
Table of Contents

Foreword	xi
Preface	xv
1. Introduction	1
Business Opportunity	2
Digital Identity Matters	3
Using Digital Identity	3
The Business Context of Identity	5
Foundational Technologies for Digital Identity	6
Identity Management Architectures	6
2. Defining Digital Identity	8
The Language of Digital Identity	8
Identity Scenarios in the Physical World	10
Identity, Security, and Privacy	11
Digital Identity Perspectives	12
Identity Powershifts	13
Conclusion	14
3. Trust	15
What Is Trust?	16
Trust and Evidence	17
Trust and Risk	18
Reputation and Trust Communities	19
Conclusion	20

4. Privacy and Identity	21
Who's Afraid of RFID?	21
Privacy Pragmatism	22
Privacy Drivers	23
Privacy Audits	24
Privacy Policy Capitalism	25
Anonymity and Pseudonymity	26
Privacy Principles	27
Prerequisites	28
Conclusion	28
5. The Digital Identity Lifecycle	29
Provisioning	30
Propagating	30
Using	31
Maintaining	31
Deprovisioning	32
Conclusion	32
6. Integrity, Non-Repudiation, and Confidentiality	33
Integrity	33
Non-Repudiation	33
Confidentiality	34
Conclusion	48
7. Authentication	50
Authentication and Trust	50
Authentication Systems	51
Authentication System Properties	59
Conclusion	62
8. Access Control	63
Policy First	63
Authorization Patterns	66
Abstract Authorization Architectures	71
Digital Certificates and Access Control	72
Conclusion	72

9. Names and Directories	73
Utah.gov: Naming and Directories	73
Naming	75
Directories	78
Aggregating Directory Information	84
Conclusion	88
10. Digital Rights Management	89
Digital Leakage	89
The DRM Battle	90
Apple iTunes: A Case Study in DRM	91
Features of DRM	91
DRM Reference Architecture	92
Trusted Computing Platforms	94
Specifying Rights	95
Conclusion	97
11. Interoperability Standards	98
Standards and the Digital Identity Lifecycle	98
Integrity and Non-Repudiation: XML Signature	99
Confidentiality: XML Encryption	101
Authentication and Authorization Assertions	102
Example SAML Use Cases	104
Identity Provisioning	107
Representing and Managing Authorization Policies	111
Conclusion	117
12. Federating Identity	118
Centralized Versus Federated Identity	118
The Mirage of Centralized Efficiency	119
Network Effects and Digital Identity Management	120
Federation in the Credit Card Industry	121
Benefits of Federated Identity	121
Digital Identity Standards	122
Three Federation Patterns	125
Conclusion	132

13. An Architecture for Digital Identity	133
Identity Management Architecture	134
The Benefits of an Identity Management Architecture	135
Success Factors	137
Roadblocks	138
Identity Management Architecture Components	140
Conclusion	141
14. Governance and Business Modeling	142
IMA Lifecycle	143
IMA Governance Model	145
Initial Steps	147
Creating a Vision	147
IMA Governing Roles	148
Resources	152
What to Outsource	153
Understanding the Business Context	154
Business Function Matrix	155
IMA Principles	157
Conclusion	160
15. Identity Maturity Models and Process Architectures	161
Maturity Levels	162
The Maturity Model	162
The Rights Steps at the Right Time	166
Finding Identity Processes	167
Evaluating Processes	167
A Practical Action Plan	169
Filling the Gaps with Best Practices	170
Conclusion	171
16. Identity Data Architectures	172
Build a Data Architecture	173
Processes Link Identities	174
Data Categorization	177
Identity Data Structure and Metadata	181
Exchanging Identity Data	183
Principles for Identity Data	185
Conclusion	186

17. Interoperability Frameworks for Identity	187
Principles of a Good IF	187
Contents of an Identity IF	188
Example Interoperability Framework	191
A Word of Warning	192
Conclusion	193
18. Identity Policies	194
The Policy Stack	194
Attributes of a Good Identity Policy	195
Determining Policy Needs	197
Writing Identity Policies	199
An Identity Policy Suite	201
Assessing Identity Policies	208
Enforcement	209
Procedures	210
Conclusion	210
19. Identity Management Reference Architectures	211
Reference Architectures	211
Benefits and Pitfalls	212
Reference Architecture Best Practices	213
Using a Reference Architecture	214
Components of a Reference Architecture	214
Technical Position Statements	214
Consolidated Infrastructure Blueprint	217
System Reference Architectures	218
Conclusion	220
20. Building an Identity Management Architecture	221
Scoping the Process	221
Which Projects Are Enterprise Projects?	222
Sequencing the IMA Effort	223
A Piece at a Time	224
Conclusion: Dispelling IMA Myths	225
Index	227