

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Reading Instructions . . . . .	1
1.2	Background . . . . .	2
1.3	Motivation . . . . .	2
1.4	Objective, Outline, and Contributions . . . . .	3
<b>2</b>	<b>Public Key Infrastructures</b>	<b>7</b>
2.1	Cryptology . . . . .	8
2.1.1	Secret Key Cryptography . . . . .	8
2.1.2	Public Key Cryptography . . . . .	9
2.1.3	Security and Performance . . . . .	10
2.1.4	Further Reading . . . . .	13
2.2	PKI Basics . . . . .	14
2.2.1	PKI Goals and Techniques . . . . .	14
2.2.2	PKI Terms and Components . . . . .	17
2.2.3	PKI Benefits . . . . .	23
2.2.4	Further Reading . . . . .	24
2.3	PKI Structures . . . . .	24
2.3.1	PKI Trust Models . . . . .	25
2.3.2	PKI Connection Methods . . . . .	28
2.3.3	Virtual Hosting . . . . .	31
2.3.4	Further Reading . . . . .	31
2.4	PKI Related Standards . . . . .	31

2.4.1	ISO and IEC . . . . .	31
2.4.2	ITU-T . . . . .	32
2.4.3	IETF . . . . .	33
2.4.4	ETSI . . . . .	36
2.4.5	RSA Laboratories . . . . .	37
2.4.6	T7 e.V. and TeleTrusT . . . . .	38
2.5	Digital Signatures and Law . . . . .	39
2.5.1	The European Directive 1999/93/EC . . . . .	40
2.5.2	National Law . . . . .	42
2.5.3	National Root CAs . . . . .	42
<b>3</b>	<b>Secure Private Key Management</b>	<b>45</b>
3.1	Problem Exposition . . . . .	46
3.1.1	Opening . . . . .	46
3.1.2	Problem, Scope, and Approach . . . . .	46
3.1.3	Related Work . . . . .	47
3.2	Security Levels and Responsibilities . . . . .	48
3.2.1	Security Level, Context, and Measures . . . . .	48
3.2.2	Own and Foreign Private Keys . . . . .	49
3.2.3	Accessing Private Keys . . . . .	50
3.2.4	Tasks and Responsibilities . . . . .	50
3.3	The Private Key Life Cycle Reference Model . . . . .	51
3.3.1	Specification . . . . .	51
3.3.2	Analysis and Use . . . . .	57
3.4	The Key Authority . . . . .	60
3.4.1	The Private Key Security Dilemma . . . . .	60
3.4.2	Specification . . . . .	61
3.4.3	Analysis and Use . . . . .	62

<b>4</b>	<b>Adaptable Software</b>	<b>67</b>
4.1	Problem Exposition . . . . .	68
4.1.1	Opening . . . . .	68
4.1.2	Problem, Scope, and Approach . . . . .	70
4.1.3	Related Work . . . . .	70
4.2	Software Requirements and Adaptability . . . . .	73
4.2.1	Abilities and Ilities . . . . .	73
4.2.2	Software Consumers and Producers . . . . .	74
4.2.3	Explicit and Implicit Ilities . . . . .	74
4.2.4	Application and Code Ilities . . . . .	75
4.2.5	Flexibility and Adaptability . . . . .	77
4.3	Ilities . . . . .	78
4.3.1	TC Ilities . . . . .	78
4.3.2	Adaptability Code Ilities . . . . .	88
4.4	The Workshop . . . . .	91
4.4.1	Specification . . . . .	91
4.4.2	Analysis and Use . . . . .	95
<b>5</b>	<b>FT-KA Implementation</b>	<b>101</b>
5.1	The FlexiTRUST Key Authority . . . . .	102
5.2	Approach . . . . .	104
5.2.1	Guidelines . . . . .	104
5.2.2	Third-Party Technology . . . . .	104
5.3	Realization . . . . .	106
5.3.1	EJB Types . . . . .	106
5.3.2	Interactions . . . . .	107
5.3.3	Components . . . . .	108
5.3.4	J2EE Tiers . . . . .	109
5.4	Internals . . . . .	110
5.4.1	Local and Remote Interfaces . . . . .	110
5.4.2	Data Persistence . . . . .	111

5.4.3	Data Access . . . . .	112
5.4.4	Data Format . . . . .	113
5.4.5	Data Input and Output . . . . .	114
5.4.6	JNDI Lookup . . . . .	115
5.5	Other Versions . . . . .	116
5.5.1	Plain Old Java Objects . . . . .	116
5.5.2	Jini . . . . .	116
5.5.3	Shared JVM with Activation . . . . .	116
5.5.4	Compatibility . . . . .	117
<b>6</b>	<b>FT-KA Security</b>	<b>119</b>
6.1	Security Requirements and Context . . . . .	120
6.2	Users, Attackers, and Threats . . . . .	121
6.2.1	FT-KA Roles . . . . .	121
6.2.2	OS Accounts . . . . .	121
6.2.3	Attackers . . . . .	122
6.2.4	Threats . . . . .	122
6.3	Security Goals . . . . .	123
6.3.1	Audit . . . . .	123
6.3.2	Authentication . . . . .	123
6.3.3	Security Enforcement . . . . .	124
6.3.4	Data Protection . . . . .	125
6.4	Security Functions . . . . .	126
6.4.1	Security Architecture . . . . .	126
6.4.2	Module I/O . . . . .	128
6.4.3	Module Logging . . . . .	129
6.4.4	Module Certification . . . . .	129
6.4.5	Module Revocation . . . . .	131
6.4.6	Module Chip Card Access . . . . .	133
6.4.7	Module Secret Sharing . . . . .	133
6.4.8	Module LDAP Access . . . . .	133

6.5	Mapping . . . . .	134
6.6	Private Keys and KA Rules . . . . .	135
6.6.1	Internal PKI . . . . .	135
6.6.2	External PKI . . . . .	136
<b>7</b>	<b>FT-KA Adaptability</b>	<b>139</b>
7.1	The FlexiTRUST TC Software . . . . .	139
7.1.1	The FlexiTRUST Architecture . . . . .	140
7.1.2	The FlexiTRUST Authorities . . . . .	140
7.2	Study: Real World FT-KAs . . . . .	142
7.2.1	JLU . . . . .	143
7.2.2	RBG . . . . .	143
7.2.3	DGN . . . . .	144
7.2.4	ARCOR . . . . .	145
7.2.5	Comparison . . . . .	145
7.3	Further FT-KA Installations . . . . .	147
<b>8</b>	<b>Conclusion</b>	<b>149</b>
8.1	Secure Private Key Management . . . . .	149
8.2	Adaptable Software . . . . .	150
8.3	FT-KA Implementation . . . . .	151
8.4	FT-KA Security . . . . .	153
8.5	FT-KA Adaptability . . . . .	154
<b>A</b>	<b>Source Code</b>	<b>157</b>
<b>B</b>	<b>Security Requirements</b>	<b>165</b>
	<b>Acronyms</b>	<b>171</b>
	<b>Websites</b>	<b>179</b>
	<b>Bibliography</b>	<b>187</b>
	<b>Index</b>	<b>207</b>