

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Problemstellung . . . . .	2
1.2	Ziele dieser Arbeit . . . . .	3
1.3	Gliederung der Arbeit . . . . .	4
<b>2</b>	<b>Grundlagen</b>	<b>7</b>
2.1	Allgemeine Begriffe der Sicherheit . . . . .	7
2.2	Kryptographische Grundlagen . . . . .	8
2.2.1	Symmetrische Chiffren . . . . .	8
2.2.2	Asymmetrische Chiffren . . . . .	9
2.2.3	Hybride Kryptographie . . . . .	10
2.2.4	Kryptographische Einwegfunktionen . . . . .	10
2.2.4.1	HMAC . . . . .	11
2.2.4.2	Hash-Ketten . . . . .	12
2.2.5	Digitale Signatur . . . . .	13
2.2.5.1	Verteiltes RSA-Signaturverfahren . . . . .	14
2.2.5.2	Verteilte Schlüsselerzeugung . . . . .	14
2.2.6	Digitale Zertifikate . . . . .	15
2.2.6.1	X.509 . . . . .	16
2.2.6.2	PGP . . . . .	18
2.3	Vertrauensmodelle . . . . .	19
2.3.1	Public-Key-Infrastructure . . . . .	20
2.3.1.1	Single CA . . . . .	21
2.3.1.2	Oligarchie . . . . .	22

2.3.1.3	Anarchie . . . . .	23
2.3.2	PKI-Implementierungen . . . . .	24
2.3.2.1	PKI auf X.509-Basis . . . . .	24
2.3.2.1.1	Zertifikatswiderufliste . . . . .	25
2.3.2.1.2	Zertifikatsprüfung . . . . .	25
2.3.2.2	PKI mittels PGP . . . . .	26
2.3.3	Digitale Zeitstempel . . . . .	27
2.3.4	Zeitstempelprotokolle . . . . .	27
2.4	Verzeichnisdienste . . . . .	28
2.4.1	X.500 . . . . .	29
2.4.2	LDAP . . . . .	29
2.5	Peer-to-Peer-Systeme/Overlay-Netze . . . . .	29
2.5.1	Unstrukturierte Overlay-Netze . . . . .	32
2.5.2	Strukturierte Overlay-Netze . . . . .	33
2.5.2.1	Chord . . . . .	34
2.5.2.2	Weitere Verfahren . . . . .	35
2.5.3	Verteilte Hash-Tabellen . . . . .	35
2.6	Dienstorientierte Architekturen . . . . .	37
2.6.1	Web Services . . . . .	38
2.7	Juristische Grundlagen . . . . .	40
2.7.1	Grundbegriffe . . . . .	40
2.7.1.1	Willenserklärung . . . . .	40
2.7.1.2	Vertrag . . . . .	41
2.7.1.3	Formvorschriften . . . . .	41
2.7.1.4	Schriftform . . . . .	42
2.7.1.5	Signaturgesetz . . . . .	44
2.7.1.6	Vergleich Schriftform und elektronische Form . . . . .	45
2.7.2	Wirksamkeit von Willenserklärungen . . . . .	47
2.7.3	Beweisfragen bei elektronischen Willenserklärungen . . . . .	47
2.7.3.1	Motivation . . . . .	48
2.7.3.2	Beweislasten . . . . .	48

2.7.3.3	Beweismittel . . . . .	49
2.8	Klassifikation von Angreifern . . . . .	50
2.8.1	Angreifermodelle . . . . .	51
2.8.1.1	Kryptographisches Modell . . . . .	51
2.8.1.2	Kommunikationstechnisches Modell . . . . .	52
2.8.1.3	Verhaltenstheoretisches Modell . . . . .	53
2.8.2	Definition eines Standardangreifers . . . . .	54
2.9	Beschreibung von Angriffen . . . . .	55
<b>3</b>	<b>Die SESAM-Marktplattform</b>	<b>57</b>
3.1	Einleitung . . . . .	57
3.2	Anforderungen . . . . .	57
3.2.1	Sicherheitsanforderungen . . . . .	59
3.3	Verwandte Arbeiten . . . . .	59
3.3.1	Web-Services . . . . .	60
3.3.2	Java Enterprise Edition . . . . .	60
3.3.3	OSGi-Framework . . . . .	60
3.3.4	JXTA-Framework . . . . .	61
3.3.5	PeerMart/PeerMint . . . . .	61
3.3.6	Zusammenfassung . . . . .	62
3.4	Entwurf . . . . .	62
3.4.1	SESAM-Basisarchitektur . . . . .	63
3.4.1.1	Kommunikationsschicht . . . . .	65
3.4.1.2	Peer-to-Peer-Schicht . . . . .	67
3.4.1.3	Systemzugangsschicht . . . . .	68
3.4.1.4	Dienstmanagement . . . . .	69
3.4.1.5	Dienste . . . . .	70
3.4.1.6	Ontologien . . . . .	71
3.4.1.6.1	Das minimale Marktmodell . . . . .	71
3.4.1.7	Marktmechanismen . . . . .	72
3.4.1.8	Anwendungen . . . . .	73

3.4.2 SESAM-ServiceNet . . . . .	73
3.4.3 SESAM-Sicherheitsarchitektur . . . . .	76
3.4.3.1 Sicherheitserweiterung der SESAM-Basisarchitektur . . . . .	78
3.4.3.1.1 Knoten-zu-Knoten-Sicherheit . . . . .	79
3.4.3.1.2 Dienst-zu-Dienst-Sicherheit . . . . .	80
3.4.3.1.3 Datensicherheit . . . . .	81
3.4.3.2 Sicherheitskomponente . . . . .	84
3.4.3.2.1 Zusammenfassung . . . . .	85
3.5 Implementierung . . . . .	86
3.6 Evaluation . . . . .	88
3.6.1 Bewertung hinsichtlich Anforderungen . . . . .	88
3.6.1.1 Allgemeine Anforderungen . . . . .	88
3.6.1.1.1 Dezentralität und Selbstorganisation . . . . .	88
3.6.1.1.2 Erweiterbarkeit und Wiederverwendbarkeit . . . . .	89
3.6.1.1.3 Rechtskonformität und Beweissicherheit . . . . .	89
3.6.1.2 Sicherheitsanforderungen . . . . .	89
3.6.1.2.1 Knoten-zu-Knoten-Sicherheit . . . . .	90
3.6.1.2.2 Dienst-zu-Dienst-Sicherheit . . . . .	90
3.6.1.2.3 Datensicherheit . . . . .	90
3.6.1.3 Zusammenfassung . . . . .	90
3.6.2 Softwareprototyp und SESAM-Demonstrator . . . . .	91
3.7 Zusammenfassung . . . . .	94
<b>4 Sichere Vertragsverhandlungen in dezentralen und spontanen Märkten</b>	<b>95</b>
4.1 Einleitung . . . . .	95
4.2 Problemstellung . . . . .	95
4.3 Anforderungen . . . . .	97
4.4 Lösungsansatz . . . . .	98
4.5 Stand der Technik . . . . .	99
4.5.1 Authentifizierungsverfahren . . . . .	100
4.5.1.1 PAP/CHAP . . . . .	100

4.5.1.2	EAP	101
4.5.1.3	SASL	101
4.5.1.4	Kerberos	102
4.5.1.5	X.509	102
4.5.2	Zertifizierungsverfahren	103
4.5.3	Signaturverfahren	104
4.5.3.1	S/MIME	104
4.5.3.2	OpenPGP	105
4.6	Entwurf	105
4.6.1	Verteilter Authentifizierungsdienst	105
4.6.1.1	Rahmenwerk	106
4.6.1.1.1	Dienstschnittstelle	106
4.6.1.1.2	Datenmodell	108
4.6.1.1.3	Vertrauensaussagen mittels SESAM-Zertifikat	110
4.6.1.1.4	Overlay-Organisation	113
4.6.1.2	Generisches Authentifizierungsprotokoll	115
4.6.1.3	Authentifizierungsmodule	119
4.6.1.3.1	PAP/CHAP-Authentifizierung	120
4.6.1.3.2	X.509-Authentifizierung	121
4.6.1.3.3	SMS-TAN-Authentifizierung	123
4.6.2	Erweiterung der SESAM-Sicherheitskomponente	126
4.6.2.1	Einfache elektronische Signatur	126
4.6.2.2	Fortgeschrittene elektronische Signatur	127
4.6.2.3	Qualifizierte elektronische Signatur	128
4.6.2.4	P2P-Signatur	128
4.6.2.4.1	Teilnehmerwahl	129
4.6.2.4.2	Verteilte Schlüsselerzeugung und Initialisierung Hash-Kette	132
4.6.2.4.3	Signaturerstellung	133
4.6.2.4.4	Integration in SESAM-Sicherheitskomponente	134
4.7	Implementierung	135

4.7.1	Verteilter Authentifizierungsdienst . . . . .	136
4.7.2	Erweiterungen der SESAM-Sicherheitskomponente . . . . .	137
4.7.2.1	Einfache elektronische Signaturen . . . . .	137
4.7.2.2	Qualifizierte elektronische Signaturen . . . . .	137
4.7.2.3	P2P-Signatur . . . . .	139
4.8	Evaluation . . . . .	140
4.8.1	Verteilter Authentifizierungsdienst . . . . .	140
4.8.1.1	Identitätsnachweis von Marktteilnehmern . . . . .	140
4.8.1.2	Sicherheit . . . . .	142
4.8.1.2.1	Marktteilnehmer täuscht Identität vor . . . . .	142
4.8.1.2.2	Marktteilnehmer streitet Identität ab . . . . .	144
4.8.1.3	Weitere nicht-funktionale Anforderungen . . . . .	145
4.8.1.4	Bewertung . . . . .	146
4.8.2	Erweiterungen der SESAM-Sicherheitskomponente . . . . .	147
4.8.2.1	Erweiterungen nach Signaturgesetz . . . . .	148
4.8.2.1.1	Integritätsschutz und Zuordenbarkeit . . . . .	148
4.8.2.1.2	Sicherheit . . . . .	148
4.8.2.1.3	Rechtskonformität und Beweissicherheit . . . . .	149
4.8.2.2	P2P-Signatur . . . . .	149
4.8.2.2.1	Integritätsschutz und Zuordenbarkeit . . . . .	150
4.8.2.2.2	Rechtskonformität und Beweissicherheit . . . . .	150
4.8.2.2.3	Sicherheit . . . . .	150
4.8.2.2.4	Robustheit . . . . .	152
4.8.2.2.5	Skalierbarkeit . . . . .	157
4.8.2.2.6	Zeitaufkommen . . . . .	158
4.8.2.2.7	Kommunikationsaufwand . . . . .	160
4.9	Zusammenfassung . . . . .	164

<b>5 Beweiserleichterung beim Zugang elektronischer Willenserklärungen</b>	<b>167</b>
5.1 Einleitung . . . . .	167
5.2 Problemstellung . . . . .	169
5.3 Anforderungen . . . . .	170
5.3.1 Funktionale Anforderungen . . . . .	170
5.3.2 Nicht-funktionale Anforderungen . . . . .	171
5.3.3 Angreifermodell . . . . .	171
5.4 Stand der Forschung . . . . .	171
5.5 Lösungsansatz . . . . .	172
5.6 Verteilter Zeitstempeldienst . . . . .	174
5.6.1 Bedrohungsanalyse . . . . .	174
5.6.2 Anforderungen . . . . .	175
5.6.3 Entwurf . . . . .	177
5.6.3.1 Organisationsstruktur des verteilten Zeitstempeldienstes . . . . .	179
5.6.3.2 Erstellung und Auswertung eines Dokumentenzeitstempels . . . . .	181
5.6.3.2.1 Erstellung und Auswertung eines Einzelzeitstempels	181
5.6.3.2.2 Erstellung von Dokumentenzeitstempeln . . . . .	182
5.6.3.2.3 Verkettung von Einzelzeitstempeln innerhalb eines Dokumentenzeitstempels . . . . .	185
5.6.3.2.4 Auswertung von Dokumentenzeitstempeln . . . . .	189
5.6.3.3 Verkettung von Zeitstempeln eines Zeitstempeldienstes . . . . .	190
5.6.3.4 Verkettung von Zeitstempeln mehrerer Zeitstempeldienste . . . . .	191
5.6.4 Implementierung . . . . .	193
5.6.4.1 Integration in das SESAM-Basisystem . . . . .	194
5.6.4.1.1 Datenmodell . . . . .	194
5.6.4.1.2 Dienstschnittstelle . . . . .	195
5.6.4.2 Integration in die Simulationsumgebung OverSim . . . . .	196
5.6.5 Evaluation . . . . .	197
5.6.5.1 Protokollierung des Zeitpunktes $t$ . . . . .	198
5.6.5.2 Eindeutige Zuordnung des Zeitstempels zum Inhalt $D$ . . . . .	199
5.6.5.3 Verifizierbarkeit durch Dritte . . . . .	199

5.6.5.4	Genauigkeit von Dokumentenzeitstempeln . . . . .	199
5.6.5.4.1	Vergleich Auswertung ohne Angreifer . . . . .	202
5.6.5.4.2	Angriff auf einen Dokumentenzeitstempel durch Rückdatieren . . . . .	203
5.6.5.4.3	Angriff auf einen Dokumentenzeitstempel durch Vordatieren . . . . .	204
5.6.5.5	Sicherheit von Dokumentenzeitstempeln . . . . .	206
5.6.5.6	Sicherheit von Protokollzeitstempeln . . . . .	208
5.6.5.7	Skalierbarkeit des verteilten Zeitstempeldienstes . . . . .	209
5.6.5.7.1	Zeitverhalten des verteilten Zeitstempeldienstes . .	210
5.6.5.7.2	Kommunikationsaufwand . . . . .	212
5.6.5.8	Robustheit des verteilten Zeitstempeldienstes . . . . .	216
5.6.5.9	Weitere nicht-funktionale Anforderungen . . . . .	220
5.6.6	Bewertung . . . . .	221
5.7	Besitznachweis . . . . .	223
5.7.1	Bedrohungsanalyse . . . . .	223
5.7.2	Anforderungen . . . . .	224
5.7.3	Entwurf . . . . .	225
5.7.4	Implementierung . . . . .	227
5.7.4.1	Integration in das SESAM-Basisystem . . . . .	227
5.7.4.2	Integration in die Simulationsumgebung OverSim .	228
5.7.5	Evaluation . . . . .	228
5.7.5.1	Funktionale Anforderungen . . . . .	228
5.7.5.2	Sicherheit . . . . .	229
5.7.5.2.1	Identität des Teilnehmers fälschen . . . . .	229
5.7.5.2.2	Dokumenteninhalt fälschen . . . . .	230
5.7.5.2.3	Zeitpunkt fälschen . . . . .	230
5.7.5.2.4	Allgemeine Sicherheitsanforderungen . . . . .	231
5.7.5.3	Zusammenfassung . . . . .	232
5.8	Zugangsnachweis . . . . .	232
5.8.1	Anforderungen . . . . .	232
5.8.2	Entwurf . . . . .	233

5.8.2.1	Grundidee	234
5.8.2.2	Einführung	235
5.8.2.3	Organisation von Zeugen	236
5.8.2.4	Auswahl von Zeugen	237
5.8.2.5	Zugangsprotokoll	240
5.8.2.5.1	Übertragung der Willenserklärung	241
5.8.2.5.2	Zustellung der Willenserklärung und Erstellung des Zugangsnachweises	243
5.8.2.5.3	Übertragung der Zugangsbestätigung	244
5.8.2.6	Integration in das SESAM-Basisssystem	245
5.8.2.6.1	Datenmodell	245
5.8.2.6.2	Dienstschnittstelle	246
5.8.3	Implementierung	247
5.8.4	Evaluation	248
5.8.4.1	Nachweis über den Zugang einer elektronischen Willenserklärung	249
5.8.4.2	Eindeutige Zuordenbarkeit von Absender und Empfänger	249
5.8.4.3	Eindeutige Zuordenbarkeit der zugegangenen Erklärung	250
5.8.4.4	Verifizierbarer Zugangszeitpunkt	250
5.8.4.5	Nutzung der verteilten Infrastruktur und dezentrale Organisationsform	251
5.8.4.6	Schutz gegenüber identifizierten Bedrohungsszenarien	252
5.8.4.6.1	Absender täuscht Zugang vor	252
5.8.4.6.2	Empfänger streitet Zugang ab	253
5.8.4.6.3	Absender bzw. Empfänger verneint fristgerechten Zugang	254
5.8.4.7	Robustheit	255
5.8.4.8	Skalierbarkeit	259
5.8.4.8.1	Zeitaufwand	260
5.8.4.8.2	Kommunikationsaufwand	264
5.8.5	Bewertung	266
5.9	Zusammenfassung	267

<b>6 Zusammenfassung</b>	<b>271</b>
6.1 Ergebnisse der Arbeit . . . . .	271
6.2 Ausblick . . . . .	273
<b>A Simulationsumgebung OverSim</b>	<b>287</b>
A.1 Integration eigener Komponenten . . . . .	288
A.2 RPC-basierter Nachrichtenaustausch zwischen Modulen . . . . .	289
<b>B Zusammenhang Overlay-Pfadlänge und Angreiferwahrscheinlichkeit</b>	<b>291</b>
<b>C Mathematische Verfahren zur Zeitstempelauswertung</b>	<b>293</b>