

Inhaltsverzeichnis

Abbildungsverzeichnis

XV

1	Einführung	1
1.1	Das eHome-Projekt	2
1.2	Motivation	4
1.2.1	Szenario	5
1.2.2	Analyse des Szenarios	6
1.3	Anforderungen	9
1.3.1	Dienstauswahl	9
1.3.2	Interaktion von Benutzern mit Diensten	9
1.3.3	Personalisierung	9
1.3.4	Schutz der Privatsphäre	10
1.3.5	Schutz von eHomes	11
1.4	Lösungsskizze	12
1.4.1	Dienstauswahl	12
1.4.2	Interaktion von Benutzern mit Diensten	13
1.4.3	Personalisierung	13
1.4.4	Schutz der Privatsphäre	14
1.4.5	Schutz von eHomes	16
1.5	Gliederung der Arbeit	18
2	Grundlagen	21
2.1	Allgemeine Begriffe und Konzepte	21
2.1.1	Benutzermodelle	21
2.1.2	Kontextbezogenes Computing	26
2.1.3	Komponentenbasierte Softwareentwicklung	28
2.1.4	Die OSGi-Service-Plattform	29
2.2	Struktur von eHome-Systemen	34
2.2.1	eHomes	34
2.2.2	eHome-Systeme	36
2.2.3	eHome-Dienste	37
2.2.4	Personalisierbare eHomes und eHome-Dienste	39
2.3	Anwendungsbeispiele für eHome-Dienste	40
2.3.1	Lichtdienst	40

2.3.2	Musikdienst	40
2.3.3	Lifesytle-Dienst	41
2.3.4	Weckdienst	41
2.3.5	Klingeldienst	41
2.3.6	Medizindienst	42
2.3.7	Sicherheitsdienst	42
2.4	Digitale Identität und Identitätsmanagement	43
2.4.1	Was ist eine Identität?	43
2.4.2	Digitale Identitäten und Teilidentitäten	45
2.4.3	Anonymität	46
2.4.4	Pseudonymität	48
2.4.5	Identitätsmanagement	50
2.5	Datenschutz und Privatsphäre	52
2.5.1	Schutzziele mehrseitiger Sicherheit und Privatsphäre	53
2.6	Zugriffskontrolle	56
2.6.1	Zugriffsmatrixmodell und Zugriffskontrollliste	56
2.6.2	Weitere Zugriffskontrollmodelle	57
2.6.3	Authentifizierung als Voraussetzung der Zugriffskontrolle	59
2.7	Kryptografie	59
2.8	Anonyme Credentials	63
2.8.1	Eigenschaften von Credentials	63
2.8.2	Bekannte Credential-Systeme	65
2.8.3	idemix	66
2.9	Zusammenfassung	71
3	Einordnung der Arbeit in den Projektkontext	73
3.1	Kirchhof: Prozesse und Infrastrukturen	73
3.2	Norbisrath: SCD-Prozess	74
3.2.1	Vom klassischen Entwicklungsprozess zum SCD-Prozess	74
3.2.2	Das eHome-Modell	81
3.2.3	Werkzeugunterstützung: der eHomeConfigurator	87
3.3	Retkowitz: kontinuierlicher SCD-Prozess	88
3.3.1	Strukturelle Adaption	89
3.3.2	Semantische Adaption	91
3.3.3	Werkzeugunterstützung	92
3.4	Bewertung	92
3.4.1	Dienstauswahl	92
3.4.2	Dienstinteraktion	93
3.4.3	Personalisierung	93
3.4.4	Schutz der Privatsphäre	96
3.4.5	Schutz von eHomes	96
3.5	Zusammenfassung	96

4 Benutzermodell	99
4.1 Entkopplung von Benutzerdaten	100
4.2 Produzenten und Konsumenten	103
4.3 Unterstützung der Intra-eHome-Mobilität	104
4.3.1 Ausführungsort vs. Auswirkungsort	105
4.3.2 Typen personalisierbarer Dienste	105
4.3.3 Rolle des Benutzermodells	109
4.4 Verwendete Ontologie	111
4.4.1 Der Ontologie-Begriff	111
4.4.2 General User Model Ontology (GUMO)	112
4.4.3 Die Datenstruktur SituationalStatement	113
4.5 Architektur des Benutzermodells	114
4.5.1 DataStorage	115
4.5.2 ProfileManager	115
4.5.3 SessionManager	116
4.5.4 Person	117
4.5.5 SituationalStatement	117
4.5.6 Beispiel	118
4.6 Zusammenfassung	120
5 Inter-eHome-Mobilität	121
5.1 Dienstauswahl und -interaktion	122
5.1.1 Erkennen und Auswählen eines eHomes	123
5.1.2 Auswahl eines Dienstes	124
5.1.3 Interaktion mit einem Dienst per Handheld	124
5.2 Personalisierung	126
5.2.1 Personalisierung durch Benutzerdaten	126
5.2.2 Personalisierung durch persönliche Dienste	132
5.3 Realisierung	141
5.3.1 Grundlegende Eigenschaften von JXTA	141
5.3.2 Neu entwickelte Komponenten	143
5.3.3 SimpleRMI: RMI auf Basis von JXTA	145
5.3.4 Architektur von SimpleRMI	148
5.3.5 MobileCommunicator und eHomeCommunicator	150
5.3.6 Verteilte Dienstkomposition und -kommunikation	155
5.3.7 Realisierung von Benutzeroberflächen	165
5.4 Zusammenfassung	167
6 Privatsphäre	169
6.1 Schutz auf eHome-Ebene	170
6.1.1 Datensparsamkeit	170
6.1.2 Unverkettbarkeit durch Anonymität	174
6.2 Schutz auf Dienstebene	183

6.2.1	Selektive Zugriffskontrolle für Benutzerdaten	184
6.2.2	Unverkettbarkeit durch Pseudonyme	186
6.3	Verschlüsselung persistenter Benutzerdaten	188
6.4	Sicherung der drahtlosen Kommunikation	189
6.5	Realisierung	189
6.5.1	Selektive Zugriffskontrolle für Benutzerdaten und deren Unverkettbarkeit	190
6.5.2	Integration von idemix in den eHome-Prototyp	194
6.5.3	Beteiligte Bausteine am Aushandlungsprozess	204
6.6	Zusammenfassung	208
7	Zugriffskontrolle	211
7.1	Schutz vor Zugriff unbefugter Benutzer	211
7.1.1	Authentifizierung über Beziehungspseudonyme	212
7.1.2	Authentifizierung über anonyme Credentials	213
7.1.3	Sonderfall: Basisdienste	214
7.2	Schutz vor Zugriff unbefugter Dienste	215
7.2.1	Sonderfall: mobil ausgeführte Dienste	218
7.3	Durchführung der Zugriffskontrolle	218
7.3.1	Durchführung durch Dienste	218
7.3.2	Durchführung durch einen Interceptor	219
7.3.3	Diskussion	220
7.4	Realisierung	221
7.4.1	Aspektorientierte Programmierung und AspectJ	221
7.4.2	Aspektorientierte Realisierung des Interceptors	224
7.5	Zusammenfassung	228
8	Werkzeugunterstützung und Demonstratoren	231
8.1	Werkzeugunterstützung im eHome	231
8.1.1	Benutzer	232
8.1.2	Identitäten	233
8.1.3	Dienste	235
8.1.4	Rollen	236
8.2	Werkzeugunterstützung auf dem Handheld	238
8.3	Demonstratoren	243
8.3.1	Der X10-Demonstrator	243
8.3.2	Der Lego-Demonstrator	243
8.3.3	Der eHomeSimulator	245
8.3.4	Der OpenSim/Second-Life-Demonstrator	246
8.3.5	Implementierte Anwendungsbeispiele	249
8.4	Zusammenfassung	250

9 Verwandte Ansätze	251
9.1 Ansätze zur Mobilität	251
9.1.1 Gaia	251
9.1.2 P2PComp	254
9.1.3 JXTA für Virtual Home Environments	256
9.1.4 R-OSGi	257
9.1.5 DIANE	258
9.1.6 DynAMITE	259
9.1.7 Mobile Geräte als Benutzerschnittstelle	260
9.2 Ansätze zur Benutzermodellierung und Personalisierung	260
9.2.1 CUMULATE	260
9.2.2 Personis, Personis-lite und PersonisAD	261
9.2.3 Der UserModelService	263
9.2.4 Weitere Ansätze	265
9.3 Ansätze zur Privatsphäre und Sicherheit	266
9.3.1 Datensparsamkeit	266
9.3.2 Anonymität durch MIXe	270
9.3.3 Sicherheit und Privatsphäre in intelligenten Umgebungen	273
9.3.4 Kooperative Schutzmechanismen	277
9.3.5 Weitere Ansätze	279
10 Schlussbemerkungen	283
10.1 Zusammenfassung	283
10.2 Ausblick	287
10.3 Fazit	288
Ausgewählte Veröffentlichungen	289
Literaturverzeichnis	291
Lebenslauf	317