



AlphaTrust PRONTO™ Server Electronic Records and Signature System

Transaction Processing Overview

AlphaTrust PRONTO™ Server ERSS is an electronic records and signature system 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.

This document is written for information technology and business process professionals (system analysts, system and application architects, developers) to provide an overview of PRONTO™ Server ERSS transaction processing and how it integrates into existing or new business applications.

June 2009



Table of Contents

| | |
|---|---|
| AlphaTrust PRONTO™ ERSS Product Overview | 2 |
| AlphaTrust PRONTO™ Server ERSS Transaction Processing | 3 |
| Commentary: | 5 |
| Document Format Requirements | 7 |
| Standards Support | 7 |
| Electronic Signatures and Digital Signatures..... | 8 |

AlphaTrust PRONTO™ ERSS Product Overview

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 recently 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 organizations 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 Electronic Records and Signature System (ERSS) software provides organizations with enterprise wide capability for phase 2 and certain phase 3 functions. These functions include:

- Obtaining proper, enforceable electronic signatures on transaction documents and records.
- Authenticating signers (knowing who they are).



- Translating documents and records into human readable formats suitable for archival, filing and document retention requirements.
- Distribution of executed documents and transaction records.
- Archival of original transaction documents and records.

AlphaTrust PRONTO™ Server ERSS is licensed to organizations for operation in their computing environments, or may be hosted by AlphaTrust as needed. PRONTO™ Server technology is also licensed to third party software and services companies as OEM software for inclusion in their end user software products.

AlphaTrust PRONTO™ Server ERSS Transaction Processing

All PRONTO™ Server transaction processing centers around the unit of work known as the “transaction”. Each transaction in PRONTO™ Server may have one or more documents associated with it. Each document may have one or more signatures (or seals) associated with that document. Documents submitted to PRONTO™ Server as part of a transaction are typically created by other software applications.

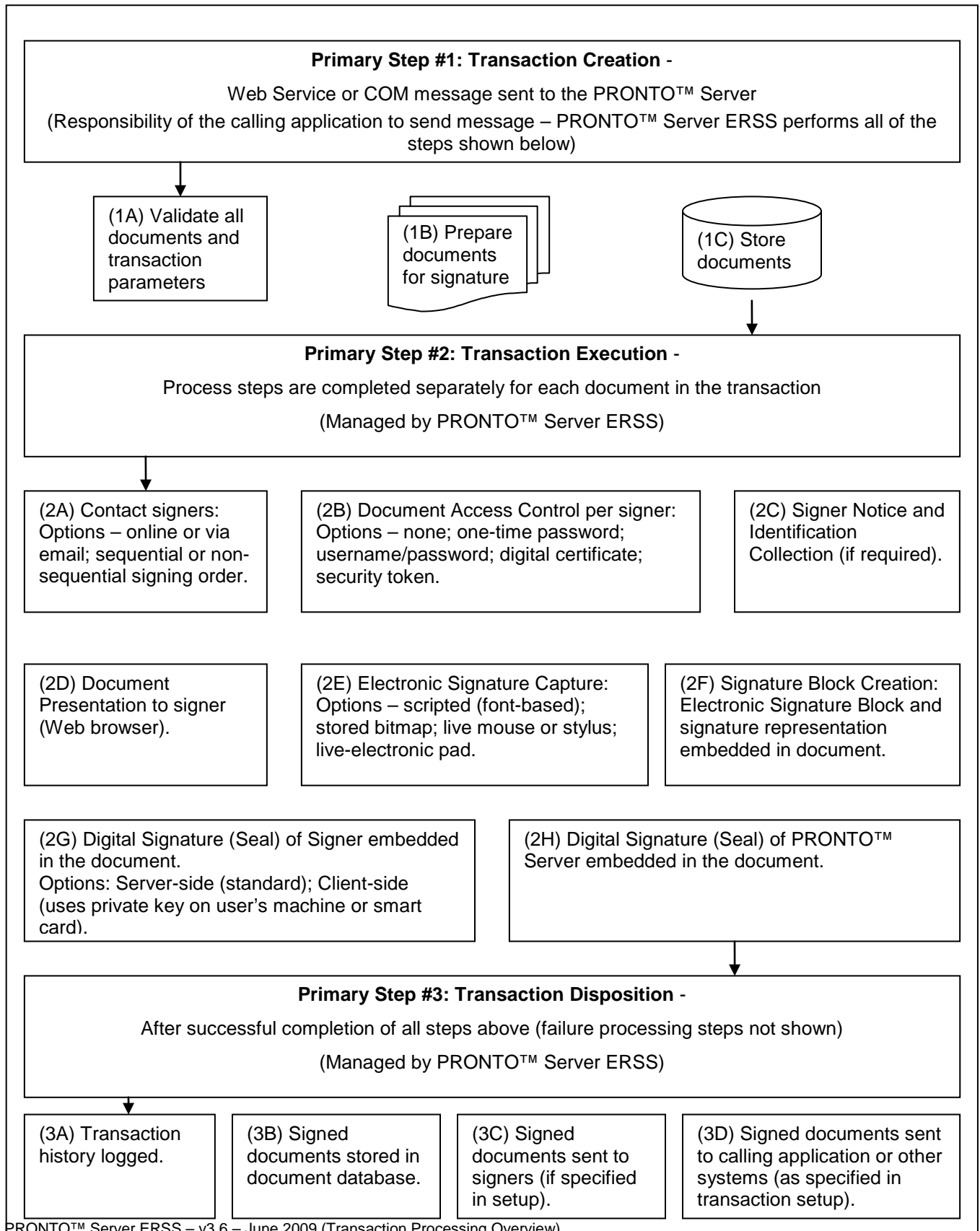
Transaction processing consists of three logical “primary steps”:

1. Transaction creation.
2. Transaction execution.
3. Transaction disposition.

In addition to transaction processing, PRONTO™ Server also supports administrative functions for user management, monitoring, reporting, logging, and accounting.

Each “primary step” has mandatory and optional “processing steps”.

The following diagram illustrates typical PRONTO™ Server transaction processing with commentary afterward:



Commentary:

- 1) Software applications communicate with PRONTO™ Server via a Web Service or COM application programming interface. PRONTO™ Server supports communication via XML over HTTP, REST, and Microsoft COM/DCOM. The XML message used to create a PRONTO™ Server transaction specifies all the parameters required for transaction completion including document information, signer information and communication methods.
- 1A) Documents processed using PRONTO™ Server are formatted as either HTML documents (HTML 3.2, HTML 4.0, HTML 4.01, or XHTML 1.0) or Adobe Acrobat® PDF documents. HTML is used to avoid the need for client side software, to meet governmental requirements for the use of open standard data formats as well as accessibility requirements for users (imposed by law and regulation). Due to advances in HTML rendering over the last several years (CSS1 / CSS2) it is usually quite easy to provide precise document layout in HTML that will meet specific formatting requirements. PRONTO™ Server validates the formatting of the document by parsing the documents submitted in the transaction and making sure they conform to processing requirements (see below). Viewing signed Adobe® PDF documents requires that users have the free Adobe® Reader (version 5 or higher is preferred) or Adobe Acrobat®. Adobe® Reader (and any other client side technology other than a Web browser) is not required to participate in any signing or other PRONTO™ Server process.
- 1B) Signature placeholders are inserted into each document at the location specified by the calling application. If no locations are specified, the signatures are added at the bottom of the document.
- 1C) Documents are stored in the PRONTO™ Server ERSS document database.
- 2A) PRONTO™ Server contacts each signer and requests that they sign their document. In the case of online users (i.e. users who have just completed a form or document and will sign immediately), the user will be enter the signing process immediately. In the case of other business processes, each signer will be contacted by PRONTO™ Server via email or via placement of a notification at a file share location. PRONTO™ Server can be configured to retry at set intervals and / or to expire the transaction after a set time.
- 2B) PRONTO™ Server supports several methods of access control (identification and authentication of signers). PRONTO™ defines two types of users: registered and unregistered. Registered users have a signature profile stored on the PRONTO™ Server. Registered users have more options available to them, such as additional access control options, and stored signature bitmaps. Registered users are typically organizational employees or members of a community of interest who use the server regularly. Unregistered users are typically casual Internet users.

Unregistered users have the following access control options: none, one-time password, and real-time authentication (requires the use of a third party data reporting service).

Registered users have the following access control options: none, user name / password, digital certificate or integration with single sign on systems.
- 2C) Signer Notice and Identification collection – some applications (such as consumer applications) require that users are informed and agree to participate in electronic transactions. Also, certain transactions may request that the user supply their name and identification information to be used in the transaction.

2D) A critical part of the signing process (a legal / regulatory process requirement) is the proper presentation of the actual document to the signer along with a request for their signature.

2E) PRONTO™ Server supports four methods of electronic signature capture (as opposed to digital signature computation) and display:

Scripted: The user's name is rendered in a blue, script-based font along with their signature block information.

Font Image: The user's name is rendered in any font available on the server.

Registered: A bitmap image of the registered user's handwritten signature is displayed using a GIF or JPG image stored in their signature profile. This requires that an image of their handwritten signature be scanned and stored in the signature profile. Otherwise, a standard signature is used.

Mouse: a Flash application is used to permit the capture of a live "handwritten" (mouse-written) signature. The PRONTO™ Server converts the captured signature into an image that is embedded in the document for display.

Signature Pad: This method captures a live handwritten signature using an electronic signature pad. In addition to capturing a picture of the handwritten signature, biometric signature information (speed, pressure, stroke, direction) is captured as well and can be used for later verification. This option requires the use of an electronic signature pad supported by PRONTO™ Server (currently SigGem or SigLite pads from Topaz Systems (www.topazsystems.com)).

2F) Once the signature is submitted by the signer, PRONTO™ Server creates the signature block and inserts it into the document (see sample below).

2G) A digital signature is computed for the document (the information displayed to the signer) and the signer's private key is used to digitally seal the document as they viewed it. Normally, signers do not possess a PKI-based digital signature key and digital certificate. In this case, the PRONTO™ Server uses its key and certificate to seal the document. The transaction can be configured to use the private key on the signer's computer (software-based or smart card-based). PRONTO™ Server currently supports client side digital signature operations on the Microsoft Windows platform using Microsoft CryptoAPI v2 operations. If you required integration with other PKI systems please contact AlphaTrust.

2H) In addition to the digital signature (seal) of each individual signer, the PRONTO™ Server also computes a digital signature (over the document and signature information) to serve as witness to the transaction and maintain document integrity over the entire transaction.

3A) PRONTO™ Server logs all transaction information and history in its SQL database.

3B) All documents are stored in the PRONTO™ Server document database in serial order by transaction number.

3C) If the transaction has been defined to send copies to signers, PRONTO™ Server will send the signers a copy of all documents in the transaction via email or Web download.

3D) The transaction may be configured to send the transaction (and signed documents) to another information system via email or the signed documents can be retrieved from the PRONTO™ Server Document database.

Document Format Requirements

PRONTO™ Server processes HTML and Adobe PDF documents. PRONTO™ Server can process HTML documents conformant to HTML 3.2, HTML 4.0, HTML 4.01 and XHTML 1.0 or PDF documents in PDF 1.3, 1.4, 1.5, 1.6, 1.7, or 1.8 formats. Documents in other formats should be converted to HTML or PDF prior to submission to PRONTO™ Server. Documents may be authored according to this specification in other data formats and using other tools, such as Microsoft Word. Documents must be saved to HTML or PDF format prior to submission to PRONTO™ Server, or use server side format conversion tools.

Standards Support

PRONTO™ Server is a Web-based work flow and transaction technology. 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, 2.0 Web Content Accessibility Guidelines
- W3C: WAI-ARIA Web Accessibility Initiative - Rich Internet Application Suite
- USA: Section 508 Rehabilitation Act (Accessibility Requirements)
- IETF: PKIX PFC 2459 X.509 Public Key Infrastructure Certificate and CRL Profile

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
- Canada: Electronic Commerce 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 Signatures 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 ERSS 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 does not require the use of any client side software, plug-ins, Java applets, ActiveX controls, or similar technology. It is designed to support wireless and PDA devices with Web browsing capabilities as well as classic Microsoft, Opera, Mozilla, and Netscape browsers on personal computers (the only exception is in the client-server PKI mode of operation, which requires Internet Explorer and an ActiveX control). If digital certificate SSL client authentication is to be used, then the Web browser must support client SSL and digital certificates must be deployed to users. Viewing signed Adobe® PDF documents requires that users have the free Adobe® Reader (version 5 or higher is preferred) or Adobe Acrobat®. Adobe® Reader (and any other client side technology other than a Web browser) is not required to participate in any signing or other PRONTO™ Server process.

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.

Further Information:

AlphaTrust Corporation
8226 Douglas Ave., Ste 625
Dallas, TX 75225
+1.214.691.2800
Email: sales@alphatrust.com
Web: www.alphatrust.com