
Contents

1	Introduction	1
1.1	Motivation and Background	1
1.2	Research Questions	3
1.3	Research Methodology	5
1.3.1	IS Research Paradigms	5
1.3.2	Design Science	6
1.3.3	Design Research Process	8
1.4	Research Overview	10
1.5	Chapter Structure	13
1.6	List of Publications	15
I	Fundamentals	17
2	Social Web	19
2.1	Web 2.0	21
2.2	Social Software	22
2.2.1	Characteristics and Existing Challenges	23
2.2.2	The PADGETS Project	24
2.2.2.1	Concept, Methodology, and Platform	24
2.2.2.2	Security and Privacy as a Major Focus	26
2.3	Social Network Sites	27
2.3.1	Defining Social Network Sites	28
2.3.2	Evolution of SNSs in Practice and Research	29
2.3.3	SNS Characteristics	31
2.3.3.1	SNS Architectures	31
2.3.3.2	SNS Stakeholders	33
2.4	SNSs in the Context of this Work	35
3	Privacy	37
3.1	Privacy Paradigms	38
3.1.1	Legal Perspective	39

3.1.2	Technical Perspective	40
3.1.3	Social Perspective	40
3.2	Privacy Adversaries	41
3.2.1	SNS Service Providers	41
3.2.2	SNS Users	42
3.3	Privacy Objectives	42
3.3.1	Awareness	43
3.3.2	Control	44
3.4	Framework for SNS Privacy	44
3.4.1	Privacy Protection Strategies from the Viewpoint of SNS Users	44
3.4.1.1	Privacy Protection Against Other SNS Users	45
3.4.1.2	Privacy Protection Against SNS Service Providers	46
3.4.2	Framing Privacy for this Work	47
4	Identity Management	49
4.1	Digital Identity Management	50
4.1.1	Basic Building Blocks of Identities	50
4.1.2	Identity Models	52
4.1.3	IdM Functions and Technologies	53
4.1.4	IdM Types	55
4.2	Social Identity Management	56
4.2.1	Theoretical Foundations of SIdM	57
4.3	SIdM Concepts on SNSs	59
4.3.1	Identity Management on SNSs	59
4.3.2	Relationship Management on SNSs	62
4.3.3	Access Management on SNSs	65
4.3.4	Context on SNSs	68
II	Requirement Elicitation and Related Work	71
5	Requirements for a Privacy-preserving SIdM Infrastructure	73
5.1	Requirement Elicitation	74
5.1.1	Identity Management Requirements	74
5.1.2	Relationship Management Requirements	75
5.1.3	Access Management Requirements	76
5.1.4	Infrastructural Requirements	77
5.2	Literature Review and Comparison	78
5.2.1	Methodology	78
5.2.1.1	Input	78
5.2.1.2	Processing	79
5.2.1.3	Output	80

5.2.2	Results of the Comparison	80
5.2.2.1	Limitations	80
5.2.2.2	Identity Management Shortcomings	81
5.2.2.3	Relationship Management Shortcomings	81
5.2.2.4	Access Management Shortcomings	82
5.2.2.5	Infrastructural Shortcomings	83
6	Impact of SNS-mediated Communication on SIdM	85
6.1	Visibility Dimensions and Information Sharing Domains	86
6.1.1	Default Information Spreading	87
6.1.2	Active Information Sharing	88
6.1.3	Past Information Availability	88
6.2	Conception and Design of the Study	89
6.2.1	Setup Phase	90
6.2.2	Default Information Spreading Questionnaire	91
6.2.3	Active Information Sharing Questionnaire	92
6.2.4	Past Information Availability Questionnaire	93
6.3	Results of the Study	94
6.3.1	Demographics and Data Statistics	94
6.3.2	Default Information Spreading	95
6.3.3	Active Information Sharing	97
6.3.4	Past Information Availability	99
6.3.5	Discussion of Results	100
III	Proposed Privacy-preserving Social Identity Management Infrastructure	103
7	Privacy-preserving SIdM Fundamentals and Concepts	105
7.1	Information Systems Improvement	106
7.1.1	Theoretical Considerations	106
7.1.2	Principles	107
7.2	Pillars of a PPSIdM Infrastructure	108
7.2.1	Autonomous and User-controlled Environment	109
7.2.2	SIdM Tools	111
7.3	SIdM Process Model	112
7.3.1	Identity Management Process	114
7.3.2	Relationship Management Process	115
7.3.3	Access Management Process	116
7.3.4	Translation Process	116
7.3.5	SNS Integration Process	117

8	Privacy-preserving SIdM Infrastructure	119
8.1	Overview	119
8.2	PPSIdM Provider Characteristics	122
8.2.1	URL-based Identities	122
8.2.2	Contact Authentication and Authorization	123
8.2.3	SNS Integration Concept	125
8.2.4	SNS Integration Workflow	126
8.2.5	Summary	126
8.3	Identity Facet Manager Component	128
8.3.1	Design Principles	128
8.3.2	Status Quo	129
8.3.3	A Generic Model for Social Identity Representation	130
8.3.4	Summary	132
8.4	Assisted Audiences Component	132
8.4.1	Data Analysis Fundamentals	133
8.4.2	Import	136
8.4.3	Clustering	136
8.4.3.1	Relationship-based Assisted Audiences	136
8.4.3.2	Access Policy-based Assisted Audiences	139
8.4.3.3	Combining Both Approaches	141
8.4.4	Manual Refinement	142
8.4.5	Summary	142
8.5	CA-RBAC Component	142
8.5.1	Status Quo	142
8.5.2	Dynamic and Context-aware Access Control	143
8.5.3	Conceptualization of Context on SNSs	145
8.5.4	Defining Contextual Constraints	146
8.5.5	Conceptual Overview of CA-RBAC	147
8.5.6	Example of Sharing of Personal Information using CA-RBAC	149
8.5.7	Summary	150
8.6	Access Policy Visualization Component	150
8.6.1	Status Quo and Current Challenges	151
8.6.2	Theoretical Considerations	152
8.6.3	Information Visualization	153
8.6.4	Access Control Policy Visualization	154
8.6.4.1	Disclosure Browser	155
8.6.4.2	Access Policy Grid	156
8.6.5	Summary	159

9	Prototype	161
9.1	Architectural Overview	162
9.2	User Interface	162
9.3	Components	165
9.3.1	Identity Facet Manager	165
9.3.2	Assisted Audiences	167
9.3.3	CA-RBAC	170
9.3.4	Access Policy Visualization	171
9.3.5	Web Services	174
9.3.6	Browser Plugin	176
IV	Evaluation and Conclusions	179
10	Evaluation	181
10.1	Scenario-based Evaluation	182
10.1.1	Identity Facet and Attribute Management	184
10.1.2	Relationship Management	186
10.1.3	Access Management	188
10.1.4	Translation Phase	191
10.1.4.1	Intra-Identity Facet Review	191
10.1.4.2	Inter-Identity Facet Review	192
10.1.5	Existing SNS Landscape Integration	194
10.1.6	CA-RBAC Evaluation from the Perspective of Contacts	197
10.2	Requirements Framework Comparison	198
11	Conclusions	205
	Appendices	209
A	AX Schema Attribute Types	211
B	OAuth Application Scenario Responses	215
	Bibliography	217