



W H I T E P A P E R

POLICY ISSUES IN E-COMMERCE APPLICATIONS:
ELECTRONIC RECORD AND SIGNATURE COMPLIANCE

FDA – 21 CFR 11

ALPHATRUST PRONTO™ SERVER

ELECTRONIC RECORDS AND SIGNATURE SYSTEM

This white paper is written for senior executives (CEO, CFO, CIO, CTO), line of business managers, legal staff, risk management staff, technical managers and security managers involved in deploying document solutions intended to comply with US Food and Drug Administration Regulations codified as 21 CFR 11. The implications for additional compliance with other legislative initiatives such as E-SIGN (US), UETA (US), and Electronic Signature Directive (EU) are also discussed.

September 2004

Bill Brice, CEO
AlphaTrust Corporation
billbrice@alphatrust.com
(214) 691-2800

Executive Summary

Electronic records and signatures, that have the legal and commercial equivalence of paper records and handwritten signatures, promise to decrease the cost of business, increase the speed at which business is done, and add needed security to electronic business transactions. Most solutions available today are offered by technology vendors. However, due to the unique business requirements placed on legal records and signatures, business managers find that technology addresses only about 30% of the business problem.

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 law and regulation?
 - b. Enforceability of transactions using the solution (legal recourse)?
 - c. Acceptance by users of the solution?
3. Does the solution provide a mechanism for managing business risk?

These requirements have been the cornerstone of most successful electronic transactions systems such as EDI, ATM, and credit card systems.

In the case of applications seeking compliance with the FDA's requirements under 21 CFR 11, many of these requirements can't be met by technology out of the box. IT vendors can provide you with some of the tools to build your solution, but they leave you to build it.

This white paper will discuss the requirements of 21 CFR 11 section by section and demonstrate how AlphaTrust's PRONTO™ Transaction System, by addressing the technical, business process, and risk management needs of an FDA compliant application, offers the superior solution.

It is important also to look at the bigger picture. While you want a solution that will meet the requirements of 21 CFR 11, electronic records and signatures are a major shift in business processes and will affect many business applications. By mid-decade, most business knowledge workers will regularly create legal electronic records and use their own electronic signatures on a daily basis. Your solution should not just address the needs of one FDA application, but be capable of extending to meet the needs of your enterprise, supply chain, industry, and governmental requirements. AlphaTrust's PRONTO™ Server ERSS software meets these requirements today and is architected to meet even larger global requirements in the near future.

Detailed Compliance Specifications – 21 CFR 11

The table that follows details important section by section requirements spelled out in 21 CFR 11 and details AlphaTrust's PRONTO™ Server ERSS software compliance with those.

Requirement	AlphaTrust PRONTO™ ERSS
11.3(b)(7) <i>Electronic signature</i> means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	PRONTO™ Server provides the workflow rules specific to 21 CFR 11 that provide for proper acknowledgement, opt-in and authorization that satisfies these requirements as well the requirements of other major legislative and regulatory initiatives such as E-SIGN and UETA.
§ 11.10 Controls for closed systems. Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	PRONTO™ Server defines unique identities for each user and can support multiple authentication methods to create a signature. These include user name/password and digital certificate. Users communicate with PRONTO™ Server using a normal Web browser. No client software is required other than a Web browser (and optionally a PDF reader for PDF formatted documents). Any authentication method that can be supported via the Web can be used to secure access to signature creation capability.
11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Electronic records created by web applications (HTML, plain text, or PDF) can be electronically signed and stored in both human readable and electronic form.
11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	PRONTO™ Server transactions are signed, under user control, on the PRONTO™ server, logged and routed according to business rules.
11.10(d) Limiting system access to authorized individuals.	See 11.10(a) above.
11.10(e) Use of secure, computer generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	PRONTO™ Server records all transaction information in its database and can integrate with document archiving solutions. Database entries can be time stamped and digitally signed for high security needs. Operational sequencing is enforced by design and by rules.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	
11.10(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Authentication and authorization are designed into PRONTO™ Server. User authentication is per 11.10(a) above. Per transaction rules are set up to define who has access to and can sign documents, and signing order can be enforced for multi-party signatures.
11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Data input control is a function of access control. User access control is defined by the transaction and by the user database.
11.10(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	User support provided by AlphaTrust. Specific training and consultation is available.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Notices can be designed into workflow rules. User accountability is a function of business procedures.
11.10(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation.	When licensed as a software platform by an organization, PRONTO™ Server documentation is restricted under licensing agreement to those who have a need to know.
§ 11.50 Signature manifestations. (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	AlphaTrust's PRONTO™ Server ERSS software, provides for the capture and preservation of all these required data elements and meet the applicable control requirements of this section.
§ 11.70 Signature/record linking. Electronic signatures and hand-written signatures executed to electronic records shall	User electronic signatures are bound to specific documents using server-side PKI-based digital signatures. Signature linking as well as full

<p>be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.</p>	<p>document data integrity can be checked at any time, including years in the future.</p>
<p>§ 11.100 General requirements. (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</p>	<p>Each electronic signature is unique to both the user and the document. Identity information is included in the document. Each digital signature that seals the document is unique to that document and the signature keys are protected in a secure environment.</p>
<p>11.100(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.</p>	<p>Original user identification procedures are administered by the organization. PRONTO™ Server supports unique user name / password enforcement for signing operations. Digital certificate ID can also be supported.</p>
<p>11.100(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.</p>	<p>FDA certification is provided by the system operator. User acknowledgement of legal enforceability is part of the user registration rules enforced by the system.</p>
<p>§ 11.200 Electronic signature components and controls. (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine</p>	<p>User access procedures are outlined above in 11.10(a). User access rules meet the requirements of this part.</p>

owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	
11.200(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Biometric authentication to PRONTO™ Server can be supported via biometrically activated digital certificates or using a signature pad with signature dynamics capabilities.
§ 11.300 Controls for identification codes/passwords. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	User name, password and other token uniqueness are enforced by the PRONTO™ Server system.
11.300(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	A function of PRONTO™ Server processing rules. Passwords can be set to require changing after a defined period.
(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Replacement access control credentials are a function of business procedures.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Access control rules can be set to lock out failed attempts to access the system and to send notification.
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	If user tokens or cards are used as access control devices, they should be tested periodically by the organizations using them.

Summary

AlphaTrust's PRONTO™ Server ERSS software is designed from the ground up to meet the historically demonstrated requirements for technical security, transaction enforceability, legal and regulatory compliance and risk management. Significant value delivered by AlphaTrust is in the non-technical arena – proper user management, system, and operational procedures, legal and regulatory compliance, and risk management.

AlphaTrust is the clear solution for meeting the challenge of FDA, UETA, E-SIGN and other electronic record and electronic signature requirements. AlphaTrust's products can function effectively in the complete absence of statutory support for electronic signatures via AlphaTrust's private Member Agreement system. We welcome the opportunity to work with you to meet your specific requirements.