

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Forschungsfragen	3
1.2	Forschungsmethodik	4
1.3	Kapitelstruktur	7
2	Kollaborative Netzwerke	11
2.1	Grundlegende Konzepte	11
2.2	EU FP7 Forschungsprojekt SPIKE	13
2.2.1	Projektübersicht	14
2.2.2	Technische Bausteine	16
2.2.3	Bewertung	17
2.3	Empirische Studie zu Online-Vertrauen	17
2.3.1	Methodik	18
2.3.2	Zielsetzung	18
2.3.3	Ergebnisse der Umfrage	19
2.3.4	Bewertung	26
3	IT-Sicherheitstechnologien.....	27
3.1	Sicherheitsrisiken in Identitätsföderation	27
3.2	IT-Sicherheit	28
3.3	Schutzziele	29
3.3.1	Schutz der Vertraulichkeit	30
3.3.2	Schutz der Integrität	36
3.3.3	Schutz der Verfügbarkeit	37
4	Identitätsmanagement	39
4.1	Digitales Identitätsmanagement	39
4.1.1	Grundlegende Konzepte	39
4.1.2	Prozesse und Technologien	42
4.1.3	Basismodelle	46
4.1.4	Reifegradmodell	47
4.2	Föderiertes Identitätsmanagement	49
4.2.1	Nutzen von FIdM	51
4.2.2	Komponenten des FIdM	52

4.2.3	FIdM-Technologien	60
4.2.4	Bewertung	67
4.3	Dynamische Identitätsföderationen	69
4.3.1	Herausforderungen von FIdM	70
4.3.2	Dynamik für FIdM	71
5	Vertrauen für Identitätsföderationen	73
5.1	Grundlegende Konzepte	73
5.1.1	Definition von Vertrauen	73
5.1.2	Definition von Reputation	75
5.1.3	Vertrauensbildende Maßnahmen	76
5.1.4	Architekturansätze	77
5.1.5	Berechnungsalgorithmen	79
5.2	Vertrauen und Risiko	80
5.3	Vertrauen und IT-Sicherheit	82
5.4	Vertrauenswürdigkeit digitaler Identitäten	86
5.4.1	Unbeglaubigte Identitäten	86
5.4.2	Beglaubigte Identitäten	87
5.4.3	Identity Assurance	88
5.5	Online-Vertrauensmodelle	94
5.5.1	Prozess des Vertrauensmanagement	95
5.5.2	Systematische Literaturstudie	97
5.5.3	Ausgewählte Online-Vertrauensmodelle	103
6	Vergleich von Online-Vertrauensmodellen	113
6.1	Eingabeparameter zur Vertrauensbildung	113
6.1.1	Harte Eingabeparameter	113
6.1.2	Weiche Eingabeparameter	117
6.1.3	Allgemeine Einflussfaktoren	119
6.1.4	Zusammenfassung	120
6.2	Klassifizierung von Online-Vertrauensmodellen	122
6.2.1	Identitätsvertrauen	122
6.2.2	Verhaltensvertrauen	124
6.3	Vergleich	126
6.3.1	Föderationsspezifische Evaluationskriterien	127
6.3.2	Sicherheitsspezifische Evaluationskriterien	128

6.3.3	Anwendungsspezifische Evaluationskriterien.....	130
6.3.4	Resultate des Vergleichs	131
6.3.5	Zusammenfassung.....	133
7	Ein Referenzmodell für dynamische Identitätsföderationen	135
7.1	Charakteristika.....	135
7.2	Modellelemente	138
7.2.1	Rollenmodell	138
7.2.2	Datenmodell.....	143
7.2.3	Prozessmodell	145
7.3	Vertrauensmodell.....	146
7.3.1	Vertrauensbildende Maßnahmen	146
7.3.2	Wertigkeit vertrauensbildender Maßnahmen.....	152
7.3.3	Richtlinien.....	158
8	DFM-Prozessmodell.....	163
8.1	Präliminarien	163
8.1.1	Prozessübersicht	163
8.1.2	Voraussetzungen.....	165
8.1.3	Formale Grundlagen.....	166
8.2	Phase 1 – Föderationsbasis	167
8.2.1	Initialisierung von Endbenutzern (P1A1)	167
8.2.2	Föderationsbeitritt (P1A2)	169
8.3	Phase 2 – Konfiguration.....	173
8.3.1	Konfiguration von Teilnehmern (P2A1)	173
8.3.2	Registrierung von Web Services (P2A2).....	178
8.4	Phase 3 – Web Service Ermittlung.....	183
8.4.1	Suchanfrage via WAYS-Service (P3A1).....	183
8.4.2	Suchanfrage via eigene Datenbank (P3A2)	186
8.5	Phase 4 – Web Service Initialisierung.....	188
8.5.1	Web Service Selektion (P4A1)	188
8.5.2	Web Service Anfrage evaluieren (P4A2)	191
8.5.3	Provisionierung (P4A3).....	208
8.6	Phase 5 – Transaktion.....	210
8.6.1	Transaktionsereignisse behandeln (P5A1).....	211
8.7	Phase 6 – Nachbereitung.....	212

8.7.1	Bewertung abgeben (P6A1)	213
8.7.2	De-Provisionierung (P6A2)	213
9	Evaluation	215
9.1	Prototyp-Architektur	215
9.1.1	Datenmodell (Model).....	216
9.1.2	Benutzerschnittstelle (View)	218
9.1.3	Applikationslogik (Controller)	219
9.2	Prototypisch implementierte Funktionalitäten.....	220
9.2.1	Interpretation und Transformation von XACML-Richtlinien.....	220
9.2.2	Autorisierung von Web Services	222
9.3	Einordnung in Kriterienkatalog.....	224
10	Schlussfolgerungen	231
10.1	Forschungsergebnisse	232
10.2	Weiterer Forschungsbedarf.....	235