
Contents

1	Introduction	1
1.1	Elections and Electronic Voting	1
1.2	Motivation	4
1.3	Contribution, Methodology, and Structure	5

Part I Fundamentals

2	Implementations of Electronic Voting	13
2.1	Classification of Election Forms	13
2.1.1	Dimensions	13
2.1.2	Categories of Election Forms	14
2.1.3	Multiple Channel Elections	19
2.2	Paper-Based Elections versus Electronic Voting	19
2.3	Examples of Electronic Voting Machines	21
2.3.1	Direct Recording Electronic Voting Machines	21
2.3.2	Digital Election Pen	22
2.4	Overview of Remote Electronic Voting	23
2.4.1	Authentication Techniques	25
2.4.2	Techniques to Ensure the Secrecy of the Vote	27
2.4.3	Client-Side Voting Software	32
2.5	Summary	34
3	Related Work – A Landscape of Requirement Catalogues	37
3.1	Regulations for Electronic Voting Machines	38
3.1.1	German Federal Ordinance for Voting Machines	38
3.1.2	Election Law of the Free and Hanseatic City of Hamburg (Germany)	39
3.1.3	American Election Regulations	40

3.2	Requirements for Remote Electronic Voting	42
3.2.1	Council of Europe Recommendations	42
3.2.2	Online-Voting System Requirements for Non-parliamentary Elections	44
3.2.3	Catalogue of the Gesellschaft für Informatik	45
3.2.4	Swiss Election Law	47
3.2.5	Austrian Election Regulations.....	48
3.2.6	Network Voting System Standards	49
3.3	Scientific Papers.....	50
3.4	Result of the Analysis.....	55
3.5	Summary.....	56

Part II Requirements

4	Process and Framework Description	61
4.1	Description of the Procedure	61
4.2	Election Principles.....	65
4.3	Threats	67
4.4	Syntax and Semantics.....	67
4.5	Beyond the Scope	69
4.6	Summary.....	71
5	Requirements for Electronic Voting Machines.....	73
5.1	Citation and Additional Notations	73
5.2	Target of Evaluation	74
5.3	Security Requirements	75
5.3.1	Security Requirements for the Polling Phase	75
5.3.2	Security Requirements for the Tallying Phase	77
5.4	Functional Requirements	79
5.4.1	Functional Requirements for the Polling Phase	79
5.4.2	Functional Requirements for the Tallying Phase	83
5.4.3	Functional Requirements for the Audit System	83
5.5	Assurance Requirements.....	84
5.6	Additional Requirements	86
5.6.1	Usability Requirements	86
5.6.2	Operational Requirements	87
5.7	Summary.....	90
6	Requirements for Remote Electronic Voting	93
6.1	Citation and Additional Notations	93
6.2	Target of Evaluation	94
6.3	Security Requirements	96
6.3.1	Security Requirements for the Polling Phase	96
6.3.2	Security Requirements for the Tallying Phase	100

6.4	Functional Requirements	101
6.4.1	Functional Requirements for the Polling Phase	101
6.4.2	Functional Requirements for the Tallying Phase	105
6.4.3	Functional Requirements for the Audit System	106
6.5	Assurance Requirements	107
6.6	Additional Requirements	109
6.6.1	Usability Requirements	109
6.6.2	Operational Requirements	110
6.7	Summary	113

Part III Evaluation

7	Evaluation Methodology	117
7.1	Common Criteria Introduction	118
7.2	Discussion of Possible Trust Models	127
7.2.1	Trustworthy Vote Casting Device	128
7.2.2	Compromising Encryptions	133
7.3	Evaluation Assurance Level According to the Requirements ..	135
7.4	Formal IT Security Model	138
7.4.1	General Introduction	139
7.4.2	Application of Available IT Security Models for Elections	141
7.4.3	Selection of Security Objectives	141
7.4.4	Formal IT Security Model for Remote Electronic Voting	142
7.5	Summary	146
8	Core Protection Profile	149
8.1	Background, History, Motivation, and Discussions	150
8.2	The GI/BSI/DFKI Protection Profile	153
8.2.1	Introduction/TOE Overview	153
8.2.2	Conformance Claims	154
8.2.3	Security Problem Definition	156
8.2.4	Security Objectives and Functional Requirements	162
8.2.5	Security Assurance Requirements	163
8.3	Comparison, Open Points, and Suggestions for Improvements .	164
8.3.1	Introduction/TOE Overview	165
8.3.2	Conformance Claims	166
8.3.3	Security Problem Definition	166
8.3.4	Security Objectives and Functional Requirements	173
8.3.5	Security Assurance Requirements	173
8.4	Summary	173

Part IV Application

9	Proof of Concept	177
9.1	Procedure Specification	177
9.2	The Estonian System	178
9.2.1	System Description	179
9.2.2	System Analysis	182
9.3	The POLYAS System	184
9.3.1	System Description	185
9.3.2	System Analysis	190
9.4	Summary	190
10	Separation of Duty Principle	195
10.1	Motivation	196
10.2	'k-resilience' Approach	199
10.3	Summary	201
11	Future Work - Open Issues	203

Part V Conclusion

12	Summary and Concluding Words	209
-----------	-------------------------------------	-----

Part VI Appendix

A	List of Acronyms	217
B	Links	219
B.1	Electronic Voting Systems	219
B.2	Electronic Voting Antagonists	220
C	Glossary	221
C.1	Election Terminology	221
C.2	Electronic Voting Specific Terms	222
C.3	Phases of the Election	223
C.4	Participants	225
C.5	Devices and Components	225
C.6	Assessing Terminology	226
C.7	Mapping: PP Glossary – Book Glossary	227
D	Removed Requirements	229
E	Protection Profile Structure	235
	References	237

Evaluation of Electronic Voting
Requirements and Evaluation Procedures to Support
Responsible Election Authorities

Volkamer, M.

2009, XIV, 248 p., Softcover

ISBN: 978-3-642-01661-5