

Inhaltsverzeichnis

TEIL I – EINLEITUNG UND PROBLEMDEFINITION

1	EINLEITUNG	1
1.1	Fragestellung zum Forschungsgebiet	5
1.2	Aufbau der Arbeit	7
2	FORSCHUNGSMETHODIK – „DESIGN RESEARCH“	11
3	AKTUELLER STAND IM BEREICH MOBILER ORTSBEZOGENER DIENSTE	15
3.1	Ortsbezogene Dienste	15
3.1.1	Übertragungsarten von ortsbezogenen Diensten	17
3.1.2	Arten von ortsbezogenen Diensten	18
3.1.3	Bereitstellung von ortsbezogenen Diensten im Mobilfunknetz	20
3.2	Herausforderungen bei der Entwicklung von kontextbezogenen Diensten	22
3.3	Schutz der Privatsphäre als zentrale Herausforderung	24
3.4	Risiken bei der Nutzung von ortsbezogenen Diensten	25
3.5	Risiken für die Privatsphäre	28
3.6	Missbräuchliche Verwendung sensibler Daten	29
3.7	Mobiles Internet	32
3.7.1	Bereitstellung von ortsbezogenen Diensten mittels spezieller Anwendungen (Apps)	32
3.7.2	Privacy-Problematik bei „Apps“	36
3.7.3	Potentielle Risiken durch die Nutzung von mobilen Anwendungen am Beispiel von „Google Maps Navigation“	38
3.8	Zukünftige Weiterentwicklung des Umfelds	38

TEIL II – RELATED WORK UND ANFORDERUNGSANALYSE 41

4	VORÜBERLEGUNGEN ZUM ARCHITEKTURAUFBAU	43
4.1	Grundlegende Anforderungen an die Architektur	43
4.2	Juristische Rahmenbedingungen zur Bereitstellung von mobilen Diensten	45
4.3	Architekturansätze zum Schutz der Privatsphäre	46
4.3.1	P3P – Platform for Privacy Preferences	46
4.3.2	Plasma	47
4.3.3	BluePoint	47
4.3.4	Privé	49
4.3.5	Prime	50
4.3.6	Alipes Plattform	52
4.4	Analyse des Related Works	54
4.5	Designentscheidungen	55
4.5.1	Monolithischer Ansatz	56
4.5.2	Feingranularer Aufbau der Gesamtarchitektur	58
4.5.3	Designentscheidung - Endgerät	59
4.5.4	Betrachtung weiterführender Designentscheidungen	60

5	KOMMUNIKATION INNERHALB DER ARCHITEKTUR	61
5.1	Anforderungen bezüglich der Kommunikation zwischen den Instanzen der Architektur	61
5.2	Serviceorientierte Architekturen (SOA)	62
5.3	Wireless Web Services	64
5.3.1	Wireless Portal Network	64
5.3.2	Wireless extended Internet	66
5.3.3	Agentenbasierter Ansatz für mobile Web Services	66
5.3.4	Wireless ad hoc network	68
5.4	Adaption von Kommunikationsansätzen zur Bereitstellung von mobilen Web Services	68
6	ABSICHERUNG DER KOMMUNIKATION	71
6.1	Anforderungen an die Absicherung der Kommunikation innerhalb der Architektur	71
6.2	Public Key Infrastructure (PKI)	71
6.2.1	Zertifikate	72
6.2.2	Web of Trust	72
6.2.3	Streng hierarchische PKI	73
6.2.4	Cross-Zertifizierung	75
6.3	Anforderung an die Zertifizierungsinstanz	76
6.4	Auswahl eines geeigneten Zertifizierungsverfahrens	77
7	UMSETZUNG DES SCHUTZES DER PRIVATSPHÄRE	79
7.1	Anforderungen an die Architektur bezüglich des Schutzes der Privatsphäre	79
7.2	Mechanismen zum Schutz der Privatsphäre bei ortsbezogenen Diensten (Related Work)	80
7.2.1	Schutz der Identität (Identity Protection)	81
7.2.2	Camouflage	81
7.3	Verschleierung der Kommunikation	85
7.3.1	Proxy-Ansatz	85
7.3.2	Anonymisierungsnetzwerke	86
7.4	Designentscheidung - Mechanismen zum Schutz der Privatsphäre	88
8	BEREITSTELLUNG VON KONTEXTINFORMATIONEN	91
8.1	Anforderungen an die Instanzen zur Positionsbestimmung	91
8.2	Ansätze zur Positionsermittlung (Related Work)	92
8.2.1	Formen der Positionsrepräsentation	93
8.2.2	Technologien zur Positionsbestimmung	95
8.2.3	Ausblick im Bereich der Lokalisierungstechnologie	103
8.3	Designentscheidung	104
9	MONETÄRE TRANSAKTIONEN	105
9.1.1	Micro-/Makropayment	105
9.1.2	Gütekriterien eines Zahlungsverfahrens	105
9.2	Anforderungen an monetäre Transaktionen innerhalb der Architektur	107
9.3	Bezahlung von Diensten im mobilen Umfeld (Related Work)	108

9.3.1	PayWord	111
9.4	Designentscheidungen zur Bereitstellung von monetären Transaktionen	113
10	AUFFINDEN VON DIENSTEN	115
10.1	Anforderungen an die Instanz zum Auffinden von Diensten innerhalb der Architektur	115
10.2	Designentscheidungen zur Bereitstellung einer Dienstsuche innerhalb der Architektur	117
11	DIENSTE DER ARCHITEKTUR	119
11.1	Anforderungen an die Architektur bezüglich der Bereitstellung von Dienstleistungen ..	119

TEIL III – ENTWICKLUNG DER ARCHITEKTUR ZUM SCHUTZ DER PRIVATSPHÄRE 121

12	AUFBAU DER ARCHITEKTUR ZUM SCHUTZ DER PRIVATSPHÄRE	123
12.1	Architekturaufbau	123
12.2	Kommunikation zwischen den Instanzen der Architektur	128
12.2.1	Modul zur Nachrichtenerstellung	130
12.2.2	Nachrichtendialog innerhalb der Architektur	131
12.3	Dienstnutzung	132
12.3.1	Personalisierte Dienstnutzung	133
12.3.2	Anonymisierte Dienstnutzung	134
12.4	Administrative Datenübermittlung	135
12.4.1	Statusinformationen	135
12.4.2	Regeln / Kontextdaten	135
12.4.3	Zahlungsinformationen	135
12.5	Nachrichtenbearbeitung auf dem Endgerät	135
12.6	Prototypische Bereitstellung der Gesamtarchitektur	136
13	BEREITSTELLUNG VON SIGNATUREN	141
13.1	Konzeption des Trust Centers	141
13.1.1	Aufbau des Trust Centers	141
13.1.2	Bereitstellung von Zertifikaten	143
13.1.3	Zertifikatserweiterung	145
13.1.4	Verzeichnisdienst	147
13.1.5	Validierungsdienst	147
13.2	Widerruf eines Zertifikates	148
14	BEREITSTELLUNG VON ORTSBEZOGENEN KONTEXTINFORMATIONEN	151
14.1	Bereitstellung von Positionsinformationen innerhalb der Architektur	151
14.2	Location Provider	153
14.2.1	Aufbau des Location Providers	154
14.2.2	Weboberfläche des Location Providers	154
14.2.3	Serverlogik des Location Providers	154
14.2.4	Webservice-Schnittstellen des Location Providers	156
14.3	An der Lokalisierung beteiligte Instanzen	157
14.3.1	Endgerät (Device)	157

14.3.2	Positioning Infrastructure	158
14.3.3	Network Positioning Infrastructure	158
14.3.4	Location Database Provider	159
14.4	Prototypische Implementierung des Location Providers	161
14.4.1	Architektur des Location Providers	161
14.4.2	Selbstlernender Location Database Provider	163
14.4.3	Fusionierung von Sensordaten	164
14.4.4	Prototypische Implementierung der Server-Komponente zur Positionsermittlung	165
14.4.5	Prototypische Implementierung der Client-Komponente zur Positionsermittlung	167
15	SCHUTZ DER PRIVATSPHÄRE BEI ORTSBEZOGENEN DIENSTEN	169
15.1	Bereitstellung von Kontextinformationen	169
15.1	Aufbau des Privacy Providers	172
15.1.1	Privacy Reasoner	173
15.1.2	Message Layer	174
15.1.3	Datenbanken des Privacy Providers	174
15.1.4	Web-Frontend	174
15.1.5	Registrierungsstelle (Registration Authority)	174
15.1.6	Location Connector	175
15.1.7	Payment Aggregator	175
15.1.8	Push-Funktionalität	175
15.2	Datenbanken	176
15.2.1	Benutzerverwaltung	177
15.2.2	Service-Datenbank	178
15.2.3	Regelrepository	179
15.2.4	Personenbezogene Daten	179
15.2.5	Datennutzungslog	180
15.3	Regelsätze	181
15.4	Bereitstellung des Benutzer-Accounts beim Privacy Provider	184
15.4.1	Initialer Zustand nach der Anmeldung beim Privacy Provider	185
15.4.2	Erstellen von Regelsätzen bei einer ersten Dienstnutzung	185
15.4.3	Überprüfung der Regelsätze zur Bereitstellung von Kontextinformationen	188
15.4.4	Anonymisierung / Pseudonymisierung	190
15.5	Nutzung von Schutzmechanismen für ortsbezogene Informationen innerhalb der Architektur	192
16	MONETÄRE TRANSAKTIONEN INNERHALB DER ARCHITEKTUR	193
16.1	Prototypische Implementierung des Clearing Providers	193
16.1.1	Payment Aggregator – Anonymisierung von monetären Transaktionen	194
16.1.2	Web-Frontend des Clearing Providers	195
16.1.3	Clearing Meta – Verzeichnisdienst für Clearinginstanzen	198
16.2	Ablauf einer Bezahlung von Dienstleistungen	198
17	AUFFINDEN VON ORTS- UND KONTEXTBEZOGENEN DIENSTEN	203
17.1	Service Register Hierarchie	203
17.2	Service Portal	205
17.3	Service Agent	206
17.4	Service Register: Metadaten	208

17.5	Erweiterung einer Service Register Hierarchie	209
17.6	Prototypische Implementierung des Service Registers	211
18	BEREITSTELLUNG VON KONTEXTBEZOGENEN DIENSTEN	215
18.1	Service Provider	215
18.2	Content Provider	217
18.3	Dienstformen	221
18.4	Prototypische Realisierung von Diensten	224
18.4.1	Kostenpflichtiger kontextbezogener Wetterdienst	224
18.4.2	Ortsbezogenes „Service Portal“	225
TEIL IV – DISKUSSION UND AUSBLICK		227
19	ABSCHLIEBENDE BETRACHTUNG UND FAZIT	229
19.1	Skalierung und Ausfallsicherung der Architektur	229
19.1.1	Kritische Infrastrukturbestandteile	230
19.1.2	Instanzen mit Kernfunktionalitäten für begrenzte Benutzergruppen	231
19.1.3	Infrastrukturbestandteile mit geringer Relevanz für die Funktionsfähigkeit der Architektur	234
19.2	Wirtschaftliche Betrachtung	234
19.2.1	Aktuelle Marktbetrachtung und Ertragsmodelle der an der Architektur beteiligten Instanzen	235
19.2.2	Exemplarisches Beispiel für monetäre Flüsse innerhalb der Architektur	243
19.2.3	Mögliche wirtschaftliche Vorteile durch die Bereitstellung der Architektur	245
19.3	Kritische Betrachtung des Architekturansatzes	247
19.4	Weiterführende Arbeiten	249
19.4.1	Reduzierung des Single Points of Trust beim Privacy Provider	250
19.4.2	Architektur	251
19.4.3	Privacy	253
19.4.4	Lokalisierung	254
19.4.5	Dienste	255
19.4.6	Organisatorische Fragestellungen	256
19.5	Beitrag dieser Arbeit	258
19.6	Abschließendes Fazit	263
TEIL V – ANHANG		265
ANHANG A – XML NACHRICHTENFORMAT		267
ANHANG B – MGEOWIKI / PUSH INFORMATION PLATTFORM		309
LITERATUR		321
CURRICULUM VITAE		333