

RECHTSGUTACHTEN¹

CO SIGN UND DIE ANFORDERUNGEN DES DEUTSCHEN SIGNATURRECHTS

ERSTELLT FÜR

ALGORITHMIC RESEARCH (AR)

FRANKFURT, JANUAR 2005

WALDECK RECHTSANWÄLTE PARTNERSCHAFTSGESELLSCHAFT
BEETHOVENSTRASSE 12-16, 60325 FRANKFURT AM MAIN

¹ Waldeck Rechtsanwälte Partnerschaftsgesellschaft (WRA) erstellt das Rechtsgutachten als unabhängiger rechtlicher – nicht technischer – Experte und repräsentiert nicht AR. Die von WRA begutachteten Rechtsfragen sind Gegenstand ungeklärter rechtswissenschaftlicher Fragestellungen. Das Rechtsgutachten enthält keine für WRA rechtsverbindlichen Erklärungen und dient allein dem internen Gebrauch von AR. WRA haftet weder gegenüber AR noch gegenüber Dritten für Schäden, soweit dies gesetzlich zulässig ist. Insbesondere haftet WRA nicht für Schäden, die durch die Benutzung von CoSign oder aufgrund von Entscheidungen entstanden sind, die auf diesem Rechtsgutachten basieren. Das Gutachten basiert auf den von AR unter www.arx.com und im Benutzerhandbuch CoSign zur Verfügung gestellten Informationen, die ungeprüft von WRA übernommen wurden. Es behandelt nicht alle rechtlichen Anforderungen des Signaturrechts.

INHALTSVERZEICHNIS

1.	PRODUKTINFORMATIONEN	3
2.	RECHTLICHE ANERKENNUNG UND RECHTSWIRKUNGEN ELEKTRONISCHER SIGNATUREN	4
3.	WESENTLICHE ANFORDERUNGEN DES SIGNATURRECHTS.....	4
4.	ERZEUGUNG ELEKTRONISCHER SIGNATUREN MIT CoSIGN.....	6
5.	SIGNATURERZEUGUNG IM AUTOMATISIERTEN VERFAHREN DURCH CoSIGN	7
5.1	AUTOMATISIERTE SIGNATURERZEUGUNG/ BATCH SIGNING.....	7
5.2	EINZELFRAGEN – LÖSUNG DURCH CoSIGN.....	7
6.	ZUSAMMENFASSUNG	12
	AUTOREN	13

1. PRODUKTINFORMATIONEN²

CoSign ist eine kombinierte Soft- und Hardwarelösung, mit der Anwendungen zur elektronischen Signatur in eine bestehende PKI integriert und eingesetzt werden können. Die Lösung bietet alle Funktionen einer Signaturanwendung, erfordert dabei aber praktisch keinen zusätzlichen Verwaltungsaufwand. CoSign stellt damit eine neuartige Lösung für das elektronische Signieren von Dokumenten, Dateien, Formularen und Transaktionen dar.

CoSign gewährleistet nach den Produktinformationen die Authentizität des Signierenden, die Integrität der signierten Daten und die Beweiseignung von Dokumenten, basierend auf herkömmlichen PKI-Technologien. Es bietet die Möglichkeit, unverfälschbare elektronische Signaturen zu erzeugen, die nicht unbemerkt dupliziert oder verändert werden können. Der Empfänger einer elektronischen Signatur, die von einem CoSign-Nutzer erzeugt wurde, kann sowohl die Integrität des elektronischen Dokumentes wie auch die Authentizität des CoSign-Nutzers und des Dokumenteninhalts überprüfen.

CoSign vermeidet mit seinem Ansatz, die privaten Schlüssel zentral zu verwalten und mit der Integration in das bestehende User-Management-System einer Organisation, einen zusätzlichen Aufwand bei der Implementierung. CoSign kann in die marktüblichen User-Management-Systeme integriert werden, beispielsweise in Microsoft Active Directory und Novell/ NDS. Diese Integration stellt sicher, dass bei der Verwaltung der Signaturkomponenten und Zertifikate kein Mehraufwand entsteht, insbesondere mit Blick auf die geheimen privaten Schlüssel der Nutzer. CoSign unterstützt weiterhin eine breite Palette von (Office-)Anwendungen, beispielsweise Microsoft Word, Adobe Acrobat, ERP (SAP) und verschiedene Webapplikationen. Weitere Funktionen in CoSign ermöglichen die Unterstützung von Massensignaturen ohne die Notwendigkeit einer individuellen Einflussnahme bei der Signaturerzeugung.

Die privaten Schlüssel und andere notwendige Signaturkomponenten sind in einer besonderen Umgebung auf der CoSign-Box gespeichert. Die Nutzer sind nur dann berechtigt, eine Signatur zu erzeugen, wenn sie im System gespeichert und Mitglieder der Nutzerliste sind. Diese kann über ein übliches User-Management-System verwaltet werden. Hat sich ein Nutzer authentifiziert, beispielsweise durch ein Passwort, eine Geheimzahl, ein privates Token oder mittels biometrischer Merkmale, so kann er eine Anfrage an die CoSign-Box senden, die den Hash-Wert des zu signierenden Dokumentes enthält. CoSign verschlüsselt den Hash-Wert des Dokumentes und verwendet dabei die geheimen und privaten Signaturkomponenten des authentifizierten Nutzers. Nachdem der Signaturprozess in der CoSign-Box stattgefunden hat, wird die Signatur zurück zum Nutzer übermittelt. Um zu verhindern, dass unberechtigte Nutzer Signaturen mit den Signaturkomponenten anderer

² Alle Aussagen dieses Rechtsgutachtens, die sich auf technische Eigenschaften von CoSign beziehen, sind auf Grundlage der Informationen getroffen, die AR auf der Website www.arx.com und im Benutzerhandbuch zu CoSign zur Verfügung gestellt hat. Technische Eigenschaften sind von WRA nicht überprüft worden.

Nutzer erzeugen, stellt CoSign einen exklusiven und verschlüsselten Zugang vom Computer des Nutzers zur CoSign-Box her.

2. RECHTLICHE ANERKENNUNG UND RECHTSWIRKUNGEN ELEKTRONISCHER SIGNATUREN

Ausgangspunkt für die rechtliche Anerkennung und die Rechtswirkungen elektronischer Signaturen ist das deutsche Signaturgesetz sowie die Signaturverordnung, die das Signaturgesetz konkretisiert. Sowohl das Signaturgesetz als auch die Signaturverordnung setzen die Europäische Signaturrechtlinie 1999/93/EG um. Ausweislich des Erwägungsgrundes Nr. 21 sowie Art. 5 Abs. 2 der Richtlinie ist es verboten, die Rechtswirksamkeit einer elektronischen Signatur nur aufgrund ihrer elektronischen Form zu leugnen. Diese Nichtdiskriminierungsregelung wurde in das System des deutschen Signaturrechts übernommen und hat zur Folge, dass alle Arten elektronischer Signaturen in Deutschland rechtliche Anerkennung finden.

Darüber hinaus kann die Nutzung elektronischer Signaturen gewisse Rechtsfolgen entfalten, wenn die Signaturen einen bestimmten und definierten Sicherheitsstandard erreichen. Die bedeutendsten Rechtsfolgen bei der Nutzung elektronischer Signaturen nach deutschem Recht sind der Ersatz der händischen Unterschrift durch eine elektronische Signatur sowie eine Beweiserleichterung im Zivilprozess. Allerdings hat nicht jede elektronische Signatur die genannten oder andere definierte Rechtsfolgen, auch wenn es verboten ist, einer Signatur allein aufgrund ihrer elektronischen Form die rechtliche Anerkennung zu verweigern. Rechtsfolgen nach deutschem Recht wie der Ersatz der händischen Unterschrift (§ 126a BGB) und die Beweiserleichterung (§ 292a ZPO) erfordern wenigstens „qualifizierte elektronische Signaturen“ nach dem Signaturgesetz. Unabhängig von der Sicherheitsstufe einer Signatur ist es jedoch wegen des Verbots der Diskriminierung elektronischer Signaturen immer zulässig, die Authentizität und Integrität eines elektronischen Dokumentes mit anderem Formen elektronischer Signaturen vor Gericht nachzuweisen.

Letztlich hängen die Rechtsfolgen der elektronischen Signatur immer auch von dem jeweiligen Kontext und dem Rechtsrahmen ab, in dem die elektronische Signatur verwendet wird. In gewissen Situationen erfordern Regelungen außerhalb des Signaturrechts bestimmte Sicherheitsstufen, so beispielsweise „fortgeschrittene elektronische Signaturen“ nach § 87a Abs. 6 AO oder „qualifizierte elektronische Signaturen“ nach § 14 Abs. 3 UStG.

3. WESENTLICHE ANFORDERUNGEN DES SIGNATURRECHTS

Die wesentlichen Anforderungen des deutschen Signaturrechts beurteilen sich vor allem nach zwei Rechtsgrundlagen, dem Signaturgesetz und der Signaturverordnung. Letztere spezifiziert bestimmte Regelungen des Signaturgesetzes und enthält weiterhin technische und organisatorische Anforderungen an Zertifizierungsdiensteanbieter sowie an die Hersteller von Produkten für die elektronische Signatur.

Insbesondere enthalten das Signaturgesetz und die Signaturverordnung Anforderungen an die definierten Sicherheitsstandards zur Erzeugung elektronischer Signaturen. Das deutsche Signaturrecht kennt drei verschiedene Signaturstufen. Ausgangspunkt ist die einfache „elektronische Signatur“, die in § 2 Nr. 1 SigG als Daten in elektronischer Form definiert ist, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Höhere Sicherheitsstufen sind „fortgeschrittene elektronische Signaturen“ und letztlich „qualifizierte elektronische Signaturen“,³ wobei jede dieser Sicherheitsstufen zusätzliche Anforderungen zu den vorhergehenden Sicherheitsstufen enthält.

Um fortgeschrittene elektronische Signaturen nach § 2 Nr. 2 SigG zu erzeugen, ist es zusätzlich erforderlich, dass die elektronische Signatur ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist (a), die Identifizierung des Signaturschlüssel-Inhabers ermöglicht (b), mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann (c), und die mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann (d).

Zur Erzeugung qualifizierter elektronischer Signaturen verlangt § 2 Nr. 3a SigG zusätzlich, dass die Signatur auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht. Nach § 2 Nr. 3b SigG ist weiterhin die Erzeugung der qualifizierten elektronischen Signatur mit einer „sicheren Signaturerstellungseinheit“ erforderlich. Eine solche sichere Signaturerstellungseinheit kann nach § 2 Nr. 10 SigG sowohl eine Software- oder auch eine Hardwareeinheit zur Speicherung und Anwendung des jeweiligen Signaturschlüssels sein.

Darüber hinaus sind Anforderungen an die sichere Signaturerstellungseinheit in § 17 Abs. 1 SigG und in § 15 Abs. 1 SigV normiert. Nach § 17 Abs. 1 SigG ist es erforderlich, dass die sichere Signaturerstellungseinheit gegen eine „unberechtigte Nutzung“ des Signaturschlüssels geschützt ist. Dieses Merkmal wird in § 15 Abs. 1 der SigV konkretisiert. Danach muss die sichere Signaturerstellungseinheit gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch „Besitz“ und „Wissen“ oder durch Besitz und ein oder mehreren biometrischen Merkmale angewendet werden kann.

Da die sichere Signaturerstellungseinheit in § 2 Nr. 10 SigG als „Software- oder Hardwareeinheit“ definiert wird, verlangt § 2 Nr. 10 SigG kein Konzept, dass ausschließlich eine Hardwarelösung beinhaltet, wie beispielsweise mittels Smartcards. Da die sichere Signaturerstellungseinheit auch eine Softwareeinheit sein kann, verbietet das Signaturgesetz nicht, qualifizierte elektronische Signaturen mittels Softwarelösungen oder kombinierten Software- und Hardwarelösungen zu erzeugen.

³ Darüber hinaus kann ein Zertifizierungsdiensteanbieter von der Regulierungsbehörde für Post und Telekommunikation nach Art. 15 SigG akkreditiert werden. Qualifizierte elektronische Signaturen, die ein Zertifikat eines solchen Zertifizierungsdiensteanbieters benutzen, haben spezielle rechtliche Wirkungen, sind aber noch immer „qualifizierte elektronische Signaturen“ und stellen keine weitere Signaturstufe dar.

4. ERZEUGUNG ELEKTRONISCHER SIGNATUREN MIT CO-SIGN

Nach Darstellung der Produktinformationen und der rechtlichen Anforderungen gemäß § 2 Nr. 1 bis Nr. 3 SigG ist festzuhalten, dass CoSign dafür ausgelegt ist, auch fortgeschrittene oder qualifizierte elektronische Signaturen zu erzeugen.

Elektronische Signaturen sind nach § 2 Nr.1 SigG Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. CoSign stellt eine logische Verknüpfung zwischen dem elektronischen Dokument und der dazugehörigen Signatur her, indem es einen einmaligen Hash-Wert zum Dokument bildet. Weiterhin erzeugt CoSign eine elektronische Signatur, die eine Authentifizierung des Nutzers ermöglicht, indem der Hash-Wert des Dokumentes mit dem privaten Schlüssel des Nutzers verschlüsselt wird und indem diese Signatur dem elektronischen Dokument beigefügt wird. Die so erzeugte Signatur kann nur mit dem öffentlichen Schlüssel des Nutzers entschlüsselt werden, der zu einem identifizierbaren Nutzer gehört. Folglich genügt CoSign den Anforderungen des § 2 Nr. 1 SigG.

Um fortgeschrittene elektronische Signaturen nach § 2 Nr. 2 SigG zu erzeugen, müssen zusätzliche Anforderungen erfüllt werden. Die wesentlichen Anforderungen sind, dass die elektronische Signatur ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist, die Identifizierung des Signaturschlüssel-Inhabers ermöglicht, mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und die mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Elektronische Signaturen, die mit CoSign erzeugt werden, sind ausschließlich dem Signaturschlüssel-Inhaber zugeordnet, da die privaten Schlüssel, die zur Verschlüsselung des Hash-Wertes eines Dokumentes benutzt werden, mit einem dem System bekannten CoSign-Nutzer verknüpft sind und da auch jeder Schlüssel eines Nutzers einmalig ist. Aus diesem Grund ermöglicht die Signatur eine Identifikation eines Nutzers. Ein CoSign-Nutzer hält die Mittel zur Signaturerzeugung unter seiner alleinigen Kontrolle, da er einen exklusiven und verschlüsselten Zugang zu seinem privaten Signaturschlüssel hat, der auf der sicheren CoSign-Box gespeichert ist und da er sich vor der Signaturerzeugung authentifizieren muss. Letztlich können elektronische Signaturen, die mit CoSign erzeugt wurden, nicht unbemerkt dupliziert oder verändert werden, da CoSign ein sicheren Hash-Algorithmus und einen sicheren RSA-Algorithmus zur Verschlüsselung des Dokumenten-Hash-Wertes benutzt. Aus diesem Grund ist CoSign dafür ausgelegt, die Anforderungen an die Erzeugung fortgeschrittener elektronischer Signaturen zu erfüllen.

Darüber hinaus kann CoSign zur Erzeugung qualifizierter elektronischer Signaturen nach § 2 Nr. 3 SigG benutzt werden, sofern zusätzlich ein zum Zeitpunkt der Signaturerzeugung gültiges qualifiziertes Zertifikat benutzt wird als auch eine sichere Signaturerstellungseinheit. Die sichere Signaturerstellungseinheit hat allgemein anerkannten Standards wie CWA 14169 der „Common Criteria“ zu entsprechen.

5. SIGNATURERZEUGUNG IM AUTOMATISIERTEN VERFAHREN DURCH COSIGN

Wo fortgeschrittene oder qualifizierte elektronische Signaturen per Gesetz oder aufgrund einer rechtlichen Vereinbarung erforderlich sind, ist es möglich, solche elektronischen Signaturen mit CoSign zu erzeugen. Die Erzeugung elektronischer Signaturen hat jedoch in vielen Fällen in einem automatisierten Massenverfahren zu erfolgen, um ökonomischen Anforderungen zu genügen. Für solche Massenverfahren können besondere Anforderungen bestehen.

5.1 AUTOMATISIERTE SIGNATURERZEUGUNG/ BATCH SIGNING

Nach dem deutschen Signaturrecht ist es grundsätzlich möglich, elektronische Signaturen in einem automatisierten Verfahren zu erzeugen. Nach dem Willen des Gesetzgebers sowohl zum Signaturgesetz 1997⁴ als auch zum Signaturgesetz 2001⁵ und auch nach der aktuellen Reform des Signaturrechts ist es möglich, elektronische Signaturen in Massenprozessen automatisiert zu erzeugen. Die Möglichkeit einer automatisierten Signaturerzeugung war dem Gesetzgeber von Anbeginn der Signaturrecht-Gesetzgebung bewusst. Ein praxisrelevanter Fall der automatisierten Erzeugung elektronischer Signaturen ist das so genannte „Batch Signing“.

Trotz der Relevanz automatisierter Signaturen für die Praxis enthält das deutsche Signaturrecht hierfür keine speziellen Regelungen. Die wesentlichen Anforderungen des deutschen Signaturrechts an sichere Signaturerstellungseinheiten sind in § 17 SigG und § 15 SigV, der § 17 SigG spezifiziert, normiert. Darüber hinaus enthält die Signaturverordnung lediglich allgemeine technische und organisatorische Anforderungen für die Hersteller von Produkten für elektronische Signaturen.

Derzeit bestehen auch keine Anzeichen dafür, dass eine weitere Reform des deutschen Signaturrechts zu neuen Regelungen zur automatisierten Signaturerzeugung führen wird. Nicht zuletzt deshalb werden einzelne, möglicherweise problematische Themen der automatisierten Signaturerzeugung gemäß dem deutschen Signaturrecht nach wie vor zwischen Wissenschaftlern und Juristen diskutiert.

5.2 EINZELFRAGEN – LÖSUNG DURCH COSIGN

Der folgende Abschnitt enthält eine Übersicht und eine Diskussion einiger möglicherweise problematischer Fragen bei der automatisierten Erzeugung qualifizierter Signaturen.

⁴ BT-Drs. 13/7385, 27 und BR-Drs. 966/96, 29.

⁵ Amtliche Begründung zu § 15 Abs.2 SigV, 28; siehe auch www.regtp.de, FAQ18; Das SigG 2005 hat keine Änderungen gebracht, s. BT-Drs. 15/3417 vom 24.6.2004.

- **AUTHENTIFIZIERUNG VOR SIGNATURERZEUGUNG**

Eine Frage, die seit der Evaluierung des Signaturgesetzes kontrovers diskutiert wird, ist, ob es erforderlich ist, sich vor jeder einzelnen Signaturerzeugung zu authentifizieren. Hierzu bestehen keinerlei Vorschriften im Signaturgesetz oder der Signaturverordnung. Ein wichtiges Indiz zur Beantwortung dieser Frage kann aber dem Willen des Gesetzgebers entnommen werden, wie er in der amtlichen Begründung zu § 15 SigV seinen Niederschlag gefunden hat.⁶ Der Gesetzgeber geht an dieser Stelle davon aus, dass sichere Signaturerstellungseinheiten so konstruiert sind, dass sie einem Nutzer regelmäßig die Möglichkeit zur Authentifizierung vor jeder einzelnen Signaturerzeugung geben oder aber zur einmaligen Authentifizierung vor der Erzeugung einer bestimmten Anzahl von Signaturen oder vor der Erzeugung von Signaturen in einem bestimmten Zeitraum. Nach dieser Begründung ist die Erzeugung von mehr als einer elektronischen Signatur nach der einmaligen Authentifizierung eines Nutzers rechtmäßig, sofern der automatisierte Prozess einen Schutz gegen Missbrauch gewährleistet. Da aber keine konkreten Vorschriften über die Anzahl von Signaturen nach einer einmaligen Authentifizierung oder über einen festen Zeitrahmen bestehen, müssen die Anforderungen in jedem Einzelfall gesondert festgestellt werden (Beispielsweise kann ein Unternehmen, das CoSign nutzt, entscheiden, dass "X" automatisiert erzeugte Signaturen vor einer nochmaligen Nutzer-Authentifizierung zulässig sind, ein anderes Unternehmen kann dagegen einen Zeitraum von "y" Minuten als zulässig definieren, bevor eine erneute Authentifizierung notwendig wird). Die Anforderungen jedes Einzelfalls hängen vom individuellen Kontext und dem jeweiligen Sicherheitsbedürfnis ab.

CoSign löst dieses Problem, indem es einem Unternehmen die Möglichkeit eröffnet, die Default-Einstellungen verbindlich zu ändern. Wird das Set-Up in CoSign so vorgenommen, dass ein Nutzer vor jeder einzelnen Signatur authentifiziert werden muss, erfüllt CoSign die Anforderung ohne weiteres. Alternativ dazu kann CoSign die rechtlichen Anforderungen erfüllen, indem das System so konfiguriert wird, dass Nutzersignaturen bis zu einem bestimmten Umfang oder innerhalb eines bestimmten Zeitrahmens nach einer einmaligen Authentifizierung erzeugt werden können und dabei der individuelle Kontext berücksichtigt wird.

- **SCHUTZ VOR UNBERECHTIGTER NUTZUNG**

Eine weitere kontrovers diskutierte Frage sind die Anforderungen an die sichere Signaturerstellungseinheit nach §§ 3 Nr. 10, 17 SigG und § 15 SigV. Danach müssen qualifizierte elektronische Signaturen mit sicheren Signaturerstellungseinheiten

⁶ Amtliche Begründung zu § 15 Abs. 2 SigV, 28; siehe auch www.regtp.de, FAQ18.

erzeugt werden. Die Signaturerstellungseinheit kann sowohl eine Soft- als auch eine Hardwareeinheit sein (§ 2 Nr. 10 SigG).

Eine Anforderung nach § 17 Abs. 1 SigG an die Signaturerstellungseinheit ist die Verhinderung der „unberechtigten Nutzung“ des privaten Signaturschlüssels eines Nutzers. Diese Anforderung ist in § 15 Abs. 1 SigV weiter spezifiziert. Nach § 15 Abs. 1 SigV darf der private Signaturschlüssel nur benutzt werden nachdem sich der Nutzer durch „Besitz“ und „Wissen“ oder durch Besitz und ein oder mehrere biometrische Merkmale identifiziert hat. Die Tatbestandsmerkmale Besitz und Wissen konkretisieren somit das Kriterium des Schutzes gegen eine unberechtigte Nutzung. Im Rahmen der Auslegung der Tatbestandsmerkmale Besitz und Wissen ist die Diskussion aufgekommen, ob mit dem Besitz der tatsächliche physikalische Besitz – im Sinne des unmittelbaren Besitzes nach dem Zivilrecht – beispielsweise eines Hardware-Tokens wie einer Chipkarte gemeint ist, oder ob der "logische" Besitz des Signaturschlüssels ausreicht. Weder die amtliche Begründung des Gesetzgebers zu § 17 SigG noch die Begründung zu § 15 SigV geben weitere Auskunft über die Bedeutung des Terminus „Besitzes“. Die Begründung zu § 15 SigV stellt lediglich klar, dass Besitz und Wissen das Merkmal des Schutzes gegen unberechtigte Nutzung spezifizieren.

Aufgrund anderer Anforderungen des § 17 SigG, die in der Vergangenheit regelmäßig nur durch Hardware-Token wie Chipkarten erfüllt wurden (beispielsweise das Erfordernis strengen Schutzes gegen die Möglichkeit, einen Schlüssel von der sicheren Signaturerstellungseinheit zu kopieren), führte die Diskussion über das Merkmal der „unberechtigten Nutzung“ zu einer Interpretation des Besitzes als tatsächlichem Besitz. Für eine solche Interpretation bestehen jedoch keine Anhaltspunkte in der Gesetzesbegründung. Demgegenüber bestehen gewichtige Argumente für eine Interpretation des Merkmals Besitz als einem logischen Besitz, wengleich diese Frage noch immer ungeklärt ist. Nach dem hier dargelegten Standpunkt ist klar, dass das Merkmal Besitz neben anderen Merkmalen vor allem das Merkmal des Schutzes gegen eine unberechtigte Nutzung zu einem Zeitpunkt spezifizieren sollte, zu dem der Gesetzgeber nur an Chipkarten als sichere Signaturerstellungseinheiten dachte, da nur Chipkarten einen sicheren Schutz gegen das Kopieren eines privaten Schlüssels gaben. Trotzdem zeigt der Wille des Gesetzgebers ganz deutlich und von Beginn an, dass eine rechtmäßige Möglichkeit der automatisierten Signaturerzeugung besteht.⁷ Aus der amtlichen Begründung, die von „Massenverfahren“ spricht, wie beispielsweise der elektronischen Rechnungsstellung, kann deutlich abgeleitet werden, dass der private Schlüssel in solch einem Massenverfahren nicht in dem alleinigen tatsächlichen Besitz eines einzelnen Nutzers stehen kann. Üblicherweise wird der private Schlüssel in einem Massenverfahren beim Signaturvorgang außerhalb der Reichweite eines einzelnen

⁷ BT-Drs. 13/7385, 27 und BR-Drs. 966/96, 29; § 15 Abs. 2 SigV (amtliche Begründung).

Nutzers, der den Schlüssel besitzt, stehen, beispielsweise in einem speziell gesicherten Raum oder möglicherweise in einem komplett anderen Gebäude. In diesem Fall kann der Schutz gegen eine unberechtigte Nutzung nicht durch den tatsächlichen physikalischen Besitz des Signaturschlüssels garantiert werden, sondern durch einen sicheren Zugriff auf den Schlüssel und eine sichere Speicherung.

Grundsätzlich dürfen ein sicherer Zugriff und eine sichere Speicherung auch durch eine Softwarelösung oder eine kombinierte Soft- und Hardwarelösung wie CoSign umgesetzt werden. Die Möglichkeit zur Erzeugung qualifizierter Signaturen mittels einer sicheren Signaturerstellungseinheit, die eine Softwareeinheit ist, ist ausdrücklich in § 2 Nr. 10 SigG genannt. Ähnliche Schlussfolgerungen zur Zulässigkeit der Verwendung von anderen als Hardwarelösungen können der jüngsten wissenschaftlichen Diskussion⁸ wie auch einer Stellungnahme der zuständigen Behörde in Österreich⁹ entnommen werden. Dabei ist zu betonen, dass Österreich ein Mitgliedsstaat der Europäischen Union ist, der die Europäische Signaturrichtlinie zum Merkmal der "alleinigen Kontrolle" für fortgeschrittene elektronische Signaturen umsetzen musste. Die zuständige Behörde in Österreich erklärt ausdrücklich, dass das Merkmal der alleinigen Kontrolle, das bei fortgeschrittenen elektronischen Signaturen gegen eine unberechtigte Nutzung schützen soll, ohne den Besitz einer speziellen Hardware erfüllt werden kann. Dafür müssten jedoch weitere Sicherheitsmaßnahmen ergriffen werden. Elektronische Daten müssten verschlüsselt und der Zugriff auf diese Daten müsste sicher gestaltet werden, um dem Signierenden die alleinige Kontrolle zu geben.

CoSign löst die Frage des Schutzes vor einer unberechtigten Nutzung nach eben diesem Prinzip. Indem einem Nutzer ein exklusiver Zugriff auf die CoSign-Box gegeben wird und indem die privaten Schlüssel in der CoSign-Box mit einem so genannten SVMK-Schlüssel verschlüsselt werden, bestehen weitreichende Sicherheitsmaßnahmen. Der SVMK-Schlüssel ist in einer manipulationsresistenten Hardwareeinheit gespeichert. Sobald die CoSign-Box geöffnet wird, wird dies von der Hardwareeinheit entdeckt und der SVMK-Schlüssel wird zerstört, wodurch alle verschlüsselten privaten Schlüssel, die in der CoSign-Box gespeichert sind, unbrauchbar werden, da sie weder gelesen noch entschlüsselt werden können.

- **REFORM DES DEUTSCHEN SIGNATURRECHTS**

Letztlich ist die Frage der Reform des Deutschen Signaturrechts von Bedeutung. Da es ein praktisches Bedürfnis nach klaren Vorschriften zur automatisierten Erzeugung von Signaturen gibt, wurde vom Gesetzgeber erwartet, bestimmte Regelungen zur

⁸ Roßnagel/Fischer-Dieskau, MMR 2004, 133 ff.

⁹ www.signatur.rtr.at.

automatisierten Signaturerstellung zu verabschieden. Tatsächlich ist dies nicht geschehen. Das neue Signaturgesetz 2005¹⁰ stellt vor allem gesetzliche Auslegungsschwierigkeiten klar und erleichtert organisatorische Maßnahmen bei der Ausgabe von Zertifikaten. Trotz allem enthält es weder systematische Neuerungen noch spezielle Vorschriften zur automatisierten Signaturerstellung.

¹⁰ Gesetz v. 4.1.2005, BGBl. I, 2.

6. ZUSAMMENFASSUNG

- Obwohl in der Vergangenheit nur Chipkarten als sichere Signaturerstellungseinheiten angesehen wurden, da diese einen ausreichenden Schutz gegen das Kopieren eines Schlüssels von der Signaturerstellungseinheit gewährleisten, ist es rechtmäßig, speziell geschützte Software- oder kombinierte Soft- und Hardwareeinheiten als sichere Signaturerstellungseinheit zu benutzen (§ 2 Nr. 10 SigG).
- Elektronische Signaturen, die auf diesem Weg erzeugt werden, sind rechtlich anerkannt und können bestimmte, definierte Rechtsfolgen entfalten. Diese Rechtsfolgen sind in der Regel außerhalb des Signaturrechts normiert.
- Es ist nach deutschem Recht zulässig, fortgeschrittene und qualifizierte elektronische Signaturen in einem automatisierten Massenverfahren (auch Batch Signing) zu erzeugen.
- Die Autoren kommen zu dem Ergebnis, dass ein Konzept wie CoSign, das Soft- und Hardwareeinheiten kombiniert, um Signaturschlüssel zu speichern, grundsätzlich geeignet ist, eine sichere Signaturerstellungseinheit darzustellen. Die sichere Signaturerstellungseinheit ist dann durch organisatorische und technische Mittel zu schützen und muss allgemein anerkannten Standards für sichere Signaturerstellungseinheiten entsprechen, wie CWA 14169 der „Common Criteria“.
- Um die erforderliche Nutzerauthentifizierung vor dem Signaturvorgang zu gewährleisten, kann CoSign in der beschriebenen Weise konfiguriert werden. Es ist möglich, CoSign so zu konfigurieren, dass eine Authentifizierung des Nutzers für jeden einzelnen Signaturvorgang erforderlich ist. In diesem Fall ist die Anforderung an eine Nutzerauthentifizierung vor dem Signaturvorgang auf jeden Fall erfüllt. Alternativ dazu kann CoSign so konfiguriert werden, dass ein Nutzer vor der Erzeugung einer bestimmten Anzahl von Signaturen oder vor der Erzeugung von Signaturen innerhalb eines bestimmten Zeitrahmens authentifiziert und dabei der konkrete Einzelfall berücksichtigt wird. In diesem Fall erfüllt CoSign ebenso diese Anforderung des Deutschen Signaturrechts.
- Die Autoren kommen zu dem Ergebnis, dass CoSign so konfiguriert werden kann, dass der Nutzer gegen eine unberechtigte Nutzung des Signaturschlüssels geschützt wird, indem ein sicherer, exklusiver Zugriff auf die CoSign-Box gewährleistet wird und indem der Zugriff auf die Box, die Signaturkomponenten und die privaten Schlüssel selbst verschlüsselt und zusätzlich mit der SVMK-Hardware-Einheit gesichert werden.
- Um qualifizierte elektronische Signaturen mit CoSign zu erzeugen, ist es neben den genannten Anforderungen erforderlich, gültige, qualifizierte Zertifikate zu verwenden. Nach Angaben von Algorithmic Research unterstützt CoSign die Integration qualifizierter Zertifikate.

AUTOREN

Dieses Gutachten wurde durch Roland Steidle, Rechtsanwalt bei Waldeck Rechtsanwälte Partnerschaftsgesellschaft und von Thomas H. Fischer, M.B.L. – HSG, Rechtsanwalt und Partner der Kanzlei erstellt. Roland Steidle ist im IT- und Multimediarecht spezialisiert. Bis zum Jahre 2003 war er wissenschaftlicher Angestellter am Lehrstuhl von Prof. H. Roßnagel für Öffentliches Recht, insbesondere Technikrecht an der Universität Kassel und Mitglied der dort ansässigen Projektgruppe „Provet“, die das Deutsche Signaturgesetz 1997 mit entworfen und an der Umsetzung der Europäischen Signaturrechtlinie mitgewirkt hat. Thomas H. Fischer, M.B.L.-HSG ist ein versierter und langjähriger Experte in internationalen Outsourcing-Projekten. Sein Focus liegt ebenso auf Rechtsfragen der Kryptographie und elektronischer Signaturen.

Weitere Informationen zu den Autoren finden Sie unter www.waldeck-rechtsanwaelte.com.