

Inhaltsverzeichnis

Vorwort	5
Inhaltsverzeichnis	9
Abbildungsverzeichnis	13
Tabellenverzeichnis	13
1 Einleitung	15
2 Die Methode KORA	19
2.1 Vorgehensweise bei der Konkretisierung	20
2.2 Internetwahlszenarien, KORA und Referenzmodell	22
3 Konkretisierung rechtlicher Anforderungen für Internetwahlen: Referenzmodell	25
3.1 Rechtliche Vorgaben	25
3.1.1 Allgemeine Wahl	25
3.1.2 Unmittelbare Wahl	26
3.1.3 Freie Wahl	26
3.1.4 Geheime Wahl	27
3.1.5 Gleiche Wahl	28
3.1.6 Öffentliche Wahl	28
3.1.7 Informationelle Selbstbestimmung	29
3.1.8 Fernmeldegeheimnis	29
3.2 Schritt 1: Rechtliche Anforderungen	30
3.2.1 Soziale Funktion der rechtlichen Vorgaben, Chancen und Risiken	30
3.2.2 Selbstbestimmung (A1)	36
3.2.3 Gleichwertigkeit (A2)	37
3.2.4 Unbestimbarkeit (A3)	37
3.2.5 Laienkontrolle (A4)	38
3.2.6 Datenschutz (A5)	38

3.3	Schritt 2: Rechtliche Kriterien	39
3.3.1	Nutzbarkeit (K1)	39
3.3.2	Erreichbarkeit (K2)	40
3.3.3	Stimmengleichheit (K3)	40
3.3.4	Neutralität (K4)	41
3.3.5	Unerkennbarkeit (K5)	41
3.3.6	Unverknüpfbarkeit (K6)	41
3.3.7	Individualkontrolle (K7)	42
3.3.8	Publikumskontrolle (K8)	43
3.3.9	Datensparsamkeit (K9)	43
3.3.10	Datentransparenz (K10)	43
3.3.11	Zweckbindung (K11)	44
3.3.12	Datenbeherrschbarkeit (K12)	44
3.3.13	Sicherung (K13)	45
3.4	Schritt 3: Technische Gestaltungsziele	47
3.4.1	Umgang mit den Wahldaten	50
3.4.2	Leitung der Wahl	54
3.4.3	Anmeldung des Wählers	58
3.4.4	Stimmabgabe	60
3.4.5	Ergebnisermittlung	65
3.4.6	Wahlnachbereitung	68
3.5	Schritt 4: Technische Gestaltungsvorschläge	71
3.5.1	Umgang mit den Wahldaten	79
3.5.2	Leitung der Wahl	88
3.5.3	Anmeldung des Wählers	95
3.5.4	Stimmabgabe	97
3.5.5	Ergebnisermittlung	107
3.5.6	Wahlnachbereitung	110
4	Geltung der rechtlichen Anforderungen für unterschiedliche Wahlszenarien	113
4.1	Wahlanwendungstypen	113
4.1.1	Parlamentarische Wahlen	113
4.1.2	Wahlen zu Organen der funktionalen Selbstverwaltung	115
4.1.3	Wahlen zu arbeitsrechtlichen Interessenvertretungen	124
4.1.4	Wahlen in privaten Körperschaften	127
4.2	Wahlform	132
4.3	Wahlrelevanz	134
4.3.1	Obligatorische Internetwahl	134
4.3.2	Fakultative Internetwahl	134
4.3.3	Begrenzt fakultative Internetwahl	134

4.4 Beispielszenario – Sozialversicherungswahlen als fakultative Brief- und Internetfernwahl	135
5 KORA und die Common Criteria 137	
5.1 Die Common Criteria	138
5.2 Verknüpfung von KORA und Common Criteria	139
5.3 Anwendungsbeispiel geheime Wahl	141
5.4 Zusammenfassung	143
6 Vertrauensumgebung der Internetwahl 145	
6.1 Vertrauenswürdigkeitsstufen nach Common Criteria	145
6.2 Angriffspotential nach Common Evaluation Methodology	147
6.3 Wert der bedrohten Rechtsgüter	151
6.4 Zuordnung von Vertrauenswürdigkeitsstufen zu Wahlwendungstypen	152
6.4.1 Parlamentarische Wahlen	152
6.4.2 Wahlen in der funktionalen Selbstverwaltung	156
6.4.3 Wahlen zur arbeitsrechtlichen Interessenvertretungen	160
6.4.4 Wahlen in privaten Körperschaften	162
7 Formale Modellierung 165	
7.1 Erläuterung des Modellierungsgegenstandes	165
7.2 Formale Grundlagen	168
7.3 Formale Modellierung der verbindlichen Stimmabgabe	178
7.3.1 Sichere Systemzustände für die verbindliche Stimmabgabe	179
7.3.2 Erlaubte Zustandsübergänge für die verbindliche Stimmabgabe	180
7.3.3 Sicherheitstheorem für die verbindliche Stimmabgabe	181
7.4 Formale Modellierung von Abbruch und Korrektur der Stimmabgabe	182
7.4.1 Erlaubte Zustandsübergänge für Abbruch und Korrektur der Stimmabgabe	183
7.4.2 Sicherheitstheorem für Abbruch und Korrektur der Stimmabgabe	188
7.5 Formale Modellierung von Quittungsfreiheit	191
7.5.1 Sichere Systemzustände für die Quittungsfreiheit	192
7.5.2 Erlaubte Zustandsübergänge für die Quittungsfreiheit	193
7.5.3 Sicherheitstheorem für die Quittungsfreiheit	195

7.6	Formale Modellierung von Verifizierbarkeit	195
7.6.1	Die Verifizierbarkeit und ihr Aufruf	196
7.6.2	Sichere Systemzustände, erlaubte Zustandsübergänge und Sicherheitstheorem für die Verifizierbarkeit	198
7.7	Zusammenführung der formalen Teilmodelle	199
7.7.1	Sichere Systemzustände	199
7.7.2	Erlaubte Zustandsübergänge	199
7.7.3.	Sicherheitstheorem	201
8	Zusammenfassung und Ausblick	205
Abkürzungsverzeichnis		207
Literaturverzeichnis		211