

**Identity Management Systems (IMS):
Identification and Comparison Study**

**Independent Centre for Privacy Protection (ICPP) /
Unabhängiges Landeszentrum für Datenschutz (ULD)
Schleswig-Holstein**

and

Studio Notarile Genghini (SNG)

2003-09-07

Contract N°19960-2002-10 F1ED SEV DE.

CONTENTS

EXECUTIVE SUMMARY	I
PREFACE	VII
ABSTRACT OF CHAPTERS	VIII
ACKNOWLEDGEMENTS	XI
1 [CHAPTER A: DEFINITION OF IDENTITY MANAGEMENT SYSTEMS]	1
1.1 Definition of Identity.....	1
1.1.1 Identity from the Sociological Perspective	1
1.1.2 Identity from the Legal Perspective	7
1.1.3 Identity from the Technical Perspective.....	18
1.2 Definition of Identity Management.....	19
1.2.1 Identity Management from the Sociological Perspective.....	19
1.2.2 Identity Management from the Legal Perspective	20
1.2.3 Identity Management from the Technical Perspective	28
1.3 Definition of Identity Management System	29
1.3.1 IMS from the Sociological Perspective.....	29
1.3.2 IMS from the Legal Perspective	30
1.3.3 IMS from the Technical Perspective.....	30
1.3.4 Multi-purpose Identity Management Application.....	32
1.4 Actors	33
1.4.1 Users	35
1.4.2 Service Providers	36
1.4.3 IMS Providers	37
1.5 Definition of Related Terms.....	37
1.5.1 Definition of Anonymity.....	37
1.5.2 Definition of Pseudonymity / Pseudonym	37
1.5.3 Definition of Unlinkability.....	38
1.6 Summary	39
2 [CHAPTER B: BASIC REQUIREMENTS AND MECHANISMS]	41
2.1 Scenarios for Identity Management	41
2.1.1 General Identity-Related Scenarios.....	41
2.1.2 General Scenarios	44
2.1.3 E-Commerce	49
2.1.4 E-Government, E-Court and E-Democracy	57
2.1.5 E-Health	66
2.1.6 Miscellaneous	68
2.1.7 Conclusion	73
2.2 Main Requirements	75
2.2.1 Functionality	75
2.2.2 Usability	76
2.2.3 Security	77
2.2.4 Privacy	78
2.2.5 Law Enforcement.....	79
2.2.6 Trustworthiness.....	81
2.2.7 Affordability	81
2.2.8 Interoperability.....	81
2.3 Mechanisms	81
2.3.1 Communication-Independent Handling and Representation of Identities.....	83
2.3.2 Pseudonyms with Specific Properties	84
2.3.3 Credentials	87
2.3.4 Identity Recovery.....	89
2.3.5 Interfaces for Communication and Import/Export	89
2.3.6 History Management.....	89
2.3.7 Privacy Control Functionality.....	89
2.3.8 Context Detection	90
2.3.9 Rule Handling	90
2.3.10 Handling of Identities in the Communication	90

2.3.11	Infrastructural Environment Requirements: Anonymous Communication Network and Secure Systems	90
2.3.12	Mechanisms for Trustworthiness	91
2.3.13	IMS Mechanisms with Respect to Co-operating Parties	92
2.4	Summary	94
3	[CHAPTER C: LIST OF EXISTING SYSTEMS]	95
3.1	Criteria	95
3.1.1	Basics	95
3.1.2	Operational Areas	95
3.1.3	Miscellaneous	96
3.2	List of IMA Ordered by Availability and Nations	98
3.3	Alphabetic List of IMA	101
3.4	Summary	103
4	[CHAPTER D: FULL SCALE COMPARISON OF THE MAIN SYSTEMS]	105
4.1	Grid of Attributes	105
4.1.1	Overview	105
4.1.2	Functionality	106
4.1.3	Categories	107
4.1.4	Platform and Environment	111
4.2	Evaluation of Identity Management Applications	112
4.2.1	Mozilla 1.4 Navigator	114
4.2.2	Microsoft .NET Passport	125
4.2.3	Liberty Alliance Project	137
4.2.4	Novell Digitalme	150
4.2.5	Yodlee	160
4.2.6	Microsoft Outlook Express 6 SP1	168
4.2.7	CookieCooker	177
4.2.8	Other Interesting Approaches	188
4.2.9	Summary	198
5	[CHAPTER E: DESIGN OF AN IDENTITY MANAGEMENT SYSTEM]	201
5.1	Basic Architectures	201
5.2	Different Zones of Trust	202
5.3	Identity Handling	203
5.3.1	Centralised vs. Federated Identity	203
5.3.2	Self-Authentication vs. External Authentication	204
5.3.3	Number of Identities per Person	204
5.3.4	Global Identity vs. Partial Identity	204
5.3.5	Transfer of Credentials	204
5.4	A Common System Design: Infomediaries	205
5.5	A Privacy-Enhancing IMS Architecture	205
5.6	Summary	206
6	[CHAPTER F: EU CAPACITY]	207
6.1	EU Capacity	207
6.1.1	Developing the Regulatory Frame	207
6.1.2	Strengthening Leadership in Specific Technologies	208
6.1.3	Cultivating Market Niches	209
6.1.4	Funding	210
6.1.5	Standardising Identity Management	210
6.1.6	Building Infrastructures	212
6.1.7	Gaining Awareness	212
6.1.8	Exporting EU Know-how	212
6.2	Summary	213
7	[CHAPTER G: VISION AND OUTLOOK]	214
7.1	Roadmap	214
7.1.1	RAPID – An Existing Roadmap on Privacy and Identity Management	214
7.1.2	An Approach to an IMS Roadmap	215
7.2	Outlook	222
7.3	Summary	224
8	[CHAPTER H: QUESTIONNAIRE]	227
8.1	Background of the Responding Experts	227

8.2	Estimations on Identity Management.....	231
8.2.1	Applications for Identity Management	231
8.2.2	Essential Functions of an Identity Management System.....	232
8.2.3	Marketability of an Identity Management System	234
8.2.4	Bottlenecks Regarding Mass Adoption of Identity Management Systems	235
8.2.5	Important Aspects of an Identity Management System for Use on a Grand Scale within Society	236
8.2.6	Degree of Centralisation with Respect to the Administration of Personal Data	237
8.2.7	Socio-Psychological Consequences of Usage of an IMS.....	238
8.2.8	Estimated Effect on Law Enforcement	240
8.3	Summary	240
REFERENCES.....		242
GLOSSARY.....		253
ANNEXES.....		255
1	QUESTIONNAIRE	255
1.1	Form Letter and Questionnaire	255
1.2	Results.....	262
1.3	Some Methodically Notes	282
1.3.1	Return Quota.....	282
1.3.2	Methodical Inadequacies and Mistakes.....	283
1.3.3	Generally Remarks on the Questionnaire (V56).....	284
2	RAPID'S ROADMAP ON PRIVACY AND IDENTITY MANAGEMENT	285
2.1	Introduction.....	285
2.2	Research Plan PET in Enterprise (R-PE)	285
2.3	Research Plan PET in Infrastructure (R-PI)	287
2.4	Research Plan Multiple and Dependable Identity Management (R-MIM).....	287
2.5	Research Plan Socio-Economic (R-SE)	288
2.6	Research Plan Legal (R-L).....	289
2.7	Overall Roadmap	289
3	ARTICLE 29 WORKING PARTY COMPARISON	292
4	LEGAL MATERIAL	293
4.1	Electronic Signature	293
4.1.1	Types of the Electronic Signature in Comprehensive Law (Europe)	293
4.1.2	Legal Effects	294
4.1.3	Probative Value.....	295
4.2	Pseudonymity	297
4.2.1	Legal	297
4.2.2	Electronic / Digital Signature.....	297
4.3	Other Legal Material	298

List of figures

Figure 1: Overview over Chapter 1	viii
Figure 2: Chapters influencing Chapter 2	ix
Figure 3: Chapters influencing Chapter 4	ix
Figure 4: Chapters influencing Chapter 5	x
Figure 5: Chapters influencing Chapters 6 and 7	x
Figure 6: The "I" and the "Me"	2
Figure 7: Structuring the "Me" of the Identity	6
Figure 8: Actors within an IMS – an Abstract Model	34
Figure 9: Actors within an IMS – an Abstract Model of an Organisation	34
Figure 10: An IMS Model in More Detail	35
Figure 11: Identity Thief Using Services without Authentication	42
Figure 12: Attack Points of an Identity Thief in a Scenario with Authentication	42
Figure 13: Data Trails When Using Internet Services	43
Figure 14: Typical Logs at Different Parties	44
Figure 15: IMA as a Gateway to the World	45
Figure 16: Identity Protector and Different Pseudo Identity Domains	47
Figure 17: The Identity Protector in an Information System	47
Figure 18: Pseudonym Domains in Assignment of Tasks	48
Figure 19: Pseudonym Domains of a Customer in an E-Shopping Scenario	51
Figure 20: E-Shopping Scenario and Paying with a Credit Card	51
Figure 21: Pseudonym Domains of Customer and Seller in an E-Auction Scenario	53
Figure 22: The Customer in the (E-)Banking Network	56
Figure 23: Pseudonym Domains of a Citizen in an E-Tax Scenario	57
Figure 24: Pseudonym Domains of a Citizen in an Inquiry Scenario	59
Figure 25: Pseudonym Domains of Plaintiff and Defendant in a Civil Action	61
Figure 26: Pseudonym Domains of Accused and Witness in Criminal Proceedings	63
Figure 27: Pseudonym Domains of a Voter in an E-Voting Scenario	65
Figure 28: Pseudonym Domains of a Patient in an E-Health Scenario	67
Figure 29: Pseudonym Domains of Author and Reviewers in a Review Scenario	69
Figure 30: Integration of Notaries as E-Witnesses	71
Figure 31: The TAM Theory	76
Figure 32: Pseudonymity as the Full Range between Identity and Anonymity	85
Figure 33: Pseudonyms With Different Degrees of Cross-Contextual Linkability	86
Figure 34: Data Flow Concerning Credentials in an IMS	88
Figure 35: Form Manager with Choice	114
Figure 36: Password Manager and Possibility of Selecting a User	116
Figure 37: Form Manager – Possibility to Fill in Automatically	117
Figure 38: Encryption When Storing Sensitive Data Activated	120
Figure 39: Overview Evaluation Mozilla Navigator	124
Figure 40: Passport	125
Figure 41: Passport – Profile	129
Figure 42: Passport – Registration	130
Figure 43: Passport – Malfunction if not using Internet Explorer	131
Figure 44: Passport – "Sign me in"	132
Figure 45: Overview Evaluation Passport	136
Figure 46: Federated network identity and circles of trust by Liberty Alliance	137
Figure 47: Liberty Alliance	143
Figure 48: Overview Evaluation Liberty Alliance	149
Figure 49: Digitalme	150
Figure 50: Digitalme – User Can Choose a Situation for the meCard	151
Figure 51: Digitalme – Visit to a Foreign meCard after Retraction of Permission	152
Figure 52: Digitalme – Register	153
Figure 53: Digitalme – VeriSign	155
Figure 54: Digitalme – "Who are you?"	157
Figure 55: Overview Evaluation Digitalme	159
Figure 56: Yodlee – Welcome	160
Figure 57: Yodlee – Accounts	162
Figure 58: Yodlee – Sign In	165
Figure 59: Overview Evaluation Yodlee	167
Figure 60: Outlook Express – Switch of Identities	168

Figure 61: Outlook Express – Management of Identities.....	169
Figure 62: Outlook Express – "Which Identity?".....	170
Figure 63: Outlook Express – "Add New Identity".....	171
Figure 64: Outlook Express – "New Identity".....	173
Figure 65: Overview Evaluation Outlook Express.....	176
Figure 66: CookieCooker – Main Window.....	177
Figure 67: CookieCooker – Web Interface.....	177
Figure 68: CookieCooker – Web Interface: "Identities..."	178
Figure 69: CookieCooker – Cookies and Identities	179
Figure 70: CookieCooker – Configuration.....	180
Figure 71: CookieCooker – "Select Identity!"	181
Figure 72: CookieCooker – Malfunction Understanding	182
Figure 73: CookieCooker – "Delete old Cookies"	184
Figure 74: CookieCooker – JAP Integration.....	186
Figure 75: Overview Evaluation of CookieCooker.....	187
Figure 76: ATUS – Components.....	188
Figure 77: ATUS – Architecture.....	189
Figure 78: ATUS – Snapshot PDA Version.....	189
Figure 79: DRIM – Architecture and Available Components.....	190
Figure 80: DRIM – Internal Structure of the Client	191
Figure 81: DRIM – Creation of Pseudonyms.....	192
Figure 82: Basic Model: IMA \leftarrow Application \leftarrow Digital Services.....	201
Figure 83: Basic Model: Application \leftarrow IMA \leftarrow Digital Services.....	201
Figure 84: Basic Model: IMA in Application \leftarrow Digital Services.....	201
Figure 85: Limited Trusted Zone	202
Figure 86: Enhanced Trusted Zone	202
Figure 87: Architecture of a Privacy-Enhancing IMA.....	205
Figure 88: Comparison EU vs. Non-EU Activities on IMS (from Chapter 3)	207
Figure 89: PIM in RAPID's Vision	215
Figure 90: Roadmap: Market Penetration Techniques	216
Figure 91: Roadmap: Market Penetration of IMS.....	218
Figure 92: Roadmap: Maturity of Concepts and Applications for IMS	221
Figure 93: Institutional Background of Responding Experts	227
Figure 94: Positions of Responding Experts in Their Organisation.....	228
Figure 95: Cultural Background of Responding Experts	229
Figure 96: Interests of Responding Experts	230
Figure 97: Marketability of IMS	235
Figure 98: Important Aspects of an IMS.....	237
Figure 99: Effects of IMS on Law Enforcement Respectively Prosecution of Claim.....	240

List of tables

Table 1: Requirements in the General IMS Scenario	46
Table 2: Requirements of the Processing of Orders Scenario	49
Table 3: Requirements of the E-Shopping Scenario	52
Table 4: Requirements of the E-Auction Scenario	54
Table 5: Requirements of the E-Banking Scenario	56
Table 6: Requirements of the E-Tax Scenario	58
Table 7: Properties with Respect to Extract from the Register	59
Table 8: Properties with Respect to Freedom of Information	59
Table 9: Properties with Respect to Access according to Data Protection Acts	59
Table 10: Requirements of the Inquiry Scenario	60
Table 11: Requirements of the Civil Action Scenario	62
Table 12: Requirements of the Criminal Proceedings Scenario	64
Table 13: Requirements of the E-Voting Scenario	65
Table 14: Requirements of the E-Health Scenario	68
Table 15: Requirements of the Review Scenario	69
Table 16: Requirements of the E-Witness Scenario	72
Table 17: Summarisation of Requirements of Scenarios	73
Table 18: IMS Mechanisms with Respect to Requirements	82
Table 19: Technology-based IMS Mechanisms with Respect to Co-operating Parties	93
Table 20: Basic Criteria	95
Table 21: Criteria Operational Areas	96
Table 22: Miscellaneous Criteria	96
Table 23: List of Identity Management Applications Ordered by Availability and Nations	98
Table 24: List of Existing Identity Management Applications	101
Table 25: Description of Functionality	105
Table 26: Description of Categories	105
Table 27: Description of Platform and Environment	106
Table 28: Compared Identity Management Applications and General Functionalities	112
Table 29: Further interesting Approaches of Identity Management Applications	112
Table 30: Comparison of Identity Management Applications	198
Table 31: Prediction PC Mass Storage	220
Table 32: Prediction Computer	220
Table 33: Potential Main Bottleneck Regarding Mass Adaption of IMS	235
Table 34: V1 – How Many Years Dealing with IMS	262
Table 35: V2 – Employees in Organisation	262
Table 36: V3 – Organisation and IMS	263
Table 37: V4 – Other Organisation	263
Table 38: V5 – Position in Organisation	263
Table 39: V6 – Other Position	264
Table 40: V7 – Do You Already Use an IMS?	264
Table 41: V8 – For Which Application?	264
Table 42: V9 – With Which Product?	265
Table 43: V10 – Interests in IMS ... Range of Functions	265
Table 44: V11 – Interests in IMS ... Usability	265
Table 45: V12 – Interests in IMS ... Privacy Protection	266
Table 46: V13 – Interests in IMS ... Security	266
Table 47: V14 – Interests in IMS ... Marketability	266
Table 48: V15 – Interests in IMS ... Politically Pushing Through	266
Table 49: V16 – Interests in IMS ... Politically Preventing it	266
Table 50: V17 – Interests in IMS ... Implementing Law	267
Table 51: V18 – Interests in IMS ... Social Impacts of Implementation / Use	267
Table 52: V19 – Interests in IMS ... Potential Psychological Consequences	267
Table 53: V20 – Interests in IMS ... Law Enforcement	267
Table 54: V21 – Interests in IMS ... Access Right Management	267
Table 55: V22 – Interests in IMS ... Multiple Application Usage	268
Table 56: V23 – Interests in IMS ... Another Important Category	268
Table 57: V24 – Interests in IMS ... Another Important Category	268
Table 58: V25 – Cultural Background	268
Table 59: V26 – IMS – State-of-the-Art	269
Table 60: V27 – IMS – Essential Functions	269

Table 61: V28 – IMS – Marketability	271
Table 62: V29 – IMS – Marketability in 10 Years.....	271
Table 63: V30 – How Long Will it Take for a Society-Wide Implementation of a Multi-Purpose IMS?.....	271
Table 64: V31 – IMS – Important for Use in Society – Range of Functions	271
Table 65: V32 – IMS – Important for Use in Society – Multi-Purpose Usage	272
Table 66: V33 – IMS – Important for Use in Society – Usability.....	272
Table 67: V34 – IMS – Important for Use in Society – Privacy Protection.....	272
Table 68: V35 – IMS – Important for Use in Society – Security	272
Table 69: V36 – IMS – Important for Use in Society – Cost.....	272
Table 70: V37 – IMS – Important for Use in Society – Controllability for Users	273
Table 71: V38 – IMS – Important for Use in Society – Controllability for Government	273
Table 72: V39 – IMS – Important for Use in Society – Tracing of Law Enforcement	273
Table 73: V40 – IMS – Important for Use in Society – Other Category.....	273
Table 74: V41 – IMS – Important for Use in Society – Specified Category.....	273
Table 75: V42 – Administration of Data.....	274
Table 76: V43 – Administration of Data – Some Comments.....	274
Table 77: V44 – Psychological Consequences.....	274
Table 78: V45 – Specified Psychological Consequences.....	275
Table 79: V46 – IMS – Improve or Worsen – Liability	276
Table 80: V47 – IMS Improve or Worsen – Crime Prosecution	276
Table 81: V48 – IMS Improve or Worsen – Clarification of Facts.....	276
Table 82: V49 – IMS Improve or Worsen – Value of Admissible Evidence	276
Table 83: V50 – IMS Improve or Worsen – Other	277
Table 84: V51 – IMS Improve or Worsen – Specified Other	277
Table 85: V52 – IMS – Bottleneck	277
Table 86: V53 – IMS – Bottleneck, Other	278
Table 87: V54 – Visionary IMS Texts	278
Table 88: V55 – Published IMS Texts	279
Table 89: V56 – Commentary	281
Table 90: V57 – Answers.....	282
Table 91: V58 – Syntax.....	282
Table 92: V59 – Reminder	282
Table 93: Return Quota	282
Table 94: Research Cluster PET in Enterprise	285
Table 95: Research Cluster PET in Infrastructure.....	287
Table 96: Research Cluster Multiple and Dependable Identity Management	287
Table 97: Research Cluster Socio-Economic PIM.....	288
Table 98: Research Cluster Legal Aspects PIM.....	289
Table 99: Selection of the Essential and Important Technology Business RTD for PIM	290
Table 100: RAPID Roadmap	291
Table 101: Comparison of the Presently Existing On-line Authentication Systems	292