

FDA 21 CFR Part 11 Compliance mit digitalen Signaturen

Secardeo GmbH, 2010

Was ist 21 CFR Part 11?

Die Nutzung von Computersystemen in „Life Sciences“ Industriezweigen wie Pharma, Biotechnologie und Medizintechnik unterliegt den Anforderungen der Zulassungsbehörden. Dies kann die unterschiedlichsten Unternehmensbereiche wie beispielsweise Produktion, Qualitätssicherung oder Forschung und Entwicklung betreffen. Die US-amerikanische Gesundheitsbehörde FDA (Food and Drug Administration) hat bereits 1997 Anforderungen für die Aufzeichnung von Daten in elektronischer Form („electronic records“) und den Einsatz von elektronischen Signaturen („electronic signatures“) festgelegt. Diese Vorgaben sind in 21 CFR Part 11 (Code For Regulations) definiert. Im Jahr 2003 wurde eine Präzisierung der Regeln für elektronische Signaturen in „FDA Guidance for Industry Part 11, Electronic Records: Electronic Signatures – Scope and Application“ veröffentlicht. Dieses Dokument hat informellen Charakter, jedoch keine formale Verbindlichkeit. Als Ergänzung hierzu wurde 2007 die „Guidance for Industry Computerized Systems Used in Clinical Investigations“ von der FDA publiziert.



In der Vergangenheit gewährte die FDA den Unternehmen eine Übergangsfrist, um die entsprechenden Richtlinien umzusetzen. Zunehmend konzentriert sich die FDA bei Inspektionen aber auf 21 CFR Part 11 Fragestellungen. Die Zunahmen der Verwarnungen sowie die Aussagen der FDA-Verantwortlichen zeigen, dass die FDA konkrete Maßnahmen und nicht mehr nur Planungen sehen möchte. Bei entdeckten Verstößen in Unternehmen wurden bereits drastische Sanktionen bis hin zur Produktionsstilllegung verhängt. Neben technischen Mechanismen müssen auch Maßnahmen auf organisatorischer Ebene implementiert werden, um ein 21 CFR Part 11 konformes System zu erhalten. Part 11 Compliance setzt eine erfolgreiche Validierung aller relevanten Computersysteme voraus. Um dabei die Anforderungen hinsichtlich elektronischer Signaturen gemäß Part 11 zu erfüllen, eignen sich für die Realisierung insbesondere so genannte digitale Signaturen.

Was sind Digitale Signaturen?

Digitale Signaturen sind Datenstrukturen, die durch eine kryptografische Berechnung eines Dokuments oder einer E-Mail mit dem privaten Schlüssel des Unterzeichners erzeugt werden. Jedermann kann die Unversehrtheit (Integrität) und Echtheit (Authentizität) eines digital signierten Dokuments mit dem öffentlichen Schlüssel des Unterzeichners prüfen und es ist nachvollziehbar, wer ein Dokument unterzeichnet hat. Das Vertrauen in den öffentlichen Schlüssel wird durch ein Zertifikat hergestellt, das von einem Trustcenter ausgestellt wird. Ein Dokument kann auch parallel oder sequenziell von mehreren Unterzeichnern digital signiert werden. Damit können typische Unterschriftsprozesse elektronisch abgebildet werden.

Worin liegt der Nutzen?

Das Risiko, beispielsweise aufgrund einer FDA Inspektion Produktionsanlagen schließen zu müssen, ist für ein Unternehmen sicher nicht tragbar. Die "21 CFR 11 Compliance" der Herstellungs- und Dokumentationsverfahren wird für Unternehmen zum kritischen Erfolgskriterium. Für die Hersteller von Medizinprodukten oder -geräten ist die Erfüllung von Part 11 eine unabdingbare Voraussetzung, um international wettbewerbsfähig zu bleiben. Eine frühzeitige Umsetzung bedeutet daher einen erheblichen Wettbewerbsvorteil. Für die Zulassungsbehörden, die mit einer stetig wachsenden Zahl von Zulassungsanträgen konfrontiert sind, ergibt sich eine Vereinfachung und schnellere Bearbeitung von Zulassungsanträgen in elektronischer Form. Die FDA zielt mit der Forderung nach elektronischen Signaturen insbesondere auf die Qualität und Nachvollziehbarkeit von elektronisch dokumentierten Prozessen ab. Darüber hinaus ergeben sich für ein Unternehmen weitere grundsätzliche Vorteile beim Einsatz digitaler Signaturen:

- Kosteneinsparung durch den Wegfall von Papier-, Druck, Kuvertier- und Transportkosten
- Beschleunigung von Abläufen durch die sofortige Verfügbarkeit elektronischer Dokumente
- Vermeidung von Medienbrüchen
- Erhöhung der Qualität von Prozessen
- Erfüllung der Vorgaben durch weitere Behörden (z.B. Finanzen)

Warum digitale Signaturen für Part 11 Compliance?

Part 11 unterscheidet grundsätzlich zwischen handschriftlichen und elektronischen Unterschriften. Der Begriff der elektronischen Signatur wird, ähnlich wie bei anderen Gesetzgebungen, als weit gefasster Oberbegriff verwendet. Als spezielle Ausprägungen definiert Part 11 die Verwendung biometrischer Merkmale sowie die digitale Signatur, basierend auf kryptografischen Methoden. Für die FDA stehen der Schutz der Integrität und Authentizität von Datensätzen sowie die Nachvollziehbarkeit von Vorgängen im Vordergrund. Für diese Anforderungen bietet die digitale Signatur nach heutigem Stand der Technik im Zusammenspiel mit den zuverlässigen Prozessen einer Public Key Infrastruktur (PKI) den höchsten Sicherheitsgrad. Digitale Signaturen erfüllen die geforderten hohen Anforderungen an die

- Unterzeichnerabhängigkeit,
- Erklärungsabhängigkeit,
- Überprüfbarkeit,
- Fälschungssicherheit und
- Dokumentenechtheit.

Damit können alle relevanten Forderungen aus dem Part 11 für Electronic Signatures, Closed/Open Systems, Signature Manifestations oder Signature/Record Linking durchgängig erfüllt werden. Die FDA fordert nicht für alle Daten den Einsatz der elektronischen Signaturen. So genannte Prädikatenregeln in den Good Practices (GxP) der FDA und weiteren Beschlüssen (Acts) legen fest, für welche Dokumente und Datensätze elektronische Signaturen erforderlich sind. Alternativ wird für solche elektronischen Datensätze das Mitführen einer damit verknüpften handschriftlichen (Papier-) Unterschrift zugelassen. Solche hybriden Systeme bedingen jedoch einen beträchtlichen Verwaltungsaufwand und entziehen die Vorteile einer durchgängigen digitalen Signaturlösung. Aufgrund des weiten Geltungsbereiches sind die unterschiedlichsten Systeme von Part 11 betroffen. Abhängig vom betrachteten Unternehmensprozess können dies DMS, ECM, ERP, EDM/PDM oder auch Workflow-Systeme sein. Wichtig ist daher oft die Verwendung interoperabler Dokumenten- und Signaturformate wie beispielsweise PDF.



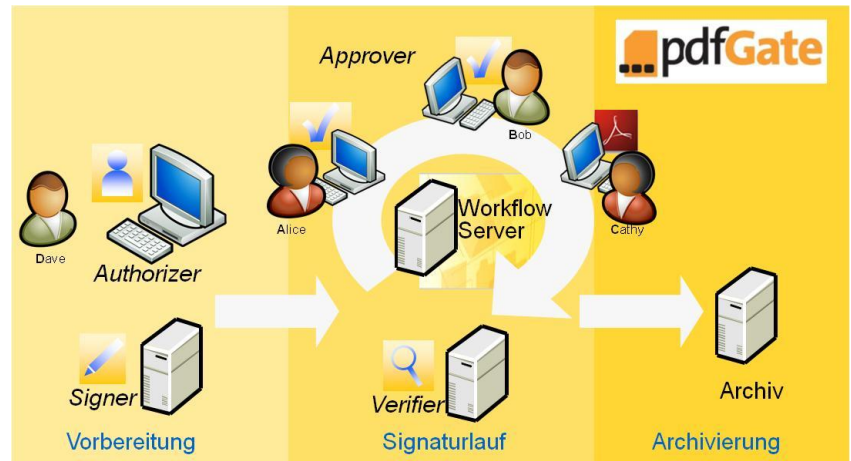
Wie kommt man zu einer zu Part 11 kompatiblen digitalen Signatur?

Für eine digitale Signatur wird ein asymmetrisches Schlüsselpaar benötigt, wobei der Prüfschlüssel durch eine Zertifizierungsinstanz (Certification Authority, CA) mit einem digitalen Zertifikat bestätigt und veröffentlicht wird. Der private Signaturschlüssel befindet sich im Idealfall auf einer SmartCard oder einem USB-Crypto-Token, kann aber auch preiswerter in Form von Software bereit gestellt werden. Die SAFE-BioPharma Association, ein Zusammenschluß von Life Sciences Unternehmen hat den Standard "Signatures and Authentication For Everyone" (SAFE) entwickelt. Ziel ist die Etablierung einer vertrauenswürdigen Gemeinschaft zur rechtskräftigen Nutzung digitaler signierter Transaktionen. Damit sollen auch die Anforderungen der FDA erfüllt werden. Die SAFE Partner bieten hierfür digitale Zertifikate für Software und Hardware Tokens an.



Als kostengünstige und maßgeschneiderte Alternative kann ein Unternehmen auch eine eigene Zertifizierungsinstanz im Rahmen einer Public Key Infrastruktur (PKI) im Hause realisieren. Die digitale Signatur wird durch eine in die Prozesse integrierte Signaturanwendung angebracht und zuverlässig überprüft. Die Protokollierung der Prüfung der einzelnen Signaturschritte ist wichtig für ein FDA Audit. Als Dokumentformat eignet sich hier beispielsweise PDF. Bei der Konzeption und Realisierung einer solchen PKI und der verwendeten Signaturverfahren müssen jedoch die Vorgaben der FDA erfüllt und dieses entsprechend dokumentiert werden.

SECARDEO bietet mit der Software pdfGate eine Plattform an, mit der Part 11 kompatible Prozesse auf der Basis von PDF-Signaturen realisiert werden können. Kernstück ist hierbei der Verifikationsserver pdfGate Verifier, der sowohl die Echtheit und Gültigkeit der in einem Prozess angebrachten digitalen Signaturen als auch die Unterschriftsberechtigung des jeweiligen Unterzeichners prüft. Die erzeugten XML-Prüfberichte können selbst mit einer digitalen Signatur geschützt und zusammen mit dem PDF-Dokument archiviert werden. Dieses Verfahren ist geeignet für einen späteren Audit. Für die Vorbereitung und Festlegung der Unterschriftsprozesse und –berechtigungen dient pdfGate Authorizer. Die Signierung erfolgt am Client mit einem hohen Benutzerkomfort mittels pdfGate Approver oder serverbasiert mit pdfGate Signer. Dabei können beliebige PDF-Dokumente signiert werden und auf eine teure Rechtfreischaltung mit Adobe Produkten verzichtet werden. Die pdfGate Komponenten haben sich seit Jahren im Einsatz von Systemen bewährt, die auch Part 11 unterliegen



Für die Vorbereitung und Festlegung der Unterschriftsprozesse und –berechtigungen dient pdfGate Authorizer. Die Signierung erfolgt am Client mit einem hohen Benutzerkomfort mittels pdfGate Approver oder serverbasiert mit pdfGate Signer. Dabei können beliebige PDF-Dokumente signiert werden und auf eine teure Rechtfreischaltung mit Adobe Produkten verzichtet werden. Die pdfGate Komponenten haben sich seit Jahren im Einsatz von Systemen bewährt, die auch Part 11 unterliegen

Wie können wir Sie unterstützen?

Die Erfüllung der Part 11-Anforderungen macht intensive Konzeptions-, Implementierungs- und Validierungsaufgaben notwendig. Für die Behandlung des Themas „Electronic Signatures“ sind vertiefte Kompetenzen und Realisierungserfahrungen zum komplexen Themenfeld „PKI / Elektronische Signaturen“ erforderlich. Insbesondere die Integration digitaler Signaturmechanismen in bestehende oder neu zu realisierende Anwendungssysteme gibt es nicht durchgängig „von der Stange“. Jedoch lässt sich durch geeignete Auswahl von Standardprodukten, Add-On Komponenten und Dienstleistungen eine Menge Zeit und Geld sparen. SECARDEO verfügt über die erforderlichen Kompetenzen und langjährige Erfahrungen aus einer Vielzahl von PKI- und Signaturprojekten, insbesondere auch im Bereich von Part 11. Wir helfen Ihnen

- bei der Durchführung von Workshops zu Part 11 / Electronic Signatures,
- bei der Analyse von bestehenden Systemen und Festlegung von Anforderungen im Hinblick auf Part 11,
- bei der Konzeption und Realisierung digitaler Signaturlösungen für Part 11 Compliance auf Basis von Standards wie PDF,
- durch Integration unserer Plattform pdfGate für auditierbare PDF-Signatur-Workflows,
- der Realisierung einer Unternehmens-PKI oder Integration eines externen Trustcenters für die Anforderungen von Part 11.

Benötigen Sie weitere Informationen?

Wenn Sie weitere Informationen wünschen, wenden Sie sich bitte an

Secardeo GmbH
 Hohenadlstr. 4, 85737 Ismaning
 Tel. 089/18935890