



**U.S. FDA Title 21 CFR Part 11  
Compliance Assessment of  
SAP Easy Document Man-  
agement and SAP Document  
Management**

**Disclaimer**

These materials are subject to change without notice. SAP AG's compliance analysis with respect to SAP software performance based on 21 CFR Part 11: (i) in no way expresses the recognition, consent, or certification of SAP software by the United States Food and Drug Administration; and (ii) applies to certain components of SAP Easy Document Management and SAP Document Management only as stated herein. The customer is solely responsible for compliance with all applicable regulations, and SAP AG and its affiliated companies ("SAP Group") have no liability or responsibility in this regard. These materials are provided by SAP Group for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.



## Content

<b>1</b>	<b>Summary .....</b>	<b>4</b>
<b>2</b>	<b>21 FDA Title 21 CFR Part 11 Assessment.....</b>	<b>5</b>
2.1	SAP Easy Document Management and SAP Document Management.....	5
2.2	Security .....	5
2.3	Electronic Records .....	5
2.3.1	FDA Requirement.....	5
2.3.2	Change Management of Documents.....	5
2.4	Digital Signature.....	6
2.5	How SAP Easy Document Management and SAP Document Management comply with FDA Title 21 Part 11 .....	7
<b>3</b>	<b>References .....</b>	<b>10</b>



## 1 Summary

On the basis of the interpretation of the FDA Title 21 CFR Part 11 rule of the U.S. Food and Drug Administration and the functions and features discussed within this document, SAP AG believes that the SAP® Easy Document Management and SAP® Easy Document Management application fully complies with FDA Title 21 CFR Part 11.



## 2 21 FDA Title 21 CFR Part 11 Assessment

### 2.1 SAP Easy Document Management and SAP Document Management

The SAP Easy Document Management application is a front end tool to support the end-user by letting him use the extensive functions of SAP Document Management application without having detailed knowledge of the later. With SAP Easy Document Management the end-user can work in a Microsoft Windows Explorer environment but has access to the full functionality of the SAP Document Management which is the background system. Therefore for security and compliance related questions the focus has to be set on SAP Document Management.

This investigation was done for SAP Easy Document Management and SAP Document Management System for ERP 2004 and ERP 2005. It is valid also for following releases.

### 2.2 Security

SAP Document Management as back-end application of SAP Easy Document Management is built on SAP NetWeaver Application Server. Therefore, all security features of SAP NetWeaver Application Server are valid for SAP Easy Document Management and SAP Document Management. For details please refer to the document "U.S. FDA Title 21 CFR Part 11 Compliance Assessment of SAP NetWeaver '04/2004s Application Server".

### 2.3 Electronic Records

#### 2.3.1 FDA Requirement

FDA requires the ability to log and track changes on Business Objects and dependent objects in a compliant software environment.

The computer system must provide functionality to log changes, creation and deletion applied to Business Objects and to depending objects (e.g. configuration data). The minimal necessary information the system has to provide is:

- Old value of an attribute of the changed Business Object
- New value of this attribute
- Person who changed the value
- Date and time of change (Application Server Time)
- Action (create, modify, delete)

#### 2.3.2 Change Management of Documents

The document management authorization objects are elements of the standard system authorization concept. They allow the usage of complex authorizations for processing documents and their original application files. *Access control lists (ACL)* are used to pass on access authorization within a folder structure.

When using SAP Document Management in a validated environment, version management and audit trail are key. In order to activate this and track historical changes to the document, you



need to create a **new version**. In Customizing for *Cross-Application Components*, you can specify whether the system generates **change documents for the document changes**. Change documents show you who made a change to the document.

You make the required settings under *Document Management* → *Control Data* → *Define Document Types*.

**Engineering Change Management** can be used in SAP Document Management: All objects that are affected by a change are grouped together in a change master record in the change department. For example, a BOM, routing, and a document can be affected if you change a material. The user departments make the object changes with reference to this change number (for example, BOM change, routing change). This means that a new data record is created for the objects. To create historical data records, documents are processed without reference to a change number. Document versions inform you of the different change statuses of a document. Integration into the change process is by means of the change number. The change number is entered in the basic data.

As indicated in 2.1 SAP Easy Document Management is a front end tool for SAP Document Management. You can either work on-line or off-line on documents. In both cases configurations like authorizations are done in SAP Document Management. Offline editing lets you load a complete structure to a local directory, so that you can then edit it there independently of the SAP R/3 system. When you log on to the SAP R/3 system again, the updated files are checked in to the central repository. When a document or structure is locally downloaded for further processing there are two possible configurations: 1. The document or structure is locked on the server and nobody can access it. It only can be accessed by somebody else again when the changed document is written on the server by the person who downloaded it. This can be done according to the configuration either automatically or manually the next time the person is online. 2. The document is not locked. Other persons have access and can change it. When the changed document is written on the server, the according person gets a message that the document has been changed in the meantime by somebody else. In this case the documents have to be compared manually.

With a status “released” changes are no more possible. To change a released document a new version has to be created.

## 2.4 Digital Signature

SAP Easy Document Management on the basis of SAP Document Management offers digital signature to fulfill the security requirements for documents that are set for executing processes in compliance with Good Manufacturing Practices (GMP): Processing steps that play a key role in how a document is processed further should only be executed by authorized persons. Digital signatures are part of an approval procedure that ensures that only authorized employees can influence how the process continues. Details have to be defined in a signature strategy. It is also possible to retrieve documents based on their digital signatures.

The digital signature in the SAP System is supported by SSF (Secure Store and Forward).

Digital approval processes must be reliable and transparent in order to comply with security requirements. For this reason, the SAP System offers the following:

- You can lock users after a customer-specific number of unsuccessful attempts to enter the correct user-id and password has been reached.
- You can monitor security-relevant activities that occurred during the signature process.
- You can analyze all activities performed in the context of the signature process.



Furthermore, by analyzing logs for digital signatures, it is possible to get an overview of the course of the signature processes and evaluate all activities performed in the course of the signature process.

## 2.5 How SAP Easy Document Management and SAP Document Management comply with FDA Title 21 Part 11

The following table summarizes how SAP Easy Document Management / SAP Document Management comply with each requirement of Part 11.

Part 11 Clause	SAP Assessment of SAP Easy Document Management and SAP Document Management
11.10(a)	All electronic records within SAP Easy Document Management / SAP Document Management provide adequate audit trails that can be reviewed for information. These records are secured from unauthorized access.
11.10(b)	<p>All electronic records generated in SAP Easy Document Management / SAP Document Management are accurate, complete, and presented in a human readable format.</p> <p>SAP Easy Document Management / SAP Document Management electronic records can be printed or exported into several industry-standard formats such as Adobe PDF and XML</p>
11.10(c)	All electronic records can be maintained in the active database or archived to accommodate all required retention periods even when software is upgraded. Access to these records is secured using standard SAP® authorization profiles. In addition, SAP Easy Document Management / SAP Document Management maintains the link between electronic signatures executed to electronic records even after archiving.
11.10(d)	Robust security administration and authorization profiles assure system access. Changes to security profiles are recorded in SAP NetWeaver Application Server.
11.10(e)	<p>SAP Easy Document Management / SAP Document Management can be configured that electronic records are generated for creating, modifying, or deleting data. If configured accordingly these records are date and time stamped and include the user ID of the individual who is logged onto the system and performed the action. The electronic record will maintain the old and new values of the change and the transaction used to generate the record.</p> <p>Complementing the requirement in 11.10(c), all electronic records can be maintained in the active database or archived to accommodate all required retention periods. In addition, SAP Easy Document Management / SAP Document Management maintains the link between electronic signatures executed to electronic records.</p>
11.10(f)	You can control the processing statuses of documents using status management and so enforce the proper sequence of operations as required by the applicable regulation:

Part 11 Clause	<b>SAP Assessment of SAP Easy Document Management and SAP Document Management</b>
	<p>You can define several <b>statuses</b> that represent important processing statuses during a processing cycle of a document. The processing cycle of a document can be represented in a <b>status network</b>. You construct this network by defining so-called document types and creating relationships between the statuses of a specific document type (predecessor/successor relationship). In each processing situation, the system determines the possible subsequent statuses of the current status. You can display and select these statuses using the possible entries function.</p> <p>The definition of a digital signature strategy supplements the status management in SAP Easy Document Management / SAP Document Management.</p>
11.10(g)	<p>SAP NetWeaver Application Server executes authority checks in conjunction with its robust security administration and authorization profiles to ensure that only authorized individuals can access the system, electronically sign a record, and access or perform the operation at hand. SAP NetWeaver Application Server also records changes to authorization profiles.</p>
11.10(h)	N/A
11.10(i)	<p>The <i>Product Innovation Lifecycle (PIL)</i> for SAP development requires that all personnel responsible for developing and maintaining SAP products have the education, training, and experience to perform their assigned tasks. A wide range of additional education and training offerings and regular assessments of individual training requirements ensure a process of continuous learning for SAP staff involved in the development and support of all SAP software.</p>
11.10(j)	<p>This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the COMPUTER system.</p>
11.10(k)	N/A
11.30	<p>For open systems, SAP NetWeaver Application Server supports interfaces with complementary software partners that supply cryptographic methods such as public key infrastructure (PKI) technology.</p>
11.50(a)	<p>Digital Signature is available within SAP Easy Document Management / SAP Document Management and contains the information</p> <ul style="list-style-type: none"> <li>▪ Printed name of the signer</li> <li>▪ System date and time when the signature was executed</li> <li>▪ The meaning (such as review, approval, responsibility or authorship) associated with the signature which is defined in the status management and signature strategy.</li> </ul>
11.50(b)	<p>Signature records can be displayed or printed whenever the associated electronic record is displayed or printed in SAP Easy Document Management / SAP Document Management. Signature data can be used to search for documents.</p>
11.70	<p>SAP Easy Document Management / SAP Document Management automatically links electronic signatures to the corresponding document. This linking prevents the signature from being deleted, copied, or changed in order to falsify any record.</p>





Part 11 Clause	<b>SAP Assessment of SAP Easy Document Management and SAP Document Management</b>
11.100(a)	SAP Easy Document Management / SAP Document Management enforces uniqueness and prevents reallocation of an electronic signature or deletion of information related to the signature once it has been used (such as user profile).
11.100(b)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the COMPUTER system.
11.100(c)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the COMPUTER system.
11.200(a)(1)	SAP NetWeaver Application Server requires two distinct components – a user ID and a password – to perform any electronic signature. By design, SAP NetWeaver Application Server does not support continuous sessions where only a single component is necessary subsequent to the first signing.
11.200(a)(2)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the COMPUTER system.
11.200(a)(3)	SAP NetWeaver Application Server user and security administration functions ensure that the attempted use of an individual's electronic signature other than by the genuine owner requires the collaboration of two or more individuals.
11.200(b)	SAP NetWeaver Application Server provides a certified interface to biometric devices such as fingerprint and retinal scanning devices. Certified vendors are listed in SAP's Partner Directory on SAP's service marketplace.
11.300(a)	SAP NetWeaver Application Server user and security administration functions provide the necessary controls to ensure that no two individuals have the same combination of identification code (user ID) and password.
11.300(b)	SAP NetWeaver Application Server can be configured to force users to change passwords at various intervals and it provides system checks to prevent users from repeating passwords or using combinations of alphanumeric characters that are included in the user ID. User ID's can also be invalidated, for example, when an employee leaves the company.
11.300(c)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the COMPUTER system.
11.300(d)	SAP NetWeaver Application Server fulfills this requirement and behaves as demanded by the requirement.
11.300(e)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the COMPUTER system.



### 3 References

For more information, look up the following references, many of which are found in the SAP Service Marketplace extranet (authorization required):

- SAP NetWeaver '04 Security Guide ([help.sap.com](http://help.sap.com))
- SAP NetWeaver 2004s Security Guide ([help.sap.com](http://help.sap.com))
- SAP White Paper “Complying with U.S. FDA Title 21 CFR Part 11 for the Life Sciences Industry”
- SAP White Paper “SAP NetWeaver – Providing the Building Blocks for Effective Governance, Risk, and Compliance Management”
- Digital Signatures in SAP Applications – SAP Best Practices
- *Digital Signature Tool*, an implementation guide available in note 700495 in the SAP Notes service
- FDA Title 21 CFR Part 11 Electronic Records; Electronic Signatures: Final Rule, March 1997
- *SAP Easy Document Management* ([help.sap.com](http://help.sap.com))
- *SAP Document Management* ([help.sap.com](http://help.sap.com))

Authors:

Dr. Anja Modler-Spreitzer, Dr. Christoph Roller  
IBU Consumer Products & Life Sciences, SAP