JUMO Cloud und JUMO smartWARE SCADA

Sicheres Datenmanagement und FDA-konforme Messdatenerfassung





Whitepaper

70181000T87Z000K000

V2.00/DE/30048742/2026-02-19

Inhalt

1 Allgemeines 4

1.1 Einleitung 4
1.2 Umsetzung der 21 CFR Part 11 4
1.3 Die Systemkomponenten der IoT-Plattform 4
1.4 Die Software-Komponenten 5
1.4.1 Edge Gateway 5
1.4.2 JUMO Cloud 5
1.4.3 JUMO smartWARE SCADA 5

2 Bewertung der Forderung 6

3 Literaturverzeichnis 21

1 Allgemeines

1.1 Einleitung

In vielen Bereichen der verarbeitenden Industrie – vor allem im Bereich der Pharma- und Lebensmittelindustrie – besteht für die Herstellung von Produkten eine Protokollierungspflicht.

Für das Aufzeichnen von Prozess- und Chargendaten lassen sich sowohl Registriergeräte auf Papierbasis als auch papierlose elektronische Bildschirmschreiber und SPS Systeme einsetzen. Um die aufgezeichneten Daten über einen langen Zeitraum sicher aufzubewahren und schnell auswerten zu können, bedarf es stabiler abgesicherter Systeme und IoT-Plattformen.

Die IoT-Plattform von JUMO zur Prozessvisualisierung, Datenerfassung, -auswertung und -archivierung ermöglicht weltweiten und bei Bedarf auch lokal begrenzten Zugriff auf Messdaten über die gängigen Webbrowser.

Mit der JUMO Cloud wird ein Online-Zugang benötigt, worüber die Kunden weltweit sicher auf ihre Daten zugreifen können. Möchte ein Kunde seine Daten und Server selbst in der Verwaltung haben, kann die JUMO smartWARE SCADA verwendet und im Kundennetzwerk installiert werden. Beide Lösungen sind technisch und optisch auf der gleichen Basis konzipiert worden.

Für die ordnungsgemäße und eindeutig nachvollziehbare Aufzeichnung der übermittelten elektronischen Prozessdaten hat die amerikanische Gesundheitsbehörde „**Food & Drug Administration (FDA)**“ 1997 den 21 CFR Part 11 (Code of Federal Regulations) verabschiedet.

In diesem Gesetz werden die Anforderungen an **Electronic Records & Electronic Signature**, also die papierlose Protokollierung von Produktionsabläufen sowie die der elektronischen Unterschrift, welche der handgeschriebenen Unterschrift entspricht, definiert.

Die Einhaltung der Forderungen des 21 CFR Part 11 bildet die Grundlage für die weltweite Akzeptanz von Produkten der Pharma- und Lebensmittelindustrie.

Dieses „White Paper“ liefert dem Anwender zu jedem Abschnitt der Gesetzestexte eine Aussage zur getroffenen Sicherstellung dieser Forderungen.

1.2 Umsetzung der 21 CFR Part 11

JUMO erfüllt mit den in Kapitel 1.4 „Die Software-Komponenten“, Seite 5 näher bezeichneten Software-Produkten und dessen Funktionseigenschaften die FDA-Forderungen der 21 CFR Part 11 in Bezug auf „Electronic Records“ (elektronische Aufzeichnung) und „Electronic Signature“ (elektronische Unterschrift).

1.3 Die Systemkomponenten der IoT-Plattform

Die IoT-Plattform JUMO Cloud bzw. JUMO smartWARE SCADA (nachfolgend Cloud und SCADA genannt) stellt mit ihren Systemkomponenten im Sinne des 21 CFR Part 11 Folgendes dar:

- Offenes System für die Cloud
- Geschlossenes System für die SCADA

1.4 Die Software-Komponenten

1.4.1 Edge Gateway

Das Edge Gateway ist eine Software, die auf verschiedenen Hardware-Geräten, PCs oder Servern installiert und betrieben werden kann. Es übernimmt die Kommunikation im jeweiligen Netzwerk und sendet die gesammelten Informationen verschlüsselt zur IoT-Plattform. Das Edge Gateway ist unter anderem in den JUMO variTRON-Geräten sowie den intelligenten JUMO-Sensoren mit Single Pair Ethernet (SPE)-Schnittstelle implementiert.

1.4.2 JUMO Cloud

Die IoT-Plattform von JUMO zur Prozessvisualisierung, Datenerfassung, -auswertung und -archivierung ermöglicht weltweiten Zugriff auf Messdaten über die gängigen Webbrowser. Mit der JUMO Cloud wird ein Internet-Zugang benötigt, mit dem die Kunden weltweit sicher auf ihre Daten zugreifen können.

1.4.3 JUMO smartWARE SCADA

Möchte ein Kunde die IoT-Plattform und seine Daten selbst in der Verwaltung haben, kann die JUMO smartWARE SCADA verwendet und im Kundennetzwerk installiert werden.
Die IoT-Plattform von JUMO zur Prozessvisualisierung, Datenerfassung, -auswertung und -archivierung ermöglicht Zugriff auf Messdaten über die gängigen Webbrowser und ist optisch und technisch auf der gleichen Basis wie die JUMO Cloud konzpiert.

2 Bewertung der Forderung

Die folgenden Ausführungen basieren auf der Annahme, dass der Leser über Kenntnisse der grundlegenden Forderungen der 21 CFR Part 11 verfügt.

Absatz	**Anforderungen:** **Subpart B: Electronic Records (Teil B: Elektronische Dokumente)**
§ 11.10	**Controls for closed systems (Kontrollen für geschlossene Systeme)**
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: Werden geschlossene Systeme zum Erstellen, Ändern, Pflegen oder Übertragen elektronischer Dokumente verwendet, sollen Verfahren und Kontrollen eingerichtet werden, um die Authentizität, die Integrität und, falls erforderlich, die Vertraulichkeit der elektronischen Dokumente sicherzustellen und zu garantieren, dass der Unterzeichnende die unterschriebenen Dokumente nicht als unecht zurückweisen kann. Derartige Verfahren und Kontrollen sollen folgende Punkte beinhalten:	
a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. Validierung von Systemen, um Genauigkeit, Zuverlässigkeit, kontinuierliche, planmäßige Leistung und die Fähigkeit, ungültige oder veränderte Dokumente zu entdecken, zu gewährleisten. **Anforderung erfüllt!** • Das System, bestehend aus dem SCADA-Server und den dazugehörigen Edge Gateways. Nur berechtigten Personen ist der Zugriff auf die Systemkomponenten erlaubt. Dieser Zugriff ist mindestens durch Benutzername und Passwort vor Manipulation gesichert. • Das Leitvorgangsarchiv (Audit Trail) zeichnet alle Konfigurations- und Dashboard-Änderungen sowie Manipulationen von Daten auf. Einträge können gefiltert werden. • Rohdaten (Messdaten aus Edge Gateways) können auf Anwendungsebene nicht verändert werden. Sollwertänderungen oder manuelle Werteingangen innerhalb der Anwendung werden im Leitvorgangsarchiv erfasst und gekennzeichnet. • Sichere und verschlüsselte Datenübertragung vom Edge Gateway zum Server. **Verantwortung des System Owners:** Der Zugang zur Hardware, auf der das Edge Gateway installiert ist, sowie zum SCADA-Server muss vor unberechtigtem Zugriff geschützt werden, um eine Manipulation zu verhindern.

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.10	**Controls for closed systems (Kontrollen für geschlossene Systeme)**
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. Die Möglichkeit, akkurate und vollständige Kopien der Dokumente sowohl in für Menschen lesbarer als auch in elektronischer Form zum Zwecke von Inspektionen, Überprüfungen und dem Kopieren durch die Behörde zu erzeugen. Die Behörde soll kontaktiert werden, wenn Zweifel darüber bestehen, ob sie derartige Überprüfungen vornehmen und die elektronischen Dokumente kopieren kann. **Anforderung erfüllt!** • Alle Daten können durch Export oder direkt aus der Datenbank in verschiedenen Formaten exportiert und Dritten zugänglich gemacht werden. • Mit VPN-Zugang ist es möglich, die Prozesswerte direkt über das User Interface einzusehen. Es wird lediglich ein Browser mit Benutzer-Account benötigt. • Mit der Berichtsfunktion können individuelle Berichte erzeugt und Dritten automatisch als PDF, z. B. per Mail, zur Verfügung gestellt werden.
c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period. Schutz der Dokumente, um ein akkurates und jederzeitiges Abrufen während der Aufbewahrungszeit der Dokumente zu ermöglichen. **Anforderung erfüllt!** • Alle Daten werden in der Datenbank des SCADA-Servers gespeichert. • Es gibt die Möglichkeit, eine Hochverfügbarkeit einzurichten, bei der mindestens zwei Server redundant betrieben werden. • Die am SCADA-Server gespeicherten Daten können von berechtigten Personen exportiert und archiviert werden. • Der Zugriff auf die Anwendung ist mit Benutzername und Passwort geschützt. Optional kann eine doppelte Authentifizierung sowie weitere Funktionen (Passwortregel etc.) vom IAM (Identity Access Management; deutsch: Zugriffsrechtesystem) verwendet werden. • Das gesamte SCADA-System (inkl. aller Daten) kann durch ein automatisiertes oder händisches Backup-Konzept gesichert und rückgesichert werden. **Verantwortung des System Owners:** Der Zugriffsschutz und die Archivierung der gespeicherten Daten muss durch den System Owner erfolgen.

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.10	**Controls for closed systems (Kontrollen für geschlossene Systeme)**
d)	Limiting system access to authorized individuals. Begrenzung des Systemzugriffs auf befugte Personen.  • Durch den im IAM hinterlegten SCADA-Systemadministrator werden zu Beginn Rechte vergeben und nach Bedarf erweitert. • Der Zugriff auf die Software-Komponenten ist durch die Vergabe unterschiedlicher Rechte auf befugte Personen begrenzt. • Jeder Benutzer muss sich durch Benutzername und Passwort anmelden.Optional kann eine doppelte Authentifizierung sowie weitere IAM-Funktionen verwendet werden. • Das Ändern von Benutzerrechten darf ausschließlich von dafür berechtigten Personen erfolgen. • Bereits gespeicherte und archivierte Daten bleiben auch bei der Änderung von Rechten unverändert. **Verantwortung des System Owners:** Der Systemzugriff muss durch den System Owner definiert, eingestellt und überprüft werden.
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. Verwendung sicherer, computergenerierter, mit einem Zeitstempel versehener Audit-Trail, um Datum und Uhrzeit von durch Bedienpersonal vorgenommenen Einträgen und Aktionen, die elektronische Dokumente erstellen, ändern oder löschen, unabhängig aufzeichnen zu können. Änderungen an Dokumenten dürfen zuvor vorgenommene Einträge nicht verdecken. Der Audit-Trail muss über einen Zeitraum aufbewahrt werden, der mindestens dem für die entsprechenden elektronischen Dokumente geforderten Dauer entspricht, und soll der Behörde zu Überprüfungszwecken und zum Kopieren zugänglich gemacht werden.  • Die Audit-Trail-Funktion wird über das sogenannte „Leitvorgangsarchiv“ angezeigt. Es zeichnet Änderungen auf der Anwendungsebene (Dashboard und Konfiguration) und auf den Gateways auf (Konfiguration senden). • Der Audit-Trail wird automatisch generiert und kann in der Anwendung nicht konfiguriert oder abgeschaltet werden. • Es ist sichergestellt, dass alle relevanten vom Bedienpersonal ausgelösten Aktionen mit Datum und Uhrzeit automatisch erfasst und im Audit-Trail gespeichert werden. • Audit-Trail-Daten können in der Anwendung nicht geändert oder gelöscht werden. • Audit-Trail- Daten können allen Benutzern jederzeit zur Überprüfung zugänglich gemacht werden (Dashboard).

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.10	**Controls for closed systems (Kontrollen für geschlossene Systeme)**
f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. Durchführung funktionaler Systemüberprüfungen, um – wo anwendbar – die erlaubte Abfolge von Schritten und Ereignissen umzusetzen. **Anforderung erfüllt!** • Die Abfolge von Schritten, wie z. B. der Chargenprotokollierung, ist festgelegt. So kann konfiguriert werden, ob für eine Chargenprotokollierung eine Aktion ausgeführt werden soll oder nicht. • Mit einem Wartungsmodul ist es möglich, die Dokumentation der Ausführung von Arbeitsanweisungen zu erstellen (Standard Operating Procedures „SOP's“).
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. Durchführung von Befugnisprüfungen zur Gewährleistung, dass nur befugte Personen das System benutzen, Dokumente elektronisch signieren, Zugriff auf die Eingabe- oder Ausgabegeräte des Betriebs- oder des Computersystems haben, Dokumente ändern oder den entsprechenden Vorgang manuell durchführen können. **Anforderung erfüllt!** • Durch den im IAM hinterlegten SCADA-Systemadministrator werden zu Beginn Rechte vergeben und nach Bedarf erweitert. • Der Zugriff auf die Software-Komponenten ist durch die Vergabe unterschiedlicher Rechte begrenzt. • Die Zugriffsrechte werden durch das IAM im System geprüft und verwaltet. • Nur befugte Personen mit entsprechenden Rechten können Benutzer anlegen, sperren oder löschen. Historische Aktivitäten von gelöschte Benutzer bleiben auch nach dem Löschvorgang erhalten. • Voraussetzung für den Systemzugang eines Benutzers ist immer eine Anmeldung über eine eindeutige Benutzerkennung (Mindestens: Benutzername und Passwort). • Die Nutzung eines Passwortes kann durch den Administrator zeitlich begrenzt werden. Nach Ablauf dieser Zeit muss der Benutzer ein neues Passwort eingeben oder er verliert die Zugriffsberechtigung. Weitere Passwortrichtlinieneinstellungen sind ebenfalls im Rahmen des IAM möglich.

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.10	**Controls for closed systems (Kontrollen für geschlossene Systeme)**
h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. Durchführung von Geräte- (z. B. Terminal-) überprüfungen, um – wo anwendbar – die Gültigkeit der Dateneingabe- oder der Funktionsbefehlsquelle bestimmen zu können. **Anforderung erfüllt!** • Die IoT-Plattform kann nur durch berechtigte Personen konfiguriert oder bedient werden. • Ein Edge Gateway ist automatisch mit einer Geräte-Identifikationsnummer verbunden und kann so eindeutig zugeordnet werden. **Verantwortung des System Owners:** Der System Owner muss sicher stellen, dass jedes im System verwendete Edge Gateway eine eindeutige Identifikation (Geräte-ID, Passwort) hat.
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. Feststellung, ob diejenigen, die Systeme für elektronische Dokumente oder Unterschriften entwickeln, pflegen oder verwenden, die für diese Aufgaben notwendige Ausbildung und Schulung durchlaufen haben und über die entsprechende Erfahrung verfügen. **Anforderung erfüllt!** • Alle an der Entwicklung der IoT-Plattform und der dazugehörigen Edge Gateway-Software beteiligten Personen wurden bezüglich der Inhalte und Anforderungen der 21 CFR Part 11 geschult.
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. Festlegen und Einhalten von schriftlichen Verfahrensanweisungen, dass Einzelne für unter ihrer elektronischen Unterschriften vorgenommene Handlungen verantwortlich gemacht werden, um so Abschreckungsmechanismen für das Fälschen von Dokumenten und Unterschriften zu schaffen. **Anforderung erfüllt!** • Die Texte zur Aufforderung der elektronischen Unterschrift können durch den Anwender frei formuliert werden. **Liegt in der Verantwortung des System Owners.**

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.10	**Controls for closed systems (Kontrollen für geschlossene Systeme)**
k)	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 systems documentation. Einsatz geeigneter Kontrollen über Systemdokumentation, inklusive: 1) Adäquate Kontrollen bei der Verteilung von, dem Zugriff auf und der Verwendung von Dokumentation zur Systembedienung und -wartung. 2) Revisions- und Änderungskontrollverfahren, um so einen Audit-Trail zu erhalten, der die zeitliche Reihenfolge der Entwicklung und Veränderung der Systemdokumenta tion dokumentiert. **Nicht zutreffend!** **Liegt in der Verantwortung des System Owners.**

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.30	**Controls for open systems (Kontrollen für offene Systeme, JUMO Cloud)**
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. Werden offene Systeme zum Erstellen, Ändern, Pflegen oder Übertragen elektronischer Dokumente verwendet, sollen Verfahren und Kontrollen eingerichtet werden, die dafür bestimmt sind, die Authentizität, die Integrität und, falls erforderlich, die Vertraulichkeit der elektronischen Dokumente von der Erstellung bis zum Erhalt sicherzustellen. Derartige Verfahren und Kontrollen müssen, wo anwendbar, die in § 11.10 dargelegten Anforderungen berücksichtigen und weitere Maßnahmen umfassen, so z. B. die Dokumentenverschlüsselung und den Einsatz geeigneter Standards für digitale Unterschriften, um, soweit unter den gegebenen Umständen notwendig, die Authentizität, Integrität und Vertraulichkeit der Dokumente zu gewährleisten.	
	Anforderung erfüllt! • Beim Betrieb als offenes System (Cloud) werden durchgängige kryptografische Verfahren nach dem aktuellen Stand der Technik verwendet. Diese stellen die Vertrauenswürdigkeit und den Manipulationsschutz während der Datenübertragung vom Edge Gateway zum Cloud Server sicher. • Das verwendete IAM-System ist für die Anforderungen an ein offenes System konzeptioniert und eingestellt worden. • Der Zugriffschutz auf Systemadministrator-Ebene (IT) ist ausschließlich befugten internen Personen gestattet. Einfache Cloud Benutzer haben keinen Zugriff. • Die erfüllten und aufgeführten Anforderungen in § 11.10 gelten, wo anwendbar, auch für das hier beschriebene offene System.

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.50	**Signature manifestations (Form der Unterschrift)**
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. Unterschriebene elektronische Dokumente müssen mit der Unterschrift verbundene Informationen beinhalten, die deutlich alle folgenden Punkte aufzeigen: 1) Name des Unterzeichnenden in Druckbuchstaben 2) Datum und Zeitpunkt, zu dem die Unterschrift angefertigt wurde, und 3) die mit der Unterschrift verbundene Bedeutung (z. B. Überprüfung, Genehmigung, Verantwortlichkeit oder Urheberschaft) **Anforderung erfüllt!** • Alle oben aufgeführten Informationen sind Teil der digitalen Unterschrift.
b)	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). Die in den Absätzen (a)(1), (a)(2) und (a)(3) dieses Paragraphen aufgelisteten Punkte sollen den gleichen Kontrollen wie elektronische Dokumente unterworfen werden und in für Menschen lesbarer Version der elektronischen Dokumente (so z. B. elektronische Anzeige oder Ausdruck) beigefügt werden. **Anforderung erfüllt!** • Alle Informationen (a)(1), (a)(2) und (a)(3) dieses Paragraphen unterliegen den gleichen Kontrollen, wie die der elektronischen Dokumente (Authentizität, Integrität und Vertraulichkeit). • Alle Informationen (a)(1), (a)(2) und (a)(3) dieses Paragraphen sind für Menschen lesbar und transparent je nach Rechtevergabe einsehbar.

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart B: Electronic Records (Teil B: Elektronische Dokumente)
§ 11.70	Signature/record linking (Verknüpfung Unterschrift/Dokument)
	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. Elektronische Unterschriften und handschriftliche Unterschriften auf elektronischen Dokumenten sollen mit den entsprechenden elektronischen Dokumenten verknüpft werden, um zu gewährleisten, dass die Unterschrift nicht entfernt, kopiert oder anderweitig zum Zwecke der Fälschung eines elektronischen Dokuments durch übliche Methoden übertragen werden können. **Anforderung erfüllt!** • Eine elektronische Unterschrift ist immer mit einer Charge verbunden. • Die Unterschrift ist immer an den angemeldeten Benutzer geknpüft. • Nur befugte Personen (konfigurierbar durch den System Owner) können Chargen elektronisch unterschreiben. Ein Kopieren oder Fälschen ist durch übliche Methoden nicht möglich. • Eine elektronische Unterschrift (Chargenprüfung) kann durch berechtigte Anwender innerhalb der „Konfiguration“ zurückgesetzt werden und muss anschließend erneut erfolgen. Ein Zurücksetzen wird im Audit Log erkannt und festgehalten. Die zuvor durchgeführte Prüfung bleibt erhalten und einsehbar.

Absatz	Anforderungen: Subpart C: Electronic Signatures (Teil C: Elektronische Unterschriften)
§ 11.100	**General requirements (Allgemeine Anforderungen)**
a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. Jede elektronische Unterschrift soll eindeutig für eine Person sein und soll von keiner anderen Person wiederverwendet oder jemand anderem neu zugeordnet werden. **Anforderung erfüllt!** • Die elektronische Unterschrift ist immer an den angemeldeten Benutzer geknüpft. • Nur befugte Personen (konfigurierbar durch den System Owner) können Chargen elektronisch unterschreiben. Ein Kopieren der Unterschrift oder neu zuordnen ist nicht möglich.
b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an in individual's electronic signature, or any element of such electronic signature, the organization shall verify the identify of the individual. Bevor ein Unternehmen die elektronische Unterschrift einer Person oder Elemente dieser elektronischen Unterschrift festlegt, zuordnet, zertifiziert oder anderweitig billigt, soll es die Identität der entsprechenden Person überprüfen. **Nicht zutreffend!** **Liegt in der Verantwortung des System Owners.**
c)	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. Werden elektronische Unterschriften verwendet, soll die Behörde vor oder zum Zeitpunkt der Verwendung eine Bescheinigung erhalten, dass die elektronischen Unterschriften im System, die seit dem 20. August 1997 verwendet werden, das rechtlich verbindliche Äquivalent der traditionellen handschriftlichen Unterschrift darstellen. **Nicht zutreffend!** **Liegt in der Verantwortung des System Owners.**
c) 1)	The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement. Die Bescheinigung muss mit einer traditionellen handschriftlichen Unterschrift versehen und in elektronischer oder Papierform eingereicht werden. Informationen darüber, wo die Bescheinigung einzureichen ist, finden Sie auf der Webseite der FDA unter „Letters of Non-Repudiation Agreement" (Vereinbarungen über die Nichtabstreitbarkeit). **Nicht zutreffend!** **Liegt in der Verantwortung des System Owners.**

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart C: Electronic Signatures (Teil C: Elektronische Unterschriften)
§ 11.100	**General requirements (Allgemeine Anforderungen)**
c) 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. Werden elektronische Unterschriften verwendet, muss auf Ersuchen der Behörde eine zusätzliche Bescheinigung oder Bestätigung vorgelegt werden, aus der hervorgeht, dass eine bestimmte elektronische Unterschrift das rechtlich verbindliche Äquivalent zur handschriftlichen Unterschrift des Unterschreibenden darstellt. **Nicht zutreffend!** **Liegt in der Verantwortung des System Owners.**

Absatz	Anforderungen: Subpart C: Electronic Signatures (Teil C: Elektronische Unterschriften)
§ 11.200	**Electronic signature components and controls (Bestandteile elektronischer Unterschriften, Kontrollen)**
a) 1)	Electronic signatures that are not based upon biometric shall: Employ at least two distinct identification components such as an identification code and password. Elektronische Unterschriften, die nicht auf Biometrik basieren, sollen mindestens zwei verschiedene Identifikationskomponenten enthalten, so z. B. eine Benutzerkennung und ein Passwort.  • Die Unterschrift ist immer an den angemeldeten Benutzer geknüpft. Dieser kann sich mindestens durch Benutzernamen und Passwort anmelden.
i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be excecuted using all electronic signature components; subsequent signings shall be excecuted using at least one electronic signature component that is only excecutable by, and designed to be used only by, the individual. Unterschreibt eine Person während einer ununterbrochenen Sitzung mit kontrolliertem Systemzugriff mehrfach, soll die erste Unterschrift unter Verwendung aller Bestandteile der elektronischen Unterschrift vorgenommen werden. Anschließende Unterschriften sollen unter Verwendung mindestens einer Komponente, die nur von dieser Person ausführbar und auch nur dieser Person zur Verwendung zugeordnet ist, vorgenommen werden  • Zu Beginn muss sich jeder Anwender mit Benutzernamen und Passwort anmelden. • Bei Durchführung einer elektronischen Unterschrift muss mindestens eine der Komponenten erneut zur Verifizierung eingegeben werden. **Die Konfiguration der Verifizierung liegt in der Verantwortung des System Owners.**
ii)	When an individual excecutes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be excecuted using all of the electronic signature components. Unterschreibt eine Person mehrfach, allerdings nicht während einer einzigen ununterbrochenen Sitzung mit kontrolliertem Systemzugriff, soll jede Unterschrift unter Verwendung aller Komponenten der elektronischen Unterschrift vorgenommen werden.  • Bei jeder unterbrochenen Sitzung muss sich der Anwender erneut mit Benutzernamen und Passwort anmelden.

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart C: Electronic Signatures (Teil C: Elektronische Unterschriften)
§ 11.200	**Electronic signature components and controls (Bestandteile elektronischer Unterschriften, Kontrollen)**
a) 2) 3)	Electronic signatures that are not based upon biometrics shall: 2) Be used only by their genuine owners; and 3) Be administered and executed to ensure that attempted use of an individual‘s electronic signature by anyone other than it‘s genuine owner requires collaboration of two or more individuals. Elektronische Unterschriften, die nicht auf Biometrik basieren, sollen: 2) nur von den eigentlichen Benutzern verwendet werden dürfen, und 3) verwaltet und ausgeführt werden, das gewährleistet ist, dass der Versuch einer Person, eine ihr nicht eigene elektronische Unterschrift zu verwenden, die Zusammenarbeit von zwei oder mehr Personen erforderlich macht. **Anforderung erfüllt!** • Durch das IAM System können neben Benutzername und Passwort weitere Maßnahmen getroffen werden, um die Anmeldung am System abzusichern (z. B. Zwei-Faktor-Authentifizierung). Hierdurch wird sichergestellt, dass ausschließlich die angemeldete Person die elektronische Unterschrift durchführt. • Zudem muss bei der Durchführung der elektronischen Unterschrift eine erneute Verifizierung vorgenommen werden.
b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. Auf Biometrie basierende elektronische Unterschriften müssen so angelegt sein, dass sie außer von den eigentlichen Benutzern von niemand anderem verwendet werden können. **Nicht zutreffend!**

Absatz	Anforderungen: Subpart C: Electronic Signatures (Teil C: Elektronische Unterschriften)
§ 11.300	**Controls for identification codes/passwords (Kontrollen für Benutzerkennungen/Passwörter)**
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: Werden elektronische Unterschriften verwendet, die auf dem Einsatz von Benutzerkennungen in Kombination mit Passwörtern beruhen, sind Kontrollen zu schaffen, die die Sicherheit und Integrität der Unterschriften gewährleisten. Derartige Kontrollen sollen folgende Punkte beinhalten:	
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. Erhalt der Einzigartigkeit jeder Kombination aus Benutzerkennung und Passwort, so dass eine Kombination nur einmal vergeben ist.  • Diese Forderung kann im IAM-System eingestellt werden. **Liegt in der Verantwortung des System Owners.**
b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). Gewährleistung, dass die Ausgabe von Benutzerkennungen und Passwörtern regelmäßig überprüft oder die Kennungen und Passwörter zurückgenommen oder überprüft werden (z. B. das Veralten von Passwörtern verhindern).  • Diese Forderung kann im IAM-System eingestellt werden. **Liegt in der Verantwortung des System Owners.**
c)	Following loss management procedures to electronically deauthorize 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. Befolgen von Verlustverfahren, um auf elektronischem Weg verlorenen, gestohlenen, fehlenden oder anderweitig möglicherweise unsicheren Marken (Tokens), Karten und anderen Vorrichtungen, die mit Benutzerkennungs- und Passwortinformationen versehen sind oder solche erzeugen, die Berechtigung zu entziehen und um unter geeigneter und strenger Kontrolle vorübergehenden oder ständigen Ersatz herauszugeben.  • Diese Forderung kann im IAM-System eingestellt werden. **Liegt in der Verantwortung des System Owners.**

2 Bewertung der Forderung

Absatz	Anforderungen: Subpart C: Electronic Signatures (Teil C: Elektronische Unterschriften)
§ 11.300	**Controls for identification codes/passwords (Kontrollen für Benutzerkennungen/Passwörter)**
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. Verwendung von Sicherheitsvorkehrungen für Transaktionen, die den unbefugten Einsatz von Passwörtern und/oder Benutzerkennungen verhindern und sofort und unter Hinweis auf die Dringlichkeit des Vorfalls jeden Versuch der unbefugten Benutzung entdecken und diesen an die Sicherheitseinheit des Systems und im Bedarfsfall an die Unternehmensführung weiterleiten. **Anforderung erfüllt!** • Diese Forderung kann im IAM-System eingestellt werden. **Liegt in der Verantwortung des System Owners.**
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 Anfängliches und im Anschluss daran regelmäßiges Testen der Geräte, wie etwa Marken (Tokens) oder Karten, die mit Benutzerkennungs- oder Passwortinformationen versehen sind oder solche erzeugen, um zu gewährleisten, dass sie ordnungsgemäß funktionieren und nicht unbefugt verändert wurden. **Nicht zutreffend!**

3 Literaturverzeichnis

[1] Mass & Peither
AG GMP Verlag
21 CFR 210/211 cGMP FOR FINISHED PHARMACEUTICALS
(Aktuelle Gute Herstellungspraxis für Fertigarzneimittel)
inkl. 21 CFR 11 electr. Records/electr. Signature
(Elektr. Dokumente/elektr. Unterschrift)
mit deutscher Übersetzung und Stichwortverzeichnis

[2] US Website „Code of Federal Regulations“
www.ecfr.gov
Title 21/Chapter I/Subchapter A/Part 11

3 Literaturverzeichnis



