Elektronische Signaturen (Stand: 05.12.2017)

Die elektronische Signatur auf digitalen Dokumenten ersetzt zunehmend die manuelle Unterschrift auf Papier. Dies bietet zahlreiche Vorteile:

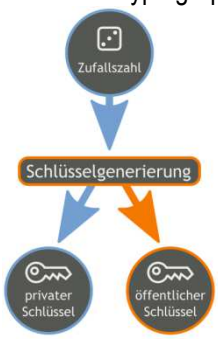
- Wegfall von Medienbrüchen, die entstehen, wenn ein digitales Ursprungsdokument nur zum Zwecke einer Unterschrift ausgedruckt und anschließend wieder eingescannt werden muss
- Nachhaltiger und beschleunigter Workflow
- Einsparung von Lager- und weiteren Logistikkosten
- Redlining direkt am Rechner unter Erhalt der ursprünglichen Qualität
- Digitale Dokumentenworkflows
- Tatsächliches Signieren des Inhalts des Dokuments und nicht nur des den Inhalt transportierenden Papiers

In Deutschland definierte zuerst das **Signaturgesetz (SigG 2001)** Arten von und Anforderungen an elektronische Signaturen. Mit der **eIDAS-Verordnung** (electronic IDentification And Signature) der EU über elektronische Identifizierung und Vertrauensdienste gilt seit Mitte 2016 eine EU-weite Regelung bzgl. der Definition von Signaturarten und -verfahren und die Möglichkeiten der bereitstellbaren Vertrauensdienste.

In diesem Dokument werden wir die im deutschen Signaturgesetz definierte „einfache elektronische Signatur“, welche im Prinzip schon durch eine einfache Mailsignatur oder gescannte Unterschrift gegeben ist, nicht weiter betrachten, da diese, von vielen bereits in der Vergangenheit genutzte, Signatur natürlich leicht fälschbar ist und kaum Beweiswert besitzt. Stattdessen betrachten wir Verfahren, welche folgende Eigenschaften sicherstellen:

Authentizität: die eindeutige Zuordnung einer Signatur zu einer natürlichen oder juristischen Person
Integrität: die Unveränderlichkeit des Inhalts eines signierten Dokumentes. Wird der Inhalt eines signierten Dokumentes geändert, muss die Überprüfung einer Signatur mit entsprechendem Hinweis scheitern.

Hierzu sind die **fortgeschrittene und die qualifizierte Signatur definiert,** welche Technologien aus der Kryptographie einsetzen, um die Authentizität eines Verfassers/Absenders und die Integrität des so signierten Dokuments zu sichern.
Dabei wird ein sogenanntes asymmetrisches Schlüsselpaar erstellt, bei dem der geheim zu haltende Teil beim Signierenden verbleibt und der andere Teil veröffentlicht werden kann bzw. sogar muss. Mit dem geheimen Schlüssel wird ein Dokument signiert.
Ein Außenstehender kann die Gültigkeit der Signatur mit dem öffentlichen Schlüssel überprüfen.



Während der mathematische Teil der Überprüfung von den verwendeten Systemen automatisch angewandt wird, muss nun allerdings der eine Signatur Überprüfende darauf vertrauen können, dass der ihm bekanntgegebene öffentliche Schlüssel auch tatsächlich zu der Person gehört, deren Autorenschaft er überprüfen möchte. Hier unterscheiden sich die fortgeschrittene und die qualifizierte Signatur voneinander.

Die fortgeschrittene Signatur

Bei der fortgeschrittenen Signatur kann man das zuvor genannte Schlüsselpaar selbst erstellen. Diese Möglichkeit ist unter anderem im frei verfügbaren Adobe Reader vorgesehen. Das Schlüsselpaar wird als kennwortgeschützte Datei erstellt, sodass der Signierende sich durch diese Datei und das nur ihm bekannte Kennwort authentifiziert.

Der öffentliche Schlüssel, der zur Überprüfung der Signatur bei einem Empfänger erforderlich ist, kann als Datei exportiert und den potentiellen Empfängern zur Verfügung gestellt werden. Diese binden sich den öffentlichen Schlüssel zum Beispiel im Adobe Reader als vertrauenswürdig ein und können damit in Zukunft die Authentizität eines vom Signierer erstellten Dokumentes überprüfen.

Damit der Empfänger nach erfolgreicher technischer Überprüfung der Signatur auch tatsächlich von der Authentizität bezüglich des Absenders überzeugt sein kann, muss der öffentliche Schlüssel ihm vorher auf sicherem Wege, z. B. per persönlicher Übergabe, signierter E-Mail (sofern hier die Authentizität klargestellt ist) oder über einen vertrauenswürdigen Verzeichnisdienst übermittelt werden.

Die fortgeschrittene Signatur alleine kann also, insbesondere bei Kommunikation mit zuvor nicht bekannten Parteien, keine gesicherten Rückschlüsse auf den tatsächlichen Autor liefern.

Die qualifizierte Signatur

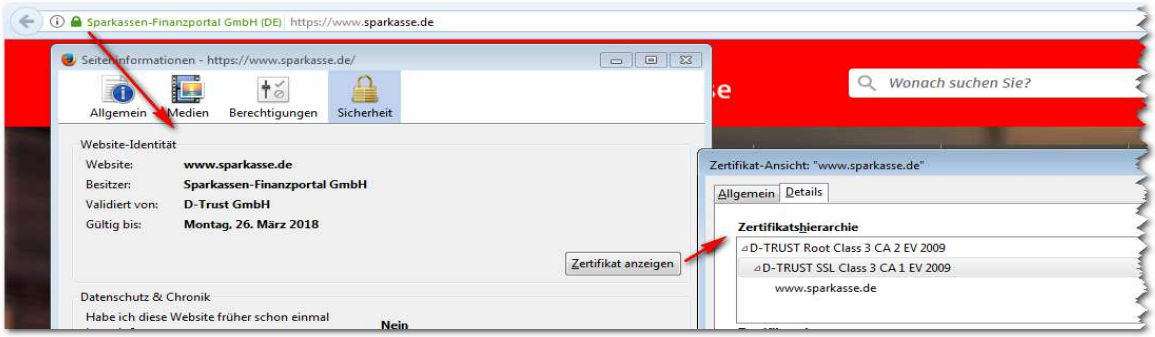
Bei der qualifizierten Signatur werden hohe Anforderungen an alle an der Signatur beteiligten Elemente (Personen, Zertifizierungsstellen, Hard- und Software) gestellt, die vorgegebene Standards einhalten und diesbezüglich zertifiziert sein müssen.

Dies beginnt damit, dass das zur Signierung verwendete Schlüsselpaar über einen zugelassenen Zertifizierungsdiensteanbieter (ZDA) eindeutig der signierenden Person zugeordnet wird, also eine Identitätsprüfung dieser Person vorgenommen wird. Der ZDA signiert nach erfolgter Identitätsprüfung dann das Schlüsselpaar wiederum mit seinem eigenen Zertifikat.

Weiterhin ist die sichere Aufbewahrung und Verwendung des erstellten Schlüssels zu gewährleisten. Dies geschieht über entsprechend zertifzierte Hard- und Software (d. h. Signaturkarten, Kartenleser, Signatursoftware usw.).

Nach erfolgreicher Signierung eines Dokuments ist dieses mit dem Zertifikat der signierenden Person und dieses Zertifikat wiederum mit den Zertifikaten des ZDA signiert. Dadurch kann ein Empfänger die Identität ohne vorherige Übermittlung des öffentlichen Schlüssels des Signierenden (vgl. fortgeschrittene Signatur) sicherstellen. Natürlich ist es dazu aber wiederum erforderlich, dass dem Zertifikat des ZDA vertraut wird und ggf. wieder dem Zertifikat mit dem der ZDA von noch hochrangiger Stelle zertifiziert wurde („Chain of Trust“, Vertrauenskette).

Dies ist z. B. mit dem Besuch einer Bank-Webseite vergleichbar. Der Webbrowser vertraut dem Zertifikat, welches hinter der Zielwebseite steckt und zeigt entsprechend das „grüne Schloss“ in der URL-Seite an. Das Vertrauen in das Zertifikat entsteht dadurch, dass das Bank-Zertifikat über eine Kette weiterer Zertifikate signiert wurde von denen schließlich der Browser-Hersteller eines als vertrauenswürdig einstuft:



Voraussetzungen

Für die Verwendung einer qualifizierten Signatur sind also mindestens **auf der Erstellerseite** zusätzliche Investitionen in

- eine Identitätsprüfung
- Signaturkarte
- Kartenleser
- Signatursoftware

erforderlich.

Aber auch auf der Empfängerseite sind oftmals der Einsatz und die Pflege/Aktualisierung von zur Überprüfung von qualifizierten Signaturen zugelassener Software erforderlich:
Mit Fortschreiten der Technik und der Regulierungsprozesse stehen immer neuere Signaturverfahren zur Verfügung, die unterstützt werden müssen. Hinzu kommt, dass alle Signaturzertifikate mit einem Ablaufdatum versehen sind und dann irgendwann einem Austausch unterliegen.

Die qualifizierte Signatur beinhaltet auch die Möglichkeit, z. B. Signaturkarten, die abhandengekommen sind, **zu sperren**. Diese können dann in Zukunft nicht mehr verwendet werden bzw. werden nach Verlust der Karte signierte Dokumente nicht mehr als authentisch gewertet. Dies funktioniert über von den ZDA geführten Sperrlisten, welche online abgerufen werden müssen, was auch hier eine **ständige Aktualisierung der verwendeten Software** und somit ebenfalls eine Online-Verbindung erfordert.

Eine freie, zertifizierte und gesichert funktionierende Software, die diese Funktionen zuverlässig erfüllt, ist dem Autor derzeit nicht bekannt, sodass auch auf der Empfangsseite eine kostenpflichtige Software erforderlich ist. Die Verwendung eines Online-Services zur Prüfung von Signaturen ist wegen des dazu notwendigen Uploads von ggf. geheim zuhaltenden Dokumenten keine Alternative. **Ohne den Einsatz einer aktuellen Überprüfungslösung, die z. B. auch als Plug-In im Adobe Reader DC erhältlich ist, zeigt z. B. letztgenanntes Produkt fälschlicherweise korrekte Signaturen als fehlerhaft oder ungültig an.**

Anwendung

Die qualifizierte Signatur kann nach § 126a BGB eine *per Gesetz oder Verordnung notwendige Schriftform* ersetzen, sofern für den jeweiligen Fall keine anderweitig gesetzliche Regelung besteht.
Da bei (privaten) Rechtsgeschäften Formfreiheit besteht, z.B. bei Kaufverträgen, bedarf es grundsätzlich keiner Signatur (siehe auch § 127 (2) BGB), wodurch dann natürlich auch eine einfache oder fortgeschrittene elektronische Signatur ausreicht.
Wo eine qualifizierte Signatur nicht gefordert wird, hat sie aber im Falle eines Rechtsstreits eine höhere Beweiswirkung (siehe auch § 371a ZPO) als eine „nur“ fortgeschrittene Signatur, welche wiederum höherwertiger ist, als die leicht fälschbare, einfache Signatur.
Weiterhin können elektronische Signaturen natürlich nicht nur bei Verträgen, sondern bei auch bei Protokollen, Prüfberichten, Freigaben usw. verwendet werden. Auch hier obliegt dann im Falle eines Rechtsstreits die Würdigung der Beweiskraft dem Gericht (§ 286 ZPO), wobei, wie bereits beschrieben, die qualifizierte Signatur eine hohe Beweiskraft besitzt.

Zusammenfassung zur fortgeschrittenen und qualifizierten Signatur

Fortgeschrittene Signatur:
Vorteile:

- Zertifikat kann selbst erstellt werden
- Funktionalität z. B. in Adobe Reader usw. bereits enthalten
- keine Installation und regelmäßige Pflege weiterer Software/Hardware erforderlich
- leichte Verwendung innerhalb der Software
- höhere Beweiskraft als lediglich „einfache Signaturen“

Nachteile:

- Austausch des öffentlichen Schlüssels muss selbst und auf sicherem Wege durchgeführt werden
- Ablage des privaten Zertifikates in einer nur durch Kennwort gesicherten Datei ist nicht sicher (z.B. kann durch Kopieren der Datei und Installation eines Keyloggers die zum Signieren notwendige Information von Dritten erlangt werden)
- Sperren von bekannt gewordenen Schlüsseldaten nicht über zentrale Infrastruktur möglich
- durch fehlende (bzw. unregulierte) Gültigkeitsdauerbegrenzung besteht die Gefahr einer technischen Überholung, insbesondere bei der Entdeckung von Angriffsmöglichkeiten auf veraltete Algorithmen
- geringere Beweiskraft als qualifizierte Signaturen
- ersetzt nicht die schriftliche Form, wo sie per Gesetz vorgeschrieben ist (§ 126a (1) BGB)

Qualifizierte Signatur:
Vorteile:

- gesetzlich geregelter Ersatz, wo die Schriftform gesetzlich gefordert wird (§ 126a (1) BGB)
- kein Schlüsselaustausch mit empfangenden Parteien erforderlich
- derzeit höchstmögliche Beweiskraft
- sehr hohe Sicherheit gegen Entwendung des Zertifizierungsschlüssels durch sichere Signierkarten, Zugangs-PIN, zertifizierte Hardware und Software

Nachteile / Voraussetzungen:

- kostenpflichtige Identitätsprüfung, Zeitaufwand, Signaturkarte und Hardware erforderlich
- Installation von Software(treibern) auf dem genutzten Rechner erforderlich
- kostenpflichtiges Plug-In z. B. innerhalb des (kostenlosen) Adobe Readers erforderlich
- regelmäßige Updates der verwendeten Zertifikate der Zertifizierungsdiensteanbieter erforderlich sowie ggf. neuer Verfahren zur Signaturerstellung und -prüfung (sofern das nicht durch die Software erfolgt und dazu auch ggf. ein Wartungsvertrag vorliegt)
- auch auf Empfängerseite, die Signaturen nur überprüfen will, ist häufig eine zusätzliche Software erforderlich
    - Wird eine nicht für die Signaturart ausgelegte oder veraltete Software verwendet, so werden Signaturen häufig falsch erkannt, d. h. nicht nur wird der Signierer nicht als authentifiziert gemeldet, sondern häufig auch das Dokument als nachträglich geändert (siehe „Integrität) eingestuft, auch wenn das nicht der Fall war.
    - Eine nicht aktuelle Version kann veraltete Sperrlisten-Informationen besitzen und damit fälschlicherweise ein mit einer gesperrten Karte signiertes Dokument als authentisch erkennen.

Übrigens ist der **elektronische Personalausweis** ursprünglich zur Authentifizierung gegenüber hoheitlichen und auch gegenüber Dritten intendiert gewesen (= Personalausweis-Funktion). Die Durchführung einer qualifizierten elektronischen Signatur ist technisch zwar auch möglich, erfordert aber eine entsprechende, noch nicht von jedem Anbieter verfügbare, technische Kompatibilität von Hard- und Software, sowie eine (kostenpflichtige) Identitätsprüfung und Einbindung eines Zertifikates in den Personalausweis selbst.

Kosten (qualifizierte Signatur)

- Kartenlesegerät — ca. 60 €
- Signaturkarte inklusive Identitätsprüfung — ca. 160 € (3 Jahre Gültigkeit)
- Software zur Dokumentensignierung / Adobe Reader-Plugin — ca. 120 €

Konkrete Produkte werden von den einzelnen Vertrauensdiensteanbietern angeboten bzw. empfohlen. Über die Webseite der Bundesnetzagentur, welches die in Deutschland zuständige Aufsichtsstelle für Vertrauensdienste ist, können entsprechende Anbieter gefunden werden (https://www.bundesnetzagentur.de/DE/Service-Funktionen/ElektronischeVertrauensdienste/QualifizierteVDA/QualVDA_node.html (Link zuletzt geprüft am 05.12.2017)).

Sonstiges

Im Folgenden soll nur noch auf weitere Möglichkeiten eingegangen werden, ohne die technischen Voraussetzungen im Detail zu klären:

„Multi"-Signaturkarten / Stapelsignatur
Neben den „Standard"-Signaturkarten, die pro Signatur die Eingabe einer PIN erfordern, gibt es auch noch „Multi"-Signaturkarten, bei denen mit einmaliger PIN-Eingabe mehrere Signaturvorgänge durchgeführt werden können. Ob dieses Feature genutzt werden kann, ist auch von der eingesetzten Software abhängig. Multi-Signaturkarten kosten oft mehr als das doppelte des Preises einer „Standard"-Signaturkarte.

Zeitstempel
Neben der Authentizität des Autors und der Integrität des Dokuments, erlauben einige Softwareprodukte auch das Signieren mit einem Zeitstempel, wobei die Uhrzeit von einem vertrauenswürdigen, externen Server geladen und mit der Signatur verknüpft wird. So kann auch der Zeitpunkt des Signaturvorganges hinterlegt werden.

Fernsignaturen
Hier wird der private Signaturschlüssel in einem „sicheren System" auf einem Server bei einem Vertrauensdiensteanbieter hinterlegt und kann aus der Ferne, z. B. über eine Webseite oder eine Smartphone-Applikation, zum Signieren von Dokumenten genutzt werden.

Biometrische Signaturen
Einige Dienste bieten die Unterzeichnung per Signatur-Tablet an auf welchem die handschriftliche Unterschrift, nun eben digitalisiert, geleistet wird. Dies alleine entspricht noch keiner fortgeschrittenen oder gar qualifizierten Signatur im Sinne der eingangs erwähnten Verordnungen und Gesetze. In Verbindung mit der Erfassung von Schreibgeschwindigkeit und Schreibdruck kann die bildliche Erfassung der Unterschrift aber z. B. durch einen entsprechenden Schriftsachverständigen vor Gericht eine hohe Beweiskraft entfalten. Hierzu muss aber, wie bei den anderen Signaturarten die Signatur fest mit dem signierten Dokument verknüpft werden, was durch den zusätzlichen Einsatz entsprechender kryptographischer Mittel möglich ist.

Langzeitarchivierung elektronisch signierter Dokumente
Mit Fortschreiten der Technik können ehemals als sicher geltende Verfahren in Zukunft unsicher werden. Um dennoch die Beweiskraft von signierten Dokumenten zu bewahren, können diese mit entsprechenden technischen Lösungen in Kombination mit vertrauenswürdigen Zeitstempeln „nachsigniert" werden, wozu das **ArchiSig**-Konzept erste Lösungsansätze bietet.

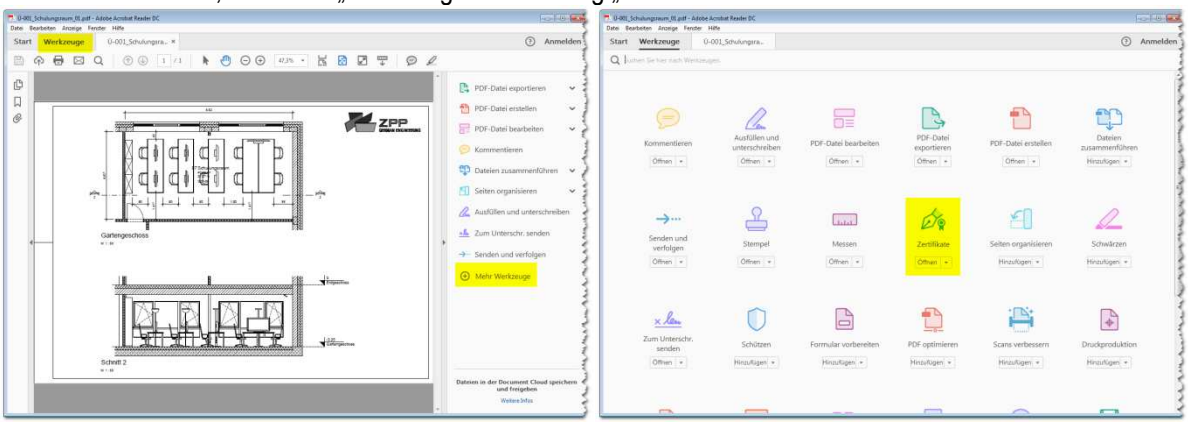
Signatur von beliebigen Dokumenten
Wurde bis jetzt und auch im folgenden Beispiel immer nur das PDF-Format erwähnt, welches ausdrücklich auch für den Einsatz digitaler Signaturen weiterentwickelt wurde (**PAdES**), so lassen sich beliebige elektronische Dokumente signieren, wie es z. B. bereits mit dem **S/MIME-Standard** für Emails der Fall ist. Mit **CAdES** (zuvor **CMS**, zuvor **PKCS#7**) und **XAdES** können auch andere Dateien signiert werden, wobei dann entweder eine Signaturdatei parallel zur Original-Datei erstellt wird, oder beide Informationen in einem gemeinsamen Container verknüpft werden.

Serverbasierte Massensignatur und -verifikation
Neben der Anwendung an einem Arbeitsplatz ermöglichen entsprechende Systeme auch die automatisierte Signatur und Verifikation von Dokumenten, was insbesondere bei zahlreichen zu signierenden oder zu überprüfenden Dokumenten große Zeitersparnis bringen kann. Gerade das massenhafte und automatisierte Signieren erfordert aber hohe Sicherheitsmaßnahmen gegen Missbrauch.

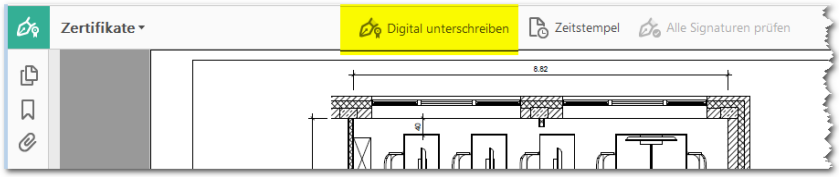
Qualifiziertes elektronisches Siegel
Was im deutschen Signaturgesetz noch nicht existierte, ist nun mit der eIDAS Verordnung neu eingeführt (eIDAS, Abschnitt 5). Anstatt ausschließlich mit einer an eine natürliche Person gebundene Signatur zu unterzeichnen, können nun auch Zertifikate für juristische Personen, also Firmen, in Form eines elektronischen Siegels ausgestellt werden. Damit wird das einheitliche und zweifelsfreie Signieren von Firmendokumenten ermöglicht, da die Ausstellung eines qualifizierten, elektronischen Siegels die Identifikation der Firma zwingend erfordert, während bei den Signaturen einer natürlichen Person eben nur diese und (im Allgemeinen nicht) deren Zugehörigkeit zu einer Firma gesichert ist.
Zum Zeitpunkt der Erstellung dieses Dokumentes gibt es nur einen einzigen Anbieter von Firmensiegeln zum Preis von 900 € (für drei Jahre).

Beispiel (mit D-TRUST card 3.0 und OpenLimit CC Sign, sowie dem Adobe Reader DC)

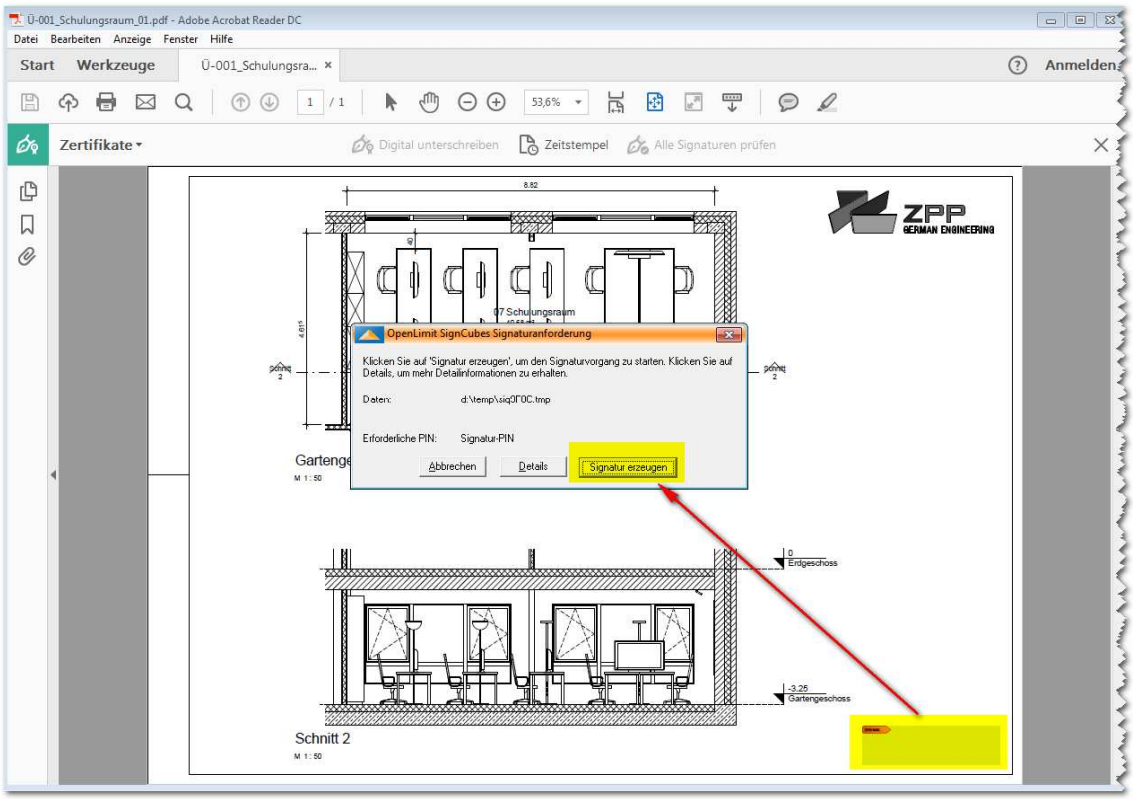
1. PDF öffnen, und unter „Werkzeuge“ den Eintrag „Zertifikate“ wählen



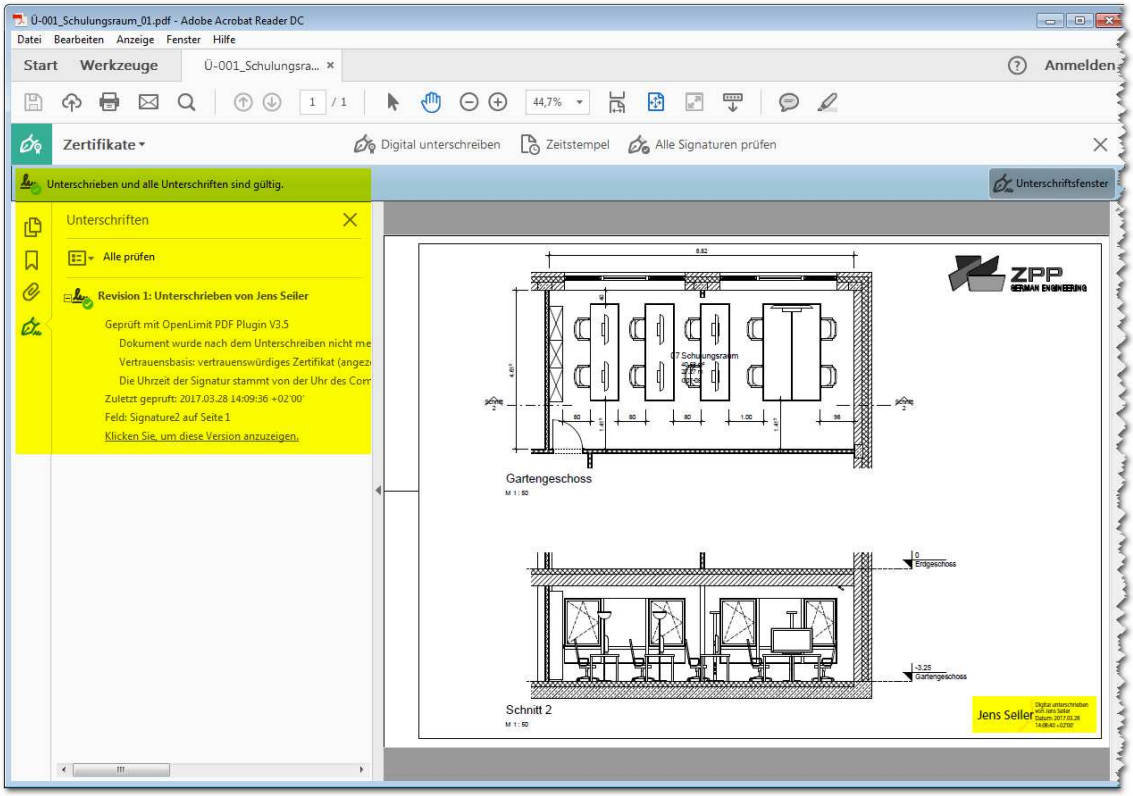
2. Die Option „Digital unterschreiben“ aus der Leiste oben auswählen und mit der Maus einen Rahmen ziehen, wo die Signatur (rein optisch) erscheinen soll



3. Nach Ziehen des Signaturrechtecks öffnet sich das Plug-In, fragt zunächst nach Bestätigung und anschließend über den Kartenleser die korrekte PIN ab



4. Anschließend ist das Dokument sowohl optisch sichtbar als auch elektronisch signiert



5. Nachträgliche Änderungen werden erkannt und angezeigt