



Erstellung, Sicherheit und Personen-Identifikation bei zertifikatsbasierten Signaturen

Die Signaturzertifikate werden von webSignatureOffice(.com) für den jeweiligen Benutzer automatisiert erstellt und verschlüsselt gespeichert. Hierzu kommen allgemein als sicher anerkannte kryptographische Verschlüsselungsalgorithmen zum Einsatz, welche das Nutzerpasswort als Schlüssel verwenden, welches seinerseits nicht auf den Servern gespeichert wird. Somit kann das Zertifikat nur durch Eingabe des richtigen Passworts durch den Zertifikatsinhaber zur Signaturerstellung verwendet werden. Diese Anwendung findet ebenfalls auf den Servern von webSignatureOffice(.com) statt, so dass der private Schlüssel diese niemals unverschlüsselt verlässt. Geht man davon aus, dass es dem einzelnen Unterzeichner nicht möglich sein dürfte die Serverinfrastruktur von webSignatureOffice(.com) zu hacken und zudem noch die sicher verschlüsselt gespeicherten Zertifikate zu entschlüsseln, so hängt die Sicherheit / Vertrauenswürdigkeit der jeweiligen zertifikats-basierten Signatur hauptsächlich von zwei Faktoren ab. Zum einem am sicheren Umgang des Unterzeichners mit seinem Passwort und zum anderen an der Stärke des Identifikationsmerkmals welches bei der Erstellung des Zertifikates zu Grunde gelegen hat. So stellt die Identifikation einer Person durch versenden einer Aktivierungs-E-Mail an deren elektronisches Postfach lediglich einen Bezug zwischen dem Zertifikat und dem Postfach her. In wie weit dieses Postfach eindeutig einer Person zuzuordnen ist oder nicht hängt von vielerlei Faktoren ab, als Beispiel sei der Unterschied zwischen einem kostenlosen Wegwerf-E-Mail-Konto, einer DE-Mail oder ePostBrief E-Mail Adresse aufgeführt. webSignatureOffice(.com) bietet daher mehrere Identifikationsmöglichkeiten an, welche neben E-Mail-Adressen beispielsweise auch Mobilfunknummern oder externe Identifikationsverfahren mit einbeziehen. Dementsprechend vergibt webSignatureOffice den Signaturzertifikaten verschieden hohe Bewertungen und ermöglicht es dem Initiator von Signaturabläufen selbst zu bestimmen welchen Sicherheitsgrad, sowie Vertrauensgrad er als Mindestanforderung für die jeweilige Signatur festlegen möchte. Diese Form der Signatur entspricht in der EU der fortgeschrittenen elektronischen Signatur.



Weitere Informationen zum Produkt:

www.webSignatureOffice.com

Produktseite webSignatureOffice

Sicherheit und Personen-Identifikation bei der Verwendung einer handschriftlichen Unterschrift

Bei Verwendung einer handschriftlichen Unterschrift welche mit Hilfe eines Signaturerfassungsgerätes aufgenommen wurde erfolgt die Zuordnung der Signatur zur Person analog zur Unterschrift auf einem Blatt Papier durch einen im Streitfall von einem Schriftsachverständigen durchgeführten Unterschriftenvergleich. Maßgeblich für die Sicherheit einer solchen Signatur ist neben der Erfassungsqualität des Unterschriftenpads vor allem die sichere Verknüpfung der biometrischen Daten der Unterschrift mit dem Dokument und deren möglichst unüberwindbare Verschlüsselung. Bei der Verwendung aktueller StepOver Signaturpads aus der naturaSign Pad Serie werden die biometrischen Daten der Unterschrift bereits im Unterschriftenpad sicher verschlüsselt und dabei im Pad so mit dem Dokument verknüpft, dass sie nicht missbräuchlich unter ein anderes Dokument gesetzt werden können. Hierbei kommt u.a. ein im Speicher des Prozessors abgelegter öffentlicher RSA-Schlüssel (2048 Bit) zum Einsatz, so dass die biometrischen Daten nicht ohne Zugriff auf den zugehörigen privaten RSA-Schlüssel entschlüsselt werden können. Dieser ist jedoch sicher bei einem Notar hinterlegt, welcher auch selbst das Schlüsselpaar erzeugt hat. Erst diese Vorgehensweise ermöglicht es im Zweifelsfall darzulegen, dass es nicht möglich war die biometrischen Daten zu entschlüsseln um diese missbräuchlich zur Unterzeichnung anderer oder geänderter Dokumente zu verwenden.

Zusätzlich wird jede Unterschrift seitens des Signaturpads nochmals mit einer digitalen Signatur versehen, so dass jeder Empfänger die Unversehrtheit des Dokumentes prüfen kann z.B. mit Hilfe des Adobe Reader. Das Pad-eigene Zertifikat zur digitalen Signatur ist pro StepOver Signaturpad einmalig und mit dessen Seriennummer verknüpft, so wird auch ein Rückschluss auf das zur Unterzeichnung verwendete Pad ermöglicht. Auch diese Form der Signatur entspricht in oben

genannter Ausführung einer Fortgeschrittene e-Signatur nach EU-Recht. Besonders vorteilhaft ist diese Form der Signatur auch dann, wenn nicht zu registrierende Unterzeichner in einen Signaturprozess eingebunden werden sollen (z.B. Laufkundschaft in einem Laden) oder andere zuvor nicht näher bekannte Personen.



Weitere Informationen:

www.webSignatureOffice.com

Produktseite webSignatureOffice

StepOver Signaturpads