

# BM-windream

Data and Document Management System



**BioMedion**

## White Paper

### Evaluation of compliance to FDA Rule 21 CFR part 11 *electronic records, electronic signatures*

Rev. 6

**BioMedion GmbH**  
Knochenmühle 3  
D-37075 Göttingen  
Germany

Tel.: +49-(0)-551-30737-0  
Fax: +49-(0)-551-30737-25

**BioMedion Inc.**  
200 World Trade Center  
939 Merchandise Mart  
Chicago, IL 60654

Tel.: 312-527-5931  
Fax : 312-527-6573

[www.biomedion.com](http://www.biomedion.com)

info@biomedion.com

---

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>FDA Rule 21 CFR part 11 overview</b>	<b>3</b>
2.1	Interpretation of rule 21 CFR part 11	3
2.2	What does the FDA expect?	3
2.3	21 CFR part 11 requirements	3
<b>3</b>	<b>Interpretation of core requirements of 21 CFR part 11</b>	<b>4</b>
3.1	Validation of computer system	4
3.2	Access control to computer system	4
3.3	Use of electronic signatures	4
3.4	Audit trails and versioning	4
3.5	Electronic archival storage	4
<b>4</b>	<b>Technical solutions</b>	<b>5</b>
4.1	Access control based on Windows NT / 2000 and BM-windream user administration	5
4.2	Use of electronic signatures	5
4.3	Change management (Audit Trail) and versioning	5
4.4	Archival storage and retrieval	6
<b>5</b>	<b>21 CFR part 11 evaluation checklist for BM-windream</b>	<b>7</b>

## Introduction

The use of computerized systems in regulated industries like pharmaceuticals, biotech, and medical devices is subject to rules issued by government regulatory authorities. In August 1997, the FDA issued a new rule, regulating the use of electronic records and electronic signatures (21 CFR Part 11, entitled “Electronic Records; Electronic Signatures – final rule”).

The rule 21 CFR part 11 sets forth the requirements that computerized systems need to fulfill in order to allow electronic signatures and electronic records in lieu of traditional paper based records and hand written signatures. 21 CFR part 11 has been developed with contributions of the pharmaceutical industry as this rule and its ongoing implementation will help to speed up the conversion process from elaborate and costly paper based documentation towards electronic systems. In combination with the expected cost reduction, a shorter time to market and streamlining of research processes are further benefits. Regulatory authorities, confronted with the ever-increasing number of new drug applications push the implementation of 21 CFR part 11 to enable fully electronic regulatory submissions that allow a faster and more accurate approval process.

## Scope

21 CFR part 11 applies to all electronic data, documents and signatures that are created, maintained and archived in any GxP/FDA regulated environment. For the pharmaceutical industry as well as medical devices and product companies this affects primarily preclinical and clinical research, submission processes, production and post-marketing surveillance.

Currently 21 CFR part 11 is legally binding for US manufacturers and suppliers and foreign companies, (e.g. from Europe) that offer products and services to the US market.

Outside the scope of the US, compliance to 21 CFR part 11 is not mandatory, but is becoming widely accepted as a new standard within the pharma industry worldwide.

It is to be expected that European regulatory authorities will impose very similar mandatory requirements to computerized systems in the future.

## 21 CFR part 11 in summary

The 21 CFR part 11 requirements are basically:

- Validation of the complete computerized system (hardware, software, users)
- Secure storage of electronic records, data reconstruction of should be possible.
- Computer generated audit trail with time stamp for all records/signatures.
- Controlled access to the computer system.
- Use of electronic/digital signatures for authentication of certain electronic documents

All FDA statements are related to computerized systems – not computers. Following FDA definition a computerized system consists of the following:

- hard- and software.
- trained users
- policies and procedures.

Customers should be well aware that the use of a specific software package does not imply compliance out of the box; instead, additional measures and policies must be implied. BioMedion offers its customers comprehensive consulting and support during implementation, validation and use of its software.

BM-windream fulfills all requirements to implement a 21 CFR part 11 compliant computer system. BM-windream has been validated by BioMedion GmbH to function in a predetermined, predictable and reproducible way according to system requirements specifications that were deduced from 21 CFR part 11 requirements. The following chapters present the results of this evaluation and can assist our customers in their system selection process.

Chapter 2 outlines the 21 CFR part 11 requirements.

Chapter 3 summarizes BioMedion’s interpretations of core 21 CFR part 11 requirements.

Chapter 4 describes the technical solutions implemented by the BM-windream DMS.

Chapter 5 checks individual paragraphs of 21 CFR part 11 against features of the BM-windream system solution.

## Chapter 2

### FDA Rule 21 CFR part 11 – an overview

#### 2.1 21 CFR Part 11 and its interpretation

The FDA regulation 21 CFR Part 11 „electronic records and electronic signatures“ came in effect on August 20, 1997, and is legally binding within the US. Compliance to the rule is now obligatory for all institutions and industries that are governed by GxP and other predicate rules. The FDA is increasingly inspecting computerized systems for 21 CFR part 11 compliance in such environments.

However, 21 CFR part 11 and its paragraphs leave room for individual interpretations, an aspect that is in a way intended by the FDA. With this rule, the FDA aims to enable the use of state of the art technology and its ongoing development in compliance with the rule. On the other hand the FDA cannot provide industry with simple step-by-step guidelines to compliance. Responsibility and interpretation of the rule lies still with the responsible persons in the companies, and it must be decided how the somewhat general rules outlined in part 11 need to be implemented in the individual situation.

Therefore the FDA as well as independent institutions like the GAMP forum published additional guidance. These documents are helpful in assisting the implementation of 21 CFR part 11 in corporate situations.

BioMedion's interpretation of 21 CFR part 11 follows widely accepted interpretations like that of GAMP and is also based on our own experience. As a solution partner, BioMedion is in constant contact and discussion with industry and regulatory authorities and is continually updating its interpretation to the current level of understanding.

#### 2.2 What does the FDA expect?

21 CFR part 11 was issued to enable the use of modern information technology in accordance with the existing regulations. Besides the expected acceleration of innovation and production processes it is the main goal of the FDA to ensure that falsification, abuse and misinterpretation as well as non-detectable changes of electronic data and electronic signatures are prevented. The FDA expects full compliance to the rule from all institutions, laboratories and organizations that are working under the GxP regulations; however, individual requirements must be judged on a case-by-case basis. Implementation of 21 CFR part 11 has an impact on most processes and equipment usage for the institutions and persons governed by the regulation.

#### 2.3 21 CFR part 11 requirements

The requirements outlined in 21 CFR part 11 relate to individual electronic records and electronic signatures as well as to the complete computer system that is used to create, maintain and save data. An electronic record is every single file that is created or changed by automated systems or employees during GxP related work. The moment a file is saved to a durable medium (e.g. hard disk drive, floppy disk, CD, DVD, etc.) an electronic record with respect to 21 CFR part 11 is created. The electronic signature is defined as the computer based registration of symbols or symbol series that are adopted, executed and released by a single person to be the legally binding equivalent of their hand written signature.

The following outline some requirements:

1. Validation of computer system (incl. hardware, software, procedures, user training...).
2. Access control to computer system.
3. Use of electronic signatures that are the legally binding equivalent of a hand written signature.
4. History and audit trail of all versions of a document. Traceability of all changes with the possibility to reconstruct previous versions.
5. Electronic archive that ensures protection of data, loss and change of data.

## Chapter 3

### Interpretation of core requirements of 21 CFR part 11

#### 3.1 Validation of computer system

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

BioMedion's understanding of validation encompasses a structured, planned and documented approach to system implementation. Starting with the definition of business-, quality- and compliance goals by senior management through the definition of user- and technical requirements up to system design, implementation, testing and release (s. fig.1 in appendix: V-model of validation process). BioMedion's services include support and assistance to internal planning and validation processes of the customer.

#### 3.2 Access control to the computer system

§ 11.10 (d) *Limiting system access to authorized individuals...*

Only authorized persons shall have access to the computer system. This is to prevent change, falsification and deletion of data through unauthorized persons. Access can be limited by physical means ("locking the doors") and logical means (user-id and password based system login, hierarchy of user authorization levels). Security measures should be sophisticated (hard to crack) but easy to use in order to assure a high degree of user acceptance.

#### 3.3 Use of electronic signatures

§ 11.50 (a) *Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:*

- (1) *The printed name of the signer;*
- (2) *The date and time when the signature was executed; and*
- (3) *The meaning (such as review, approval, responsibility, or authorship) associated with the signature....*

An electronic signature must be the legal equivalent of a hand written signature. Users have to be aware of this. The system must clearly notify users each time before they execute such a legally binding electronic signature. This signifies that the signer bears the responsibility for the result of the act of signing. Falsification and deletion as well as masquerade and impersonation of the electronically signed data should be easily and readily detectable by the average user as well as by inspecting authorities.

#### 3.4 Audit trails and versioning

§ 11.10 (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.*

In BioMedion's understanding the audit trail is a complete track of all operations, which modify the contents or format of any electronic file during the entire document lifecycle. Audit trails should be irreversibly bound to the respective data files. Audit trail entries will be created by the system automatically and not accessible to changes or deletions by the user. Audit trail entries consist of listing of involved users as well as electronic date and time stamps and user comments if necessary. Versioning allows to trace back different versions and pre-versions without loss of information.

#### 3.5 Electronic archival storage

§ 11.10 (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. (c) Protection of Records to enable their accurate and ready retrieval throughout the record retention period.*

All data saved shall be archived in a manner that is readable to human beings as well as to machines. Where proprietary formats are in use, the timely conversion in long-time compatible formats (e.g. PDF or ASCII) is strongly recommended. Physically archived data are stored to stable media – preferably magneto-optical devices (CD, DVD, WORM) – which guarantee data stability and recoverability for at least as long as the stored data need to be kept available for inspection.

## Chapter 4 Technical Solutions

### **With BM-windream, BioMedion offers a complete solution package for the 21 CFR Part 11 compliant management and archiving of electronic data and documents.**

Technical requirements of 21 CFR part 11 that are to be met by system specifications are:

- System access control
- Use of electronic signatures
- Documentation of file history (audit trail and versioning)
- Long term archival and retrieval

#### **4.1 Access control based on Windows NT / 2000 and BM-windream user administration**

The requirements regarding access control can be met with the following BM-windream functions.

- ✓ Centralized user administration (create, lock, de-activate, assign to groups) can be managed by system administrator.
- ✓ Unique combination of user-ID and password. Passwords are centrally administered on the basis of Windows NT / 2000 and encrypted in a database.
- ✓ User authorization levels for different users and groups.
- ✓ Nesting of groups possible.
- ✓ Password aging (users need to change passwords after a given time according to user specific configuration).
- ✓ System is able to ask for a new password upon first login.
- ✓ Users can be disabled following n (n= user definable number) unsuccessful login attempts; only system administrator can re-enable the user account.
- ✓ Automated logoff after a predetermined interval of user-inactivity (user definable).
- ✓ Login and logoff without the need for complete system (client) shutdown.
- ✓ Log-functions / audit trail: all administrator-actions, online-actions: login, logoff (manually), logoff (automatically), invalid entries of user name and password, system lockup after repeated unsuccessful login attempts, change of password through user.
- ✓ User accounts cannot be deleted. Only inactivation of individual accounts is possible.

BM-windream offers an SOPhisticated security and access management that complies with all 21 CFR Part 11 requirements. Authorization to read, change or administrate specific documents or files can be assigned to individual persons or user groups. Even complex authorization structures can be reproduced through nesting of user groups.

#### **4.2 Use of electronic signatures**

BM-windream provides the use of electronic signatures on the basis of SmartCard technology. This solution allows:

- ✓ Administration of signatures (date and time stamp, user, reason for signature, signature) within the BM-windream-database.
- ✓ Administration of private keys on smart cards.
- ✓ Use of existing PKI-structures is possible.

#### **4.3 Audit trail and version control**

BM-windream tracks changes by the following means:

- audit trail (who has created/changed the document/file, date, time?) and
- version control (track of all previous versions)

All actions and operations performed with or within a document/file are automatically tracked through BM-windream in the background. Every operation is recorded automatically with an electronic date and time stamp. This record includes type of operation/change performed as well as the user that performed the operation. Additionally different versions of a document can be created, thus enabling reconstruction of a change history. The system administrator can define rules governing the versioning. Less important documents can be processed like in the file system whereby user and date of operation are recorded in the audit trail, yet versions are not automatically created. For use in quality-critical environments the system can be configured to force new versions by default when

documents are processed. BioMedion will assist with recommendations on system configuration on an individual basis.

#### **4.4 Archiving and retrieval**

BM-windream offers a scalable approach to longtime archival to best serve the different requirements of our customers. Archival storage is usually performed with CD/DVD or WORM-Jukebox technology. Other technical storage options are also available. Besides the files themselves all meta information (indexes, signatures, user authorization, audit trail, etc.) concerning the files is archived along with the respective data files.

Data in archival storage devices is nonetheless kept available for online retrieval. Users and auditors can access data in long time archival storage anytime. However, these files cannot be changed or altered anymore. All data sets (meta information, audit trail, versioning etc.) are recorded in a relational database. Digital signatures are recorded into this database as index information of a given document as well.

All files are recorded in their original file format. Long time archival storage is operated by an internal archiving system that triggers the CD-, DVD- or WORM-Jukebox. To minimize possible problems with proprietary file formats the next release of BM-windream will include a file render engine that automatically converts archived data to standard, long term formats like ASCII or PDF. Manually invoked conversion is already possible in the current release.

All file versions can be retrieved and exported to non-BM-windream systems. Meta information (indexes, signatures, user authorization, audit trail, etc.) are exported in HTML- or XML-format and are therefore available for off-site inspection.

## Chapter 5

### Evaluation checklist for BM-windream

Use of computerized systems in regulated industries like pharma, biotechnology and medical devices is subject to respective regulations issued by the regulatory authorities, especially the FDA rule 21 CFR Part 11 concerning electronic records and signatures. BM-windream is able to fulfill all the technical requirements that are imposed by this rule. The following list checks individual requirements of the rule against the features offered by BM-windream.

21 CFR 11 § No.	Question/requirement	Yes / No	Comments to BM-windream
<b>Electronic record</b>			
Paragraph 11.10: Controls for closed systems			
§ 11.10 (a)	Is the system validated?	Yes	BioMedion is following the V- phase model according to GAMP (4) guidelines for system- and software validation (DQ, IQ, OQ, PQ). The system and all relevant functions have been tested and validated. For full regulatory compliance, the system needs also to be validated at the customer's site on implementation. BioMedion supplies test procedures, documentation and validation services for BM-windream.
§ 11.10 (a)	Is it possible to discern invalid or altered records?	Yes	All operations and changes to or within a file or document are automatically recorded in the background by BM-windream. Every action is recorded with an electronic date and time stamp. Type of operation is recorded as well as the user that is performing the changes. A change history is created via versioning.
§ 11.10 (b)	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?	Yes	BM-windream, includes an electronic archive system. Long time archival storage is on CD-, DVD- or WORM-jukeboxes (other options available). Archiving includes the original data as well as meta-data such as audit trail, version information, e-signatures etc. All files are readily exportable in their original format. Meta information (indexes, audit-trail, etc.) is exported in HTML- or XML-format for off-line inspection or import into other systems.
§ 11.10 (c)	Are there records readily retrievable throughout their retention period?	Yes	Storage on devices like CD-R, DVD-R, WORM ensures long time revision-proof access and stability of electronic records. The BM-windream archive manages and tracks long-term storage media for quick retrieval.
§ 11.10 (c)	Can data retention set to a given time?	Yes	BM-windream features an automatic life-cycle management that can be set to manage the storage, retention and ultimate deletion of files and associated meta-data. Multiple life-cycles with different retention periods can be managed simultaneously to accommodate varying retention requirements under different predicate rules.
§ 11.10 (c)	Are there any tools/utilities that enable the use of records that have been created with expired software that is now unavailable and ensure readability of such records in the future?	Yes	Proprietary file formats can be converted to open/generic formats like ASCII, TIFF or PDF for long-term archival. BM-windream archives the files in both original format and generic format for future retrieval.

§ 11.10 (c)	Is there a given procedure for archival storage and data maintenance during retention time?	Yes	Electronic records can be archived and retrieved on CD / DVD / WORM using the BM-windream long-term archive. Other mass storage devices can be easily connected or data can be transferred to an already existing archive system.
§ 11.10(d)	Is system access limited to authorized individuals?	Yes	BM-windream is based on Windows NT/2000 user administration, which restricts access to authorized users. Windows NT/2000 user management has to be configured accordingly.
§ 11.10 (d)	Are there policies and procedures that regulate access control?	Yes	BioMedion assists in establishing policies and procedures for access control. Sample SOPs can be provided. The BM-windream module „SOP management“ can be used to create, control and publish SOPs.
§11.10(e)	Is there a secure, computer generated time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?	Yes	All operations that change a document are automatically tracked in the background by BM-windream. Every operation is recorded with an electronic date and time stamp. This includes type of operation/change as well as the user who performed the task. Thus a detailed audit-trail for each document is generated over the entire document lifecycle. Users cannot ultimately delete data files.
§ 11.10 (e)	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?	Yes	Depending on user requirements the system can be set to create a new document version by default each time the document is saved. Previous versions are retained and secured against any changes. The resulting “version trail” allows reconstructing a seamless change history. In some cases, (e.g. SOP development) versioning is not recommended for each save operation. Versioning should be invoked during the review/authorization/publishing process. BioMedion offers support for SOP development and system configuration.
§ 11.10 (e)	Is the reason for a change/operation recorded?	Yes	A comment field is available in the audit trail and version trail functions. An SOP for the users of the system should govern use of this field.
§ 11.10 (e)	Is the audit trail of a given electronic record retrievable during the retention period?	Yes	Yes, there is a direct, inseparable relation of the audit trails to the file (SQL-Database).
§ 11.10 (e)	Is the audit trail available for review and copying by the FDA?	Yes	The audit trail can be viewed via the document properties. Audit trail information can be exported in HTML-or XML-document format together with respective documents or files. Thereby the audit trail is available for off-site inspection without the need for the auditor to have direct access to the BM-windream system/software.

§ 11.10 (e)	Time records of audit trail should refer to a given standard time.	Yes	Recommended server: Windows 2000. Using NET-TIME the server calibrates with public timer servers. All connected clients are synchronized automatically with the Primary Domain Controller (PDC).
§ 11.10 (f)	If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process control system)?	No	BM-windream is not a process control system. Process control systems can be linked up to the system. A separate workflow module is available for BM-windream, which allows modeling of document workflows.
§ 11.10 (g)	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?	Yes	Authorisation to read or change certain folders or documents can be assigned to departments, groups or single users. Electronic documents can only be signed by authorized individuals in BM-windream.
§ 11.10 (h)	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminal) does the system check the validity of the source of any data or instructions received?	Yes	The system can be set to check the data source (i.e. input device) and refuse data from any non-valid sources.
§ 11.10(i)	Is there documented training, including on the job training for system users, developers, IT support staff?	Yes	BioMedion offers user training with respect to system use, 21CFR11 compliance and compliant system administration.
§ 11.10(i)	Documented evidence of education, training and experience of persons that develop, service and use ER/ES systems is required.	n.a.	Training and education of BioMedion-employees is documented. Education and training of customer's employees can be performed and documented through BioMedion.
§ 11.10(j)	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	n.a.	This is the customer's responsibility. Customers should decide on an operating agreement to implement digital signatures as legally binding equivalent. BioMedion offers support on drafting of such agreements.
§ 11.10(k)	Are the distribution of, access to, and use of systems operation and maintenance documentation controlled?	Yes	This is the customer's responsibility. BioMedion offers consulting and assistance to customers for drafting the needed policies and SOPs.
§ 11.10 (k)	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail of changes?	Yes	This is the customer's responsibility. BM-windream can be used manage this type of documentation in a compliant way.
<b>Electronic signatures</b>			
Paragraph 11.50: Signature Manifestation			
§ 11.50 (a)	Do signed electronic records contain the following related information? -The printed name of the signer -The date and time of signing -The meaning of the signing (such as approval, review, responsibility)	Yes	The signature-history of BM-windream records the requested information. The signature history can be printed with any document.
§ 11.50 (b)	Is the above information shown on displayed and printed copies of the electronic record?	Yes	The signature history window shows date, time of signature and the name of the signer and the meaning of the signature on the screen. This information can also be printed. The signature check function allows to verify that the document remained unchanged since it had been signed.

Paragraph 11.70: Signature/record linking.			
§ 11.70	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	Yes	The digital signature links the signer with the signed documents. A special algorithm creates a new encrypted code (hash value) from the signature each time a document is signed. This code confirms the identity of the signer and prevents undetected falsification.
<b>Electronic signatures (general)</b>			
Paragraph 11.100: general requirements			
§ 11.100 (a)	Are electronic signatures unique to an individual?	Yes	The digital signature is executed as a combination of private key and PIN-number. The private key that is encrypted on a SmartCard is assigned to its genuine owner. SmartCards are issued upon request for each individual owner by a trusted certification centre.
§ 11.100 (a)	Are electronic signatures ever reused by, or reassigned to, anyone else?	n.a.	SmartCards are unique. It is the customer's duty to ensure that only authorized and trained employees receive SmartCards.
§ 11.100 (b)	Is the identity of an individual verified before an electronic signature is allocated?	Yes	The SmartCard includes the private key of the genuine user and the tamper-proof signature software. Smart cards can only be activated by the genuine user by inserting the card in the card reader and the entry of the users' unique (secret) PIN. If the card gets lost or stolen, the system can be set not to accept this card anymore.
§ 11.100 (c)	Confirmation with regulatory authority that electronic signatures are used as an equivalent to handwritten signatures.	n.a.	FDA needs an informal confirmation that electronic signatures are to be used in the company.
Paragraph 11.200: Electronic signatures (non-biometric)			
§ 11.200 (a)(1)(i)	Is the signature made up of at least two components, such as an identification code and password, or an ID card and password?	Yes	SmartCards issued for individual users by a trust center can only be activated by the genuine user by inserting the card in the card reader and the entry of the user's PIN. Signed documents are encrypted asymmetrically, decryption of this document is only possible if public and private keys match.
§ 11.200 (a)(1)(ii)	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session)	Yes	During a continuous session several signatures can be executed with repeated PIN entry. The system <u>always</u> records both signature components.
§ 11.200 (a)(1)(ii)	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	Yes	SmartCard and PIN-Number must be used every time a document needs to be signed regardless whether the session is continuous or not.
§ 11.200 (a)(2)	Are non-biometric signatures only used by their genuine owners?	n.a.	It is the customer's duty to ensure that SmartCards are only used by their genuine owner and the PIN-number is not disclosed to anyone.
§ 11.200 (a)(3)	Has it been shown that biometric electronic signatures can only be used by their genuine owner?	n.a.	The system does not employ biometric signatures.

Paragraph 11.300: Control of identification codes and passwords			
§ 11.300(a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	Yes	Yes, Win NT/2000 functionality and SOP's.
§ 11.300(b)	Are procedures in place to ensure that the validity of identification codes is periodically checked?	n.a.	Must be governed by an SOP.
§ 11.300(b)	Do passwords periodically expire and need to be revised?	Yes	Win NT / 2000 functionality. Validity of passwords can be defined (Password-aging)
§ 11.300(b)	Is there a procedure for recovering identification codes and passwords if a person leaves or is transferred?	No	Data can only be recovered by a super-user login. This requires the simultaneous login two or more authorized administrators (4-eye principle).
§ 11.300(b)	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	Yes	BM-windream can be configured to disable authentication of SmartCard / PIN-combinations after n (n= configurable by system administrator) unsuccessful login attempts. Disabling of a user can only be reverted by the system administrator.
§ 11.300(c)	Is there a procedure for changing an identification code or password if it has been potentially disclosed or lost?	Yes	Smart card owners themselves can change passwords. Minimum requirements for passwords can be defined (length, characters, mixture etc.)
11.300(c)	Is there a lost management procedure to be followed if a device is lost or stolen?	Yes	Lost SmartCards can be permanently invalidated by the trust center.
§ 11.300(d)	Is there a procedure for detecting attempts of unauthorized use and for informing security?	Yes	All attempts of unauthorized access are recorded. Analysis of these protocols has to be governed by an SOP.
§ 11.300(e)	Is there initial and periodic testing of tokens and cards?	Yes	An SOP should govern procedures for initial and continuous verifying of SmartCards.
§ 11.300(e)	Does this testing check that there have been no unauthorized alterations?	Yes	The trust center issues a certificate that includes a unique identification of its owner and its public key for signature verification. The trust center is able to control whether unauthorized persons have altered the certificate.