Tools to Aid in 21 CFR Part 11 Compliance with EZChrom Elite Chromatography Data System

White Paper

By Frank Tontala

Agilent Technologies
Software & Informatics
Life Sciences & Chemical Analysis Group
Tools to Aid in 21 CFR Part 11 Compliance with EZChrom Elite CDS

Introduction
Agilent Technologies, Inc. is pleased to offer the EZChrom Elite chromatography data system (CDS) as a solution for chromatography labs seeking to operate in a regulated environment. EZChrom Elite represents over 14 years of experience in the CDS market. Its use of industry standard technology such as Microsoft’s® COM, DCOM, ActiveX and .NET, and its awareness of regulatory compliance requirements, enables EZChrom Elite to be a powerful CDS for enterprise deployments.

EZChrom Elite is able to control over 330 modules from approximately 25 different vendors. While the technology provides a powerful offering for the research laboratory in the industrial sector, we have also paid close attention to the needs of laboratories that must adhere to regulatory requirements. One of the most important of these requirements is that of the FDA’s 21CFR Part 11 regulations.

This document is intended to provide an overview of the compliance capabilities of EZChrom Elite version 3.2 and higher as they relate to 21 CFR Part 11. It is not a certificate of validation or compliance, nor a warranty of such.

General Overview
The final Food and Drug Administration (FDA) ruling on electronic records and electronic signatures has been in effect since August 20, 1997.

While EZChrom Elite provides significant and extensive compliance tools to facilitate compliance, the ultimate responsibility rests with the enterprise employing the technology. Complete compliance therefore requires that the enterprise employing this functionality have the appropriate internal Standard Operating Procedures (SOP). Articles that can only be satisfied by an SOP are indicated as such in the detail below.

This section will outline the top-level issues. The next section will go into some detail and it will follow the organization of the ruling.
General Considerations

EZChrom Elite is a scalable enterprise data system that can be installed as a single workstation or in a full client/server configuration. When installed and managed in a compliant manner, EZChrom Elite is defined a ‘Closed System’. The ruling defines a closed system as:

... an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.\(^1\)

In addition to the minimum Electronic Signature (e-sig) requirements specified by the FDA, EZChrom Elite offers some additional important enhancements:

1. Up to 5 levels of signature hierarchy. The roles are definable by the system administrator and hence can be tailored to the specific SOP requirements.
2. Reasons for a signature are definable by the system administrator; once set, they are fixed and are unalterable by users. An additional free text field is available for any supplemental comments.
3. Time-outs are definable by the administrator to ensure that only the appropriate individual is involved in the e-signature process.
4. While allowable, e-signature revocation can only be performed by the highest signatory in the hierarchy. Of course all activities are recorded in the appropriate log or audit trail.

Subpart B: E-Records: Controls for Closed Systems

11.10a Has the system been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?

Yes  Agilent Technologies, Inc. has extensively validated EZChrom Elite’s performance with tests written to specifically evaluate accuracy, reliability and consistent performance. All data, sequences and methods have embedded audit trails that are CRC checksummed to discern invalid or altered records.

11.10b Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by the FDA?

Yes  EZChrom Elite maintains the integrity of all data files using a unique checksum algorithm. These files and the resulting reports are available for review and inspection.

11.10c Are the records protected to enable the accurate and ready retrieval throughout the record retention period?

Yes  All records are protected in secure storage locations and are readily retrievable. For additional long-term protection and archiving, the Agilent OL ECM (Electronic content Manager) may be utilized.

---

\(^1\) Federal Registrar, Part II, Department of Health and Human Services, FDA, 21 CFR Part 11, Sect. 11.3 - Definitions, Item 4, pg. 13465.
11.10d Is system access limited to authorized individuals?
Yes EZChrom Elite works with the Microsoft Windows Active Directory (AD) user lists to authenticate users based on their AD login name and password. The system administrator assigns rights to each function in the software on a per individual or AD Group basis.

11.10e Is there a secure, computer-generated, time-stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records?
Yes The secure, computer-generated, time-stamped audit trail is embedded with the data itself to insure long-term retention and association. For additional long-term retention, archiving and data management, the Agilent OL ECM (Electronic content Manager) may be utilized.

11.10e When records are changed, is previously recorded information left unchanged?
Yes All versions of the data and methods are maintained. In addition, all changes are added to the audit trail. There is no overwriting of information.

11.10e Are electronic audit trails kept for a period at least as long as their subject electronic records' and available for agency review and copying?
Yes Audit trails exist for the system and for each instrument, as well as for methods, sequences and data and report templates. The secure, computer-generated, time-stamped data audit trail is embedded in the file itself to insure long-term retention and association.

11.10(f) Are operational system checks used to enforce permitted sequencing of steps and events?
Yes Within EZChrom Elite, users are stepped through sequences and events; data cannot be acquired unless parameters are within valid instrument and data processing ranges. Users are prompted with an error message when steps are performed out of sequence.

11.10(g) Are authority checks in place 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?
Yes EZChrom Elite works with the Microsoft Windows Active Directory (AD) user lists to authenticate users based on their AD login name and password. The system administrator assigns rights to each function in the software on a per individual or AD Group basis.

11.10(h) Are device checks used to determine, as appropriate, the validity of the source of data or operational instruction?
Yes Integration with instruments through comprehensive automation and control provides various levels of device and validity checks depending on the instrument make and model.
<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.10(i)</td>
<td>Do the persons who develop, maintain, or use electronic records/signature systems have the education, training, and experience to perform their assigned tasks? Yes</td>
</tr>
<tr>
<td></td>
<td>Records of the educational and employment history of Agilent Technologies, Inc. employees are verified and kept with personnel records that can be made available during an on-site audit of Agilent. In addition, all Agilent Technologies, Inc. employees have attended training workshops on regulatory requirements. Users of EZChrom Elite at a customer location will be required to show records or education, training and/or experience with the system. Training is available from Agilent Technologies, Inc.</td>
</tr>
<tr>
<td>11.10(j)</td>
<td>Have written policies been established, and adhered to, that hold individuals accountable and responsible for actions initiated under their e-signatures in order to deter record and signature falsification? N/A</td>
</tr>
<tr>
<td></td>
<td>It is the responsibility of the organization implementing electronic signatures to develop written policies that ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature.</td>
</tr>
<tr>
<td>11.10(k)(1)</td>
<td>Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance? N/A</td>
</tr>
<tr>
<td></td>
<td>While documentation is available for EZChrom Elite users and administrators, controls over the storage and distribution of this material are the responsibility of the end user.</td>
</tr>
<tr>
<td>11.10(k)(2)</td>
<td>Are there formal revisions and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation? Yes</td>
</tr>
<tr>
<td></td>
<td>Agilent Technologies, Inc.’s ISO 9001 certified quality process includes formal written revision and change control procedures for systems documentation. The process includes the use of the Agilent OL ECM for the maintenance of system documentation. All revisions to the documents kept and are time stamped and audit trailed.</td>
</tr>
</tbody>
</table>

**Controls for Open Systems**

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.30</td>
<td>Are there procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt? N/A</td>
</tr>
<tr>
<td></td>
<td>EZChrom Elite is a closed system.</td>
</tr>
<tr>
<td>11.30</td>
<td>Are additional measures used to ensure the confidentiality of the electronic records from the point of their creation to the point of their receipt? N/A</td>
</tr>
<tr>
<td></td>
<td>EZChrom Elite is closed system.</td>
</tr>
</tbody>
</table>
Signature Manifestations

11.50 (a) Do the signed electronic records contain information associated with the signing that clearly indicates the following:
1. Printed name of signer,
2. Date and time that the signature was executed
3. The meaning associated with the signature?

Yes Both the machine-readable data and the human readable report contain the name, date / time and meaning. An electronic signature time-out is provided for added security.

11.50 (b) Are these items part of any human readable form of the electronic record?

Yes Both the machine-readable data and the human readable report contain the name, date / time and meaning.

Signature / Record Linking

11.70 Is the electronic signature linked to its respective electronic record to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means?

Yes Signed records have a unique checksum that prevents signatures from being excised, copied or otherwise transferred.

General Requirements

11.100 (a) Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?

Yes Through the use of Microsoft® Active Directory security, users signatures are unique and cannot be reused or reassigned.

11.100 (b) Are the identities of the individual verified prior to the establishment, assignment, and certification or otherwise sanctioning an individual’s electronic signature or any element of an electronic signature?

N/A This would be a requirement of the customer before implementing electronic signature procedures and/or assigning electronic signature privileges to an individual.

11.100 (c) Has the Company delivered its corporate electronic signature certification letter to the FDA?

11.100 (c)(1) Is it in paper form with a traditional handwritten signature?

11.100 (c)(2) Can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer’s handwritten signature?

N/A It is the Company’s responsibility, before a submitting electronically signed documentation to the FDA, to register their intent to use electronic signatures. In addition, training programs must be in place to ensure that users signing documents electronically understand the legal significance of their electronic signature.
**Electronic Signature Components and Controls**

**11.200 (a)(1)** Does the e-signature employ at least two distinct identification components such as User ID and password?

Yes  
The EZChrom Elite electronic signature tools employ two distinct components, username (unique) and password.

**11.200 (a)(1)(i)** When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components?

Yes  
When an individual signs the first of a series of documents during a single period of controlled access the user is required to enter both signature components; username / password.

**11.200 (a)(1)(ii)** When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed using at least one electronic signature component that is only executable by, and designed to be used by, the individual?

Yes  
When an EZChrom Elite user executes a series of continuous electronic signatures (defined as signatures executed within a system administrator determined period of time) they are required to enter username, password and reason on the first signature only. Each subsequent signature requires only the user’s password, which is known only to the user.

**11.200 (a)(1)(ii)** When an individual executes a series of signings not performed during a single, continuous period of controlled system access; does each signing executed require all signature components?

Yes  
When an EZChrom Elite user executes a series of non-continuous electronic signatures (defined as signatures executed outside of a system administrator determined period of time) they are required to enter username, password and reason on each signature.

**11.200 (a)(2)** Are controls in place to ensure that only their genuine owners can use the electronic signature?

Yes  
Through the use of Microsoft Windows Active Directory security, no two users can have the same username and password.

**11.200 (a)(3)** Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual’s electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals?

Yes  
EZChrom Elite uses the user’s user name and password to initiate the electronic signature. The system can be configured such that an administrator can assign an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this manner, the username / password combination is known only to the individual.
### Controls for Identification Codes / Passwords

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>11.300 (a)</strong></td>
<td>Are controls in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Through the use of Microsoft Windows Active Directory security, no two users can have the same username and password.</td>
<td></td>
</tr>
<tr>
<td><strong>11.300 (b)</strong></td>
<td>Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Through the use of Microsoft Windows Active Directory security, identification codes and passwords can be periodically checked, recalled and revised.</td>
<td></td>
</tr>
<tr>
<td><strong>11.300 (c)</strong></td>
<td>Are there loss management procedures in place to electronically disable lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>An EZChrom Elite administrator can at any time disable a user account, or issue a new password to an existing account in the event the account becomes compromised. If an EZChrom Elite user forgets his / her password, the system administrator can issue a new one. The user can be required to change this temporary password at their next login attempt.</td>
<td></td>
</tr>
<tr>
<td><strong>11.300 (d)</strong></td>
<td>Are transaction safeguards in use to prevent unauthorized use of passwords and/or identification codes?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EZChrom Elite can be configured such that only the user knows their username / password identification code. Passwords are always displayed as asterisks and are stored encrypted within the database so that even an administrator cannot see them.</td>
<td></td>
</tr>
<tr>
<td><strong>11.300 (d)</strong></td>
<td>Are transaction safeguards in use 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?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EZChrom Elite can be configured such that unauthorized access attempts lock out the user account and send email notification to a system administrator.</td>
<td></td>
</tr>
</tbody>
</table>