

Wendelin Bieser
Heinrich Kersten

Chipkarte statt Füllfederhalter

**Daten beweissicher
„elektronisch unterschreiben“
und zuverlässig schützen**

Inhalt

1 Von der eigenhändigen zur digitalen Signatur	1
Vom Papier zu elektronischen Datenträgern	1
Die digitale Signatur („elektronische Unterschrift“)	1
Die Ressource „Information“	2
2 Gefahren der Datenmanipulation und des Datendiebstahls	3
Veränderbarkeit elektronischer Daten	3
Computer am Netz bilden ein „offenes Tor“ zu Ihren Daten	4
Abhörmöglichkeiten in öffentlichen Netzen	6
Wirtschafts- und Konkurrenzspionage	7
Information Warfare	12
Manipulation beim elektronischen Zahlungsverkehr	13
Manipulation beim Erzeugen digitaler Signaturen	14
Vielzahl von Angriffsmethoden und Angriffen	14
Schäden durch Angriffe	16
3 Wie Sie Ihre Daten wirksam schützen können	17
Anwendung gesetzlich anerkannter digitaler Signaturen	17
Anwendung weiterer Sicherheitsfunktionen	18
Die Sicherheit zahlt sich aus	18
4 Die gesetzlich anerkannte digitale Signatur	20
Nachweis des Urhebers und der Unverfälschtheit von Daten	20
Wie funktioniert eine digitale Signatur?	20
Gesetzliche Anforderungen	24
Hohe Sicherheit	28
Hoher Beweiswert vor Gericht	32
Zurechnung digitaler Signaturen	33
Vergleich zum papiergebundenen Schriftdokument	34

5 Wann sind digitale Signaturen erforderlich?	36
Übermittlung und Speicherung beweiserheblicher Daten	36
Alternative zur gesetzlichen Schriftform	37
Erschließung eines hohen Rationalisierungspotentials	37
6 Typische Anwendungsfelder für digitale Signaturen	38
Geschäfts- und Behördenverkehr	38
Online-Dienste und Teleshopping	39
Zahlungsverkehr	40
Datendokumentation	42
Entwicklungs- und Produktionsdaten	43
Software	43
Urhebernachweis	45
Gesundheitswesen	45
Datenschutz	46
7 Internationale Anwendung digitaler Signaturen	47
Wie können digitale Signaturen international angewendet werden?	47
Welchen Beweiswert haben digitale Signaturen aus und in anderen Staaten?	48
8 Wie erzeugen und prüfen Sie eine digitale Signatur und worauf sollten Sie zu Ihrer eigenen Sicherheit achten?	49
Wie erhalten Sie Signaturschlüssel und Signaturschlüssel-Zertifikate?	49
Wie können Sie Vertretungsrechte für Dritte oder berufsrechtliche Zulassungen in ein Zertifikat aufnehmen?	53
Wie schützen Sie Ihren privaten Signaturschlüssel vor Mißbrauch?	56
Wann und wie sind Zertifikate zu sperren?	56

Welche technischen Komponenten benötigen Sie für digitale Signaturen?	57
Wie erzeugen Sie eine digitale Signatur?	60
Wie prüfen Sie eine digitale Signatur?	60
Wie überprüfen Sie die Gültigkeit von Zertifikaten?	61
Wann ist ein Zeitstempel erforderlich?	65
Wie können Unternehmen und Behörden digitale Signaturen nutzen?	66
Was ist bei automatischem Erzeugen digitaler Signaturen zu beachten?	67
Wann sind erneute digitale Signaturen erforderlich?	68
9 Wichtige weitere Sicherheitsfunktionen	69
„Digitaler Ausweis“ für die Kommunikationsnetze	69
Zugriffskontrolle und Protokollierung	71
Verschlüsselung	72
10 Geprüfte Sicherheit „Made in Germany“	79
Sicherheitsgeprüfte Produkte	79
Prüfungen bei Manipulationsverdacht und zur Prävention	80
11 Zusammenfassung	82
12 Ausblick	85
Anhang:	
1 Signaturgesetz	87
2 Signaturverordnung	96
3 Unterrichtung nach § 6 Signaturgesetz (Muster)	107
4 Adressen	109
Autoren	116