21 CFR Part 11 Solutions for Domino and Notes

How Secur*Trac* and Secur*Esign* Help to Enable Compliance?

DOC ID SEWPCFR211103

Disclaimer

THIS DOCUMENTATION IS PROVIDED FOR REFERENCE PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS DOCUMENTATION, THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER AND TO THE MAXIMUM EXTENT PERMITTED, IBM DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SAME. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, DIRECT, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS DOCUMENTATION OR ANY OTHER DOCUMENTATION. NOTWITHSTANDING ANYTHING TO THE CONTRARY, NOTHING CONTAINED IN THIS DOCUMENTATION OR ANY OTHER DOCUMENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENT GOVERNING THE USE OF THIS SOFTWARE.

List of Trademarks

Domino, Domino Designer, Lotus, Lotus Notes, LotusScript, and Notes are trademarks or registered trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both. Java, JavaScript, and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
All other trademarks are the property of their respective owners.

Contact for More Information

This paper has been provided by Extracomm Inc.

Extracomm Inc.
Suite 201, 100 Mural St
Richmond Hill, Ontario
L4B 1J3
www.extracomm.com
Voice: (905)709-8602

Table of Contents

A. Introduction

21 CFR Part 11 is a Food & Drug Administration (FDA) regulation, enacted in 1997, which covers electronic records/electronic signatures when used for FDA regulated activities. Part 11 describes the process for creating, modifying, maintaining, archiving, retrieving, and transmitting electronic records, and the use of electronic signatures when complying with the Federal Food, Drug, and Cosmetic act or any other Food and Drug Administration regulation. The focus of this regulation is to ensure the integrity, trustworthiness/reliability, traceability, and accountability of a company's record management process.

Examples of companies affected by this regulation include those who produce pharmaceuticals, color additives, food additives, livestock feed, medical devices, and who convey food. Domino provides the tools to help administrators and system/application designers to create applications that meet the compliance requirements.

The purpose of this paper is to provide technical guidance to our customers who are building or modifying applications that may be used as part of the compliance process. The focus of this paper is on Domino as an application development platform with the Notes client. The instructions and guidance within this document highlight SecurTrac Electronic Signature Module and options available within Domino to assist our customers in building compliant and secure applications for their environment.

The intended audiences for this paper are system administrators who manage the systems, and system/application designers who develop applications. We expect that administrators and designers already will be familiar with the 21 CFR 11 requirements and how they apply to their company's procedures. For additional information on Domino Designer and Domino security, go to the Lotus Developer Domain (formerly Notes.Net) at http://www.lotus.com/ldd. This paper includes the text of the 21 CFR 11 regulation, identified by lines around the text. Sections 11.1 through 11.3 are informational sections, which are provided to assist in understanding the scope, implementation, and definitions used in the 21 CFR 11 regulation.

Note: Other technologies such as Web-based access are also available but, when dealing with the Web, developers need to be aware that browsers have fewer capabilities and design options than Notes clients. In particular, browsers do not yet support digital signatures and document-level encryption. These limitations may make things more challenging for the designer of the application.

Important: Content of this paper has been sourced from Lotus Software White Paper “21 CFR Part 11 Requirements for Domino and Notes” January 2003. Secur*Esign* is the implementation of the recommendations in the paper. Secur*Esign* is designed to assist regulated companies meet the strict requirements of Part 11.

B. Compliance Summary Chart

This following chart is intended to provide a summary of the key points in interpreting parts of 21 CFR pertaining to electronic signatures and records.

In the chart there is mention of two products. Each product functions independently, but when used together they can be part of a complete compliance enabling solution:

Secur*Trac* – generates detailed audit records such as data changes, signature histories

- Database monitoring including data, design, ACL (security information)
- Domino Directory Monitoring
- Mail monitoring – all attributes
- Notes.ini file monitoring
- Intrusion Detection for applications that complements your existing network security
- Real-time monitoring and alerts

Secur*Esign* – generates electronic signatures based on Notes.id

- Quick design element application to database
- Utilize proven authentication approach – Notes.id
- LotusScript configuration of specific values
- Reason for change comments attached to signature

Part 11 Requirements	How Secur*Esign* / Secur*Trac* Enables Compliance
Sec. 11.1 Scope (a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. (b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means. (c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997. (d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required. (e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	This section of the 21 CFR Part 11 regulation is included here for reference.

Sec. 11.2 Implementation (a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met. (b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that: (1) The requirements of this part are met; and (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	This section is included here for reference.

Sec. 11.3 Definitions (a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. (b) The following definitions of terms also apply to this part: (1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). (2) Agency means the Food and Drug Administration. (3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. (4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. (5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. (7) Electronic signature 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. (8) Handwritten signature means the scripted name or legal mark of an	**Digital signatures** In Domino and Notes, digital signatures are secured by cryptographic means. Signatures are created with the private key from a user's Notes ID. The assignment of a digital key in a Notes ID is a unique public/private value. (A Notes ID contains encryption keys and certificates that Domino uses to verify the authenticity of a file.) Signatures are stored in documents along with the public key and a list of certificates from the sender's ID. Secur*Esign* is based on and utilizes Domino's and Notes well-proven electronic signing function to create electronic signatures.

individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. (9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	
Sec. 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.	**Digital signatures in Notes applications** Lotus Notes/Domino has the ability to track any alterations/changes by dates and digital signatures. Notes uses digital signatures as defined in Section 11.3(5). Additional requirements such as Section 11.100(a) require uniqueness of the name. Section 11.50 "Signature manifestations" requires additions to the record that must be supplied by the application, such as the role of the signer. <u>Uniqueness of the name</u> **Secur*Esign*** programmatically creates a unique number based on the hash of the public key in the ID file. Example: Signed By: CN=Alex Chan/O=Extracomm : *0345ED9E7C6338AE5E905831FE9193A4* Where *0345ED9E7C6338AE5E905831FE9193A4* is the 128bit MD5 hash of the user's public key, which is unique for any individual. <u>Ensure the authenticity, integrity and non-repudiation</u> An electronic signature verifies that the person who originated the data is the author and that no one has tampered with the data. As part of the database design, the database designer can determine whether or not users can sign fields, and whether or not sections of a database can be signed. Designer combines the data in a signature-enabled field with the private key from the sender's user ID to create a unique electronic signature. Designer stores the signature, along with the public key and the list of certificates from the sender's ID, in the document.

	Databases can be designed to enable signing of one or more fields on a form. Designer can easily control what fields to be signed by setting the field names into the Secur*Esign* Control field SCTFieldToSign. Setting SCTFieldToSign to null means all fields will be signed. In addition, designer can easily turn on or turn off the signing function by setting the Secur*Esign* Control SCTSign to "1" or "0". **Note:** Secur*Esign* is compatible with existing document Notes Section signatures. Example of signature verification 1. Mary saves a **Secur*Esign***-enabled document. **Secur*Esign*** uses the private key from Mary's User ID and the specified field data to create a unique signature. **Secur*Esign*** also stores Mary's public key and certificates with the signed document to read it. David must document. 2. David opens the have read access to the document. 3. SecurEsign checks to see if the document was **Secur*Esign*** signed. If it was, **Secur*Esign*** checks the signature against the data to see if it matches. 4. **Secur*Esign*** checks the certificates that came from Mary's ID against David's ID to see if they share a common certifier or cross-certificate in the ID. 5. One of the following occurs: • If the signature and data are verified, displays a message indicating who and when signed it. • If the data has been modified, Notes displays a message indicating that the document has been changed or corrupted since Mary saved it. David should not assume that the content of the document is what Mary created. • If the signature can't be verified or David and Mary don't share a common certificate, **Secur*Esign*** displays a message that the signature can't be verified. David should not assume that Mary created the document. Ensure confidentiality Employ Notes security • Server Access Control • Database Access Control • Document Access Control • Section Access Control • Field encryption

(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. (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Secure storage and record retention policies must be part of a customer-defined standard operating procedure.
(d) Limiting system access to authorized individuals.	Secure storage and record retention policies must be part of the customer-defined standard operating procedure. Employ Notes security • Server Access Control • Database Access Control • Document Access Control • Section Access Control • Field encryption to ensure only authorized individuals can access the system.
(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.	Secur*Trac* generates detailed field-level audit trail on document Open/Update/Create/Delete. On action Update, Secur*Trac* will also capture the before and after image of the field value. The audit trail retention policies must be part of the customer-defined standard operating procedure.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Formula, LotusScript, Java, and JavaScript code provide an integral programming interface to Lotus Domino Designer. You can attach code to various design elements to perform operational system checks.
(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.	Secur*Trac* provides full audit trail to the systems. Security officer or Notes administrators can perform periodic authority checks to look for misuse and then remedy or refine access control of the systems. This is a customer-defined standard operating procedure.

(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.	This is a customer-defined standard operating procedure.
(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.	This is a customer-defined standard operating procedure.
(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.	This is a customer-defined standard operating procedure.
Sec. 11.30 Controls for open systems Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	• Employ Notes field encryption or Document encryption to ensure confidentiality. • Employ Secur*Esign* to ensure record authenticity and integrity.

(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).	Following is a typical example of electronic signature section showing in the Notes document. Example: **Signature:** AD68228DEDFB6011255B83EB4DCCBF7C **Signed Fields:** Form; From; AbbreviateFrom; AltFrom; AltLang; ThreadId; Remote_User; MainID; AbrFrom; Body; readers; NewsLetterSubject; Path_Info; Subject; Categories; WebCategories; $SCTFieldSigned; $SCTSigner; $SCTSignSectionTime **Signed By:** CN=Alex Chan/O=Extracomm : 0345ED9E7C6338AE5E905831FE9193A4 **Signed At:** 03/27/2003 05:51 PM ZE8 Where **Signature** is the electronic signature of the signed fields. **Signed Fields** lists out all the fields in the document that are signed. **Signed By** lists out the name of the signer and the hash value of his/her Notes public key **Signed At** lists out the date time of the signing. Lastly, when the document is signed, it can optionally prompt for the reason for change. (This is application controllable.) This electronic signature section is readable and printable.
Sec. 11.70 Signature/record linking Electronic signatures and handwritten signatures executed to electronic records shall 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.	**Signature protection** The product is built based on cryptographic best practices for signatures. This implementation links the signature with the digital bits in the document. A change of even one bit in the document signed invalidates the signature. The product provides no ability to cut and paste signatures. The cryptography of the signature would fail even if someone somehow managed to copy a signature.
Sec. 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.	The assignment of a digital key in a Notes ID is a unique public/private value. The customer policy must have processes to limit this to a single individual.

(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.	This is a customer policy requirement.
(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.	This is a customer policy requirement.
Sec. 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.	Two distinct identification components: • Notes ID file • Notes 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.	First signing requires both Notes ID file and password to execute. Subsequent signings requires also both Notes ID file and password to execute. Secur*Esign* can force user to sign-on (input password) every time when the user changes/saves a document.

(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.	Signing always requires both Notes ID file and password to execute.
(2) Be used only by their genuine owners; and	This is a customer policy and training requirement.
(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.	If customer policy allows “anyone other than its genuine owner” to sign document, Notes can assign multiple passwords to those IDs. Using multiple passwords requires that a group of administrators, rather than one person, work together to access an ID. You also can specify that only a subset of the assigned passwords be required to access the ID.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	This requirement does not apply to Notes/Domino. Notes/Domino does not distinguish between devices used (for example, biometric devices, smartcards, etc.). Password recommendations apply independently of access method.
Sec. 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.	The ID file assigned to the user is unique. No two individuals have the same public keys. As a result, Identification codes = ID file = <User Name> + <Hash of Public Key> is unique for any individual.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The Domino Administrator provides options for password checking, expiration of passwords, etc. For more information, see the chapter "Securing and Managing Notes IDs" in Administering the Domino System, Vol. 2.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate	When an identification token (a Notes ID) is deauthorized, the public key is removed from the Domino Directory, which prevents a user from using the ID file. The document with valid signatures remains in the system and can still be audited. This would be done as part of the policy defined by the customer.

identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	
(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.	The administration interface using the password management facility can set a value to 'lock out' the ID file on a per-user basis. Messages are logged to the server console when someone tries to access a server to which they do not have access. Administrators can set up Event Handlers to record the occurrence of these events.
(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.	This is a customer policy requirement.

C. Login/Password Options – Electronic Signatures

There are various scenarios for setting up logins for accessing electronic resources. Having multiple levels of access adds additional security and authentication for applications that are to be compliance enabled.

Authentication Types	Description
Workstation Operating System User Login (Local Workstation Login Authentication)	- The workstation operating system (OS) has a login and password that may be configured to allow access to the workstation. The desktop OS must be certified and have suitable authentication capabilities.
Server Network Operating System User Login (Network Login Authentication)	- The network operating system user login allows individuals to login to access server and other network resources.
Notes/Domino System User Login (notes.id) (Notes Login Authentication)	- The notes.id is used to provide client access to Notes (controlled by Domino) - Secur*Esign* can use this login and password to generate electronic signatures for electronic records.
Notes Application User Login (Authentication controlled by Notes/Domino and **Secur*Esign***)	- A notes.id is used to provide client access to a specific application or group of applications. - Secur*Esign* is used to enable authentication in to the application and generating of electronic signatures/records.)

Scenarios of Use for Access and Electronic Signatures

With single sign-on logins it is possible to provide a single login/password for workstation to application access.

In order to increase security and deter unauthorized access, multiple logins and passwords may be used The following scenarios provide some possible options for authentication:

Scenario One:
- RS Company has single sign-on to the workstation, network and into Notes.
- The notes.id (login, password) is used for application access as well.
- Secur*Esign* will prompt the user to re-authenticate with their notes.id upon opening or saving actions on the database application. (electronic signature generation for the application).

Scenario Two:
- SR Company has a single sign-on login for workstation and network access.
- When launching Notes, the user must authenticate to the notes.id in order to access Notes and the applications.
- The notes.id may be the same login name as workstation/network access but a different password, or the login and password may be totally unique form the workstation/network access login and password.
- Secur*Esign* will prompt the user to re-authenticate with their notes.id upon opening or saving actions on the database application. (electronic signature generation for the application).

Scenario Three:
- TR Company has a login/password for access to the workstation
- A separate login/password is required for network access.
- When launching Notes, the user must authenticate to the notes.id in order to access Notes and the applications.
- Secur*Esign* will prompt the user to re-authenticate with their notes.id upon opening or saving actions on the database application. (electronic signature generation for the application).

Scenario Four:
- Any combination of single or multiple logins are provided to get access to workstation, network and Notes.
- A separate notes.id (login, password) must be authenticated to access a specific application.
- Secur*Esign* will prompt the user to re-authenticate with their notes.id upon opening or saving actions on the database application. (electronic signature generation for the application).

The Management Issue

Managing logins/password and signatures can be a time consuming task. This is particularly true if multiple logins/passwords are used as several administration tools may be needed to be to create and update items.

With **Secur*Esign*,** administration of logins/passwords and signatures are managed consistently. The Domino Administrator tools are used to manage logins/passwords and signatures. No external software, databases or tools are needed.

The advantages of utilizing a Notes based solution includes:
- No learning curve for administration
- Quick implementation on any application
- No external non-Notes databases or compliance applications to manager and monitor
- Significant time and cost savings

D. Summary:

Secur*Esign* utilizes notes.id cryptology and a proven signature and record approach.

Secur*Esign* will also complement **Secur*Trac***. **Secur*Trac*** provides a full audit trail for data changes, electronic signatures and more.

Through the implementation of **Secur*Esign*** and **Secur*Trac***, electronic signatures/records and auditing compliance can be enabled quickly and cost effectively.

New and existing applications can have signatures and data tracking added consistently providing instant scalability.

All records and management are kept within the Domino environment eliminating the need for non-Notes solutions.