BMG LABTECH

Software Manual – Part IV: FDA 21 CFR part 11

Version 5.10

This manual was designed to guide Omega users through the software features related to compliance with FDA 21 CFR part 11.

Although these instructions were carefully written and checked, we cannot accept responsibility for problems encountered when using this manual. Suggestions for improving this manual will be gratefully accepted.

BMG LABTECH reserves the right to change or update this manual at any time. The Revision-Number is stated at the bottom of every page.

TABLE OF CONTENTS

1 FDA 21 CFR part 11 compliance

1.1 Overview

The Omega software contains all features necessary to establish a FDA 21 CFR part 11 compliant system, but keep in mind, the software is only a part of the system. In addition to the software, you need people, who are trained regarding 21 CFR part 11 requirements (and regarding GLP / GMP ... requirements) and it will usually be necessary to set up a set of Standard Operational Procedures (SOPs).

1.1.1 What is 21 CFR part 11?

CFR stands for Code of Federal Regulations, which is a collection of regulations issued from federal authorities of the U.S.A.. The title 21 contains the regulations issued by the FDA (Food and Drug Administration). Part 11 of this title contains the FDA regulations regarding electronic records and electronic signatures.

21 CFR part 11 contains rules, **HOW** to create and handle electronic records and signatures. Aim: Electronic records and electronic signatures should be used equal to paper based documents and signatures.

It does **NOT** describe **WHAT** needs to be documented and signed. You will find this kind of information in predicated rules, like 21 CFR part 58 (GLP) or part 211 (GMP).

The rule 21 CFR part 11 has been a law since 20. September 1997 and is, therefore, legally binding in the U.S.A.. It is also binding for products which are intended for the US market.

There are other similar documents like, for example, the OECD GLP Consensus Document No. 10 (“The application of the principles of GLP to computerized systems”, issued by the Organisation for Economic Co-Operation and Development, 1995) or the German ChemG GLP Appendix 1 (Anhang “Archivierung”). The requirements regarding record handling described in these rules are very similar to the requirements stated in 21 CFR part 11. The EPA (Environmental Protection Agency of the U.S.A.) has published the CROMERR (Cross Media Electronic Reporting and Record-keeping Rule) draft. The record-keeping part will be presumably finished in 2004. The requirements known so far are similar or identical to FDA 21 CFR part 11.

1.1.2 Definitions

The following definitions are taken from ***21 CFR p. 11 Subpart A – General Provisions***.

- ***Electronic Record***

  “Electronic record means any combination of text, graphics, data, audio, pictorial, or other **information** representation in digital form **that is created, modified,** maintained, archived, retrieved, or distributed **by a computer system**.” *§11.3 (6)*

  Concerning the BMG LABTECH software an electronic record means one measurement data set creating by performing a test protocol (Test Run), stored in Absolute Data Base and / or ASCII format.

- ***Electronic Signature***

  “Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the **legally binding equivalent of the individual's handwritten signature**.” *§11.3 (7)*

- ***Digital Signature***

  “Digital signature means an **electronic signature based upon cryptographic methods** of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. *§11.3 (5)*

  The BMG LABTECH software contains a function to digitally sign electronic records and to verify these signatures using the RSA (cryptographic) method (see chapter 1.2 Digital Sign Function *and software manual part III: Data Analysis).*

1.1.3 Requirements

This chapter will list the requirements established in the FDA 21 CFR part 11 rule and how these requirements can be fulfilled using the *BMG LABTECH software*.

21 CFR p. 11 Subpart B - Electronic Records

❑ **§ 11.10 Controls for closed systems**

Procedures and controls shall include:

❑ Validation of systems to ensure accuracy, reliability, consistent intended performance, and the **ability to discern invalid or altered records**.
Protection of records to enable their accurate and ready retrieval throughout the records retention period.

1. Absolute Data Base format:

The BMG LABTECH software will protect the data against manipulation by adding a hash value (SHA1, 160 bit) to each data record. This hash value will protect the record in the measurement data base overview table (Measure.dbf) and the whole content of the raw data file (<Number>.dbf). This hash value also includes the audit trail and any potential signatures (see below).

The hash value will be created when the control part of the BMG LABTECH software creates the data record. It will be updated every time a change of the data has been performed using the BMG LABTECH Data Analysis software, e.g. by changing a sample ID, by removing outliers from the evaluation procedure or by changing the comment field. It will also be updated, when a change of the audit trail has taken place or after adding a signature. This hash value is stored with the data inside the measurement data base.

The hash value will be checked every time a data record is opened in the BMG LABTECH Data Analysis software. In addition, there is a tool ('Check Data Integrity') as part of the BMG LABTECH software package available that can be used to verify this hash value anytime you like (see chapter 1.3).

2. ASCII format:

The protection of the ASCII format data is optional (see chapter Program Configuration *in software manual part II: Control Software). If you use this option, there will be an additional file created for each ASCII file. This file will contain an anti manipulation hash value and the audit trail for the data stored in the connected ASCII file. The SHA1 hash value will protect the whole ASCII file and the audit trail entries.*

The hash value will be created when the control part of the BMG LABTECH software creates the ASCII data file. It can be checked using the above mentioned 'Check Data Integrity' tool.

❑ The ability to generate accurate and complete **copies of records in both human readable and electronic form** suitable for inspection, review, and copying.

Measurement data can be stored in Absolute Data Base and / or in ASCII format. The ASCII format is human readable (using any text editor program, like Notepad) and can easily be printed. The Absolute Data Base format can be used in a wide range of programs, including BMG LABTECH's own Data Analysis program. From there, it can be printed out or saved in XLS (Excel) format or converted into PDF (Acrobat Reader) format (when the Acrobat Distiller or a similar program has been installed).

❑ **Limiting system access** to authorized individuals.

This is achieved in the BMG LABTECH software by using a login function (see software manual part II: Control Software). Setting up user accounts with different privileges (administrator, standard user, user with only permission to execute pre-defined protocols = run only user) is possible. The administrator can define password policies, as for example a minimum length of passwords and a minimum number of non-alpha characters. The user data base is protected against manipulation, passwords will not be stored anywhere (the data base only contains a cryptographically secure hash value); there are options for password aging and alert messages.

***Recommendation** for program usage in a 21 CFR part 11 compliant environment: Change the administrator password to something other than 'bmg', define a password for the default user 'USER', disable Auto Login, define a minimum password length of 6 characters including at least one non-alpha character, use the disable accounts function after three invalid login attempts, use*

password aging (92 days = 3 months or 183 days = half a year) and switch on the alert message for invalid login attempts (see chapter 1.3 of software manual part II: Control Software).

- ❑ 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.

  *All important user actions, such as logging on, defining a test protocol, changing offset or filter values, performing a measurement and so on, can be logged into a **program usage log file**, see chapter 1.3.2 of software manual part II: Control Software. It is possible to start a new log file at every program start or at program start on a new day / week / month / year or after the file has reached a certain size (100 KByte / 1 MByte / 10 MByte). When starting a new log file, the old log file can be renamed or erased. This log file is protected against manipulation by storing a hash value (160 bit SHA1) in an additional file ("Program usage.hv"). The integrity of the log file will be checked at every program start. If manipulation has been detected, the program usage can be blocked and an alert message can be sent (administrator selectable, see chapter 1.3.3 of software manual part II: Control Software). In addition, the 'Check Data Integrity' tool (see chapter 1.3 of this manual) can be used to check the integrity of the log file.*

  *The **audit trail for Absolute Data Base data records** will be stored inside the measurement data base. The first entry of the audit trail will be produced by the control part of the BMG LABTECH software at the same time as the control software creates this data record (immediately after finishing the measurement and transferring the raw data from the reader to the computer). Additional entries will be produced by the BMG LABTECH Data Analysis software when changes of the data have taken place or after copying or signing a data record. The Audit trail will be shown on the 'Protocol Settings' sheet of the BMG LABTECH Data Analysis software. In addition, you can use the 'Check Data Integrity' tool to display or print the audit trail.*

  *The **audit trail function for ASCII format data** is optional (as is the anti manipulation protection), see chapter 3.3.4 of software manual part II: Control Software. If you use this option, the audit trail will be stored in an additional hash value and audit trail file (see the data protection chapter above) created for each ASCII file. You can use the 'Check Data Integrity' tool to display, print or check the audit trail. In addition, you can use any text editor program, like Notepad, to display the audit trail.*

- ❑ Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

  Where appropriate, the BMG LABTECH software / firmware checks that necessary sequences of steps are done in the right order (e.g. priming the pumps before performing a test protocol which uses injections).

- ❑ Use of device checks to determine the **validity of the source of data input or operational instruction**.

  The measurement data is generated by the BMG LABTECH reader and transmitted to the computer using a proprietary communication protocol. The serial number of the reader used is stored with the measurement data (for ASCII format files use the 'Long header' or 'Full header' option, see chapter 3.3.4 of software manual part II: Control Software).

  The log file 'Program usage.log' can be used to keep track of who logged on and modified or performed a test protocol or changed settings, etc..

- ❑ Determination that persons who develop, maintain, or use electronic record / electronic signature systems have the education, training, and experience to perform their assigned tasks.

  Users' responsibility.

- ❑ 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.

  Users' responsibility.

- 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 system documentation.

BMG LABTECH keeps track of the distribution and uses a version / revision management system for the documentation delivered with the software (Software User Manual, ActiveX and DDE Manual), but keep in mind that the BMG LABTECH software is only a part of the whole system, which is the responsibility of the user.

§ 11.30 Controls for open systems

- Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the **authenticity, integrity, and, as appropriate, the confidentiality** of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 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.

Our products are targeted for use in closed systems. The data records will be protected to ensure authenticity and integrity and the BMG LABTECH software uses a cryptographically secure digital signature system, but the data itself is not encrypted. If confidentiality is required, only closed systems should be used.

§ 11.50 Signature manifestations

- Signed electronic records shall contain information associated with the signing that clearly indicates:

  - the **name** of the signer
  - the **date and time** when the signature was executed
  - the **meaning**.

All above mentioned items will be included when using the built-in sign function (see chapter 1.2 Digital Sign Function*). In addition the signer can add a comment.*

To sign Absolute Data Base format data records use the data analysis part of the software, see software manual part III: Data Analysis or use the 'Check Data Integrity' tool described in chapter 1.3.

By using the 'Check Data Integrity' tool, you can also sign ASCII files.

The above mentioned signature parts will be protected against manipulation as the signed data itself. These signature parts will be displayed in the Protocol Settings sheet of the data analysis software (see software manual part III: Data Analysis) or using the 'Check Data Integrity' tool. A print out is possible.

§ 11.70 Signature/record linking

- Electronic signatures and handwritten **signatures** executed to electronic records **shall be linked to their respective electronic records** to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

The BMG LABTECH software uses a public / private key system (RSA with 512, 1024 or 2048 bit key length). The electronic (digital) signature(s) are stored as part of the data record.

Signatures of data records in Absolute Data Base format will be verified every time the data record is opened in the BMG LABTECH Data Analysis software. In addition, you can use the 'Check Data Integrity' tool anytime you would like to view and verify signatures. This tool can also be used for verifying or displaying signatures of ASCII files.

21 CFR p. 11 Subpart C - Electronic Signatures

❑ § 11.100 General requirements

- ❑ Each electronic signature shall be **unique** to one individual.

  This will be ensured by the BMG LABTECH software. The software uses digital signatures created by a cryptographic public / private key system (see chapter 1.1.1 of software manual part II: Control Software). The keys are stored for each user account inside the user data base. The private key (necessary to create a signature) is stored in an encrypted version, and can therefore only be used by its owner (after logging on, see below). A signature is verified using the public key of the signer. When verifying a signature it will also be checked whether the public key (and therefore the signature) belongs to the signer named inside the signature.

  ***Recommendation**:*
  To prevent, that a user name is reused, you should not delete user accounts which are no longer needed (but might have been used in the past to sign data records), just disable these accounts (see chapter 1.2 of software manual part II: Control Software).

- ❑ 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**.

  Users' responsibility (SOP).

- ❑ 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.

  Users' responsibility.

❑ § 11.200 Signature components and controls

- ❑ Electronic signatures that are not based upon biometrics shall:
  - Employ at least **two components** such as an id code and password.
  - **Be used only by their genuine owners**.
  - 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.

  *The BMG LABTECH software uses a cryptographic public / private key system. Before signing, the user needs to log on using his **user name** and **password** (see chapter 1.2* Digital Sign Function*). Both components are required for all signings.*

  The private keys of the users (necessary for signing) are stored inside the user data base in an encrypted version. A private key will only be decrypted for the sign procedure after the user has logged on using his user name and password. The password itself is not stored anywhere in the system. Without knowing the user password even the administrator can not gain access to the private key of a user or to the sign function.

❑ § 11.300 Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

- ❑ Maintaining the **uniqueness of each combined identification code and password**, such that no two individuals have the same combination of identification code and password.

  Done by the Login function.

- ❑ Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as **password aging**).

  Password aging options are available as part of the Login function (see chapter 1.3.1 of software manual part II: Control Software). If a user leaves, the account can be disabled or deleted.

- ❑ Following loss management procedures to electronically **deauthorize** lost, stolen, missing, or otherwise **potentially compromised password information**, and to issue temporary or permanent replacements using suitable, rigorous controls.

  The administrator can disable user accounts or select a function, which will ask the user at next login to change his password (see 'Account Properties' in chapter 1.2 of software manual part II: Control Software).

- ❑ 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.

  There is an option to disable user accounts after a pre-defined number of invalid login attempts (see chapter 1.3.1 of software manual part II: Control Software). Optionally there will be an alert email and / or an alert file after such attempts.

  ***Recommendation** for program usage in a 21 CFR part 11 compliant environment: Use the function to disable a user account after three invalid login attempts and switch on the alert message for this case.*

- ❑ 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.

  The user data base is protected against manipulation. When detecting a manipulated user entry, this account will automatically be disabled and an alert message (see chapter 1.3.3 of software manual part II: Control Software) will be sent.

  Manipulation of the administrator settings (e.g. the password restrictions or alert message settings) will also be automatically detected. In such cases, the program usage will be disabled. To re-enable the program usage the administrator needs to log on.

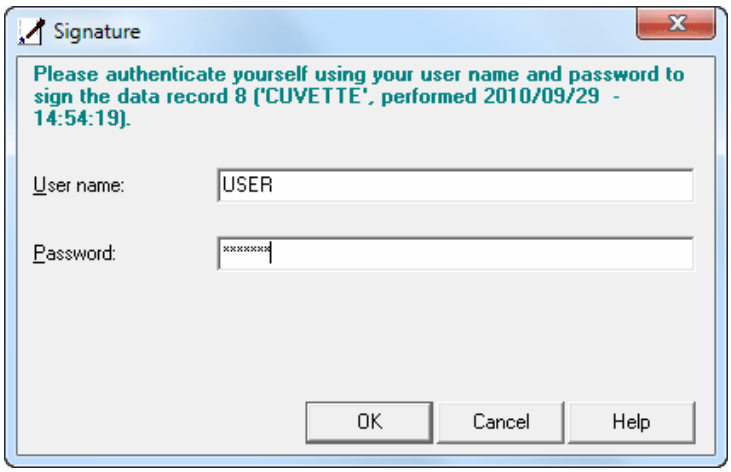
1.2 Digital Sign Function

If you want to sign a data record in Absolute Data Base format use the 'Sign current test run' function in the data analysis software (see software manual part III) or use the 'Check Data Integrity' tool (see chapter 1.3). Using this tool you can also sign ASCII files.

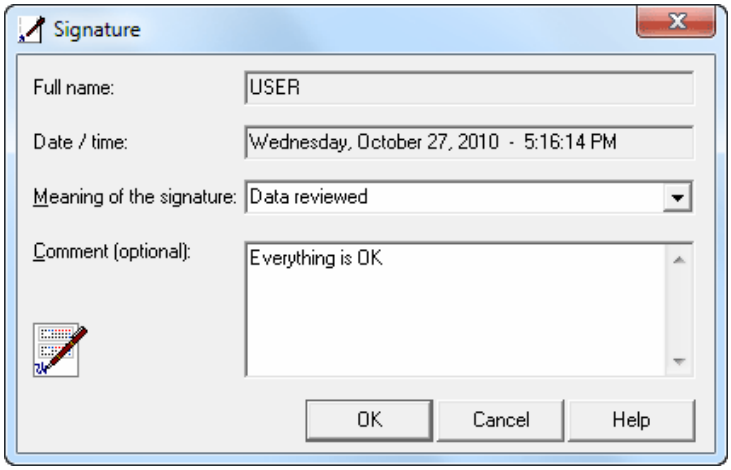
After selecting the sign function an authentication window appears. Please log in using your user name and password as defined using the 'Login' screen (see chapter 1 of software manual part II: Control Software).

Notes: It is possible, that another person signs the current data record than who is currently logged on.

You need to have a pair of RSA keys to be able to use the sign function (see chapter 1.1.1 of software manual part II: Control Software).



After you have successfully logged in, the following dialogue box will appear:



The full name of the signer (as defined in the keys dialogue) and the current date and time will be automatically added to the signature.

You need to define the meaning of the signature, e.g. 'Data audited' or 'Data released'. You can select from the pre-defined list or you can type something in. In addition you can add a comment.

Note: The date and time is displayed here using the format as defined in the Windows Control Panel (Regional Settings) under long date and long time format.

1.3 Check Data Integrity Tool

With the BMG LABTECH software a tool ‘Check Data Integrity’ will be installed. You can use this tool to check the integrity of test run data (Absolute Data Base and ASCII format) produced by BMG LABTECH software.

If there are signatures attached to the data, these signatures can be verified as well.

It is also possible to add new signatures.

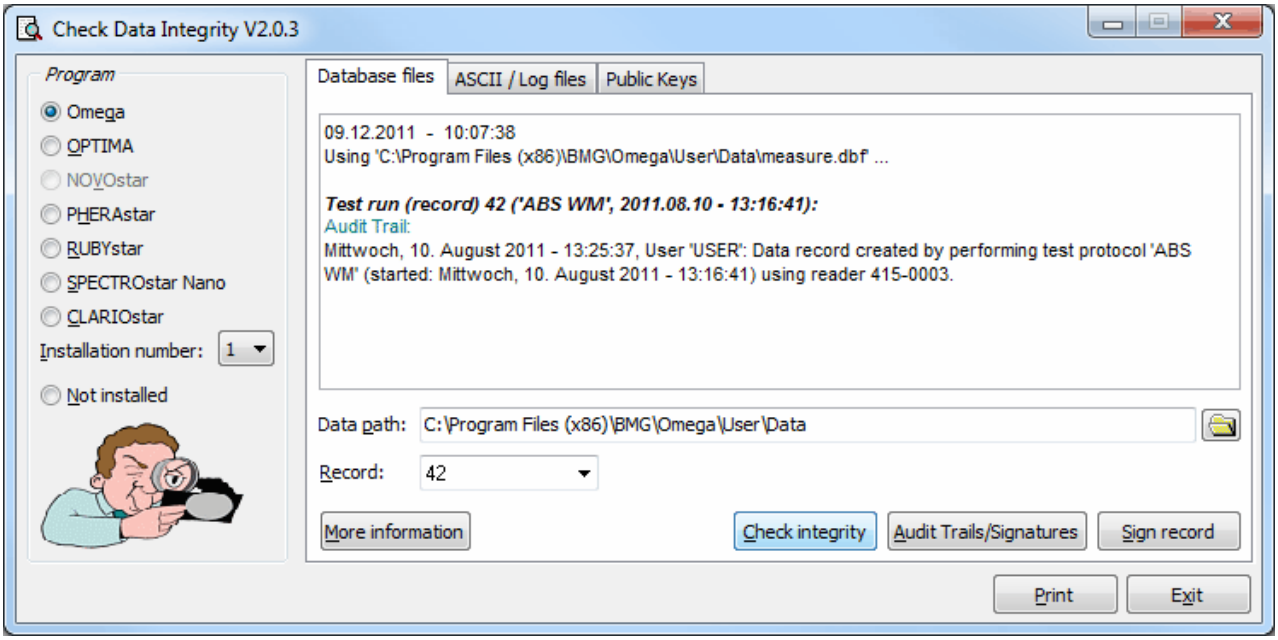
You can also check the integrity of the program usage log files.

To start this tool use the ‘Start | Programs | BMG LABTECH | Omega | Check Data Integrity’ entry form the Windows start menu.

Please select the BMG LABTECH program used to create the data on the left side of the program window. If you are using the ‘Check Data Integrity’ tool on a computer, where the BMG LABTECH software itself has not been installed, choose ‘Not installed’ in the program selection box (see also the explanation for ‘stand alone usage’ at the end of this page).

1.3.1 Absolute Data Base Files

The ‘Check Data Integrity’ tool contains three sheets. Use the first sheet to check data records in Absolute Data Base format.



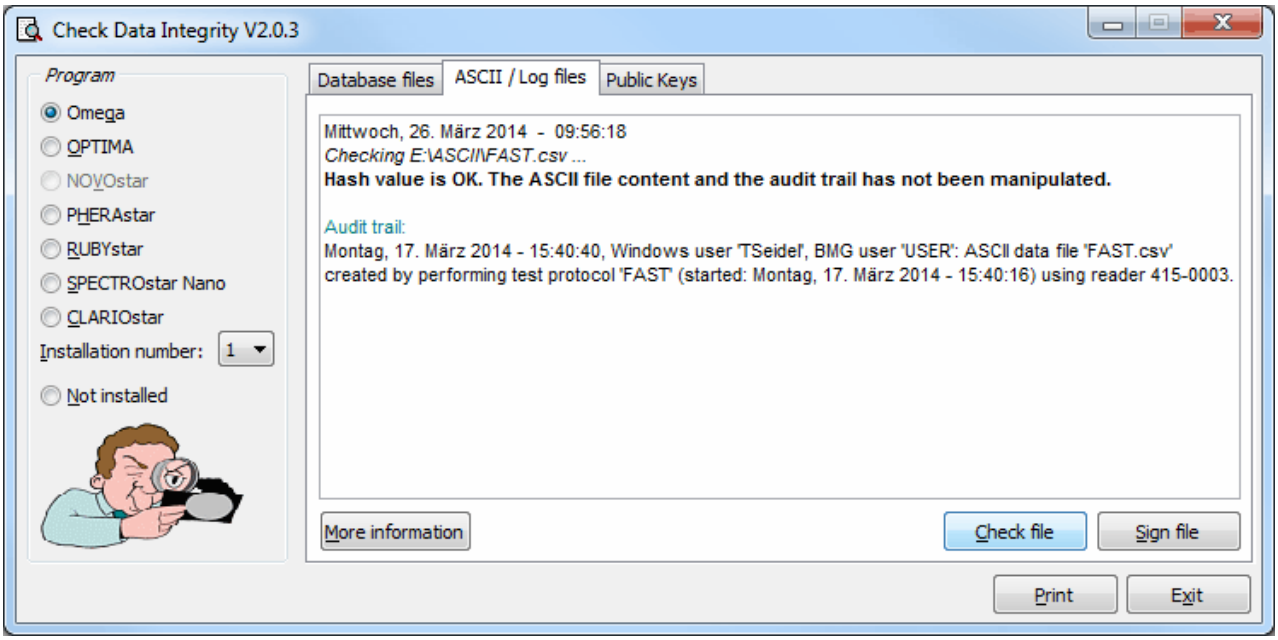
After selecting the **data path** you can choose which **record** you want to check or you can select ‘All records’. To check the integrity of the data and the audit trail and to verify the signatures (if signatures exist) click the ‘**Check integrity**’ button. To display the audit trail and the signatures use the ‘**Audit Trails / Signatures**’ button.

Use the ‘Sign record’ button to sign a data record. The same signature dialogue (see chapter 1.2) will appear as when using the ‘Sign Current Test Run’ command of the data analysis software (see software manual part III).

Note: It is not possible to sign more than one record at a time.

1.3.2 ASCII / Log Files

The second sheet of the 'Check Data Integrity' tools allows you to check data records in ASCII format and to check the program usage log files.

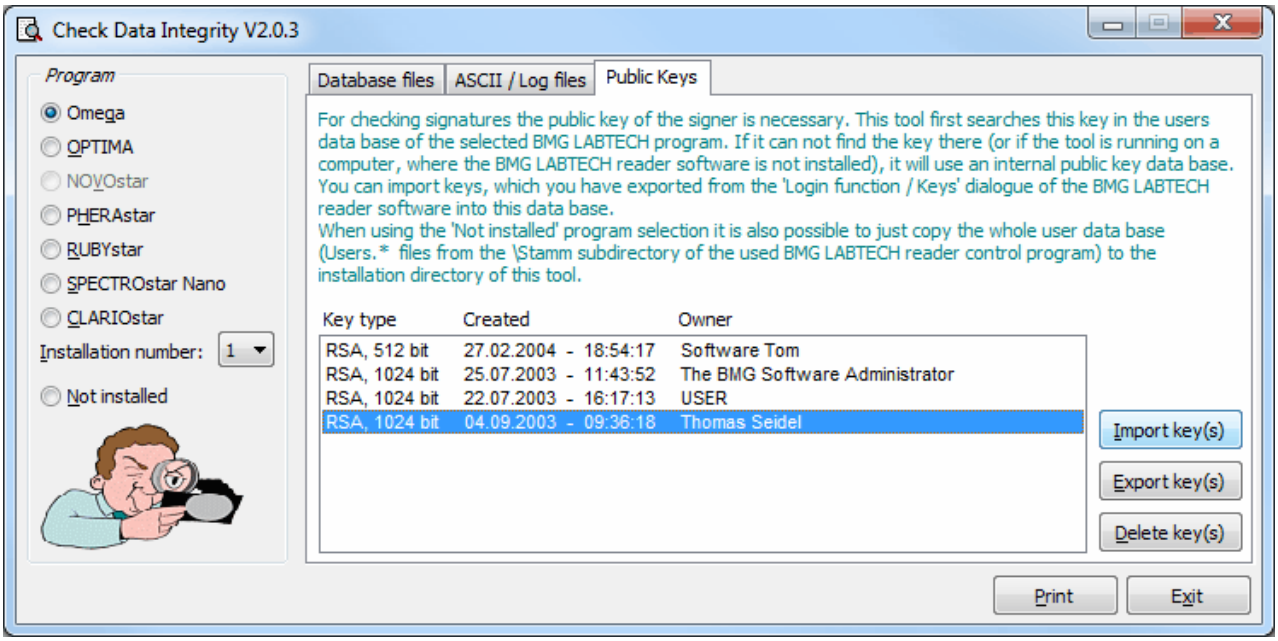


To check the integrity of the data and the audit trail of an ASCII or log file and to verify the signatures (if signatures exist) click the '**Check file**' button. The audit trail and the signatures will be displayed together with the check result.

Use the 'Sign file' button to sign a file. A signature dialogue (see chapter 1.2) will appear.

1.3.3 Public Keys

To verify a signature the public key of the signer is necessary. The BMG LABTECH software stores this key together with the signature, therefore verifying a signature is always possible. Nevertheless, checking the authenticity of the public key is a critical part of verifying digital signatures. The signature verify function of the BMG LABTECH software will try to check the authenticity of the public key by searching this key in the user data base. The 'Check Data Integrity' tool contains a separate public key data base, which is used in addition to the user data base of the reader control program. Using this data base, the 'Check Data Integrity' tool can also be used on computers where the BMG LABTECH reader software has not been installed. It is possible to export keys from the user data base and to import these keys in the public keys data base of the 'Check Data Integrity' tool.



In the Public Keys sheet you can see which public keys are stored in the public key data base. Use the '**Import key(s)**' button to add keys to this data base.

You can also select keys and **export** them (as a backup or to use them on another computer) or you can **delete** keys, which are no longer necessary.

1.3.4 Stand Alone Usage

If you want to use this tool on a computer, where the BMG LABTECH reader software is not installed, copy all files from the '~:\Program Files\BMG_CheckDataIntegrity\' folder and its subfolders into a folder of your choice on the target computer. The Borland Database Engine (BDE) needs to be installed on this computer. Alternatively you can use the normal Omega installation CD-ROM. You only need to perform one installation (Control or Data Analysis part). Please perform a custom installation, where you deselect everything besides the 'Borland Database Engine' and the 'Check Data Integrity' tool.

It is recommended to copy the files from the subfolder '…_CheckDataIntegrity\AdditionalFilesForStand-AloneUsage\<Program Name>' into the directory, where you have installed the 'Check Data Integrity' tool (otherwise this program will ask you to specify the location of the DLLs).

If you want to verify signatures, you should export the public keys from the user data base (see chapter 1.1.1 of software manual part II: Control Software) and import these keys into the public keys data base of this tool (see chapter 1.3.3). Alternatively you can copy the whole user data base (all 'Users.*' files from the '~:\Program Files\BMG\Omega\Stamm' folder into the directory, where you have installed the 'Check Data Integrity' tool.

If you want to sign, you need to copy the user data base to the target computer.

Note: This tool displays date and time information using the format as defined in the Windows Control Panel (Regional Settings) under long or short date and long time format.

2 Support

If you have any problems / questions regarding the software / the instruments, you should visit our web page (http://www.bmglabtech.com) and read the information on the Support page. If you can not find an answer there, please contact BMG LABTECH using the following email addresses:

- Problems / questions regarding software:
  support@bmglabtech.com
- Problems / questions regarding the instruments:
  tech.service@bmglabtech.com

You can also use our on-line bug report form:
http://www.bmglabtech.com/support