



White Paper Series

Addressing FDA CFR 21 Part II Compliance

Date: February 23, 2005
Rev 2.5

Information in this document is subject to change without notice and does not represent a commitment on the part of Ingenuus Software Inc.

Copyright © 2003-2005 Ingenuus Software Inc. All rights reserved. This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording storage, in an information retrieval system, or otherwise, without prior written permission of Ingenuus Software Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the government is subject to restrictions as set forth in sub-paragraphs (C) (1) (ii) of the rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and 48 CFR 52.227-19.

The product described in this White Paper may be protected by one or more U.S. patents, foreign patents, or pending applications.

Trademarks

Ingenuus, Ingenuus Smart Expediter, Power of the Process, Integration Gateway, Integration Gates, Task Flows, and Solution Suites are trademarks or registered trademarks of Ingenuus Software Inc. in the United States.

All other trademarks or registered trademarks are the property of their respective owners.

This publication is provided “AS IS” without warranty of any kind, either express or implied. All warranties, including, but not limited to, the implied warranties of merchantability fitness for the particular purpose, or non-infringement are specifically disclaimed.

This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. These changes will be incorporated in new editions of the publication. Ingenuus Software Inc. may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Table of Contents

Table of Contents	3
Introduction	4
FDA Rule – 21 CFR Part 11.....	4
Ingenuus Solution Suites	4
Addressing The Requirements of 21 CFR Part 11	5
Subpart B – Electronic Records	5
Section 11.10 Controls for Closed Systems	5
Software development methodology, processes and standards	12
Section 11.30 Controls for Open Systems	13
Section 11.50 Signature Manifestations	13
Section 11.70 Signature/Record Linking.....	14
Subpart C – Electronic Signatures.....	14
Section 11.100 General Requirements	15
Section 11.200 Electronic Signature Components and Controls	15
Section 11.300 Controls for Identification Codes/Passwords.....	16
Summary	17
Revision History.....	18

Introduction

The requirements in 21 Code of Federal Regulations Part 11 (21 CFR Part 11, or Part 11) set forth the criteria under which the Food and Drug Administration (FDA) 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 on paper. It applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements in agency regulations.

One major problem with these criteria is that they do not specify the scope of each requirement with regard to the different areas under FDA purview. As a result, every organization affected by Part 11 attempts to interpret the regulations to determine how they are affected. This white paper provides a brief description of the requirements imposed by Part 11 in the context of Ingenuus' Smart Expediter.

As with any other write-up on Part 11, this paper describes Ingenuus' interpretation of the regulations and is provided for general information purposes only.

FDA Rule – 21 CFR Part 11

21 CFR Part 11 has been in effect since August 1997 and establishes the FDA's requirements for electronic records and electronic signatures to be trustworthy, reliable, and essentially equivalent to paper records and handwritten signatures.

Part 11 applies to all FDA program areas, but does not mandate electronic record keeping. Part 11 describes the technical and procedural requirements that must be met if an organization chooses to maintain records electronically and use electronic signatures. Part 11 applies to those records required by an FDA predicate rule and to signatures required by an FDA predicate rule, as well as signatures that are not required, but appear in required records.

Organizations who choose to use electronic records must comply with this rule for those records covered by FDA regulations. To fully comply with the rule it is important for an organization that uses electronic records and electronic signatures to have and to apply Standard Operating Procedures (SOP's) that support and complement software functionality.

The rule contains two major sections: one that addresses requirements for electronic records (Part 11 Subpart B) and one for electronic signatures (Part 11 Subpart C). Electronic records are defined as "any combination of text, graphics, data, audio, pictorial, or other information in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."¹ The rule applies to any records covered by FDA regulations that exist in an electronic form – including records that are required to be maintained whether they are submitted to the FDA or not. Electronic signatures are defined as "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."²

The determination of whether to use an electronic signature is up to the individual organization.

Ingenuus Solution Suites

Ingenuus Software Inc. is the technology leader in affordable, enterprise class process automation solutions. Ingenuus' Web-based Task Flows™ and Solution Suites™ provide families of automated business processes that coordinate execution between various processes and databases. All the Ingenuus Solution Suites meet the 21 CFR Part 11 requirements as outlined in this white paper because all of the

¹ Federal Register / Vol. 62, No 54 / Rules & Regulations / Part 11, Section 11.3 (6) Electronic Record

² Federal Register / Vol. 62, No 54 / Rules & Regulations / Part 11, Section 11.3 (7) Electronic Signature

Solution Suites are built utilizing the Ingenuus Smart Expediter™. It is the Smart Expediter that meets the 21 CFR Part 11 requirements and as such, is what is referred to in this document.

Addressing The Requirements of 21 CFR Part 11

The table below summarizes how Ingenuus' products and services cover the requirements of Part 11:

21CFR Part 11 Section Number	Solution Suite Support	Comments
Subpart B		
Closed Systems		
11.10 (a) Validation	-	SOP Development
11.10 (b) Inspection	Current	
11.10 (c) Protection	Current	
11.10 (d) Security	Current	
11.10 (e) Audit	Current	
11.10 (f) Operational	Current	
11.10 (g) Authority	Current	
11.10 (h) Device	Current	
11.10 (i) Personnel	-	<i>Ingenuus audit</i>
11.10 (j) Policies	-	SOP Development
11.10 (k) Documentation	-	SOP Development
Open Systems		
11.30 Authenticity	Current	
11.30 Integrity	Current	
11.30 Confidentiality	Current	
11.30 Digital Signature	<i>Future</i>	
Signature Manifestations		
11.50 (a) Signing	Current	
11.50 (b) Display/print	Current	
11.70 Linking	Current	
Subpart C		
Electronic Signatures		
11.100 (a) Uniqueness	-	SOP Development
11.100 (b) Verification	-	SOP Development
11.100 (c) Certification	Current	
11.200.1 (i) Signature	Current	
11.200.1 (ii) Signing	Current	
11.200.2 Identity	Current	
11.300 (a) Uniqueness	Current	
11.300(b) Passwords	Current	
11.300 (c) Lost codes	Current	
11.300 (d) Attempts	<i>Future</i>	
11.300 (e) Devices	<i>Far out</i>	

The following sections outline the FDA's requirements for electronic records and electronic signatures and how Ingenuus addresses each requirement with its products and services.

Subpart B – Electronic Records

Section 11.10 Controls for Closed Systems

This section outlines controls that must be in place for “closed systems,” defined as an environment in which the persons who are responsible for the content control system access. An example of a closed system would be an information system that is contained within an organization's local area network or Intranet. These controls require that “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.” The following are the specific requirements of Section 11.10 and how the Smart Expediter addresses these requirements:

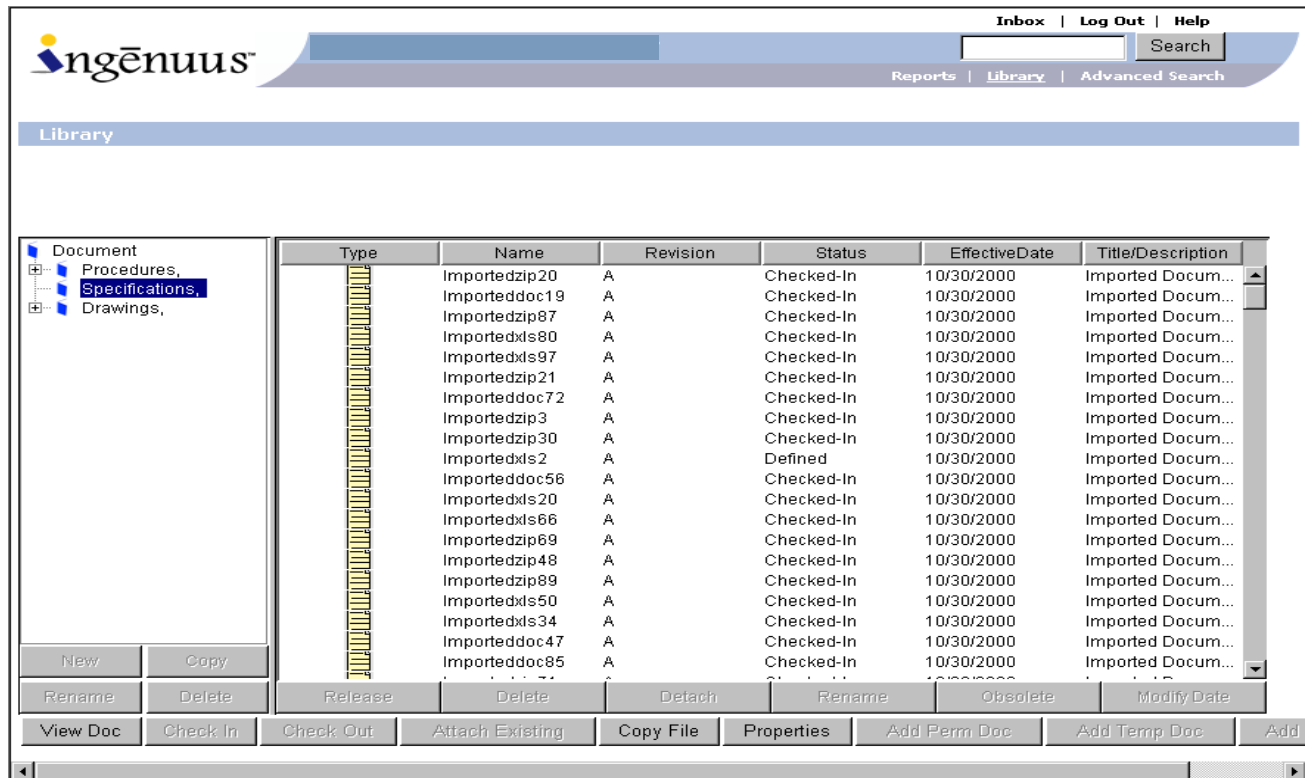
(a) Requirement: Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

In deploying the Smart Expediter an organization should implement policies and procedures that include a periodic audit of the production system to ensure accuracy, reliability and consistent intended performance in the installed, active environment. Ingenuus can provide services to assist in the development of policies and procedures as well as in system configuration to ensure that the system is set up correctly and used in a way that complies with this ruling.

The Smart Expediter provides a comprehensive auditing function that tracks creation, modification and deletion of records identifying both user and date of action. No alteration to records can be accomplished without an audit trail entry being created.

(b) Requirement: 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.

The Smart Expediter stores unstructured records (i.e., documents or files) in their native format as binary objects, which can then be individually opened using an application that was used for their creation or using another application that can view their content.



The Smart Expediter stores structured records in a secure database. This structured data can be viewed via the forms used to enter and review the data or via printable reports as illustrated by the screens below:

Inbox | Log Out | Help

Manufacturing Change Manager Search

Reports | Library | Advanced Search

Number: 01-0072 Title: Status: In Progress

General
Description Of Change
Revised Items

Materials Disposition
Revised Documents
Attachments

Dates
Audit Trail
Where Used

<p>Type: <input type="text" value="Hardware"/></p> <p>Priority: <input type="text" value="Standard"/></p> <p>Class: <input type="text" value="I (Major)"/></p> <p>Originator: <input type="text" value="ADMIN"/></p> <p>Resp Eng: <input type="text" value="Susan"/></p>	<p style="border: 1px solid #ccc; padding: 2px;">Factories Affected</p> <p style="border: 1px solid #ccc; padding: 2px;">NYMFG TXMFG</p>	<p style="border: 1px solid #ccc; padding: 2px;">Reasons For Change</p> <p style="border: 1px solid #ccc; padding: 2px;">Cost Reduction Customer Request Design Correction Document Correction Enhancement</p>
--	--	--

Company Name			
Engineering Change Order Report			
Title: Testing Bug			
Run By:	Admin	Date and Time:	07/17/2001 16:42
ECO No:	01-0009	Priority:	Urgent
Originator:	Josh Schlotterer	Status:	Defined
Responsible Engineer	Dan Christy	Type:	Design
Class	YES		

Key Dates	
Origination Date:	05/30/2001
Approval Date:	
Released Date:	
Cancellation Date:	

Factories Affected
<ul style="list-style-type: none"> • EF

Reason for Change
<ul style="list-style-type: none"> • Cost Reduction

Description of Problem
testing a bug

FDA staff can be given secure read-only access to the system to review and inspect records as appropriate. In addition to the structured and unstructured records, access would include any associated system metadata such as the owner, permissions, and audit trail events. All unstructured records can be exported and provided to the Agency as requested, either as documents in their native forms or as PDF. Structured records can be exported and provided to the Agency in HTML format.

(c) Requirement: Protection of records to enable their accurate and ready retrieval throughout the records retention period.

An organization should develop policies and procedures covering record retention. The specific rules for deletion and purging should be included in the policy. Ingenuus can provide services to assist in the development of these policies and procedures as well as in system configuration. Platform and environment specific backup and recovery scenarios can be provided and customized as necessary.

The Smart Expediter does not contain any specific archiving mechanism. Instead, all records are available for ready retrieval until they are actively deleted. This includes both the records themselves and associated metadata. In the Smart Expediter an unlimited number of revisions of a specific object is retained.

(d) Limiting system access to authorized individuals.

The Smart Expediter requires a login name and password in order to gain access to the Solution Suite applications. When the user chooses their password, it is encrypted using a one-way algorithm and stored in the database. During login, the Smart Expediter verifies the password entered. It encrypts the password using the same algorithm and compares the encrypted password with the stored version. The encrypted password cannot be decrypted.

The system Administrator is normally responsible for setting up user access. An organization should implement policies and procedures that control the circumstances under which system access is granted. At any point in time each combination of login name and password is unique within 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.

The Smart Expediter tracks all changes made to a *Released* record. Field level changes to draft records are not tracked. However, all events that move a draft record from one step in its lifecycle to the next are tracked.

The screenshot shows the Ingenuus software interface. At the top, there is a navigation bar with 'Inbox | Log Out | Help' and a search box. Below this, the record details are displayed: 'Packet: ECO' with a 'Go!' button, 'Number: 01-0072', 'Title: replace screen', and 'Status: In Progress'. A central menu contains several options: General, Materials Disposition, Dates, Description Of Change, Revised Documents, Audit Trail, Revised Items, Attachments, and Where Used. On the left, there is a vertical list of actions: Approve, Reject, Release, Cancel, Send, Save, Report, Set Notification, Set Participant, and View Comment. At the bottom, an 'Approvers' section is visible, with a radio button selected for 'All:'. Below this is a table with the following data:

Recipient	Department	Task	Action	Time In	Time Out	Hours	Comments	Escalated
ADMIN		ECO Originator	In Progress	6/7/2001		163.13		
ADMIN		ECO Originator	In Progress	6/7/2001		163.13		
ADMIN		ECO Originator	In Progress	6/7/2001		163.13		
ADMIN		ECO Originator	In Progress	6/7/2001		163.10		

The audit trail event records cannot be modified or deleted from the system. Most audit trail data can be mined using external report writing tools.

- Item Info
- View EC
- Back

Revision History

Item Number: 151-0000 Revision: A
 Description: Palm Device B

<input checked="" type="checkbox"/>	Old Item Number	Old Rev	New Item Number	New Rev	EC No.	Description Of Change
<input type="checkbox"/>	--	--	151-0000	A		
<input type="checkbox"/>	151-0000	A	151-0000	42bc4	01-0054	replace screen
<input type="checkbox"/>	151-0000	A	151-0000	3e048	01-0012	replace screen
<input type="checkbox"/>	151-0000	A	151-0000	B	01-0072	replace screen
<input type="checkbox"/>	151-0000	A	151-0000	3f952	01-0026	replace screen

In the Smart Expediter, a *Released* record is never updated in place. A new draft revision is automatically created before the record can be updated. However, a user with the appropriate privileges can update metadata associated with a Released record. Typically, such privilege will

Approve ECR: 01-0054

- Send
- Cancel

Comment:

Verify Password:

Approvals:

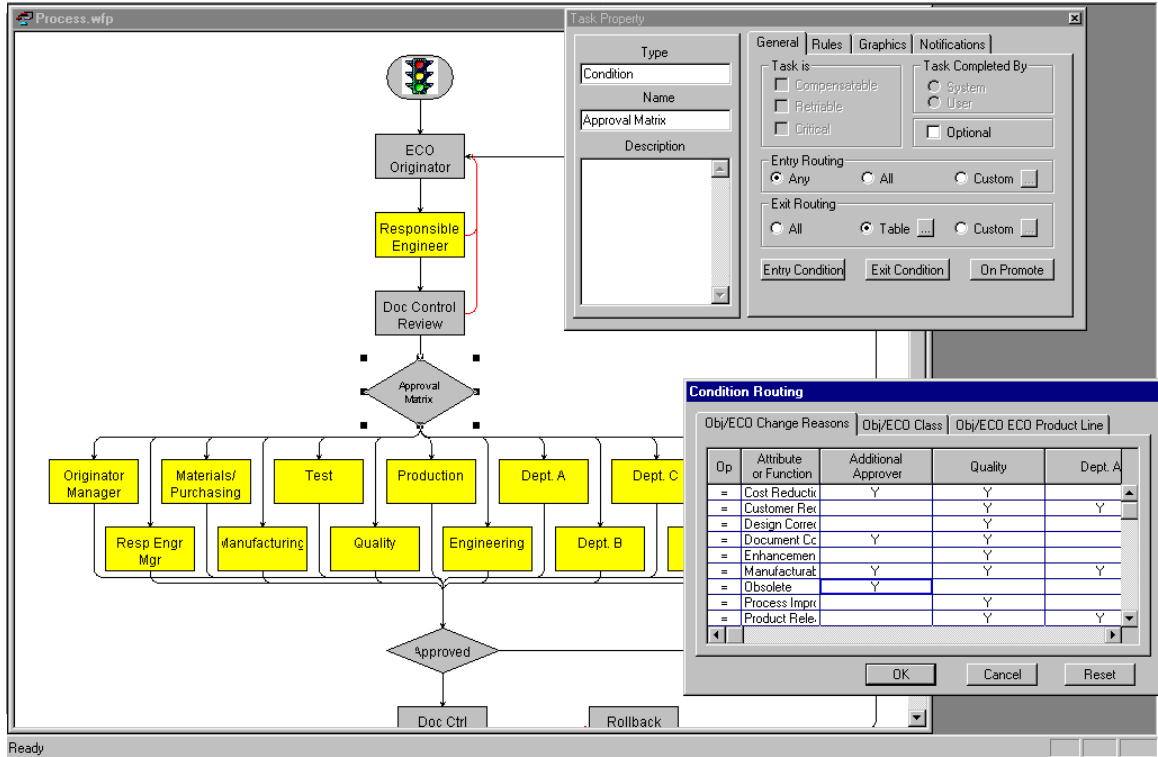
Department	Task Name	Approver	Date	Status
	Originator's Manager	ADMIN		

only be assigned to select administrative personnel in the organization. Ingenuus can provide services to assist in developing policies governing permissions and authorities of the users of the Smart Expediter within the organization.

(f) Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.

The Smart Expediter is primarily a stateless system in that it does not enforce a strict sequence of events. A user can begin a fetch function and abandon it before completion. In the Smart Expediter it is the responsibility of the user to ensure that each function is completed to their satisfaction.

For record lifecycle management, the Smart Expediter provides a powerful Task Flow engine that ensures strict enforcement and deterministic sequencing of events. As each step in the Task Flow is started the appropriate task is created for the users or roles involved and added to their *Inboxes*. The tasks for the next steps in the Task Flow are not created until the previous step is complete. In some cases a Task Flow step can reference a group of users, each of whom gets an assigned task. The Task Flow designer can select whether one or all users need to complete their tasks before this step is deemed complete. If the Task Flow designer wants to have a more exotic condition, the Ingenuus Flow Designer™ provides comprehensive user programmability of the flows.

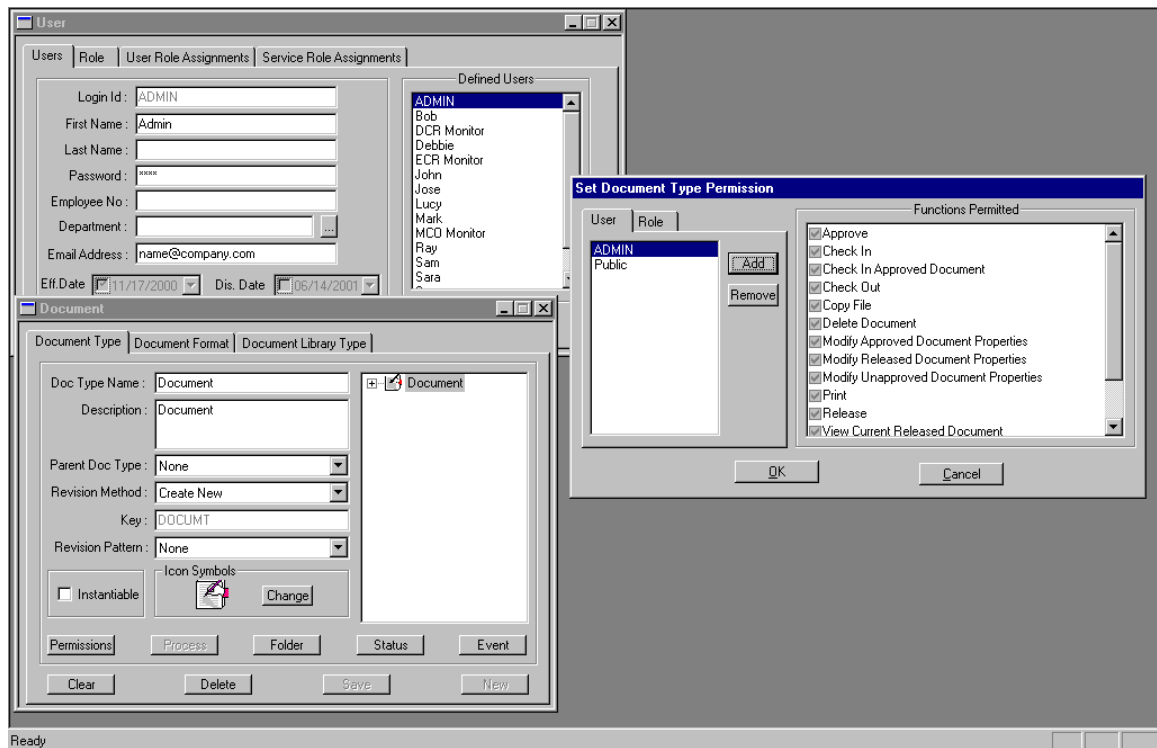


(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

The login name controls every operation executed within the Smart Expediter via permissions and authorities. The Smart Expediter allows a user access to records based on permissions set up by the Smart Expediter administrator. Enabling only the permitted action buttons imposes further access controls.

Each record has multiple levels of permissions and authorities forming a complex and comprehensive access control scheme.

All Approve/Reject/Cancel actions in a Task Flow require the user to enter a comment that gets logged in the audit trail. Also, the user identity is verified by a required password re-entry.



(h) Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

When a user logs-in to the Smart Expediter Inbox an encrypted "cookie" is created and saved by the web browser on that users personal computer and retained until the browser is closed. This cookie is presented to the web server as identification each time the user clicks a link during the session. The web server decrypts the cookie and it is used by the Smart Expediter to verify the login name and password and to check what permission that user has for each object. The Smart Expediter enforces inactivity timeout, which is set by the administrator. The Smart Expediter has a configurable, hierarchical inactivity timeout setting by user/role in addition to a global timeout.

Organizations should develop policies and procedures for protecting user workstations from unauthorized access. For instance the use of a time-out facility should be enforced when the machine is left unattended.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have education, training, and experience to perform their assigned tasks

In deploying the Smart Expediter an organization will have the opportunity to perform a quality assurance audit of Ingenuus development processes, procedures and standards and should review the history of employee training. Ingenuus will provide access to personnel and documentation as necessary to support the following quality assurance activities:

- Organizational structure, history & background
- Personnel qualifications and training
- Security
- Disaster recovery and backup/restore procedures
- Software quality control
- Change management
- Documentation

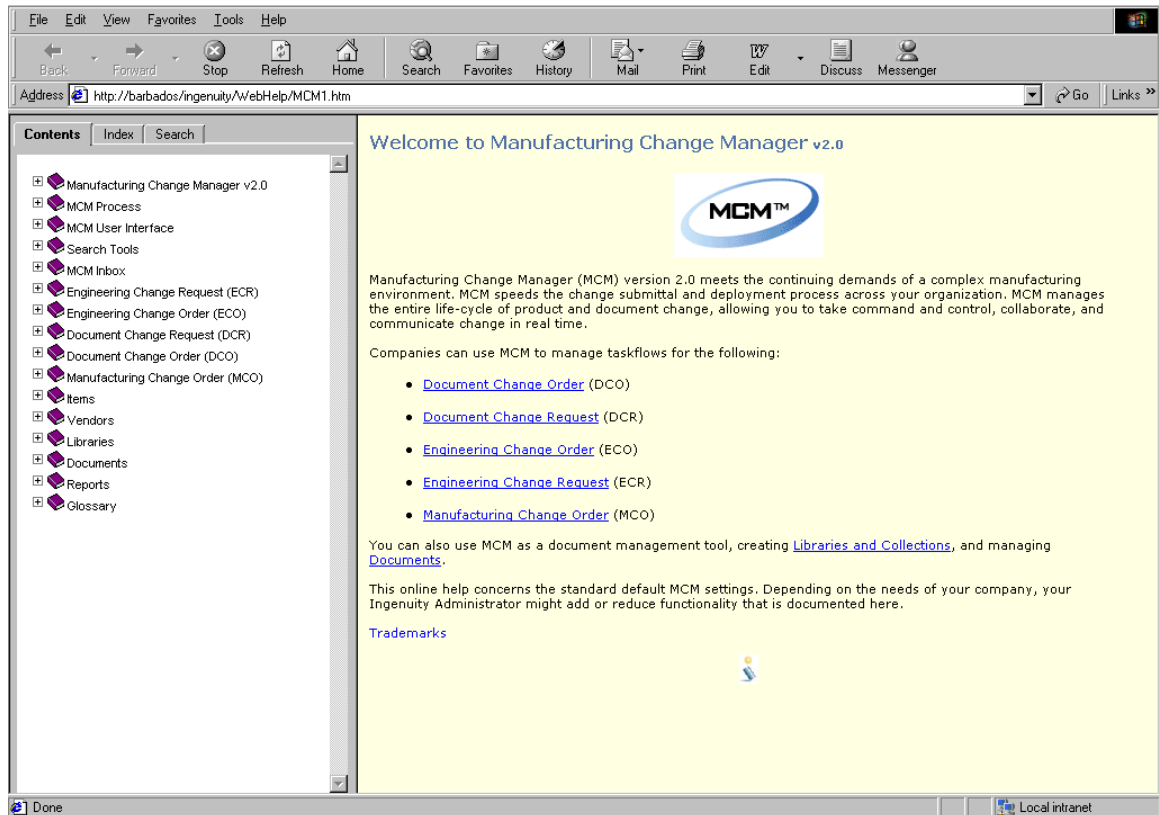
It should be noted that Ingenuus is using the Smart Expediter internally to manage and release requirements, specifications, and internal SOPs.

Software development methodology, processes and standards

An organization should ensure that training is provided for employees who will use the system. Ingenuus provides both on-site and off-site training for both end users and administrators. There are general, basic, end-user courses as well as specialized courses covering such things as system design, administering users and groups, Task Flow design.

A complete list of available courses can be found at:
<http://www.ingenuus.com>

The Smart Expediter system contains a comprehensive online help facility including a "contents" menu and full search capabilities.



(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.

In deploying the Smart Expediter an organization should develop policies and procedures covering system related actions for administrators such as user and group set-up, password management, permissions management and for end users such as object creation, review and approval. Ingenuus can provide services to assist in the development of these policies and procedures as well as in system configuration.

(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.*

In deploying the Smart Expediter an organization should develop policies and procedures covering the control of system operational documentation, system maintenance schedules and software upgrade activities. The Smart Expediter itself is an excellent tool for controlling system documentation.

Section 11.30 Controls for Open Systems

This section outlines controls that must be in place for “open systems,” or an environment that is not controlled by persons who are responsible for the content of electronic records that are on the system. A good example of an open system is the Internet.

(a) Requirement: 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 confidentiality of electronic records from the point of their creation to the point of receipt.

In deploying the Smart Expediter an organization should implement usage policies and procedures needed to satisfy this requirement. The Smart Expediter provides user authentication, data integrity and confidentiality as follows:

Authentication: System access is controlled through the use of login names and passwords. See the response to 11.10 (d).

Integrity: It is impossible overwrite an existing object using the Smart Expediter system. A user with appropriate permissions may only add a new revision, either directly or Task Flow action. The ability to delete an object can be strictly controlled through the use of access permissions.

Confidentiality: To ensure confidentiality, the Smart Expediter should be deployed in a secure communications network employing the Secure Sockets Layer (HTTPS) security mechanism that adds data encryption to the data stream from the browser to the server. Firewalls and proxy servers can be used to limit access to a specific, pre-defined set of users and IP addresses. Within Smart Expediter, each object has multiple levels of access permissions inherited from its container object. The owner of an object can change the permissions to restrict access to confidential records. See the response to 11.10 (g).

Digital Signatures: The Smart Expediter does not have the facility for digital signatures. Ingenius will be looking for partners that can provide this technology for integration with the Smart Expediter.

Section 11.50 Signature Manifestations

This section requires signature manifestations to contain information associated with the signing of electronic records.

(a) Requirement: Signed electronic records shall contain information associated with the signing that indicates the printed name of the signer, the date and time of the signing, and the meaning associated with the signature (such as review, approval, responsibility or authorship).

The Smart Expediter with its powerful Task Flow engine provides the Task Flow audit trail, which contains the printed name of the signer, the signature timestamp, and the user action and user comments. In addition, the Smart Expediter Task Flow designer allows multiple action items per step, each of which is displayed in the audit trail. A step is not complete until all mandatory action items are completed.

(b) Requirement: The items identified in (a) shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of electronic record (such as electronic display or printout).

The screenshot shows the Ingenuus Manufacturing Change Manager interface. At the top, there are navigation links for 'Inbox', 'Log Out', and 'Help'. Below that, the 'Manufacturing Change Manager' title is displayed. A search bar is present on the right. The main content area shows a record with 'Number: 01-0054', 'Title: replace screen', and 'Status: In Progress'. A left sidebar contains a list of actions: Approve, Reject, Release, Cancel, Send, Save, Report, Set Notification, Set Participant, and View Comment. A central menu includes General, Description Of Change, Related Documents, Attachments, Audit Trail, Related Items, and Dates. Below this is an 'Approvers' section with a dropdown set to 'All'. A table displays the audit trail data:

Recipient	Department	Task	Action	Time In	Time Out	Hours	Comments	Escalated
ADMIN		ECR Originator	Sent	6/7/2001	6/7/2001 7:31 AM	0.04		
ADMIN		Originator's Manager	In Progress	6/7/2001		165.17		
ADMIN		Originator's Manager	In Progress	6/7/2001		165.17		
ADMIN		Originator's Manager	In Progress	6/7/2001		165.17		

The Smart Expediter implicitly maintains the association between records and their respective metadata. There are no controls provided in the user interface that would enable any user to break that link. With our complex interlocks in the database, it is extremely difficult for anyone with malicious intent to break the link between a record and its metadata.

Section 11.70 Signature/Record Linking

This section specifies a requirement that signatures be linked with records and that the signature cannot be removed from the record.

Requirement: Electronic signatures and handwritten signatures applied to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be removed, copied, or transferred to falsify an electronic record.

The Smart Expediter ties all electronic signatures to the corresponding Task Flow instance used to update a record. Every revision of a structured record has the associated Task Flow instance stored in its metadata, which provides the link to all the electronic signatures that applied to the approval and subsequent release of the record. Again, because of the multiple interlocks in the metadata, it is extremely difficult to alter, copy, or otherwise modify the electronic signature information.

The Smart Expediter does not directly support handwritten signatures of electronic records. This can however be accomplished using manual policies and procedures.

Subpart C – Electronic Signatures

Section 11.100 General Requirements

The section specifies general requirements for electronic signatures.

(a) Requirement: Each electronic signature will be unique to an individual and shall not be reused by, or assigned to, another individual.

In deploying the Smart Expediter an organization should implement policies and procedures to ensure that a login name is assigned to only one individual, that each individual set their own password on first login and that each individual agrees not to divulge their password under any circumstances. See response to 11.10 (d).

(b) Requirement: Before an organization establishes, assigns, or certifies an individual's electronic signature, the organization shall verify the identity of the individual.

In deploying the Smart Expediter an organization should implement policies and procedures to ensure that login names are assigned to individuals with proper authorization and approval from their superiors.

(c) Requirement: Persons using electronic signatures shall certify to the FDA that they are using electronic signatures intended to be the legally binding equivalent of a traditional handwritten signatures, and may be required to provide additional certification that a given electronic signature is the equivalent of the signer's handwritten signature.

In the Smart Expediter, all users having signing authority can be assigned to a particular role. A report can then be generated to provide the FDA with the list of users that will be applying electronic signatures. A Task Flow can also be created in the Smart Expediter, which will be used to add new users into the system. This would attest to the legally binding equivalence of users and their electronic signatures.

Section 11.200 Electronic Signature Components and Controls

This section outlines requirements for electronic signatures not based on the use of biometrics, which would include the Smart Expediter.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Requirement: Electronic signatures not based upon biometrics shall employ two distinct identification components such as an identification code and password.

The Smart Expediter utilizes a combination of login name and password as the two components of the electronic signature. See the response to 11.10 (d).

(i) Requirement: When executing a series of signings during a continuous period, the first signing shall be executed using all signature components and subsequent signings at least one signature component.

The Smart Expediter has this facility, the user logs-in with both login name and password once for a session and then re-enters the password when asked to authenticate again during an approve/reject workflow action. See the response to 11.50 (b).

(ii) Requirement: When an individual executes one or more signings not performed during a continuous period, each signing shall be executed using all of the electronic signature components.

The Smart Expediter enforces session continuity by inactivity timeout. Once a session timeout occurs, the user has to login again using all of the electronic signature components.

(2) Requirement: Electronic signatures shall be used by their genuine 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.

A user must be logged- in to the system to change their password. If a user forgets their password or there have been illegal attempts to login, the administrator can change the password so that the user can once again access the system. The user can be forced to select a new password on first subsequent log- in. See the response to 11.10 (d).

In most organizations the desktop PCs will be set-up with an inactivity screen that starts after a fixed period and locks the PC until the correct login name and password are entered. The Smart Expediter also enforces inactivity timeout to prevent unauthorized use of an individuals account.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

The Smart Expediter does not support electronic signatures based on biometrics at this time.

Section 11.300 Controls for Identification Codes/Passwords

This section covers controls that must be in place to ensure security and integrity when using electronic signatures based on identification codes and passwords.

Requirement: Persons who use electronic signatures based upon identification codes and passwords shall employ controls to ensure their security and integrity.

These controls should include the following:

- (a) Maintain the uniqueness of each combined identification code and password to avoid duplication of the same combination of identification code and password.**
- (b) Ensure that identification code and password issuance are periodically checked, revoked, or revised.**
- (c) Follow loss management procedures to electronically deauthorize lost, stolen, or compromised tokens, cards, and other devices that bear or generate identification code and password information, and provide for the issuance of 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 attempts at misuse.**
- (e) Initial and periodic testing of devices that bear or generate identification code or password information to ensure they function properly and have not been altered.**

The Smart Expediter addresses the requirements above in the following ways:

- (a) The system ensures that each login name is unique.
- (b) A global or per user/role password expiration period can be set-up by the system administrator.
- (c) The Smart Expediter allows for login names and/or passwords to be revoked and replaced at any time by an authorized system administrator.
- (d) The Smart Expediter does not have the facility to monitor login attempts for detection of misuse. This feature will be added in the near future.
- (e) Not applicable to the Smart Expediter at this time.

Summary

Coordinating the efforts of research and development, production, distribution and marketing, while achieving regulatory compliance, are challenges that face many FDA regulated organizations today. The opportunity to cut costs and reduce dependency on paper processes is of enormous benefit. 21 CFR Part 11 is a key regulation that medical device manufacturers and pharmaceutical companies need to conform to if they wish to take advantage of electronic records and electronic signatures. The regulations seek to reduce fraud while ensuring that electronic signatures and records are as reliable as their traditional paper versions.

The Smart Expediter is a solution that allows companies to closely adhere to these regulations.

FDA regulated organizations rely on the Smart Expediter to:

- store and access e-Records for change management,
- deliver information about clinical trials,
- track regulatory applications,
- manage records,
- communicate and assign tasks,
- monitor research and development, and
- control Task Flows and processes.

Revision History

Date	Version	Author	Comment
June 14 th , 2001	0.5	Vivek Prasad	Draft for initial review
August 14 th , 2003	1.0	Vivek Prasad	Released
February 23 rd , 2005	2.5	Chris Williams	Various updates.