



U.S. FDA TITLE 21 CFR PART 11 COMPLIANCE ASSESSMENT OF SAP NetWeaver®

**SAP NetWeaver® Version '04 and SAP NetWeaver
Application Server Version 2004s**

Disclaimer

These materials are subject to change without notice. SAP AG's compliance analysis with respect to SAP® software performance based on FDA Title 21 CFR Part 11: (i) in no way expresses the recognition, consent, or certification of SAP software by the U.S. Food and Drug Administration; and (ii) applies to certain components of SAP NetWeaver® platform version '04 and the SAP NetWeaver Application Server component version 2004s 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.

CONTENTS

- Summary 4
- FDA Title 21 CFR Part 11 Assessment 5
- Security 5
- E-Records 5
- Digital Signature 6
- How SAP NetWeaver Application Server Complies with Part 11 7
- References 8

SUMMARY

Based upon 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 NetWeaver® platform version '04 and the SAP NetWeaver Application Server (SAP NetWeaver AS) component version 2004s technically comply with the intent and requirements of the Part 11 rule.



FDA TITLE 21 CFR PART 11 ASSESSMENT

Security

- SAP NetWeaver AS 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 AS also records changes to authorizations.
- SAP NetWeaver AS can be configured to force users to change passwords at various intervals and provides system checks to prevent users from repeating passwords or using combinations of alphanumeric characters that are included in the user ID. User IDs can also be invalidated when necessary, such as when an employee leaves the company.
- Robust security administration and authorizations assure secure system access. Changes to authorizations are recorded in SAP NetWeaver AS.
- An electronic record of all failed attempts (for either logon or signature) is maintained in the security audit log (SAP NetWeaver AS ABAP™ programming language) or Java log (SAP NetWeaver AS Java). SAP NetWeaver AS also generates electronic records for the locking and unlocking of users.
- SAP NetWeaver AS user and security administration functions provide robust system checks and configurable security procedures to establish and maintain a unique signature for each individual. This includes prevention of signature reallocation and deleting information relating to the electronic signature once it has been used. SAP NetWeaver AS requires two distinct components – a user ID and a password – to perform every electronic signature. By design, SAP NetWeaver AS does not support continuous sessions where only a single component is necessary subsequent to the first signing.
- SAP NetWeaver AS generates an SAP express mail within the SAP system and sends it to a defined distribution list to notify the security administration “in an immediate and urgent manner.” In addition, any MAPI-compliant messaging system can be interfaced to SAP NetWeaver AS to send this message externally to e-mail systems such as Microsoft Exchange or even a paging system.

- SAP NetWeaver AS user and security administration functions ensure that the attempted use of an individual’s electronic signature by someone other than the genuine owner requires the collaboration of two or more individuals.

E-Records

- E-records (change document objects) are application requirements and therefore not part of SAP NetWeaver Application Server.

Time Stamp

Global Application

- Processes that cover more than one time zone primarily affect logistic functions such as availability checks, production planning, delivery scheduling, statistics, and service provision. However, they also affect financial accounting in areas such as treasury, intercompany transactions, and so on.
- The time-stamp function enables you to use dates and times that are comparable and exchangeable in applications implemented worldwide. For time-related applications, the SAP® software can use local dates and times for proposed dates and validations (for example, to ensure that a requested delivery date is not in the past).
- Generally, users think and act in terms of their local time and expect to use their local time in business transactions. When the SAP software is used for global transactions that span time zones, business partners and systems will have different local times. These differences in local times can lead to problems such as late postings and missed background processing.
- Local times can be compared and exchanged as long as they share the same time zone. However, for business processes spanning time zones, inaccuracies of up to 24 hours could occur. By normalizing date and time internally, the time-stamp function eliminates problems that can arise from users working in different time zones.

Integration

- The time-stamp function is fully integrated into the SAP software. This integration allows for faster conversions between the software and local dates and times.
- The terms “system date” and “system time” refer to the database server’s date and time. Since application servers are synchronized with the database server, these terms also correspond to the application server’s date and time.

Internal and External Representations of Time

- To compare the local times of users in different time zones, the SAP software represents times differently externally and internally. The external representation of the time corresponds to a context-dependent local time. For example, in Germany, the time is represented in Central European Time (CET) and in New York in Eastern Standard Time (EST).
- In some instances, the SAP software normalizes the internal system time to Universal Coordinated Time (UTC), which serves as a reference time. UTC corresponds to Greenwich Mean Time (GMT). By converting all local, relative times to absolute times based on UTC, the system can compare times and use them in calculations.

Digital Signature

Encapsulated Signature Tool in SAP NetWeaver Application Server

- This powerful functionality enables customers to include signature functionality in any transaction or business process within the mySAP™ ERP application or mySAP Business Suite applications.
- The tool can be integrated into any business areas in mySAP Business Suite.
- All transactions and workflow of mySAP Business Suite can include signature functionality, with the new encapsulated signature tool 6.20 application basis or higher necessary. For further information refer to the implementation guide entitled *Digital Signature Tool* (note 700495).



How SAP NetWeaver Application Server Complies with Part 11

The following table summarizes how SAP NetWeaver AS complies with each requirement of Part 11.

SAP NetWeaver® AS Part 11 Compliance

Part 11 Clause	Additional Comments
11.10(a)	N/A
11.10(b)	N/A
11.10(c)	N/A
11.10(d)	Robust security administration and authorizations assure secure system access. Changes to authorizations are recorded in SAP NetWeaver® AS.
11.10(e)	N/A
11.10(f)	N/A
11.10(g)	SAP NetWeaver AS 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 AS also records changes to authorizations.
11.10(h)	Input devices such as terminals, measurement devices, and process control systems, in addition to remote logon, are maintained through the same SAP® security administration features and require authorizations for connection to SAP NetWeaver AS and mySAP™ ERP.
11.10(i)	The <i>Product Innovation Lifecycle (PIL)</i> for SAP development requires that all personnel responsible for developing and maintaining SAP NetWeaver AS 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 staff involved in the development and support of all SAP software.
11.10(j)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.
11.10(k)	N/A
11.30	For open systems, SAP NetWeaver AS supports interfaces with complementary software partners that supply cryptographic methods.
11.50(a)	N/A
11.50(b)	N/A

11.70	Electronic records of signatures are permanently linked to the executed electronic record. This link cannot be removed, copied, or transferred to falsify other electronic records by any ordinary means. When the electronic records are archived, this link remains.
11.100(a)	SAP NetWeaver AS user and security administration functions provide robust system checks and configurable security procedures to establish and maintain a unique signature for each individual. This includes the prevention of reallocating a signature and deleting information relating to the electronic signature once it has been used.
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 AS requires two distinct components – a user ID and a password – to perform every electronic signature. By design, SAP NetWeaver AS 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 AS user and security administration functions ensure that the attempted use of an individual's electronic signature by someone other than the genuine owner requires the collaboration of two or more individuals.
11.200(b)	SAP NetWeaver AS provides interfaces for digital signatures and authentication. You can also use secure network communications (SNC) to provide for secure authentication instead of using the traditional user ID and password-based authentication. To protect users' private keys to SAP applications, you can use hardware tokens (such as smart cards) issued to each individual. The keys are stored on the hardware token, and the hardware token is designed never to reveal the private key. Users have to authenticate themselves to their hardware tokens, either using biometrics (for example, a fingerprint) or knowledge (for example, a PIN, password, or pass-phrase entry) and can then use the hardware token to create digital signatures or encrypt documents. Look for certified vendors in the SAP complementary software program.
11.300(a)	SAP NetWeaver AS 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.

REFERENCES

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

- SAP NetWeaver Application Server Version 2004s Java Security Guide
- SAP NetWeaver Application Server 2004s ABAP Security Guide
- SAP Web Application Server Version '04 Security Guide (ABAP and Java)
- SAP NetWeaver Version '04 Security Guide
- SAP NetWeaver 2004s – Overview on Release Enhancements, July 2006
- “Complying with U.S. FDA Title 21 CFR Part 11 for the Life Sciences Industry” (white paper, www.sap.com/usa/solutions/grc/pdf/BWP_FDA_Title21.pdf)
- *Digital Signatures in SAP Applications – SAP Best Practices Guide*
- *Digital Signature Tool*, an implementation guide available in note 700495 in SAP Notes
- FDA Title 21 CFR Part 11 Electronic Records; Electronic Signatures: Final Rule, March 2007 (www.fda.gov/ora/compliance_ref/part11/)

Part 11 Clause	Additional Comments
11.300(b)	SAP NetWeaver AS can be configured to force users to change passwords at various intervals. It provides system checks to prevent users from repeating passwords or using combinations of alphanumeric characters that are included in the user ID. User IDs can also be invalidated when necessary, such as 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 AS provides the following features to satisfy 11.300(d): <ul style="list-style-type: none"> ■ When the number of failed attempts (for either logon or signature) is exceeded, SAP NetWeaver AS prevents the user from further access without intervention from security administration. Note: the number of failed attempts allowed is configurable. ■ SAP NetWeaver AS generates an SAP express mail within the SAP software system and sends it to a defined distribution list to notify security administration “in an immediate and urgent manner.” In addition, any MAPI-compliant messaging system can be interfaced to SAP NetWeaver AS to send this message externally to e-mail systems such as Microsoft Exchange or even a paging system. ■ An electronic record of all failed attempts (for either logon or signature) is maintained in the security audit log and Java log. SAP NetWeaver AS also generates electronic records for the locking and unlocking of users.
11.300(e)	This clause covers a procedural requirement for customers and is not related to the functions or capabilities of the computer system.

Authors: Dr. Christoph Roller

Dr. Anja Modler-Spreitzer

IBU Consumer Products & Life Sciences, SAP