E-ConsentPro mobile / E-DocumentPro

Sicherheit der elektronischen Unterschrift

Mit E-ConsentPro mobile und E-DocumentPro können mobile Endgeräte wie Tablets für die Patientenaufklärung und Bearbeitung kundeneigener Bögen genutzt werden. Dies ermöglicht ein ortsunabhängiges Aufklärungsverfahren mit größeren Gestaltungs- und Handlungsspielräumen.

Zudem ist ein durchgängiger digitaler Workflow möglich, vom Ausfüllen des Bogens bis hin zur elektronischen Unterschrift und digitalen Archivierung.

Das elektronische Unterschreiben ist ein zentraler Prozess-Schritt im digitalen Workflow. Nur mithilfe der elektronischen Unterschrift lässt sich ein durchgängiger Ablauf ohne Medienbruch realisieren. Doch wie ist die Sicherheit der elektronischen Unterschrift einzustufen? Wie wird erreicht, dass keine Manipulation der Unterschrift möglich ist? Und was passiert im Fall einer gerichtlichen Auseinandersetzung, falls die Echtheit der Unterschrift angezweifelt wird?

Dieses Dokument enthält Informationen rund um das elektronische Unterschreiben auf dem Tablet. Es erläutert die Bestandteile einer elektronischen Unterschrift und beschreibt, wie Unterschrift und unterschriebenes Dokument geschützt werden. Ebenso wird erklärt, wie im Fall eines Rechtsstreits die Echtheit der Unterschrift bewiesen werden kann.

Apps für den mobilen Workflow

Für Tablets stehen drei einfach zu bedienende Apps zur Verfügung: „Anamnese mobil“, „Aufklärung mobil“ und „E-DocumentPro“.

Mit der App „Anamnese mobil“ können Patienten vor dem Aufklärungsgespräch die Anamnesefragen beantworten. Der Arzt kann die Daten auswerten und sich so gezielt auf das Aufklärungsgespräch vorbereiten.

Beim Arzt-Patienten-Gespräch kann der Arzt die Angaben des Patienten in der App „Aufklärung mobil“ einsehen und bearbeiten. Der Eingriff kann mithilfe von Bildern und Aufklärungsfilmen anschaulich erläutert werden. Zudem sind Individualisierungen durch handschriftliche Anmerkungen möglich. Dem Aufklärungsbögen können Eintragungen, Einzeichnungen, Freihandskizzen sowie eigene Zeichnungsvorlagen hinzugefügt werden.
Am Ende des Gesprächs kann der Aufklärungsbogen mit einem geeigneten Tablet-Stift auf dem Tablet unterschrieben werden. Die App „Aufklärung mobil“ zeigt entsprechende Felder für die Unterschrift des Arztes und des Patienten an.

Die App „E-DocumentPro“ ermöglicht die Bearbeitung kundeneigener Bögen. Checkboxen und Freitextfelder können ausgefüllt und Hervorhebungen und Freihandzeichnungen hinzugefügt werden. Zum Abschluss werden die ausgefüllten Bögen elektronisch unterschrieben und für das digitale Archivsystem bereitgestellt

Wenn E-ConsentPro an ein digitales Archivsystem angebunden ist, kann das unterschriebene Dokument abschließend in das Archiv übertragen werden.

Abb. 1 Feld für die elektronische Unterschrift auf dem Tablet

Elektronisch unterschreiben – aber sicher!

Bei der in E-ConsentPro verwendeten Technologie besteht eine elektronische Unterschrift aus zwei Komponenten: dem statischen Bild der Unterschrift und den biometrischen Merkmalen wie Auf- und Absetzpunkte, Schreibgeschwindigkeit und Schreibdruck.

Statisches Bild

Biometrische Merkmale

Abb. 2 Bestandteile einer elektronischen Unterschrift

Die biometrischen Daten werden während des Unterzeichnens aus der Schreibbewegung abgeleitet und aufgezeichnet. Voraussetzung für die Aufzeichnung der biometrischen Daten ist, dass ein Tablet-Stift verwendet wird und eine Verbindung zwischen App und Tablet-Stift besteht.

Thieme Compliance

Informationen zu empfohlenen Geräten für die elektronische Unterschrift finden Sie in den Systemvoraussetzungen für E-ConsentPro.

Biometrische Merkmale sind bei den Unterzeichnenden individuell ausgeprägt. Auch wenn die einzelnen Unterschriften derselben Person nicht ganz identisch sind, lassen sie sich anhand der biometrischen Merkmale dem Unterzeichnenden zuordnen.

Die elektronische Unterschrift wird zudem verschlüsselt und fest mit dem unterschriebenen Dokument verbunden. Das verwendete Verfahren stellt sicher, dass weder die elektronische Unterschrift noch das unterschriebene Dokument manipuliert werden können. Elektronisch unterschriebene Dokumente haben somit eine vergleichbare Beweiskraft wie unterschriebene Papierdokumente.

Im Folgenden wird das Verschlüsselungsverfahren näher erläutert.

Verschlüsselung der Unterschrift mit AES und RSA

Die biometrischen Daten einer elektronischen Unterschrift werden mit einer Kombination aus AES und RSA doppelt verschlüsselt. Beide Verfahren sind allgemein anerkannte, weit verbreitete Standardverfahren und gelten nach derzeitigem Stand der Informationstechnologie als sicher. Durch die Kombination der beiden Verfahren wird eine schnelle und gleichzeitig sichere Verarbeitung des unterschriebenen Dokuments erreicht.

Die biometrischen Daten werden zunächst mit einem individuellen, zufällig erzeugten AES-Schlüssel verschlüsselt. Dieser AES-Schlüssel wird wiederum geschützt, indem er mit einem RSA-Verfahren verschlüsselt im Dokument gespeichert wird.

Abb. 3 Doppelte Verschlüsselung der biometrischen Daten

Für das RSA-Verfahren wird ein zuvor generiertes Schlüsselpaar mit digitalem Zertifikat verwendet. Das Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel, die nur in Kombination funktionieren. Informationen, die mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten Schlüssel wieder entschlüsselt werden.

Das Schlüsselpaar wird von Thieme Compliance generiert. Mit E-ConsentPro wird jedoch nur der öffentliche Schlüssel ausgeliefert und nicht der private Schlüssel. Der private Schlüssel ist somit nicht öffentlich zugänglich; weder E-ConsentPro-Kunden noch Patienten noch unbefugte Dritte haben darauf Zugriff. Diese Handhabung stellt sicher, dass die biometrischen Daten der elektronischen Unterschrift nicht unbefugterweise entschlüsselt werden können. Ein nachträgliches Entschlüsseln und Manipulieren der Unterschrift ist somit technisch nicht möglich.

Vom Aufklärungsbogen zum unterschriebenen PDF-Dokument

Mit E-ConsentPro mobile wird der Aufklärungsbogen am Ende des Aufklärungsvorgangs in ein PDF-Dokument im archivierungsfähigen PDF/A-Format umgewandelt, das dem internationalen Standard ISO 32000 entspricht. Das PDF-Dokument wird elektronisch unterschrieben.
Unterschriebene kundeneigene Bögen (E-DocumentPro) werden als PDF-Dokument bereitgestellt.

Mithilfe von Integritätswerten und einer digitalen Signatur wird das finale PDF-Dokument gegen Manipulation geschützt. Integritätswerte (Englisch „hash values“) sind Werte, die aus dem Dokumentinhalt errechnet werden und den Dokumentinhalt repräsentieren.

Durch dieses Verfahren lässt sich jederzeit Folgendes feststellen:
- die Echtheit der elektronischen Unterschrift
- Datum und Uhrzeit der elektronischen Unterschrift
- die Verbindung zwischen elektronischer Unterschrift und Dokument, d.h. welches Dokument mit welchem inhaltlichen Stand elektronisch unterschrieben wurde
- die Unversehrtheit des Dokuments.
  Es ist sichergestellt, dass das Dokument nach der Verarbeitung durch die App „Aufklärung mobil“ nicht mehr verändert wurde.

Die folgende Grafik gibt einen Überblick über die Schritte, die im Einzelnen in E-ConsentPro mobile ablaufen:

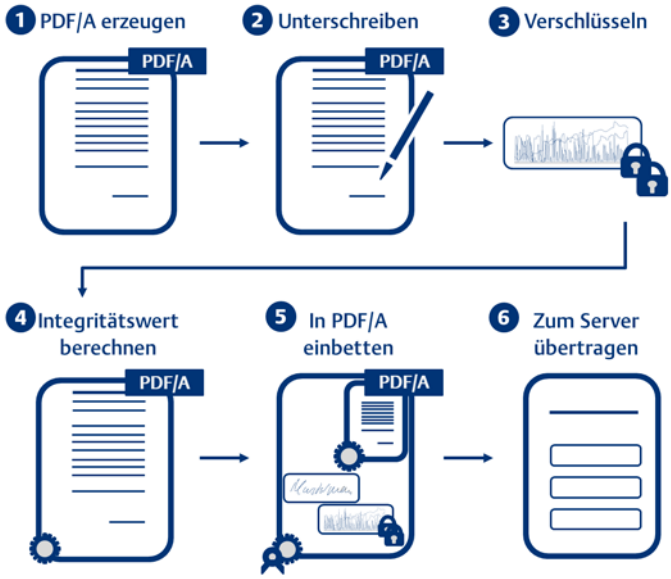

Abb. 4 Vom Aufklärungsbogen zum elektronisch unterschriebenen PDF-Dokument

1. E-ConsentPro mobile generiert aus dem Aufklärungsbogen ein PDF/A-Dokument, das dem internationalen Standard ISO 32000 entspricht.

2. Arzt und Patient unterschreiben das PDF/A-Dokument auf dem Tablet. Die App „Aufklärung mobil“ zeigt entsprechende Felder für die Unterschrift an. Die Unterschrift erfolgt mit einem für diesen Zweck geeigneten Tablet-Stift.

3. Die biometrischen Daten der jeweiligen Unterschrift werden mit einem AES-Schlüssel verschlüsselt. Der AES-Schlüssel wird wiederum mit dem öffentlichen Schlüssel des von Thieme Compliance generierten RSA-Schlüsselpaares verschlüsselt.

4. Aus dem Original-PDF/A-Dokument wird ein Integritätswert berechnet, der spezifisch für das Originaldokument ist und dessen Inhalt repräsentiert. Der Integritätswert und die Länge des Originaldokuments werden bei den biometrischen Daten gespeichert. So ist sichergestellt, dass die biometrischen Daten genau zu diesem PDF/A-Dokument passen.

5. Die verschlüsselten biometrischen Daten, die statischen Bilder der Unterschriften, der erste Integritätswert und die Länge des Originaldokuments werden nun von der App „Aufklärung mobil“ in das PDF/A-Dokument eingebettet. Im PDF/A ist auch gespeichert, zu welchem Zeitpunkt das Dokument elektronisch unterzeichnet wurde.

   Für das unterschriebene PDF/A-Dokument wird nun ein zweiter Integritätswert berechnet. In diesen Integritätswert fließen die biometrischen Daten der Unterschriften, der erste Integritätswert, die Länge des Originaldokuments und die statischen Bilder der elektronischen Unterschriften ein.

   Der zweite Integritätswert wird mit dem Zertifikat der App „Aufklärung mobil“ digital signiert und im PDF/A gespeichert. Die digitale Signatur bestätigt, dass das Dokument von der App „Aufklärung mobil“ verarbeitet und danach nicht mehr verändert wurde.

   Mit diesem Verfahren ist sichergestellt, dass elektronisch unterschriebene PDF/A-Dokumente nachträglich nicht geändert werden können. Wenn das Dokument nach der Unterschrift geändert wird, wird dies dokumentiert und wäre technisch nachweisbar.

6. Abschließend wird das elektronisch unterschriebene und integritätsgesicherte PDF/A-Dokument von der App zum E-ConsentPro Server übertragen.

Das für E-ConsentPro mobile beschriebene Verfahren gilt genauso für E-DocumentPro.

Warnhinweise im Adobe Reader

Im Adobe Reader wird Ihnen beim Öffnen der PDF/A-Dokumente folgender Warnhinweis angezeigt: „Die Identität des Unterzeichners ist nicht bekannt, weil sie sich nicht in der Liste der vertrauenswürdigen Zertifikate befindet.“

Dieser Hinweis ist irritierend. Der Adobe Reader geht davon aus, dass jeder Unterzeichner mit seinem persönlichen digitalen Zertifikat signiert. Da aber in der Realität kaum jemand ein persönliches Zertifikat hat, hat Thieme Compliance ein eigenes System entwickelt, um die Sicherheit zu garantieren.

Die Apps „Aufklärung mobil“ und „E-DocumentPro“ verwenden ein selbstsigniertes Zertifikat, um das finale PDF-Dokument digital zu signieren. Dieses selbstsignierte Zertifikat ist dem Adobe Reader und dem lokalen PC nicht bekannt und verursacht deshalb einen Warnhinweis. Dennoch kann der Adobe Reader wirkungsvoll verifizieren, dass das Dokument seit der digitalen Signatur nicht verändert wurde.

Die digitale Signatur gibt keine Auskunft über die natürliche Person des Unterzeichners. Sie bestätigt lediglich, dass das Dokument von der App „Aufklärung mobil“ bzw. „E-DocumentPro“ verarbeitet und danach nicht mehr verändert wurde. Die Verbindung zur natürlichen Person des Patienten wird vielmehr über die biometrischen Daten hergestellt, die verschlüsselt im PDF-Dokument eingebettet sind. Die Echtheit der biometrischen Daten kann mit dem beim Notar hinterlegten privaten Schlüssel verifiziert werden.

Aufbewahrung des privaten Schlüssels

Der private Schlüssel, der zum öffentlichen Schlüssel für die biometrischen Daten gehört, ist bei einem Notar hinterlegt. Er wird nicht mit der Software ausgeliefert. Dadurch haben weder E-ConsentPro-Kunden noch Patienten Zugriff auf den privaten Schlüssel.

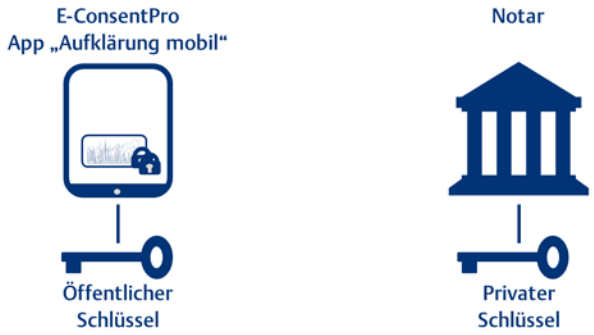

Abb. 5 Aufbewahrung des privaten Schlüssels zur Entschlüsselung der biometrischen Daten

Dieses Verfahren dient zum Schutz der E-ConsentPro-Kunden im Fall einer gerichtlichen Auseinandersetzung. Da E-ConsentPro-Kunden keinen Zugriff auf den privaten Schlüssel haben, ist es ihnen technisch nicht möglich, eine elektronische Unterschrift zu fälschen oder nachträglich zu manipulieren.

Aufbewahrung der PDF/A-Dokumente

Die Nachweise über einen ordnungsgemäßen Aufklärungsprozess müssen langfristig und sicher aufbewahrt werden.
Das PDF/A-Format ist ein internationaler Standard für systemunabhängige Archivierung. Der Standard stellt sicher, dass PDF/A-Dokumente unabhängig vom erzeugenden Programm langfristig angezeigt werden können.

Für eine sichere Aufbewahrung empfehlen wir, die erzeugten PDF/A-Dokumente in einem digitalen Langzeitarchiv zu archivieren und bei der Archivierung Zeitstempel einzusetzen.
E-ConsentPro bietet hierfür eine entsprechende Schnittstelle an.

Im Fall einer gerichtlichen Auseinandersetzung

Sollte es zu einer gerichtlichen Auseinandersetzung kommen, weil beispielsweise die Echtheit der elektronischen Unterschrift angezweifelt wird, kann ein Schriftsachverständiger die biometrischen Daten der Unterschrift analysieren und deren Echtheit nachweisen.

Hierzu benötigt der Sachverständige den privaten Schlüssel, den er vom Notar erhält. Nur mithilfe des privaten Schlüssels lassen sich die biometrischen Daten der elektronischen Unterschrift entschlüsseln und anschließend analysieren.

Zur Analyse wird ein spezielles Analyseprogramm verwendet. Das Programm ermöglicht es, das Unterschriftenbild visuell zu prüfen und die unsichtbaren biometrischen Merkmale aus der Schreibbewegung zu analysieren, beispielsweise Schreibgeschwindigkeit, Auf- und Absetzpunkte von Schriftabschnitten, Schreibdruck usw.

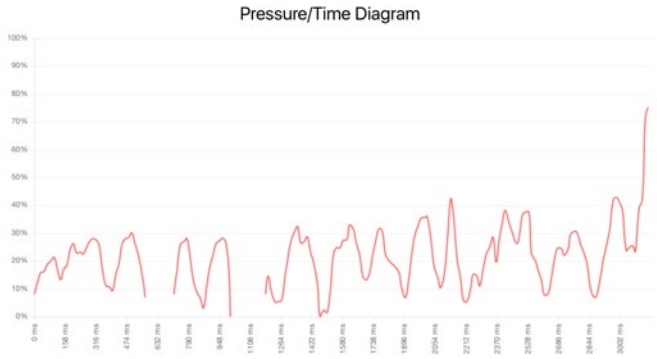

Abb. 6 Analyse der biometrischen Merkmale einer elektronischen Unterschrift

Über Thieme Compliance

Führender Systemanbieter für medizinische Patientenaufklärungs- und Informationsmedien (Praxen, MVZ, Krankenhäuser) mit mehr als 30 Jahren Markterfahrung

Spezialisiert auf **maßgeschneiderte Lösungen für die Patientenaufklärung**

Umfassendstes Sortiment an Aufklärungsprodukten am Markt:

- → Über 2.000 Aufklärungsbögen der Sortimente Diomed und proCompliance
- → Jedes Fachgebiet in bis zu 20 Sprachen
- → Alle gängigen Medien: Print- und Digitalprodukte, Filme, Durchschreibesätze

Höchste inhaltliche Qualität und Aktualität der Aufklärungsprodukte:

- → Expertenteam aus über 400 medizinischen Autoren, Redakteuren und Juristen
- → Permanente Anpassung an medizinische und rechtliche Anforderungen
- → Zertifiziertes Qualitätsmanagementsystem (DIN EN ISO 9001 und EN ISO 13485)

Empfohlen von führenden Fachverbänden und Versicherungen

Stand: Juni 2019

Thieme Compliance GmbH
Am Weichselgarten 30a
91058 Erlangen
www.thieme-compliance.de

Tel.: +49 9131 93406-40
Fax: +49 9131 93406-74
E-Mail: support@thieme-compliance.de

Thieme Compliance