



AlphaTrust PRONTO™ Server Electronic Records and Signature System

Product Overview

AlphaTrust PRONTO™ Server ERSS is server-based software that automates the creation of legally enforceable, permanent business records that are the commercial and legal equivalent of paper records, including support for electronic signatures that comply with a variety of laws and regulations around the world.

June 2009

AlphaTrust PRONTO™ Server ERSS Product Overview

Executive Summary

AlphaTrust's PRONTO™ Server Electronic Records and Signature System (ERSS) is a proven server-based software solution for managing the entire process of getting documents completed, signed, approved, routed, and stored. PRONTO™ Server ERSS can meet your document completion, execution, verification, and archiving needs for business documents requiring signature or approval (forms, contracts, documents). The PRONTO™ Server ERSS software runs entirely on a Web server and there is no requirement for end users to install any software or download any Web browser components.

Presentation and signing of documents is done using a Web Browser and, optionally, e-mail. Documents are properly signed according to law and regulations and secured using the cryptographic technology. The user's experience is simple point-and-click. Printing, signing, and shipping of signed documents are eliminated along with the significant delays caused by manual, physical routing.

PRONTO™ Server ERSS is used today by many organizations to manage their online document signing / approval processes. Production applications include: online contracting, human resource documentation, health care documentation, and financial service applications.

Background

Creating enforceable electronic transactions is a major long term initiative for enterprise and governmental organizations. Except for a few specialized markets, most business transactions are documented on paper today. The credit / debit card industry has created a method for enforceable electronic transactions using electronic networks over the last 25 years. It is effective for small value purchases. Electronic Data Interchange (EDI) exists in certain vertical markets among large enterprises.

Until 2000 there was not a method to effectively create the electronic equivalent of a binding commercial or governmental transaction that could replace paper documentation, and in many cases, the requirement for ink signatures on that documentation. Even within organizations, there are many internal processes that require documented approval, acknowledgement, or acceptance. This documentation, as well, must meet standards for accountability, enforceability, permanence, auditability, and document retention.

Business documents and records that evidence transactions have a life cycle divided into three phases:

Phase 1: Creation, collaboration and review: creating and putting a transaction record in final form.

Phase 2: Approval, acknowledgement or acceptance: creating evidence of transaction execution, often through the use of signatures or initials.

Phase 3: Distribution, storage and destruction: mailing, filing, archiving and document retention.

Much of phase 1 of the transaction record life cycle has been automated. Many transaction records are generated by automated systems such as desktop software (i.e. word processing and spreadsheet software), Web-based forms and work flow as well as mainframe systems. Some records, mostly forms, are created on paper. The move to automated systems for phase 1 records has saved businesses considerable time and money.

Phase 2, the transaction execution phase, could not be automated until the legal framework supporting electronic document and record enforceability was in place. The only alternative method was to use private, contractual systems to gain enforceability (as credit card and EDI systems have used). Over the past several years the legal framework for enforceable electronic records has fallen into place. Both statutory legislation and administrative regulations have been put in place in most developed countries (including the USA, Canada, Mexico, Japan, Singapore, Australia, New Zealand, India, Russia and the European Union as well as others) that provide for the use, acceptance, and enforceability of electronic records and electronic signatures.

AlphaTrust PRONTO™ Server ERSS provides organizations with capability for some phase 1 (form filling and completion), for all phase 2 and certain phase 3 functions. These functions include:

- Collecting information from reviewers / signers / approvers: form filling, etc.

- Obtaining proper, enforceable electronic signatures on transaction documents and records.
 - Authenticating signers (knowing who they are).
 - Applying the proper signing ceremony process rules required under laws and regulations.
- Translating documents and records into human readable formats suitable for archival, filing and document retention requirements (Acrobat PDF, HTML, XHTML, and plain text).
- Distribution of executed documents and transaction records.
- Archival and retrieval of original transaction documents and records.

AlphaTrust PRONTO™ Server ERSS is sold directly to organizations as licensed software and may be hosted by AlphaTrust as needed.

Standards Support

PRONTO™ Server ERSS is a Web-based work flow and transaction system. AlphaTrust is committed to open standards, both technical and legal/regulatory.

PRONTO™ actively supports technical standards initiatives including:

- W3C: HTML 4.01 HyperText Markup Language
- W3C: XHTML 1.0 Extensible HyperText Markup Language
- W3C: CSS Level 1 Cascading Style Sheets
- W3C: XML 1.0 Extensible markup Language
- W3C: XML Namespaces Namespaces in XML
- W3C: WCAG 1.0 Web Content Accessibility Guidelines
- IETF: PKIX PFC 2459 X.509 Public Key Infrastructure Certificate and CRL Profile
- Adobe: PDF Support for PDF 1.3, 1.4, 1.5, and 1.6 (through Acrobat 7)

PRONTO™ actively supports legal and regulatory standards including:

- USA: E-SIGN Electronic Signatures in Global and National Commerce Act
- USA: UETA Uniform Electronic Transactions Act (State law)
- USA: FDA 21 CFR 11 Electronic Signature Regulations
- USA: HHS-HIPAA HIPAA Security Standards (Proposed)
- USA: SEC / NASD Electronic Signature and Records Standards (Brokerage)
- USA: Federal Reserve/OCC Electronic Records Standards
- USA: GPEA Government Paperwork Elimination Act
- USA: Dept. of Education Standards for E-Signatures in Electronic Student Loan Transactions
- USA: DoD Support for DoD PKI and Common Access Card Program
- USA: IRS Electronic Signature Requirements
- Canada: Electronic Commerce Acts (Provincial)
- Canada: Personal Information Protection and Electronic Documents Act
- EU: ESD EU Electronic Signatures Directive (all EU Countries)
- Hong Kong Electronic Transactions Ordinance
- India Information Technology Act
- Japan Law Concerning Electronic Signatures
- Australia Electronic Transactions Act
- Singapore Electronic Transactions Act
- South Korea Basic Law on Electronic Commerce
- Others Inquire

Electronic Signature and Digital Signatures

You have likely heard these terms used interchangeably. In reality, they are very different, and the fact that both terms use the word “signature” has caused no end of 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 PRONTO™ Server ERSS 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 PRONTO™ Server uses digital signature technology in its electronic signature processes.

No End User Software Requirements

One of the strengths of the PRONTO™ Server architecture is that the only user software requirement is a Web browser. PRONTO™ Server ERSS does not require any client side software, plug-ins, Java code, ActiveX controls, or similar technology. It is designed to support wireless and PDA devices with Web browsing capabilities as well as industry standard Web browsers on personal computers

Typical Uses

PRONTO™ Server ERSS is typically integrated into Web-based business process work flow 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.

PRONTO™ Server ERSS features	Feature
Types of Transactions:	
PDF Document Form Filling	Yes
PDF Document User Data Collection (i.e. payment information)	Yes
Web form and Web document signing (HTML format)	Yes
PDF document signing (PDF format)	Yes
Online signing in current Browser session	Yes
Online signing via email notice (work flow routing for signature)	Yes
Signers per document, maximum	No Limit
Types of Signatures Supported:	
Standard Scripted (dark blue font)	Yes
Mouse signature	Yes
Live signature capture using electronic signature pad	Yes
Stored signature image	Yes
End-User digital certificate signing (client PKI support)	Yes
Types of Built-In User Authentication:	
Per signature password / PIN	Yes
Assigned User Name / Password **	Yes
Biometric authentication through handwriting analysis **	Yes
User digital certificate (SSL cert. auth.) **	Yes
Archival: Full document archive and transaction audit trail	Yes
Signature Profile Features (included with the software):	
Unique User Name and Password access per user (to protect access to signing in that user's name)	Yes
Stored image of handwritten signature used to sign documents.	Yes
Use of biometric user verification with optional signature pads.	Yes
Digital certificate (SSL client auth) access to signature profile. ESPs are not required simply to sign using a digital certificate.	Yes

System Requirements for PRONTO™ Server Software (when purchased as a software license):

Microsoft Windows Server 2003 (SP2 or higher) or Microsoft Windows Server 2008. Both 32-bit and 64-bit OS versions are supported. Microsoft Database software (SQL Server 2000 / 2005, 2005 Express, 2008 or 2008 Express). You may use an existing SQL Server in your computing environment. Dedicated hardware is not required. Virtual server deployments (i.e. VMWare) are supported.

System Requirements for Web Applications that use the Services of PRONTO™ Server Software:

Any OS (Linux, Unix, Windows, AS/400, Mainframe, etc.) that can communicate via HTTP. Communication protocols: XML over HTTP/HTTPS, XML HTTP Form POST (HTTP POST), Windows COM/DCOM.

Client (End-User) System Requirements:

Any device with a modern Web browser (Internet Explorer 6+, Firefox, Netscape 6+, Opera 7+, Apple Safari, Google Chrome). Use of optional electronic signature pads is supported on Windows (2000, XP, Vista) with Internet Explorer v6.0 or higher. Use of optional end-user digital certificates is supported for certificates and PKI software that interoperates with Microsoft CryptoAPI (requires Windows 2000, XP or Vista with Internet Explorer 6.0 or higher).

AlphaTrust Corporation

Toll Free (US): 866.613.7446 option 1

Phone: +1.214.234.9200 option 1

Email: sales@alphatrust.com, Web: <http://www.alphatrust.com>