

Reihe: Electronic Commerce



© 2008 AGI-Information Management Consultants
May be used for personal purposes only or by
institutions associated to the Dandelion network.

Herausgegeben von Prof. Dr. Dr. h. c. Norbert Szyperski, Köln, Prof. Dr. Beat
F. Schmid, St. Gallen, Prof. Dr. Dr. h. c. August-Wilhelm Scheer, Saarbrücken,
Prof. Dr. Günther Pernul, Essen, und Prof. Dr. Stefan Klein, Münster

Dr. Torsten Költzsch

Geschlossene Public-Key- Infrastruktur-Lösungen

Mit einem Geleitwort von Prof. Dr. Günter Müller, Albert-Ludwigs-
Universität, Freiburg i. Br.



JOSEF EUL VERLAG
Lohmar • Köln

INHALTSVERZEICHNIS

Inhaltsübersicht	IX
Inhaltsverzeichnis	XI
Abbildungsverzeichnis	XV
Tabellenverzeichnis	XVII
Abkürzungsverzeichnis	XIX
Kapitel Einführung	1
1.1 SICHERHEIT-BESTIMMENDER FAKTOR ELEKTRONISCHER TRANSAKTIONEN.....	1
1.2 DIGITALE SIGNATUREN UND PUBLIC-KEY-INFRASTRUKTUREN.....	3
1.3 SKALIERUNG VON PKI.....	7
1.4 AUFBAU.....	8
Kapitel 2 Elemente von Public-Key-Infrastrukturen	11
2.1 ELECTRONIC-COMMERCE - EINSATZFELD FÜR PUBLIC-KEY-INFRASTRUKTUREN., 11	
2.2 SICHERHEIT IM E-COMMERCE.....	16
2.2.1 Schutzziele der Mehrseitigen Sicherheit.....	18
2.2.2 Kryptografische Mechanismen zur Realisierung von Schutzzielen.....	22
2.2.2.1 Symmetrische Kryptografie.....	24
2.2.2.2 Asymmetrische Kryptografie.....	25
2.3 ZERTIFIKATE.....	28

2.4	ZERTIFIZIERUNGSSTELLEN.....	30
2.4.1	Ökonomischer Nutzen von Zertifizierungsstellen.....	31
2.4.1.1	Bedarf an Intermediären für das Wirtschaften.....	31
2.4.1.2	Auswirkungen auf den Bedarf an Intermediären durch das Internet?.....	36
2.4.2	Aufgaben von Zertifizierungsstellen.....	39
2.4.2.1	Identifizierung und Registrierung.....	40
2.4.2.2	Bereitstellung von Signaturschlüsseln und Identifikationsdaten.....	41
2.4.2.3	Zertifizierung.....	42
2.4.2.4	Personalisierung.....	42
2.4.2.5	Verteilung und Sperrung von Zertifikaten.....	43
2.4.2.6	Erstellung von Zertifizierungsrichtlinien.....	44
2.4.2.7	Bereitstellung von Zeitstempeln.....	44
2.4.2.8	Zusammenfassung und Antragstellung.....	45
2.4.3	Zertifizierungsrichtlinien.....	47
2.4.3.1	Certificate-Policy.....	48
2.4.3.2	Certification-Practice-Statements.....	50
2.4.3.3	PKI-Disclosure-Statement.....	51
2.4.3.4	Bewertung der Arten von Zertifizierungsrichtlinien.....	51
2.5	ORGANISATIONSFORMEN FÜR PUBLIC-KEY-INFRASTRUKTUREN.....	52
Kapitel 3 Vergleich hierarchischer Public-Key-Infrastruktur-Modelle.....		57
3.1	BESCHREIBUNGSKRITERIEN HIERARCHISCHER PUBLIC-KEY-INFRASTRUKTUREN	58
3.2	OFFENE, GESETZLICH REGULIERTE PKI.....	59
3.2.1	Oberblick über die offene, gesetzlich regulierte PKI nach Signaturgesetz.....	60
3.2.2	Merkmale offener, gesetzlich regulierter PKI.....	64
3.2.2.1	Einsatzzweck und Nutzerkreis.....	64
3.2.2.2	Digital signierte Dokumente als Beweismittel.....	65
3.2.2.3	Risikoverteilung und Haftung.....	65
3.2.3	Bewertung offener, gesetzlich regulierter PKI.....	67
3.2.3.1	Einsatzzweck und Nutzerkreis.....	68
3.2.3.2	Digital signierte Dokumente als Beweismittel.....	70
3.2.3.3	Risikoverteilung und Haftung.....	75
3.3	GESCHLOSSENE PKI.....	80
3,3.1'	Merkmale geschlossener Public-Key-Infrastrukturen.....	81
3.3.1.1	Einsatzzweck und Nutzerkreis.....	81
3.3.1.2	Digital signierte Dokumente als Beweismittel.....	82
3.3.1.3	Risikoverteilung und Haftung.....	82

3.3.2	Bewertung geschlossener Public-Key-Infrastrukturen.....	83
3.3.2.1	Einsatzzweck und Nutzerkreis.....	83
3.3.2.2	Digital signierte Dokumente als Beweismittel.....	85
3.3.2.3	Risikoverteilung und Haftung.....	85
3.4	ZUSAMMENFASSEND BEWERTUNG DER HIERARCHISCHEN PKI-MODELLE.....	87
Kapitel 4 SigG97 - Referenz für Zertifizierungsstellen und Nutzer.....		91
4.1	REFERENZ FÜR ZERTIFIZIERUNGSSTELLEN.....	93
4.1.1	Aufgabenübergreifende Anforderungen und Maßnahmen.....	94
4.1.2	Identifizierung und Registrierung von Antragstellern.....	100
4.1.3	Schlüsselerzeugung, Zertifizierung und Personalisierung.....	101
4.1.4	Verzeichnisdienst.....	102
4.1.5	Bereitstellung von Zeitstempeln.....	104
4.1.6	Kostenbetrachtung aus Sicht einer Zertifizierungsstelle.....	105
4.2	REFERENZ FÜR NUTZER.....	109
Kapitel 5 Einsatzszenarien für die Untersuchung geschlossener Public-Key-Infrastrukturen.....		113
5.1	SCENARIO I: GESCHLOSSENE PKI FÜR EIN UNTERNEHMEN - BEISPIEL ONLINEBANKING.....	115
5.1.1	Ausgestaltung einer geschlossenen PKI für Szenario 1.....	119
5.1.2	Bewertung von Szenario 1.....	128
5.1.2.1	Bankkunden-Perspektive.....	128
5.1.2.2	Bank-Perspektive.....	130
5.1.2.3	Risikoverteilung zwischen Bank und Kunden.....	135
5.1.2.4	Zusammenfassende Bewertung und Vorgehensvorschläge.....	141
5.2	SCENARIO II: GESCHLOSSENE PKI FÜR MEHRERE UNTERNEHMEN- BEISPIEL TRANSAKTIONSPLATTFORM.....	143
5.2.1	Ausgestaltung einer geschlossenen PKI für Szenario II.....	147
5.2.2	Bewertung von Szenario II.....	149
5.2.2.1	Handhabung von ex-ante Risiken.....	150
5.2.2.2	Handhabung von ex-post Risiken.....	153
5.2.2.3	Zusammenfassende Bewertung und Vorgehensvorschläge.....	156

5.3	SZENARIO III: VERBINDUNGSMÖGLICHKEITEN ZWISCHEN GESCHLOSSENEN PUBUC-KEY-INFRASTRUKTUREN.....	161
5.3.1	Cross-Zertifizierung.....	163
5.3.2	Konzept der hierarchischen Erweiterung.....	166
5.3.2.1	Grundlagen der hierarchischen Erweiterung.....	166
5.3.2.2	Beispiel: Identrus.....	168
5.3.3	Bridge-Certification-Authority-Konzept.....	171
5.3.3.1	Grundlagen des Bridge-CA-Konzeptes.....	172
5.3.3.2	Beispiele für Bridge-CA's.....	176
5.3.4	Konzept mit Validierungsintermediär.....	179
5.3.4.1	Grundlagen des Konzepts mit Validierungsintermediär.....	179
5.3.4.2	Beispiel: ValiCert.....	182
5.3.5	Zusammenfassende Bewertung der Verbindungsmöglichkeiten zwischen Public-Key-Infrastrukturen.....	183
Kapitel 6	Fazit und Ausblick.....	187
	Literaturverzeichnis.....	191