the document with a cryptographic digital signature, and record the details in an audit trail.

**Dispute Resolution and Admissibility:**
Electronic signature laws do not require the use of the processes and security measures employed by AlphaTrust e-Sign, but they are invaluable in establishing best practices, data integrity, and chain of custody. In the event an electronically signed document is disputed, the most likely challenges to the document will be one of the following:

1. "It wasn't me. I did not sign that document."
2. "I signed a document, but that is not the one I signed. It was changed."

AlphaTrust e-Sign will provide the following information to assist in refuting these claims:

- A time-stamped audit trail of document review and signing.
- A record of the Internet IP address of the signer.
- Authentication methods used to identify the signer.
- The actual signed document with cryptographic verification that the document has not been altered since it was signed. This is accomplished by verifying the cryptographic, time-stamped, digital signature of the document.

In addition to this information, your business process will also have additional evidence that weighs on the case. Examples include user authentication employed, for example by a customer portal application, and "course of dealing" history, i.e. how the parties acted before and after the transaction.

**Document and Data Integrity:**
One of the key security elements of a document processed by AlphaTrust e-Sign is the digital signature computed for each signed document. In a standard deployment of AlphaTrust e-Sign, each document, whether in HTML or PDF format, is hashed and digitally signed including a time stamp. The data comprising the digital signature is stored in the database used by AlphaTrust e-Sign. Web links are also embedded each document that, when clicked, will link to a web page that produces the audit trail and verification information for the digital signature. In addition, copies of signed documents not stored within AlphaTrust e-Sign may also be verified using programming interfaces provided by the software.

As an optional step, and only for PDF formatted documents, an additional cryptographic digital signature may be embedded in the PDF document itself. This PDF digital signature may then be independently verified by products such as Adobe® Reader or Adobe® Acrobat on a standalone basis, without any link to the original AlphaTrust e-Sign database. Key audit trail data is also embedded as metadata in the PDF document.

**Client-side Requirements:**
One of the strengths of the AlphaTrust® e-Sign SaaS architecture is that the only user software requirement is a web browser. AlphaTrust® e-Sign does not use any client-side software, plug-ins, Java code, ActiveX controls, or similar technology. It supports wireless touch devices such as smart phones and tablets, as well as standard PC and Mac computers. Adobe Acrobat® Reader v7.0 or higher (or another standards-based PDF viewer) is required for viewing signed PDF documents but is not required for the review and signing process.

**System Requirements:**
For on-customer-premise deployments, AlphaTrust e-Sign operates on Windows Server 2012 R2 or Windows Server 2016 servers connected to an MS-SQL Server database (SQL Server 2012 or later).

**Getting Up and Going the Easy Way:**
We understand the business, technical, and legal requirements for successful deployments of electronic signatures as well as wider document processing projects. You tell us your business objectives and we will work to deliver those results.

**Summary:**
AlphaTrust e-Sign is designed from the ground up to meet the requirements for technical security, transaction enforceability, and legal and regulatory compliance.

AlphaTrust e-Sign offers the clear solution for meeting the challenge of UETA, E-SIGN, SOX, GLB, EU eIDAS, ETSI, and other electronic record and electronic signature requirements, no matter what the application requirement. We welcome the opportunity to work with you to meet your specific business needs