Document and Business Record Automation (European Union)

White Paper

TEST RESULTS

Agreement

Notice

CONTRACT

MEMO

confidential

AlphaTrust

Document and Business Record Automation (European Union)

White Paper

About AlphaTrust

We pioneered electronic signature solutions in 1998, and since then our solutions have processed millions of critical business transactions each year for satisfied customers in banking, insurance, financial services, and other industries. We are trusted by some of the largest enterprise, technology service provider, and consulting services companies globally.

Our solutions easily integrate with existing applications enabling high volume, digital transaction management to reduce costs and dramatically improve the overall customer experience while adhering to strict regulatory and compliance requirements.

Through continuous innovation we are delivering the most advanced and cost effective eSignature workflow orchestration solutions on the market.

To learn more, visit www.alphatrust.com and follow us on Twitter, LinkedIn and Facebook.

Table of Contents

Executive Summary

Electronic forms, documents, and business records executed with electronic signatures today have the legal and commercial equivalence of paper records and 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.

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

1) Does the technology 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 (i.e., eIDAS)?
   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 electronic workflow in general and discusses how the AlphaTrust® e-Sign product family offers superior solutions for reducing cost and capturing increased business by keeping workflow electronic and avoiding paper processes requiring manual signature or approval.

Within the EU (European Union), national legislation is in place in most member countries implementing the EU Community Framework for Electronic Signatures (Directive 1999/93/EC) and the superseding EU Regulation (EU) N°910/2014, also known as eIDAS, took effect July 1, 2016. All solutions must meet these baseline requirements after that date. In addition to basic legal 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 electronic solution should not merely address the needs of one eSignature application 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 eSignature solutions on the market. AlphaTrust's strength and difference is on our focus on the full needs of paperwork automation for the enterprise, not just eSignature. We offer:

- An enterprise-grade software platform for automating paperwork processes, including robust eSignature capabilities.
- Deployment flexibility: host the solution internally or use a cloud deployment, fully managed by AlphaTrust with fully 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 electronically signed document files produced by an eSignature system. You need to be able to prove them, often years down the line.
- Ease of integration with other business processes and document management systems.
- Advice, consulting, and best practices as applied to your needs.
- A 15-year history of serving diverse needs across some of the largest enterprise and technology service provider customers worldwide.

AlphaTrust® e-Sign product family of software products and services address the full requirements of paperwork automation, ensuring successful projects.

Our software platforms have been in production use since 2001 with a wide variety of applications.
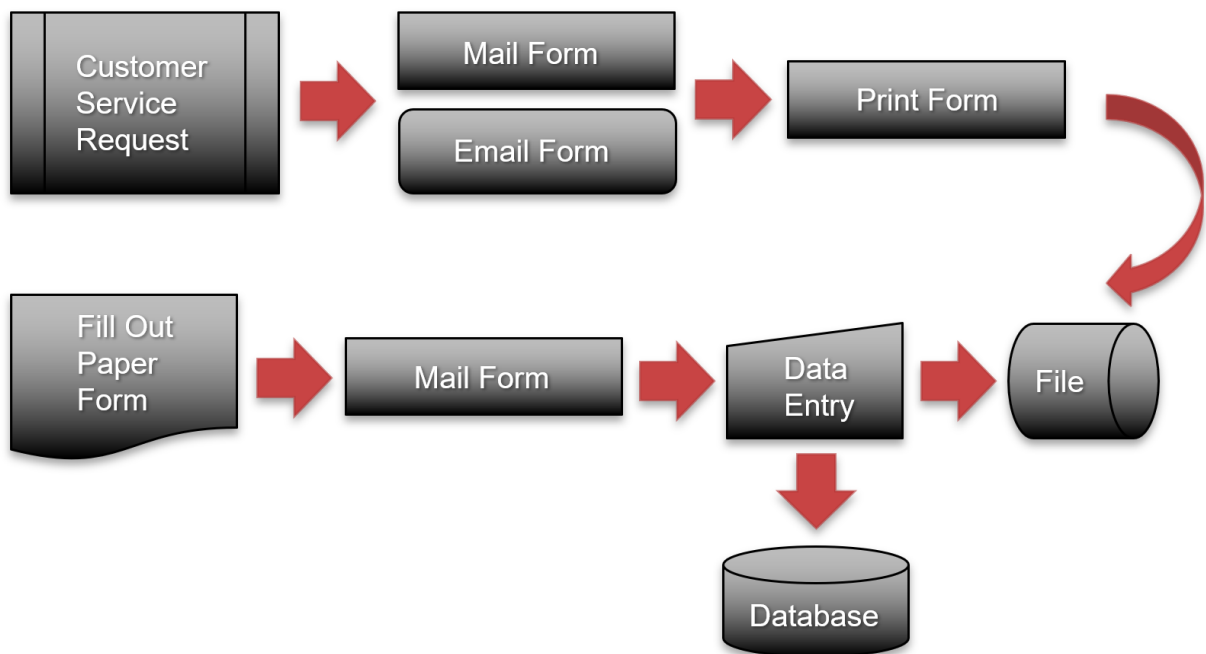
Electronic Document Workflow

Electronic document workflow processes generally fall into two specific types:

Type 1 – Static: static workflow starts with static documents (typically forms and applications such as new accounts applications, forms and customer service requests). Data from static documents usually end up in databases while the documents themselves become part of a file or archive.

Type 2 – Dynamic: dynamic documents typically start from templates but are customized for each requirement (e.g. contracts). Dynamic documents typically go through multiple draft and revision cycles before being ready for execution or approval.

Type 1 - Static Document Workflow Example

Figure 1: Static Document Workflow Example

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 € 5.00 to € 50.00 per document. Non-response rates vary with the application but result in lost business opportunity.

Type 2 - Dynamic Document Workflow Example

Contracts require a fair amount of documentation and collaboration. The documents themselves typically go through several draft and revision cycles. These documents are often sent via email.

Using AlphaTrust® e-Sign, you can design a web-based workflow that dynamically creates documents and presents them for acceptance and signature, while maintaining a full audit trail, central control and archiving of documents.
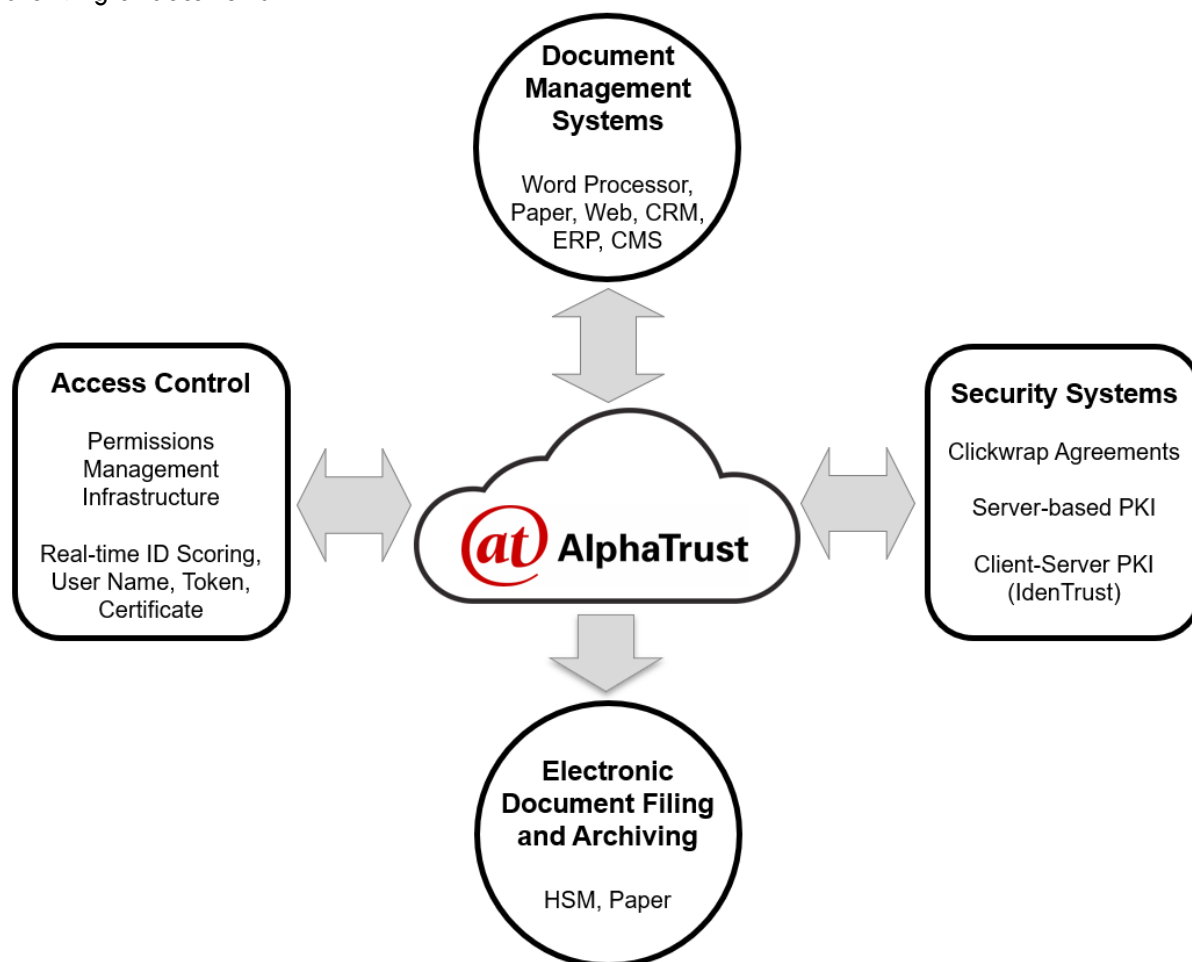

Figure 2 - Dynamic Document Workflow

AlphaTrust® e-Sign manages the completion / execution 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 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 in the area of 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).

AlphaTrust® e-Sign Architecture

AlphaTrust® e-Sign software is an application server-based transaction system. It is available as a cloud service, or for on-premise installation where it can be easily embedded within an existing business application or workflow. 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, and,
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 use cases, your applications communicate with AlphaTrust® e-Sign software 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 don't need integration and developer / IT resources for a Workflow use case. AlphaTrust® e-Sign provides the tools, access via a web browser, for designing, testing, and publishing workflows for other users to use.

<u>Ad-Hoc Work</u>

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, mail) but low elimination of human processing and intervention
- Fast to deploy

The Ad-hoc approach is what most people have had exposure to if they have used eSignature tools at all. The approach here 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 but it only achieves the tactical benefit of getting a document signed faster, and depends on the tool user to get everything right (no process control).

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

<u>Transactions in AlphaTrust® e-Sign</u>

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 review, approval without signature, eSignature (including initials were needed), form completion, or secure delivery and receipt.

Each participant is authenticated using one of a number of access control methods before being allowed to perform tasks. AlphaTrust® e-Sign communicates with signers via web and e-mail 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 may be authenticated using single sign on via federated authentication or with a defined user name 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 other features not available to unregistered users. Unregistered users may either be unauthenticated, be 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 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 PDF format prior to execution, which is done automatically. Industry groups have studied their long-term requirements and concluded that the open, standard PDF formatted documents best meets the need for permanent electronic documents. The reasons are many. PDF:

1) Is an open standard.
2) Will be long lived and supported.
3) Supports data embedding and mining.

For example, the mortgage industry has a long-term archive requirement. There is concern with using proprietary formats such as Word files as to whether old file versions will be supported more than a few years out. Additionally, such formats often use "active content" technologies (which means the documents are programmable), which can cause them to be unenforceable. AlphaTrust® e-Sign natively supports and is designed with the requirements of PDF documents in mind. Additionally, the trend in government applications, such as online filing, is to accept only open document standards like PDF. So, 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 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 digital signature has 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 2019. It easily integrates with Web processes operating on UNIX, Linux, or mainframe applications using either a Web services programming interface (WS-*) or REST interface.

AlphaTrust® e-Sign is also available as a cloud service hosted by AlphaTrust. With our cloud service there is no software to purchase and AlphaTrust will manage the entire process for you.

Electronic and Digital Signatures

You have likely heard these terms used interchangeably. 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. What you must achieve with any business process that requires an enforceable document, is to obtain a legally valid electronic signature for that document using the proper 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 (for example to support EU Advanced or Qualified Electronic Signatures). 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 software will insert their signature block into the document, seal the document with a cryptographic digital signature and records 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 these:

- It wasn't me. I did not sign that document.
- 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 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 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, (standard in our SaaS service), 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.

No End User Software Requirements

One of the strengths of the AlphaTrust® e-Sign architecture is that the only user software requirement is a web browser for both a mobile and a desktop environment. 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 smartphones and tablets (Apple iOS, Android), as well as standard PC and Mac desktop and laptop computers. Adobe Acrobat® Reader v9.1 or higher is recommended for viewing signed Adobe® PDF documents but is not required for the review and signing process.

Typical Uses

AlphaTrust® e-Sign is typically integrated into web-based business process workflows to perform the function of creating legally enforceable documents including the proper gathering of electronic signatures from all parties to a transaction. The software is broadly applicable to any business process requiring documents or records in permanent form.

Summary

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

AlphaTrust offers a clear solution for meeting the challenge of EU eIDAS, VAT invoicing, ETSI technical requirements as well as other electronic record and electronic signature issues. We welcome the opportunity to work with you to meet your specific business needs.

Thank you for your interest in AlphaTrust products and services. For further information, visit www.alphatrust.com, call us at +1.214.234.9200, option 1, or send us an email at info@alphatrust.com.

Corporate Headquarters

8226 Douglas Avenue
Suite 625
Dallas, TX 75225 USA

Sales Inquiries

Phone: +1.214.234.9200, option 1
Toll Free: 866.613.7446, option 1
Email: sales@alphatrust.com

Follow Us Online

twitter.com/alphatrust

facebook.com/alphatrustcorporation

linkedin.com/company/alphatrust

AlphaTrust

Learn more.
www.alphatrust.com