

Inhaltsverzeichnis

Vorwort	vii
Kurzfassung	ix
Abstract	xi
1 Einführung und Motivation	1
1.1 Motivation / Ziele	3
1.2 Übersicht über diese Arbeit	5
2 Stand der Technik	7
2.1 Ubiquitous Computing	7
2.2 Hardwarebasierte Forschung für Ubiquitous Computing	10
2.3 Kommunikationstechniken für Ubiquitous Computing	12
2.3.1 Verteilter gemeinsamer Speicher und assoziativer Speicher	12
2.3.2 Tuplespaces	13
2.3.3 Peer-to-Peer-Techniken	24
2.3.4 Zusammenfassung und kritische Diskussion	28
2.4 Zugriffskontrolle für Ubiquitous Computing	32
2.4.1 Verschlüsselungsalgorithmen	32
2.4.2 Zugriffskontrollestechniken	34
2.4.3 Zugriffskontrolle in Peer-to-Peer-Systemen	40
2.4.4 Zusammenfassung und kritische Diskussion	50
3 Die InfoSpace-Applikation	55
3.1 Idee und Motivation	55
3.2 Ziele	58
3.3 InfoSpaces	59
3.3.1 LocalSpaces	60
3.3.2 CommonSpaces	62
3.3.3 Operationen in InfoSpaces	67
3.4 Softwarearchitektur für InfoSpaces	73

Inhaltsverzeichnis

3.4.1	Peer-to-Peer-Bausteine	73
3.4.2	Generische Softwarearchitektur der InfoSpaces	75
3.5	Beispielimplementierungen	77
3.5.1	Beispielimplementierung für PC	77
3.5.2	Beispielimplementierung für ein Embedded System	84
3.6	Zusammenfassung	86
3.6.1	Ausblick	90
4	Peer-to-Peer-Zugriffskontrolle: ein neuer Ansatz	93
4.1	Motivation	93
4.2	Beispiel-Szenarien	94
4.2.1	Tagung / Messe	94
4.2.2	Prüfungsszenario	96
4.3	Ziele	97
4.4	Das Schlüssel-Schloss-Paradigma	98
4.5	Umsetzung des Paradigmas	101
4.5.1	Access Control InfoSpace Matrix	101
4.5.2	Bindung zwischen elektronischen Identitäten und Benutzern	102
4.5.3	Umsetzung der Rechte in das Schlüsselsystem	104
4.6	Protokollbausteine für die Zugriffskontrolle	107
4.6.1	Verschlüsselte Verbindungen	108
4.6.2	ISA-Verteilung	108
4.6.3	Zugriffskontrolle der Teilnahme an einem CommonSpace . .	111
4.6.4	Zugriffskontrolle für Angebote	112
4.6.5	Zugriffskontrolle für Transferanfragen	114
4.6.6	Rechtmanagement	115
4.6.7	Gruppenmanagement	119
4.6.8	Identitätsmanagement	121
4.6.9	Vollzugriff-Rechtmanagement	123
4.6.10	Objektzugriffskontrolle	126
4.7	Implementierung des Protokolls und Messungen	128
4.7.1	Kryptographie mit Java	129
4.7.2	Umsetzung des Protokolls	132
4.7.3	Messungen	136
4.8	Zusammenfassung	143
5	Zusammenfassung	147
	Abbildungsverzeichnis	150

Tabellenverzeichnis	152
Verzeichnis der Algorithmen	155
Häufig genutzte Abkürzungen	157