

Public Key Infrastructure

Eignung von PKI zur Erfüllung zivilrechtlicher Anforderungen
aus Gesetz und Vertrag innerhalb einer Unternehmung
(B2B, B2C und B2E)

DISSERTATION

der Rechtswissenschaftlichen Fakultät
der Universität Zürich
zur Erlangung der Würde eines Doktors
der Rechtswissenschaft

vorgelegt von

Daniel Markwalder
von
Würenlos AG

Genehmigt auf Antrag von
Prof. Dr. iur. Rolf H. Weber

Inhaltsübersicht

Literaturverzeichnis	XXIII
Erster Teil: Einleitung und Grundlagen	1
§ 1 Einleitung	1
§ 2 Technische und organisatorische Aspekte	7
§ 3 Überblick der gesetzlichen Grundlagen	41
Zweiter Teil: Aktuelle Rechtsfragen	67
§ 4 Form	67
§ 5 Vertretung	105
§ 6 Haftung	139
§ 7 Beweis	181
§ 8 Geheimnisschutz	225
Dritter Teil: Ergebnisse	265
§ 9 Zusammenfassung	265

Inhaltsverzeichnis

Abkürzungsverzeichnis	XIX
Literaturverzeichnis	XXIII
Zitierte Standards	XXXV
Materialien- und Gesetzesverzeichnis	XXXVII
Erster Teil: Einleitung und Grundlagen	1
§ 1 Einleitung	1
I. Ausgangslage	1
A. Funktion und Begriff der Public Key Infrastructure	1
B. Umfeld der Public Key Infrastructure	2
II. Thematik der Arbeit	3
A. Ziel und Abgrenzung	3
B. Gliederung	4
§ 2 Technische und organisatorische Aspekte	7
I. Vorbemerkungen	7
II. Technische Aspekte	7
A. Sicherheitsbedürfnisse	7
1. Einführung in die Problematik	7
2. Integrität	8
3. Authentizität	9
4. Vertraulichkeit	11
5. Nichtabstreitbarkeit	12
6. Exkurs: Verfügbarkeit	13
B. Kryptografie	13
1. Grundprinzipien und Begriffe	13
2. Symmetrische Verschlüsselung	15
3. Asymmetrische Verschlüsselung	15
4. Hybride Verfahren	16
5. Hashverfahren	17
6. Digitale Signatur	17

	7. Authentifikation	
	8. Zeitstempel	
	9. Kryptografische Sicherheit	
	10. Zwischenergebnis Kryptografie	
C.	Public Key Infrastructure	
	1. Vertrauensmodell	
	2. Zertifikat	
	a) Definition	
	b) Zertifikatsinhalt	
	c) Status	
	3. Certification Authority	
	4. Validierung	
	a) Ausgangslage	
	b) Verifikation zum Verifikationszeitpunkt (Schalenmodell)	
	c) Verifikation zum Signierzeitpunkt (Kettenmodell)	
	d) Kombination: Modifiziertes Schalenmodell	
	e) Exkurs: Verifikationsmodell in der Signaturgesetzgebung	
	5. PKI-Anwendungsgebiete	
	a) Einleitung	
	b) Signierung von anzuzeigenden Inhalten	
	c) Signierung von ausführbaren Inhalten	
	d) Datenverschlüsselung	
	e) Kommunikationsverschlüsselung	
	f) Authentifikation	
III.	Organisatorische Aspekte	
	A. Einleitung	
	B. Zertifikatsausstellung (Zertifizierung)	
	1. Schlüsselgenerierung und -übergabe	
	2. Registrierung	
	3. Signierung des Zertifizierungsantrags	
	C. Zertifikatsverwendung	
	1. Validierung	
	2. Auswertung spezifischer Zertifikatsinhalte	
	3. Aufbewahrung und Verwendung der Geheimschlüssel	
	4. Zertifikatssperrung	
IV.	Zusammenfassung	
	A. Allgemeine Bemerkungen	
	B. Erstellung von Geheimschlüssel und Zertifikat	
	C. Verwendung von Geheimschlüssel und Zertifikat	
§ 3	Überblick der gesetzlichen Grundlagen	
I.	Vorbemerkungen	
	A. Digitale Signatur	
	1. Gesetzliche Regelung	

2. Gesetzlich geforderte Verwendung	42
B. Verschlüsselung	42
1. Gesetzliche Regelung	42
2. Gesetzlich geforderte Verwendung	43
C. Authentifikation	44
1. Gesetzliche Regelung	44
2. Gesetzlich geforderte Verwendung	45
D. Zwischenergebnis	45
II. PKI-relevante Rechtsgrundlagen	46
A. ZertES, VZertES und TAV	46
1. Motivation und Ziel der Regelung	46
2. Kernpunkte der Regelung	47
a) Signaturklassen	47
aa) Elektronische Signatur	47
bb) Fortgeschrittene elektronische Signatur	47
cc) Qualifizierte elektronische Signatur	50
dd) Qualifizierte elektronische Signatur beruhend auf einem qualifizierten Zertifikat einer anerkannten Anbieterin	52
b) Anerkennungsvoraussetzungen	52
c) Erstellung und Inhalt von qualifizierten Zertifikaten	53
d) Pflichten anerkannter Anbieterinnen von Zertifizie- rungsdiensten	53
e) Haftung von Anbieterinnen von qualifizierten Zertifizie- rungsdiensten	54
B. OR-Novelle	55
1. Motivation und Ziel der Regelung	55
2. Kernpunkte der Regelung	55
a) Surrogat der Handunterschrift	55
b) Haftung des Schlüsselhalters	56
C. ELDI-V	57
1. Motivation und Ziel der Regelung	57
2. Kernpunkte der Regelung	58
D. GeBüV	61
1. Motivation und Ziel der Regelung	61
2. Kernpunkte der Regelung	62
3. Exkurs: Harmonisierung zwischen GeBüV und ELDI-V	63
III. Zusammenfassung	65
A. System der Signatur- und Zertifikatsklassen	65
B. Gesetzlich vorgesehene Rechtswirkungen	66

Zweiter Teil: Aktuelle Rechtsfragen

	67
§ 4 Form	67
I. Ausgangslage und Fragestellung	67
II. Rechtliche Anforderungen	68
A. Gesetzliche Formvorschriften	68
1. Funktion	68
2. Wirkungen	69
3. Arten	70
a) Einfache Schriftlichkeit	70
b) Exkurs: Textform	71
c) Qualifizierte Schriftlichkeit	72
d) Öffentliche und qualifizierte öffentliche Beurkundung	73
e) Sonderformen	74
B. Gewillkürte Formvorschriften	74
1. Funktion	74
2. Wirkungen	74
3. Arten	75
C. Formvorschriften im weiteren Sinne	76
1. Funktion	76
2. Wirkungen	77
3. Arten	77
III. Beurteilung Public Key Infrastructure	77
A. Allgemeines	77
1. Digitale Signatur	77
a) Qualifizierte elektronische Unterschrift	77
aa) Anforderungen an das Zertifikat	77
bb) Anforderungen an die Signaturerstellung	79
cc) Anforderungen an die Signaturprüfung	80
dd) Aspekte der Willenserklärung	82
b) Fortgeschrittene elektronische Unterschrift	85
aa) Anforderungen an das Zertifikat	85
bb) Anforderungen an die Signaturerstellung	85
cc) Anforderungen an die Signaturprüfung	86
dd) Aspekte der Willenserklärung	86
c) Einfache elektronische Unterschrift	87
d) ELDI-V konforme elektronische Unterschrift	87
aa) Anforderungen an das Zertifikat	87
bb) Anforderungen an die Signaturerstellung	88
cc) Anforderungen an die Signaturprüfung	88
dd) Aspekte der Willenserklärung	88
e) GeBüV konforme elektronische Unterschrift	89
aa) Anforderungen an das Zertifikat	89
bb) Anforderungen an die Erstellung des Hashwertes	90

	cc) Anforderungen an die Signaturprüfung	90
	dd) Aspekte der Willenserklärung	90
	2. Verschlüsselung	90
	3. Authentifikation	92
B.	PKI-Applikationen	93
	1. Signierung von anzuzeigenden Inhalten	93
	a) Fallbeispiel PDF-Signaturen	93
	aa) Einfache Schriftlichkeit	93
	bb) Gewillkürte Formen	94
	cc) ELDI-V konforme Signaturen	94
	dd) GeBüV konforme Signaturen	95
	b) Fallbeispiel S/MIME	96
	aa) Einfache Schriftlichkeit	96
	bb) Gewillkürte Formen	97
	cc) ELDI-V konforme Signaturen	98
	dd) GeBüV konforme Signaturen	98
	2. Signierung von ausführbaren Inhalten	99
	3. Authentifikation	100
	4. Datenverschlüsselung	100
	5. Kommunikationsverschlüsselung	101
IV.	Ergebnis	101
	A. Formvorschriften im engeren Sinne	101
	B. Formvorschriften im weiteren Sinne	102
	C. Gewillkürte Formvorschriften	102
	D. Übersicht PKI-Anwendungsgebiete	103
§ 5	Vertretung	105
	I. Ausgangslage und Fragestellung	105
	II. Rechtliche Anforderungen	106
	A. Wesen und Wirkungen der Stellvertretung	106
	B. Voraussetzungen der Stellvertretung	107
	1. Handeln in fremdem Namen	107
	2. Exkurs: Handeln unter fremdem Namen	108
	3. Vertretungsmacht	109
	C. Vertretung ohne Vertretungsmacht	110
	1. Grundsatz	110
	2. Ausnahmen	110
	a) Fiktion von Artikel 37 OR	110
	b) Gutgläubensschutz	110
	aa) Vorbemerkung	110
	bb) Rechtsscheinvollmacht	111
	cc) Duldungsvollmacht	111
	dd) Anscheinsvollmacht	112
	D. Gesetzliche Regelung der Attribute und Attributzertifikate	112

III. Beurteilung Public Key Infrastructure	11
A. Vertretungsszenarien bei den PKI-Anwendungen	11
1. Signierung	11
2. Entschlüsselung	11
3. Authentisierung	11
B. Anzeige der Vertretungsmacht: Attribute und Attributzertifikate	11
1. Gegenstand des Attributs und des Attributzertifikats	11
2. Kundgabe des Vertreters als Handeln in fremdem Namen	11
a) Vorbemerkung	11
b) Signierung von anzuzeigenden Inhalten	11
aa) Fallbeispiel PDF-Signierung	11
bb) Fallbeispiel S/MIME-Signierung	11
c) Signierung von ausführbaren Inhalten	11
d) Kommunikationsverschlüsselung	12
aa) Fallbeispiel S/MIME-Verschlüsselung	12
bb) Fallbeispiel HTTPS	12
e) Datenverschlüsselung	12
f) Authentifikation	12
g) Zwischenergebnis	12
3. Kundgabe des Vertretenen als Grundlage für eine externe Vollmacht	12
a) Vorbemerkung	12
b) Qualifizierte Zertifikate	12
c) Fortgeschrittene und einfache Zertifikate	12
d) Zwischenergebnis	12
C. Weitergabe des Signierschlüssels	12
1. Vorbemerkung	12
2. Handeln in fremdem Namen	12
3. Vollmacht	12
4. Externe Vollmacht	12
a) Exkurs: Verhältnis zu Artikel 59a OR	12
b) Rechtsscheinvollmacht	12
c) Duldungsvollmacht	12
d) Anscheinsvollmacht	13
e) Zwischenergebnis	13
5. Relevanz der Zertifikatsklasse	13
a) Qualifizierte Zertifikate einer anerkannten Anbieterin	13
b) Qualifizierte Zertifikate einer nicht anerkannten Anbieterin	13
c) Fortgeschrittene Zertifikate	13
D. Weitergabe des Entschlüsselungsschlüssels	13
E. Weitergabe des Authentisierschlüssels	13
F. Falschzertifizierung	13
IV. Ergebnis	13

A.	In Attributen beschriebene Vertretungsmacht	135
B.	Diskrepanz zwischen Schlüsselhalterin und zertifizierter Person	136
C.	Übersicht	138
§ 6	Haftung	139
I.	Ausgangslage und Fragestellung	139
II.	Rechtliche Anforderungen	140
A.	Vorbemerkungen	140
B.	Haftung der CA	142
1.	Artikel 16 ZertES	142
a)	Haftungssubjekt	142
b)	Haftungsvoraussetzungen	143
aa)	Schaden	143
bb)	Widerrechtlichkeit	144
cc)	Kausalität	146
dd)	Kein Verschulden nötig – milde Kausalhaftung	146
ee)	Weitere Voraussetzungen	147
c)	Rechtsfolgen	147
2.	Vertrag	147
a)	Verhältnis der CA zum Zertifikatsinhaber	147
b)	Verhältnis der CA zum Zertifikatsauswerter	148
3.	Sonstige Anspruchsnormen	148
a)	Verhältnis der CA zum Zertifikatsinhaber	148
b)	Verhältnis der CA zum Zertifikatsauswerter	149
4.	Exkurs: Bedeutung von CP und CPS für die Haftung der CA	150
5.	Zwischenergebnis Haftung der CA	151
C.	Haftung des Schlüsselinhabers	151
1.	Artikel 59a OR	151
a)	Haftungssubjekt	151
b)	Haftungsvoraussetzungen	152
aa)	Schaden	152
bb)	Widerrechtlichkeit	152
cc)	Kausalität	153
dd)	Verschulden	153
ee)	Weitere Voraussetzungen	154
c)	Rechtsfolge	154
2.	Vertrag	155
a)	Verhältnis des Schlüsselhalters zur CA	155
b)	Verhältnis des Schlüsselhalters zum Zertifikatsauswerter	155
3.	Sonstige Anspruchsnormen	156
4.	Zwischenergebnis Haftung des Schlüsselhalters	157
D.	Haftungsbeschränkungen im Zertifikat	158
1.	Ausgangslage	158
2.	Wirkungen	159

	a) Qualifizierte Zertifikate	
	b) Fortgeschrittene und einfache Zertifikate	
	3. Inhalt	
	4. Zwischenergebnis	
	E. Zusammenfassung rechtliche Grundlagen	
III.	Beurteilung Public Key Infrastructure	
	A. Allgemeine Schadensrisiken der PKI-Anwendungen	
	1. Signierung von anzuzeigenden Inhalten	
	2. Datenverschlüsselung	
	3. Signierung von ausführbaren Inhalten	
	4. Kommunikationsverschlüsselung	
	a) Fallbeispiel S/MIME	
	b) Fallbeispiel HTTPS	
	5. Authentifikation	
	6. Zwischenergebnis Schadensrisiken der PKI-Anwendungen	
	B. Sorgfaltspflichten bei der Zertifikatserstellung	
	1. Generierung des Schlüsselpaares	
	2. Antragserstellung, -übermittlung und -überprüfung	
	3. Signierung des Requests	
	4. Dokumentation und Information	
	5. Zeitstempel	
	C. Sorgfaltspflichten im Umgang mit dem Geheimschlüssel	
	1. Speicherung und Aktivierung des Geheimschlüssels	
	2. Bestimmungsgemäße Verwendung des Geheimschlüssels	
	D. Sorgfaltspflichten bei der Zertifikatsverwendung	
	1. Publikation der Zertifikate	
	2. Software	
	3. Revokation	
	E. Zusammenfassung: Regelungsbedarf der Sorgfaltspflichten	
	1. Regelung der Pflichten der CA und des Zertifikatsinhabers	
	2. Form der Regelung	
IV.	Ergebnis	
	A. Risiken und Risikoverteilung	
	B. Übersicht Haftung bei der Zertifikatserstellung	
	C. Übersicht Haftung im Umgang mit Geheimschlüsseln	
	D. Übersicht Haftung bei der Zertifikatsverwendung	
§ 7	Beweis	
	I. Ausgangslage und Fragestellung	
	II. Rechtliche Anforderungen	
	A. Beweisgegenstand	
	1. Tatsachen	
	2. Erfahrungssätze	
	3. Rechtssätze und Handelsbräuche	

B.	Beweisarten	183
1.	Unmittelbarer und mittelbarer Beweis	183
2.	Hauptbeweis, Gegenbeweis, Beweis des Gegenteils	183
C.	Beweislast	184
1.	Grundsatz	184
2.	Beweislastumkehr	185
3.	Vermutungen	185
a)	Widerlegbare gesetzliche Vermutung	185
b)	Unwiderlegbare gesetzliche Vermutung	186
4.	Vertragliche Beweislastregelung	186
a)	Problematik	186
b)	Voraussetzungen	187
c)	Beweislastverträge im Arbeitsverhältnis (B2E)	188
d)	Beweislastverträge im Kundenverhältnis (B2C und B2B)	188
D.	Beweismass	189
1.	Strikter Beweis	189
2.	Glaubhaftmachung	190
3.	Kausalzusammenhang: Überwiegende Wahrscheinlichkeit	190
4.	Anscheinsbeweis	190
5.	Exkurs: Tatsächliche Vermutung	191
6.	Vertragliche Beweismassregelung	192
a)	Zulässigkeit	192
b)	Voraussetzungen	192
E.	Beweismittel	193
1.	Allgemeines	193
2.	Numerus Clausus	194
a)	Zeugnis	194
b)	Urkunden	194
c)	Augenschein	194
d)	Gutachten	195
e)	Schiedsgutachten	195
f)	Schriftliche Auskunft	195
g)	Parteibefragung und Beweisaussage	196
F.	Beweiswürdigung	196
1.	Freie Beweiswürdigung	196
2.	Beweisregeln	196
G.	Gesetzliche Anforderungen an digitale Dokumente	197
1.	Kantonale ZPO und VE-ZPO	197
2.	ZertES, V-ZertES und TAV-ZertES	197
3.	GeBüV	197
4.	MWSTGV und ELDI-V	199
H.	Beweisführung mit digitalen Dokumenten	199
1.	Zulassung zum Prozess	199

2.	Zuordnung zu den bestehenden Beweismitteln	200
3.	Beweiswert	200
4.	Beweiserleichterung	200
III.	Beurteilung Public Key Infrastructure	201
A.	Relevanz des Speichermediums	201
1.	Herkömmliche Informationsträger	201
2.	Digitale Datenträger	201
3.	Unveränderbare Datenträger	202
4.	Veränderbare Datenträger	202
B.	Beweiseignung der PKI-Anwendungen	202
1.	Vorbemerkungen	202
2.	Digitale Signatur	203
a)	Beweiskette	203
b)	Signierschlüssel – Prüfschlüssel	204
c)	Prüfschlüssel – Schlüsselhalter	204
d)	Schlüsselhalter – Unterzeichner	205
e)	Unterzeichner – signierte Datei	208
f)	Signierte Datei – (gültige) Signaturprüfung	209
g)	Zwischenergebnis Beweiseignung der digitalen Signatur	209
3.	Verschlüsselung	212
a)	Integrität durch Vertraulichkeit	212
b)	Problem der Authentizität	212
c)	Zwischenergebnis Beweiseignung der Verschlüsselung	213
C.	Beweiswert der PKI-Anwendungen	213
1.	Vorbemerkungen	213
2.	Signierung von anzuzeigenden Inhalten	213
a)	Fallbeispiel PDF-Signaturen	213
b)	Fallbeispiel S/MIME	214
3.	Datenverschlüsselung	215
4.	Kommunikationsverschlüsselung	217
a)	Fallbeispiel S/MIME	217
b)	Fallbeispiel HTTPS	218
5.	Signierung von ausführbaren Inhalten	218
6.	Authentifikation	219
IV.	Ergebnis	220
A.	Beweiseignung der PKI-Technologie	220
B.	Beweiswert und Beweiserleichterung bei PKI-Anwendungen	221
C.	Übersicht	223
1.	Beweiseignung	223
2.	Beweiswert	224
§ 8	Geheimnisschutz	225
I.	Einleitung und Fragestellung	225
II.	Rechtliche Anforderungen	226

A.	Aus Gesetz	226
1.	Datenschutz	226
a)	Hintergrund	226
b)	Persönlicher Geltungsbereich	227
c)	Sachlicher Geltungsbereich und Begriffe	227
d)	Grenzen des Datenschutzes	230
e)	Rechtsfolgen	232
2.	Bankkundengeheimnis	233
a)	Hintergrund	233
b)	Persönlicher Geltungsbereich	233
c)	Sachlicher Geltungsbereich	234
d)	Grenzen des Bankkundengeheimnisses	235
e)	Rechtsfolgen	236
B.	Aus Vertrag	237
1.	Zulässigkeit und Inhalt	237
2.	Folgen der Verletzung	237
C.	Grenzen und Einhaltung der Vertraulichkeitsverpflichtung	238
1.	Rechtfertigungsgründe	238
2.	Nicht bestimmbare Daten	239
a)	Anonymität	239
b)	Pseudonymität	240
c)	Verschlüsselung	241
D.	Zwischenergebnis Anforderungen an die Vertraulichkeit	242
III.	Beurteilung Public Key Infrastructure	242
A.	Allgemeine Aspekte	242
1.	Digitale Identität	242
a)	Begriff	242
b)	Feststellung	243
2.	Zertifikate	244
3.	Verzeichnisdienste	245
a)	Ausgangslage	245
b)	Angaben des Ausstellers	245
c)	Angaben des Inhabers	245
4.	Informationelle Selbstbestimmung durch PKI	247
a)	Ausgangslage	247
b)	Attributzertifikate	248
c)	Pseudonyme	249
d)	Exkurs: Blinde Signaturen	250
aa)	Funktionsweise und Anwendungen	250
bb)	Gestaltung der PKI	250
B.	Betrachtung der PKI-Anwendungsgebiete	251
1.	Datenverschlüsselung	251
a)	Vorbemerkungen	251

b) Schlüsselemente	253
aa) Schlüssellänge	253
bb) Aufbewahrung	254
cc) Wahl und Standort der CA	254
c) Verschlüsselungsmethoden	255
d) Verschlüsselungsprogramme	256
e) Folgen ungenügender Datenverschlüsselung	256
2. Kommunikationsverschlüsselung	257
a) Unterschiede zur Datenverschlüsselung	257
b) Fallbeispiel S/MIME-Verschlüsselung	258
c) Fallbeispiel HTTPS	258
d) Folgen ungenügender Kommunikationsverschlüsselung	259
3. Signierung von ausführbaren Inhalten	260
4. Signierung von anzuzeigenden Inhalten	260
5. Authentifikation	260
IV. Ergebnis	262
A. Allgemeine Risiken und Chancen der PKI-Technologie	262
B. Eignung der PKI-Anwendungen zur Erfüllung von Geheimhaltungspflichten	262

Dritter Teil: Ergebnisse 265

§ 9 Zusammenfassung	265
I. Eignung der PKI-Technologie zur Erfüllung rechtlicher Anforderungen	265
A. Signierung von anzuzeigenden Inhalten	265
B. Signierung von ausführbaren Inhalten	266
C. Datenverschlüsselung	266
D. Kommunikationsverschlüsselung	267
E. Authentifikation	267
II. Ergebnisse aus der Optik der Rechtsgebiete	268
A. Form	268
B. Vertretung	269
C. Haftung	270
D. Beweis	271
E. Geheimnisschutz	272
III. Würdigung	273