

## 6. FDA 21 CFR Part 11 – Electronic Signatures

In diesem Workshop erhalten Sie eine technische Einführung für digitale Signaturen, eine Übersicht über die Signaturgesetzgebung sowie eine Erläuterung der Anforderungen aus 21 CFR Part 11 (Code For Regulations) der FDA (Food and Drug Administration). Sie erfahren, wie Sie diese Anforderungen mittels PDF-Dokumenten und digitalen Signaturen umsetzen und mit einer für Sie passenden Lösung Part 11-Compliance erreichen können.

Dieser Workshop richtet sich an Qualitäts-Manager und Compliance-Verantwortliche sowie an IT-Leiter in Bereich Life-Sciences. *Dauer 1 Tag.*

Die SECARDEO GmbH ist ein Vorreiter auf dem Gebiet von Unternehmenslösungen mit digitalen Signaturen und Zertifikaten. Wir bieten dazu kompetente Beratung, wegweisende Produkte und integrierte Lösungen an.

Unsere Referenten konnten Erfahrungen beim Aufbau von großen Unternehmens-PKIs gewinnen und sind aktiv an unseren Beratungs- und Realisierungsprojekten beteiligt. Damit stellen wir sicher, dass zusätzlich zu den notwendigen Grundkenntnissen auch das für die Praxis relevante Know-how vermittelt wird.

## SECARDEO Workshops

### Was ist PKI und wozu dienen digitale Signaturen?

Eine Public Key Infrastruktur (PKI) stellt Schlüssel, Zertifikate und weitere Dienste bereit, mit denen ein effizientes und verlässliches Security Management möglich ist. Mit digitalen Ausweisen (Zertifikaten) kann heute eine Vielzahl von Anwendungen auf einem äußerst hohen Niveau abgesichert werden. Probleme mit vergessenen oder geknackten Passwörtern und damit verbundenen Helpdesk-Kosten sowie der systemübergreifenden Verwaltung digitaler Identitäten (Identity Management) lassen sich damit minimieren. Erst mit einer PKI ist auch der Einsatz digitaler Signaturen möglich. Damit kann die Unversehrtheit und Echtheit digitaler Dokumente zweifelsfrei geprüft werden und es ist nachvollziehbar, wer ein Dokument unterzeichnet hat.

### Warum sollten Sie diese Workshops besuchen?

PKI und digitale Signatur sind mittlerweile integraler Bestandteil vieler Standardanwendungen und Systeme. Ob Windows Certificate Services, Windows VPN, Microsoft® Office, Adobe Acrobat®, Adobe Reader®, Firefox, Outlook®, Lotus® Notes oder Cisco® Router, viele Komponenten warten nur darauf, sicher auf Basis einer PKI betrieben zu werden. Durch Einsatz einer Unternehmens-PKI und digitaler Signaturen sind signifikante Einsparungen, beschleunigte Unternehmensprozesse und eine erhöhte Service-Qualität möglich. Die notwendigen Investitionen sind durch Nutzung von kostengünstiger Standardsoftware überschaubar.

### Was lernen Sie hier?

Wir informieren Sie über die zugrunde liegende Technik, organisatorische Fragestellungen und rechtliche Aspekte. Der Schwerpunkt liegt auf praktischen Aspekten und Einsatzszenarien für diese Technologien im Unternehmen. Relevante Projektbeispiele und Neuigkeiten zu den Themen werden laufend aktualisiert.

## Workshops



## Workshops

Unsere Workshops vermitteln Ihnen Kenntnisse zu den Grundlagen und dem praktischen Einsatz von Public Key Technologien und digitalen Signaturen mit Standardprodukten. Mit einer Public Key Infrastruktur (PKI) schaffen Sie die Grundlage für ein verlässliches „Trusted“ E-Business.

Unsere Workshops können Sie an unserem Standort in Ismaning bei München besuchen oder als Inhouse-Schulung für Ihre Mitarbeiter buchen.



### 1. PKI Grundlagen und Realisierungskonzepte

Dieser Workshop vermittelt Ihnen fundierte Grundkenntnisse über Einsatzmöglichkeiten und den technischen sowie organisatorischen Aufbau von Public Key Infrastrukturen. Dabei werden die Mechanismen und Komponenten einer PKI sowie typische Anwendungen vorgestellt, die digitale Zertifikate zur Verschlüsselung, digitalen Signatur oder starken Authentisierung nutzen. Die rechtlichen und organisatorischen Aspekte werden ebenso erläutert wie die möglichen Realisierungsalternativen. Hierbei wird verglichen welche Vor- und Nachteile der Aufbau einer internen PKI oder die Nutzung eines externen Dienstleisters bieten und welchen Mehrwert der Einsatz von SmartCards bietet. Eine Kosten- und Nutzenbewertung dient zur Orientierung für die Planung eines PKI-Projektes. Dieser Workshop richtet sich an IT-Leiter und IT-Sicherheitsbeauftragte. *Dauer 2 Tage.*

### 2. Aufbau einer Windows PKI

In diesem Workshop lernen Sie wie Sie eine PKI basierend auf Windows Active Directory Certificate Services in Ihrem Unternehmen aufbauen und nutzen können. Der Workshop erläutert die technischen Grundlagen einer PKI und die Architektur der Certificate Services.

Sie lernen die Vorgehensweise bei der Installation und Konfiguration eines Windows CA Servers, die Nutzung und Anpassung vorgefertigter Certificate Templates, Policy- und Exit-Module und die Integration von SmartCards als Schlüsselspeicher kennen.

Ein Schwerpunkt sind die verschiedenen Registrierungs- und Enrollmentverfahren. Sie erfahren, wie die ausgestellten Zertifikate in Standardanwendungen wie Outlook, Acrobat oder Internet Explorer sowie für SmartCard Logon und VPN genutzt werden können. Auch wichtige organisatorische Maßnahmen wie PKI Rollen & Berechtigungen und Backup & Recovery erläutern wir Ihnen.

Dieser Workshop richtet sich an IT-Infrastrukturverantwortliche, Systemadministratoren sowie IT-Projektleiter.

*Dauer 2 Tage.*

### 3. Einsatz von PDF-Signaturen

Wir vermitteln Ihnen in diesem Workshop die technischen Grundlagen von digitalen Signaturen in PDF-Dokumenten. Die relevanten Gültigkeitsmodelle und gesetzlichen Rahmenbedingungen zu digitalen Signaturen werden erläutert.

Wir zeigen Ihnen dann am Beispiel von Adobe Acrobat und anderen Anwendungen, wie die digitale Signatur bei PDF-Dokumenten funktioniert. Die verschiedenen Typen und Eigenschaften von PDF-Signaturen werden erklärt und Unterschiede in den PDF- und Acrobat-Versionen verglichen. Wichtige Einsatzszenarien wie z.B. die elektronische Rechnungsstellung oder Genehmigungsprozesse werden vorgestellt.

Schließlich zeigen wir Ihnen, wie Sie signierte PDF-Dokumente erzeugen, in Ihren Workflow integrieren und damit Zeit und Geld sparen können.

Dieser Workshop richtet sich an Verantwortliche im Bereich Dokumentenverwaltung, BPM und Formularwesen sowie Projektleiter und Administratoren in diesem Themenumfeld. *Dauer 2 Tage.*

### 4. Digitale Signaturen im Unternehmen

Sie lernen in diesem Workshop die Grundlagen von digitalen Signaturen und Zertifikaten kennen. Neben den technischen Kenntnissen wird auch ein Verständnis für Gültigkeitsmodelle und die gesetzlichen Rahmenbedingungen vermittelt. Typische Signaturanwendungen für E-Mail-, File- oder Dokumentsignaturen werden verglichen. Die praktische Nutzung der Signatur mit Standardanwendungen wie Outlook, MS-Office und Adobe Acrobat wird veranschaulicht. Auch besondere Varianten wie Massensignaturen, mobile Signaturen, Zeitstempel und Langzeitsignaturen lernen Sie kennen. Typische Einsatzgebiete wie elektronische Rechnungen, Formulare, Signatur-Workflows und Behördenprozesse werden vorgestellt und eine Kosten- und Nutzenbetrachtung durchgeführt. Dieser Workshop richtet sich an die Leiter IT, Dokumentenverwaltung, Formularwesen sowie Projektleiter in diesem Themenumfeld. *Dauer 2 Tage.*

### 5. PKI Interworking

Dieser Workshop erläutert die Herausforderungen und stellt Lösungen zur Kopplung einer bestehenden PKI mit anderen PKIs vor.

Hier werden Verfahren und Mechanismen zum öffentlichen Zugriff auf Zertifikate wie Zertifikatsserver oder LDAP-Proxies und zur Etablierung von Vertrauen in diese Zertifikate wie Certificate Trust Lists, Cross-Certificates oder PKI-Bridges sowie zu deren Validierung mittels CRL oder OCSP vorgestellt und bewertet. Dieser Workshop richtet sich an PKI-Verantwortliche sowie IT-Sicherheitsbeauftragte von Organisationen mit einer bestehenden oder geplanten PKI. *Dauer 1 Tag.*

