

Einsatz digitaler Signaturen

Secardeo GmbH, 2009

Einsatz Digitaler Signaturen im Unternehmen

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.

Die Signaturgesetzgebung (SigG, SigV) regelt die rechtlichen Rahmenbedingungen hierfür. Vorgänge, bei denen per Gesetz die Schriftform festgelegt wird, werden auch mittels einer so genannten qualifizierten elektronischen Signatur rechtswirksam, von wenigen Ausnahmen abgesehen. Für die überwiegende Mehrzahl von Vorgängen existieren jedoch keine solchen Formerfordernisse. Diese können mit fortgeschrittenen elektronischen Signaturen auf demselben technischen Niveau abgesichert werden und erhalten zusammen mit entsprechenden organisatorischen Maßnahmen auch eine hohe Beweiskraft.

Worin liegt der Nutzen?

In Unternehmen und Behörden gibt es heute viele Geschäftsprozesse, bei denen Dokumente ausgedruckt, manuell unterschrieben und in Papierarchiven aufbewahrt werden. Durch den Einsatz digitaler Signaturen lassen sich diese Vorgänge effizienter und kostengünstiger abwickeln. Zunehmend schreiben Behörden für die elektronische Abwicklung von Vorgängen auch elektronische Signaturen vor. Digitale Signaturen können prinzipiell zur Erhöhung der Sicherheit für beliebige Anwendungen und Dokumente eingesetzt werden. Der Einsatz digitaler Signaturen ist jedoch insbesondere dort sinnvoll, wo die Verbindlichkeit und Nachvollziehbarkeit von Vorgängen erforderlich ist. Dies betrifft in erster Linie solche Vorgänge, bei denen heute handschriftliche Unterschriften geleistet werden müssen. Die Einführung der digitalen Signatur bedeutet zunächst eine Investition in neue Technologien und Verfahren. Die langfristigen Vorteile rechtfertigen diese Investition und können oftmals beachtliche Einsparungen mit sich bringen.



- **Zeiteinsparung**
Durchlaufzeiten für Papierprozesse mit mehreren standortübergreifenden Unterzeichnern können mehrere Tage betragen. Eine Reduktion auf wenige Stunden ist mit digitalen Signaturen möglich.
- **Kostenreduktion**
Die Kosten für Papierunterschriften setzen sich typischerweise aus Druck-, Kuvertier-, Frankier- und Transportkosten sowie Kosten für die Archivierung zusammen. Beim Umstieg auf elektronische Rechnungen beispielsweise, die per Gesetz eine elektronische Signatur benötigen, kann mit Einsparungen von mehreren Euro pro Transaktion gerechnet werden.
- **Erhöhte Sicherheit**
Handunterschriften zweifelsfrei zu prüfen ist mit hohem Aufwand verbunden und das Risiko von irrtümlich akzeptierten Fälschungen ist daher relativ hoch. Oft ist die Zuordnung einer Unterschrift zu einer Person für den Prüfer gar nicht oder nur mit Aufwand möglich. Eine digitale Signatur erhöht die Sicherheit und Zuverlässigkeit der Signaturprüfung drastisch.
- **Einhaltung von Regulierungen (Compliance)**
In bestimmten Bereichen wird gefordert, dass die Umstellung von Papier auf elektronische Prozesse nur mittels elektronischer Signaturen erfolgt. Ein Beispiel sind die von der FDA für die Hersteller von Pharma- und Medizinprodukten vorgegebenen Regeln in 21 CFR Part 11.

• Konformität mit der Gesetzgebung

Der Gesetzgeber sieht für Vorgänge mit Schriftformerfordernis auch die Verwendung der elektronischen Form mit einer qualifizierten Signatur vor, die gleichwertig mit einer Handunterschrift ist.

Wer kann von digitalen Signaturen profitieren?

In fast jedem Unternehmen finden sich Vorgänge, die Unterschriften benötigen und bei denen digitale Signaturen einen erheblichen Nutzen darstellen können. Tabelle 1 zeigt eine Reihe von unterschriftsrelevanten Prozessen, die sich in vielen Organisationen, quer durch alle Branchen wieder finden.

<p>Personal</p> <ul style="list-style-type: none"> • Urlaubsantrag • Überstundenantrag • Dienstreisenabrechnung 	<p>IT-Infrastruktur</p> <ul style="list-style-type: none"> • Antrag auf Systemzugang • Änderung von E-Mail und Telefon • Bestellung von HW, SW, Services
<p>Entwicklung und Produktion</p> <ul style="list-style-type: none"> • Freigabe Konstruktionszeichnungen • Prüfprotokolle • Qualitätssicherung • Produkthaftung 	<p>Einkauf</p> <ul style="list-style-type: none"> • Bestellungen • Dienstleistungsverträge • Einholen verbindlicher Angebote
<p>Verkauf</p> <ul style="list-style-type: none"> • Abgabe verbindlicher Angebote • Vertragsabschlüsse 	<p>Finanzen</p> <ul style="list-style-type: none"> • Rechnungsstellung • Prüfung von Eingangsrechnungen • Umsatzsteuer (UStG)
<p>Geschäftsleitung</p> <ul style="list-style-type: none"> • Geschäftsbriefe • Rundschreiben • Vertraulichkeitsvereinbarungen • Haftungsfragen 	<p>Formularwesen</p> <ul style="list-style-type: none"> • Antragsformulare • Formularprozesse

Tabelle 1: Prozesse für digitale Signaturen

Es gibt ferner branchenspezifische Anforderungen und Regulierungen, die den Einsatz digitaler Signaturen betreffen, vgl. Tabelle 2. Im öffentlichen Bereich kommen bei E-Government-Dienstleistungen auf Beschluss der deutschen Bundesregierung qualifizierte elektronische Signaturen zum Einsatz, wenn es erforderlich oder geboten ist. Bundesbehörden müssen eingehende IT/TK-Angebote in Papierform nicht mehr akzeptieren und verlangen mit der elektronischen Vergabe eine digitale Signatur. Im Bereich Pharma/Medizintechnik werden durch die US-amerikanische Gesundheitsbehörde FDA (Food and Drug Administration) mit 21 CFR Part 11 entsprechende Vorgaben für die Signatur von Electronic Records gemacht. Im Energiesektor müssen Anlagenbetreiber und Sachverständige für die Teilnahme am Emissionshandel eine qualifizierte elektronische Signatur verwenden (§ 4 TEHG). Im Gesundheitswesen sollen künftig Fachkräfte mit ihrem Heilberufsausweis auch digitale Signaturen, beispielsweise für elektronische Rezepte, ausstellen können. Im Bereich der Justiz kann in Deutschland die rechtswirksame Einreichung von Klagen, Erklärungen und Schriftsätzen an die Gerichte mit qualifizierter Signatur erfolgen. In der Industrie steht die Automatisierung von Geschäftsprozessen im Vordergrund, aber auch Maßnahmen zur Erfüllung von Compliance-Vorgaben wie z.B. SOX oder KontraG und Vorgänge, die für eine Produkthaftung relevant sind können mit digitalen Signaturen abgesichert werden.

Öffentliche Verwaltung <ul style="list-style-type: none"> • E-Government, E-Vergabe • ELSTER • EU-Dienstleistungsrichtlinie 	Pharma & Medizintechnik <ul style="list-style-type: none"> • Compliance 21 CFR Part 11 • HIPAA
Energie <ul style="list-style-type: none"> • Stromhandel • Emissionshandel 	Gesundheitswesen <ul style="list-style-type: none"> • Patientenakte • E-Rezept • Verwaltungsabläufe
Justiz <ul style="list-style-type: none"> • Elektronischer Rechtsverkehr • Elektronisches Gerichts- und Verwaltungspostfach 	Industrie <ul style="list-style-type: none"> • Prozessautomatisierung • Compliance • Produkthaftung
Banken & Versicherungen <ul style="list-style-type: none"> • Elektronischer Kontoauszug • Online-Banking 	Telekommunikation <ul style="list-style-type: none"> • Online Rechnungen • Behördenprozesse

Tabelle 2: Branchen und digitale Signaturen

Wie kommt man zu einer 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. Zunehmend implementieren Unternehmen solche Zertifizierungsinstanzen im Rahmen einer Public Key Infrastruktur (PKI) im eigenen Hause. Mit den damit ausgestellten Signaturzertifikaten können fortgeschrittene Signaturen realisiert werden. Dies kann mit gängigen Standardanwendungen wie Microsoft Office, Outlook, oder Adobe Acrobat erfolgen. Ausgelöst wird die Signatur durch Eingabe einer PIN oder eines Passworts. Fortgeschrittene Signaturen sind damit äußerst kostengünstig, einfach zu nutzen und decken die Mehrzahl der Geschäftsprozesse ab. Für die Vorgänge, wo der Gesetzgeber qualifizierte Signaturen fordert, muss sich der Anwender eine SmartCard und ein qualifiziertes Zertifikat bei einem behördlich angezeigten oder akkreditierten Trustcenter beschaffen. Ferner soll der Benutzer Chipkartenlesegeräte mit Tastatur und Anwendungssoftware einsetzen, für die eine Bestätigung oder eine Herstellererklärung gemäß SigG vorliegt. Damit sind qualifizierte Signaturen teurer und oft umständlicher in der Handhabung, dabei jedoch technisch nicht unbedingt sicherer als fortgeschrittene Signaturen.



Wie läuft der Einsatz digitaler Signaturen ab?

Typisch in einem Unternehmen sind Workflows für Antrags-, Freigabe- oder Genehmigungsprozesse. Abb. 1 zeigt einen Unterschriftslauf, bei dem drei Personen, Alice, Bob und Cathy nacheinander ein Dokument unterzeichnen und dieses dann weiterleiten. Eric wird im Geschäftsprozess anschließend prüfen, ob das Dokument auch von den geforderten Personen unterschrieben wurde.

Dieser Vorgang kann traditionell mit Papier und Handunterschrift, oder elektronisch durch digital signierte Dokumente erfolgen. Der Ablauf, der Dokumentinhalt und die Unterzeichner können dabei unverändert bleiben. Selbst die Darstellung der Dokumente kann durch geeignete Formate wie PDF originalgetreu abgebildet werden. Workflow Management Systeme dienen zur aktiven Steuerung solcher Prozesse.

Der eigentliche Signaturvorgang wird über das Menü der Signaturanwendung oder im Beispiel von PDF-Dokumenten

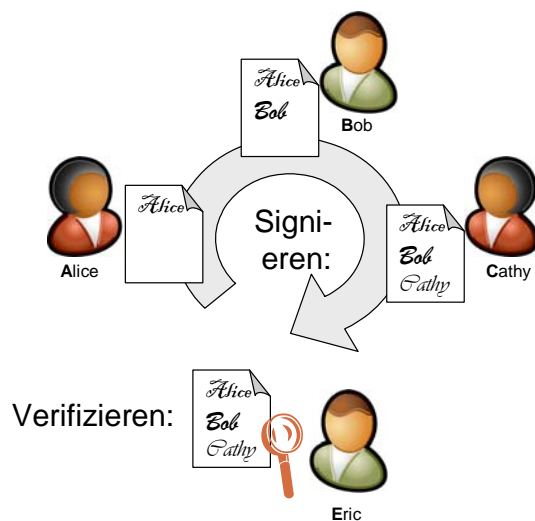


Abbildung 1: Signaturlauf

durch einfache manuelle oder automatische Auswahl eines vorgegebenen Signaturfeldes ausgelöst, vgl. Abb. 2. Die Eingabe der korrekten PIN führt zur Freischaltung der eingelegten SmartCard und kryptografischen Berechnung des Signaturwertes.

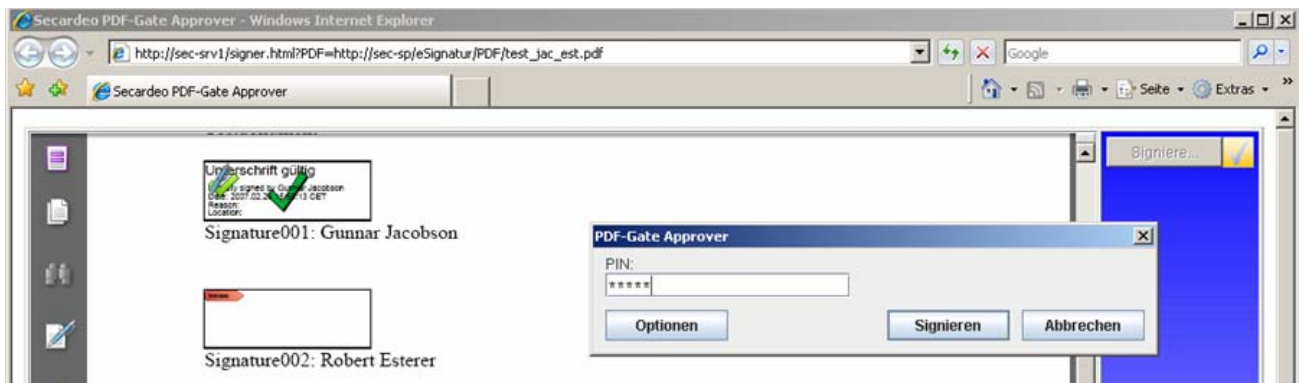


Abbildung 2: PDF-Signiervorgang

Der Empfänger eines solchen Dokuments kann die Echtheit der enthaltenen digitalen Signaturen sowie die Gültigkeit der verwendeten Zertifikate über das entsprechende Anwendungsprogramm einfach prüfen und das Dokument, falls gefordert, auch digital gegenzeichnen.

Die zu einem Vorgang gehörenden Dokumente können samt digitalen Signaturen archiviert und später bei Bedarf wieder zu einer Überprüfung herangezogen werden. Für eine Langzeitarchivierung sollten geeignete Dokumentformate verwendet werden und es können weitere Mechanismen wie eingebettete Statusinformationen und digitale Zeitstempel in die Prozesse mit integriert werden.

Welche Anwendungen sind für Dokumentsignaturen geeignet?

Bei der Einführung digitaler Signaturen muss festgelegt werden, welche Dokumentformate und welche Signaturformate verwendet werden sollen. Heutige Standardanwendungen wie MS Office, MS InfoPath oder Adobe Acrobat unterstützen digitale Signaturen.

Mit Office 2007 wurde durch Microsoft ein offenes Dokumentformat auf der Basis von XML eingeführt. MS InfoPath, vgl. Abb. 3, basiert bereits in der Version 2003 auf XML. Mit Vista wurde ferner von Microsoft die XML Paper Specification (XPS) als Konkurrenzformat zu Adobe PDF eingeführt. XPS wird in Windows Vista und im .NET-Framework 3.0 für Windows XP unterstützt. Alle diese Werkzeuge von Microsoft unterstützen nun digitale Signaturen in dem vom W3C standardisierten XMLSIG Format.

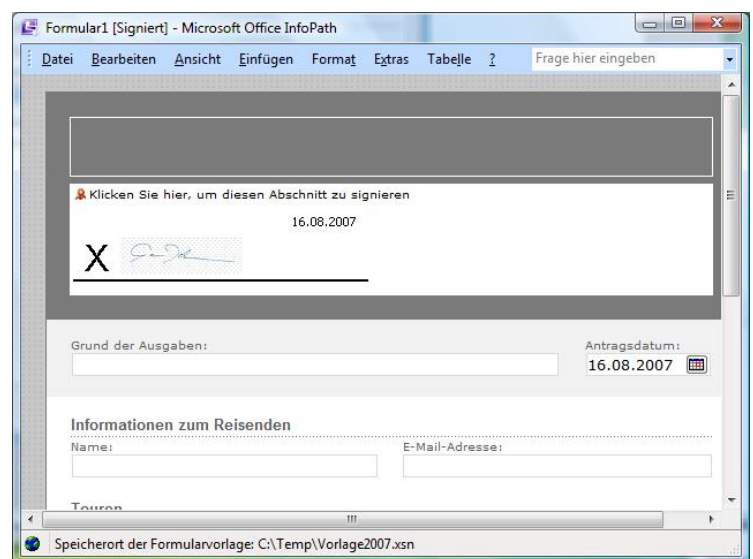


Abbildung 3: XML Signatur

Adobe Acrobat und der weit verbreitete kostenlose Adobe Reader unterstützen digitale Signaturen in dem gängigen PKCS#7 Format seit der Version 6. Mit der kostenpflichtigen Acrobat Vollversion können beliebige PDF-Dokumente signiert werden. PDF-Dokumente, für welche die Signierfunktion mit einem Adobe LiveCycle Reader Extensions Server (oder limitiert auch mit Adobe Acrobat Professional) frei geschaltet wurde, können auch mit dem Adobe Reader digital signiert werden. Die Signaturprüfung ist auch ohne die Freischaltung eines PDF-Dokumentes möglich. Ein PDF-Dokument kann beliebig viele digitale Signaturen enthalten, wobei das Dokument mit jeder neu hinzu gefügten Signatur als neue Dokumentversion (Revision) abgespeichert wird.

Wie können wir Sie unterstützen?

SECARDEO verfügt über vertiefte technische Expertise und langjährige Erfahrungen bei der Planung, Realisierung und dem Betrieb von Lösungen mit digitalen Signaturen. Wir stellen Ihnen unser Wissen und Können zur Verfügung durch

- Inhouse-Seminare und Workshops,
- Analyse Ihrer Randbedingungen und Anforderungen,
- Erstellen eines technischen und organisatorischen Lösungskonzepts,
- Auswahl geeigneter Standardprodukte und Dienste,
- Ergänzung durch Integration von SECARDEO pdfGate Signaturkomponenten,
- Entwicklung von Prototypen und Proof-of-Concept,
- Realisierung von Lösungen für Signatur-Workflows,
- Unterstützung bei der Pilotierung und dem Betrieb.

Benötigen Sie weitere Informationen?

Wenn Sie weitere Informationen wünschen, wenden Sie sich bitte an

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