

DIFFRAC^{plus} BASIC

MEETING THE REQUIREMENTS
OF THE FDA'S "21 CFR PART 11"
REGULATION

WHITE PAPER



The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights reserved.

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections are included in subsequent editions. Suggestions for improvement are welcome.

Order no. DOC-M88-EXX069. Version 2.1. Updated: Nov 30, 2004.

© 2003 - 2004 BRUKER AXS GmbH, Karlsruhe, West Germany.

All trademarks and registered trademarks are the sole property of their respective owners.

Printed in the Federal Republic of Germany.

BRUKER AXS GMBH
ÖSTLICHE RHEINBRÜCKENSTR. 49
D-76187 KARLSRUHE
GERMANY

TEL. (+49) (721) 595-2888
FAX (+49) (721) 595-4587
www.bruker-axs.de
Email: info@bruker-axs.de

BRUKER AXS, INC.
5465 EAST CHERYL PARKWAY
MADISON, WI 53711-5373
USA

TEL. (+1) (800) 234-XRAY
TEL. (+1) (608) 276-3000
FAX (+1) (608) 276-3006
www.bruker-axs.com
Email: info@bruker-axs.com

DIFFRAC^{plus} BASIC

Meeting the Requirements of the FDA's "21 CFR Part 11" Regulation

Support for
Electronic Records and
Electronic Signatures

Checklist for FDA Requirements

White Paper

Contents:

- 1 INTRODUCTION.....3
- 2 SUPPORT FOR 21 CFR PART 114
 - 2.1 System safety4
 - 2.2 Audit trails5
 - 2.3 Electronic records.....5
 - 2.4 Electronic signatures.....6
- 3 CHECKLIST7
- 4 GLOSSARY13

1 INTRODUCTION

The purpose of this white paper is to show how the DIFFRAC^{plus} BASIC software helps to meet the requirements of the FDA's 21 CFR Part 11 regulation.

DIFFRAC^{plus} BASIC is being developed by applying a formal design process and product development life cycle according to Bruker AXS's ISO9001 certified product development procedures. Written standards exist such as coding standards, configuration management, programmer qualifications, software version control, maintenance, formal testing of software/hardware, incident reporting and tracking, and disaster recovery.

To integrate into an FDA's 21 CFR Part 11 (or OECD) compliant laboratory, DIFFRAC^{plus} BASIC offers several tools to provide and guarantee authenticity, integrity and confidentiality of electronic records and electronic signatures including

- Secure system log-ins
- Automatic audit trail generation
- Electronic signatures with reports and data
- Network security with Windows NT4 / 2000
- Tamper proof data files with the ability to discern invalid or altered records

The following sections detail how relevant requirements of the 21 CFR Part 11 regulation are implemented in DIFFRAC^{plus} BASIC.

Bruker AXS is also happy to provide tools and expertise to help you to meet the requirements of equipment qualification EQ (including design qualification DQ, installation qualification IQ, operation qualification OQ, and performance qualification PQ) for system validation (21 CFR Part 11, §B11.10a), which is the ultimate responsibility of the system owner.

2 SUPPORT FOR 21 CFR PART 11

DIFFRAC^{plus} BASIC is compliant to the requirements for a closed system as defined by 21 CFR Part 11. In section 11.3 a closed system is defined as

“an environment in which the system access is controlled by persons who are responsible for the content of electronic records that are on the system”.

Controls of closed systems and the security for closed systems are addressed in section 11.10:

“Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure authenticity, integrity, and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as genuine”.

The following sections outline, how system safety, audit trailing, electronic records and electronic signatures are implemented in DIFFRAC^{plus} BASIC to prevent fraud in the generation and signing of electronic records.

2.1 System safety

Operation of DIFFRAC^{plus} BASIC is possible using a local PC, PCs within a LAN or via Internet. Security is ensured due to a two-stage security system, that is the mandatory and independent Windows NT4/2000 and DIFFRAC^{plus} BASIC secure logons. Logon can be restricted to any PCs using their unique IP address.

An administrator has to configure Windows NT4/2000 secure logons for controlling access to the system and should also install and configure suited backup and disaster recovery procedures.

Successful login to the Windows NT4/2000 system is required to launch and logon to DIFFRAC^{plus} BASIC, each login attempt to DIFFRAC^{plus} BASIC is added to the system audit trail (see section 2.2).

To prevent unauthorized access to the system, the number of unsuccessful login attempts to a user account is limited and can be configured by the administrator. If the number of unsuccessful login attempts is exceeded, the DIFFRAC^{plus} BASIC user account is disabled and must be reactivated by the administrator before it can be used again. If an account is deactivated a message is displayed informing about deactivation. The deactivation message is also added to the system audit trail (see section 2.2). If there are repeated failed logons the time between again opening the logon dialog will be increased considerably to prevent password guessing.

The combination of username and password is enforced to be unique by the system. Usernames can not be reused, reassigned or deleted. The administrator can disable user accounts and set a new password, but can not read any passwords of any user. He can also define the minimum length, expiration date or expiry period and configure a user login timeout.

DIFFRAC^{plus} BASIC predefines three predefined user account levels configured with default rights: "Administrator", "LabAdministrator" and "Operator". An administrator can modify the rights of the subordinated accounts and also create new accounts, but can not delete any of the 3 default groups.

2.2 Audit trails

DIFFRAC^{plus} BASIC uses two audit trail types to automatically document who has accessed a computer system and what operations he or she has performed during a given period of time:

1. The system audit trail records any events related to the system such as, logins, logouts, any configuration changes of user accounts by the administrator and changes of passwords.
2. Electronic record audit trails are history logs protocolling any activities related to electronic records such as modification of electronic records and electronic signing. An electronic record audit trail is always saved together with its related electronic records in a single ZIP compatible file (section 2.3).

Auditing trailing is always enabled, it cannot be disabled, nor can it be bypassed. Audit trails always record the event type, the username of the person causing the event, the date/time of the event, and all operator entries. Audit trails are tamper-resistant text files protected using SHA checksums. They can be read with any common text editor and are therefore easily available for review and copying by the FDA.

2.3 Electronic records

21 CFR Part 11 defines electronic records as

"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".

In DIFFRAC^{plus} BASIC typical electronic records comprise instrument configuration files, instrument control files, measurement (raw) data files and files containing evaluation results created by application software. For each file an electronic record audit trail is automatically created and stored together with the electronic record in a single ZIP compatible file forming an entity.

For data evaluation all evaluation steps performed within application software are recorded in an electronic record audit trail which is automatically associated with result files written by this software package. Whenever the user decides to save new evaluation results as a results file, this file can be electronically signed (section 2.4) and will be added to the ZIP file as a new revision. The related electronic record audit trail allows to unambiguously link these different revisions with the respective evaluation steps performed.

All electronic records are protected from both modification and deletion using Windows NT4/2000 file security mechanisms. In addition, each electronic record, audit trail as well as the ZIP files are failure (e.g. power breakdown) and tamper protected by individual SHA checksums, which are listed in a SHA inventory file (which is also SHA checksum protected) and even provide protection against individuals with administrator privileges.

The readability of all file formats is guaranteed by the respective application software throughout a minimum retention period at least as long as that required for the subject electronic records. Archiving is possible with any common archiving tools.

2.4 Electronic signatures

In DIFFRAC^{plus} BASIC non-biometric electronic signatures are implemented and include both the user name and the full printed name of the signer, the date and time when signed, and the meaning of the signature (such as review or approval). The identity of the user is verified at login to DIFFRAC^{plus} BASIC (section 2.1).

All sessions are treated as non-continuous sessions, signing always requires user-name and password. Each electronic signing is logged into both the system audit trail and the respective electronic record audit trail (section 2.2).

An electronic signature is stored in the same electronic record that is signed and therefore directly linked to the electronic record. A SHA checksum protects tampering of both the electronic signature and the electronic record in its entity.

As an alternative to electronic signatures DIFFRAC^{plus} BASIC also allows to print and manually sign paper records, which are tamper protected and linked to the respective electronic record by both a SHA checksum and the unique file name and path, printed on each page of the paper record.

3 CHECKLIST

The following table lists the specific sections of the 21 CFR Part 11 Rule and provides an explanation of how DIFFRAC^{plus} BASIC fulfills each of the FDA requirements.

| Section | Requirement | Implementation |
|---------------------------|--|--|
| Electronic Records | | |
| §B11.10 | 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: | DIFFRAC ^{plus} BASIC is being developed by applying a formal design process and product development life cycle according to Bruker AXS's ISO9001 certified product development procedures. To integrate into an FDA's 21 CFR Part 11 (or OECD) compliant laboratory, DIFFRAC ^{plus} BASIC offers several tools to provide and guarantee authenticity, integrity and confidentiality of electronic records and electronic signatures. Bruker AXS also provides tools to meet the requirements of EQ (including DQ, IQ, OQ, PQ). |
| (a) | Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | It is the responsibility of system owners to validate their applications using an established life cycle methodology. DIFFRAC ^{plus} BASIC protects electronic records against tampering using SHA checksums. Audit trails record all changes to electronic records. |
| (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. | DIFFRAC ^{plus} BASIC is using proprietary file formats, and saves all electronic records together with their related electronic record audit trail in ZIP compatible files. Audittrails are text files and can be read with any common editor. The readability of all proprietary file formats is guaranteed by DIFFRAC ^{plus} BASIC throughout a minimum retention period at least as long as that required for the subject electronic records. |
| (c) | Protection of records to enable their accurate and ready retrieval throughout the records retention period. | Electronic records are protected against tampering using SHA checksums. System security, archiving and disaster recovery are within the responsibilities of the system owner. |

| Section | Requirement | Implementation |
|---------|--|--|
| (d) | Limiting system access to authorized individuals. | <p>System access requires independent Windows NT4/2000 and DIFFRAC^{plus} BASIC secure logons, which are to be configured and maintained by the system owner.</p> <p>DIFFRAC^{plus} BASIC predefines three pre-defined user accounts configured with default rights. An administrator can modify the rights of subordinated accounts and also create new accounts, but can not delete any of the 3 default groups. He can also define password aging, minimum password length, username and password uniqueness, user login timeouts and considerably increased time between login trials after a number of unsuccessful login attempts.</p> <p>The system audit trail protocols all administrator and user activities related to the access to the DIFFRAC^{plus} BASIC system.</p> |
| (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. | <p>DIFFRAC^{plus} BASIC uses two audit trail types, the system audit trails recording any events related to the DIFFRAC^{plus} BASIC system, and the electronic record audit trail which is saved with its related electronic records in ZIP compatible files.</p> <p>Auditing trailing is always enabled and cannot be disabled or be bypassed. Audit trails always record event type, username, date/time, and all operator entries. All audit trails are text files protected using SHA checksums against tampering, and can be read with any common text editor.</p> <p>Electronic records cannot be modified or deleted. New electronic records created e.g. as a result of data evaluation are added to the ZIP file as revisions. The electronic record audit trail records all evaluation steps and unambiguously links them to the related revisions.</p> |
| (f) | Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | Not applicable. System steps or events are not defined in DIFFRAC ^{plus} BASIC. |
| (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. | <p>DIFFRAC^{plus} BASIC provides controls to limit system access to authorized individuals as described in §B11.10d.</p> <p>It is the system owner's responsibility to verify the identity of the individual to whom an electronic signature will be issued.</p> |
| (h) | Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | Not applicable. Instruments operated with DIFFRAC ^{plus} BASIC are stand-alone units. |

| Section | Requirement | Implementation |
|----------------|--|--|
| (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. | <p>Bruker AXS trains its personnel according to its quality procedure, Q521. Training includes GxP and 21 CFR Part 11 requirements, where applicable. Bruker AXS is ISO 9001 certified and follows these guidelines when developing all products.</p> <p>It is the system owner's responsibility to ensure all persons operating DIFFRAC^{plus} BASIC have the necessary levels of education, training, and experience to perform their assigned tasks.</p> <p>Bruker AXS provides a comprehensive selection of training classes for system owner's service personnel and end-users.</p> |
| (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. | Not applicable. System owner's responsibility. |
| (k) | Use of appropriate controls over systems documentation including: | Bruker AXS provides all necessary documentation with the delivery of any system and also provides checks as part of the IQ procedure. |
| | (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. | System owner's responsibility. |
| | (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | System owner's responsibility. All software and firmware, as well as printed documentation supplied by Bruker AXS, contain version information that can be incorporated into the system owner's documentation control system. |
| §B11.30 | 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 §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. | Not applicable. DIFFRAC ^{plus} BASIC is compliant to the requirements for a closed system |

| Section | Requirement | Implementation |
|-----------------|--|--|
| §B11.50 | Signature manifestations | |
| (a) | <p>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</p> <ul style="list-style-type: none"> (1) The printed name of the signer (2) The date and time when the signature was executed (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature | <p>DIFFRAC^{plus} BASIC supports non-biometric electronic signatures including name of the signer, the date and time when signed, and the meaning of the signature.</p> <p>The identity of the user is verified at login to DIFFRAC^{plus} BASIC.</p> |
| (b) | <p>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).</p> | <p>All electronic signings are recorded in the electronic record's audit trail in human readable form.</p> |
| §B11.70 | Signature/record linking | |
| | <p>Electronic signatures and hand-written 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.</p> | <p>In DIFFRAC^{plus} BASIC electronic records and paper records are linked using both a SHA checksum and the unique file name and path, printed on each page of the paper record.</p> <p>Electronic signatures are stored in the same electronic records that are signed, a SHA checksum protects both the electronic signature and the electronic record in its entity.</p> |
| §C11.100 | General requirements | |
| (a) | <p>Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</p> | <p>Electronic signatures are always based on the unique combination of user name and password, enforced by DIFFRAC^{plus} BASIC.</p> <p>User names cannot be reused, reassigned or deleted.</p> |
| (b) | <p>Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.</p> | <p>Not applicable. It is the system owner's responsibility to verify the identity of the individual to whom an electronic signature will be issued.</p> |

| Section | Requirement | Implementation |
|-----------------|---|--|
| (c) | <p>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.</p> <p>(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.</p> <p>(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.</p> | <p>Not applicable. System owners responsibility.</p> |
| §C11.200 | Electronic signature components and controls | |
| (a) | <p>Electronic signatures that are not based upon biometrics shall:</p> <p>(1) Employ at least two distinct identification components such as an identification code and password.</p> <p>(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.</p> <p>(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.</p> <p>(2) Electronic signatures that are not based upon biometrics shall be used only by their genuine owners</p> <p>(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.</p> | <p>Signing always requires a combination of username and password which is enforced to be unique by the system.</p> <p>Not applicable. Sessions are handled as non continuous sessions in general. Signing always requires user name and password.</p> <p>Not applicable. Sessions are handled as non continuous sessions in general.</p> <p>Not applicable. System owner's responsibility.</p> <p>No individual including administrators can read the password of any user.</p> |
| (b) | <p>Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.</p> | <p>Not applicable. Not supported.</p> |

| Section | Requirement | Implementation |
|-----------------|---|---|
| §C11.300 | Controls for identification codes/passwords | |
| (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. | DIFFRAC ^{plus} BASIC enforces an unique combination of username and password. |
| (b) | Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | He can also define password aging, minimum password length, username and password uniqueness, and account lock-out after a reasonable number of unsuccessful login attempts. The system audit trail protocols all administrator and user activities related to the access to the DIFFRAC ^{plus} BASIC system. |
| (c) | Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. | In DIFFRAC ^{plus} BASIC the administrator can disable user accounts and set a new password. The system audit trail protocols all administrator and user activities related to the access to the DIFFRAC ^{plus} BASIC system. Cards or tokens are not used. |
| (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 number of unsuccessful login attempts to a DIFFRAC ^{plus} BASIC user account is limited and can be configured by the administrator. Exceeding the number of unsuccessful login attempts results in disabling of the DIFFRAC ^{plus} BASIC user account, which must be reactivated by the administrator. Any login attempts and user account blockings are recorded by the system audit trail |
| (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. | Not applicable. Cards or tokens are not used. |

4 GLOSSARY

Electronic Record:

Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature:

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.

Handwritten Signature:

The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate writing in a permanent form.

Digital Signature:

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.

Biometrics:

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.

Closed System:

An environment in which system access is controlled by persons responsible for the content of electronic records on the system.

Open System:

An environment in which system access is not controlled by persons responsible for the content of electronic records on the system.

SHA checksum protection:

SHA (secure hash algorithm) is a procedure designed by NIST to calculate unique and secure checksums of electronic records.