

Inhaltsverzeichnis

1	Privatsphäre: Eine Frage des Vertrauens?	1
1.1	Alles oder nichts	1
1.2	Erweiterung des Vertrauensmodells	4
1.3	Die Vorgehensweise	4
2	Delegation von Rechten am Beispiel CRM	7
2.1	Rechtliche Anforderungen der informationellen Selbstbestimmung	7
2.2	Einseitiges CRM	11
2.3	Mehrseitiges CRM	22
2.4	Ergebnis	28
3	Mehrseitigkeit von gegenwärtigen Sicherheitssystemen	31
3.1	Delegationssysteme und CRM	31
3.2	Transparenzsysteme und CRM	43
3.3	Identitätsmanagementsysteme und CRM	47
3.4	Ergebnis	73
4	DREISAM: Identitätsmanagementsystem mit der Delegation von Rechten	79
4.1	Protokolle zur Delegation von Rechten und zu deren Widerruf . .	79
4.2	Systementwurf	94
4.3	Implementierung	124
4.4	Ergebnis	127
5	Evaluation von DREISAM	137
5.1	Angriffsfälle nach dem IT-Grundschutz	137
5.2	Schutzwirkung von DREISAM	142
5.3	Ergebnis	151
6	Potentiale von DREISAM	155
6.1	Behördliche und medizinische Dienstleistungen	155
6.2	Digital Rights Management	157

Anhang	161
A Public-Key Infrastruktur (PKI)	163
B Commitments (Festlegschema)	165
C Zero-Knowledge Beweissystem (ZKP)	169
Literaturverzeichnis	179
Sachverzeichnis	189