Elektronische Wahlen: Verifizierung vs. Zertifizierung

Melanie Volkamer[1], Guido Schryen[2], Lucie Langer[1], Axel Schmidt[1], Johannes Buchmann[1]

[1]CASED
Technische Universität Darmstadt
volkamer@cased.de
langer,axel,buchmann@cdc.informatik.tu-darmstadt.de

[2]International Computer Science Institute, Berkeley
schryen@winfor.rwth-aachen.de

Abstract: Der Beitrag diskutiert die kontroversen Ansätze – Verifizierung versus Evaluation/Zertifizierung – zur Sicherung elektronischer Wahlen mit Wahlgeräten. Dabei spielt das Urteils des Bundesverfassungsgerichts [BVG099] eine zentrale Rolle. Hierin wird entschieden, dass die Zertifizierung des Wahlgerätes nicht ausreicht und es werden Verifizierungsfunktionen gefordert, die den Wählern die Möglichkeit geben sich von der Integrität des Wahlergebnisses zu überzeugen. Der Beitrag zeigt auf, dass auch mit der Implementierung entsprechender Verifizierungsfunktionen nicht auf Zertifizierung verzichtet werden kann, da an ein Wahlgerät auch andere Anforderungen wie etwa hinsichtlich des Wahlgeheimnisses gestellt werden. Es wird außerdem die Frage diskutiert, warum der Zertifizierung hinsichtlich dieser zusätzlichen Anforderungen vertraut werden kann, während dies nicht der Fall bei der Integritätsanforderung ist.

1 Einleitung

Elektronische Wahlgeräte werden in einigen Ländern schon seit mehreren Jahrzehnten eingesetzt. In Deutschland können sie bereits seit 1999 bei Bundestags- und Europaratswahlen sowie bei einigen Kommunal- und Landtagswahlen eingesetzt werden. Bei der Bundestagswahl 2005 waren immerhin 2100 der 80000 Wahllokale mit den Geräten ausgestattet. Die wichtige Voraussetzung für den Einsatz dieser Geräte ist Transparenz und Vertrauen. Dabei werden in der Vergangenheit zwei Ansätze kontrovers diskutiert: Während die einen Verifizierbarkeit für den Wähler und die Öffentlichkeit für die einzige Möglichkeit halten, sichere elektronische Wahlen durchzuführen, gilt dies für die anderen nur dann, wenn das Wahlgerät positiv evaluiert und zertifiziert ist, also nachgewiesen ist, dass es die gewünschten Eigenschaften hat. Der Begriff der Verifizierung ist nicht mit den Begriffen Verifikation zu verwechseln. Bei letzteren handelt es sich um Techniken, die zur Evaluation eingesetzt werden können, um Eigenschaften eines Systems formal nachzuweisen.

Dabei wird jeweils begründet, warum die jeweils andere Technik nicht benötigt wird. So wird beispielsweise in [VK06] argumentiert, dass es sich bei Verifizierungsfunktionen in der Regel um misstrauensbildende Maßnahmen handelt. Auch rechtlich herrschte fast zehn Jahre lang die Auffassung, dass eine Evaluierung und Zertifizierung der eingesetzten Wahlgeräte ausreichend ist [BWGV99].

Im Urteil des Bundesverfassungsgerichts [BVG09] vom 3. März 2009 entschied nun aber der Zweite Senat, dass die bisher eingesetzten elektronischen Wahlgeräte sowie die Bundeswahlgeräteverordnung [BWahlGV] verfassungswidrig sei, da keine Verifizierbarkeit für den Wähler bzw. die Öffentlichkeit implementiert wird und daher der Grundsatz der Öffentlichkeit der Wahl verletzt ist. Im Urteil wird begründet, dass diese Öffentlichkeit „eine wesentliche Voraussetzung für begründetes Vertrauen der Bürger in den korrekten Ablauf der Wahl“ [BVG09 Absatz 106] schafft. Insbesondere wird festgelegt, dass der Wähler „nicht darauf verwiesen werden [darf], nach der elektronischen Stimmabgabe alleine auf die technische Integrität des Systems zu vertrauen“ [BVG09 Absatz 120]. Weiter legt das Urteil fest, dass die Maßnahmen zur geforderten öffentlichen Kontrolle „nicht dadurch ausgeglichen werden [kann], dass Mustergeräte im Rahmen des Verfahrens der Bauartzulassung [..] auf ihre Übereinstimmung mit bestimmten Sicherheitsanforderungen und auf ihre technische Unversehrtheit hin überprüft werden“ [BVG09 Absatz 123].

Motiviert durch die Aussage des Urteils, dass eine Zertifizierung der Wahlgeräte für parlamentarische Wahlen nicht ausreicht und Verifizierungsfunktionen gefordert werden, diskutiert dieser Artikel Möglichkeiten, beide Ansätze zu kombinieren. Der Fokus liegt dabei auf unvernetzten Wahlgeräten, die im Wahllokal für parlamentarische Wahlen zum Einsatz kommen sollen. Um die beiden Ansätze – Evaluation/Zertifizierung und Verifizierung - im Laufe des Beitrages gegenüberstellen und später verbinden zu können, werden im zweiten Kapitel beide Ansätze definiert. Das dritte Kapitel vergleicht beide Ansätze und erarbeitet ihre Vor- und Nachteile. Im folgenden Kapitel werden Vorschläge zur Kombination beider Ansätze vorgestellt. Diese Vorschläge werden im fünften Kapitel diskutiert. Abschließend werden die wichtigsten Aspekte inklusive offener Forschungsfragen zusammengefasst.

2 Definitionen

In diesem Kapitel werden die Begriffe Evaluation, Zertifizierung, Verifizierbarkeit (individuell und universell) und Plausibilitätskontrolle definiert.

2.1 Evaluation und Zertifizierung

Da es sich bei elektronischen Wahlen um IT-Systeme handelt, wird hier allgemein die Evaluation und Zertifizierung von IT-Systemen definiert.

Unter der Evaluation eines IT-Systems versteht man die Prüfung, ob ein IT-System die gestellten Eigenschaften/Anforderungen erfüllt. Es findet eine Prüfung durch Experten (i.d.R. durch anerkannte Instanzen - Prüfungslabors) statt und nicht durch den einzelnen Laien, der das System später benutzten wird. Neben der eigentlichen Systemprüfung umfasst eine Evaluation i.d.R. auch die Prüfung der Entwicklungsdokumente, der Entwicklungsumgebung und des Auslieferungsprozesses. Eine solche Evaluation kann unterschiedlich tief und damit unterschiedlich ausführlich und intensiv sein. Außerdem kann eine Evaluation unterschiedliche Vertrauens- bzw. Angreifermodelle zugrunde legen.

Es werden zwei Ansätze unterschieden: Entweder der Evaluator prüft jedes System vor seinem Einsatz oder nur ein Referenzsystem (wie bei der Bauartprüfung in [BWGV99]), und die Übereinstimmung jedes Exemplars erfolgt entweder manuell durch eine Herstellererklärung oder technisch, beispielsweise über einen Prüfsummenvergleich.

Der Evaluationsbericht enthält in der Regel weit umfangreichere Informationen als die duale Bewertung „sicher/unsicher“ oder „ok/nicht ok“. Diesem Bericht ist unter anderem zu entnehmen, welche Tests durchgeführt wurden und wie das untersuchte System die geprüften Eigenschaften erfüllt.

Nach positiver Evaluation eines IT-Systems wird im Rahmen der Zertifizierung ein Zertifikat zur Bestätigung von einer anerkannten Instanz ausgestellt. Die zertifizierende Instanz überwacht i.d.R. die Evaluation und trifft ihre Entscheidung auf Basis des Evaluationsberichts. Darüberhinaus beruht das Vertrauen der zertifizierenden Instanz in die Validität des Evaluationsergebnisses darin, dass sie die evaluierende Instanz zuvor akkreditiert hat.

Das Zertifikat enthält das Merkmal zur eindeutigen Identifikation des Systems, die Anforderungen gegen die geprüft wurde, das Vertrauens- bzw. Angreifermodell auf dessen Basis evaluiert wurde und die Prüftiefe (d.h. wie umfangreich geprüft wurde – angefangen mit einer High-Level Sichtung der Architektur über verschiedene Tests, einer Source Code Analyse bis hin zu einem formalen Beweis, dass das System, die geforderten Eigenschaften erfüllt). Das Zertifikat gilt genau für diese Zusammensetzung. Mit der erfolgreichen Zertifizierung weist der Hersteller eines IT-Systems nach, dass sein Produkt die erforderlichen Sicherheitsanforderungen erfüllt. Das Produkt wird damit für den Benutzer vertrauenswürdig, da er weiß, dass es von einer qualifizierten und unabhängigen Stelle überprüft und für sicher befunden wurde. Idealerweise wird die Evaluation und die Zertifizierung von zwei unterschiedlichen und unabhängigen Instanzen durchgeführt.

Für IT-Systeme existiert bereits eine Reihe von Evaluationsstandards: Die bekanntesten sind die Common Criteria Evaluation Methodology (ein internationaler Standard zur Prüfung und Bewertung der Sicherheit von Informationstechnik) [CC3.1], die vorrangig Softwareprodukte adressieren und die FIPS 140-1/2-Criteria [FIPS140], die nur die Sicherheitseigenschaften von kryptographischen Modulen untersuchen.

2.2 Verifizierung bei elektronischen Wahlen

Die Idee der Verifizierbarkeit besteht darin, dass der Wähler der Korrektheit der Wahl nicht vertrauen muss, da er diese Eigenschaften selbst prüfen kann. Die gebotene Verifizierbarkeit umfasst laut Urteil „das Wahlvorschlagsverfahren, die Wahlhandlung (in Bezug auf die Stimmabgabe durchbrochen durch das Wahlgeheimnis) und die Ermittlung des Wahlergebnisses“. Darüber hinaus finden sich in der Literatur weitere unterschiedliche Definitionen für Verifizierbarkeit (siehe hierzu zum Beispiel [NSW05, SP06]). Insgesamt wird für diesen Beitrag zwischen folgenden fünf Dimensionen unterschieden:

- Adressat: Dabei wird zwischen individueller Verifizierbarkeit durch den Wähler und universeller Verifizierbarkeit durch die interessierte Öffentlichkeit (inkl. Wähler, Wahlhelfer, Wahlvorstand und Wahlbeobachter) unterschieden (diese Begriffe wurden in [SK95] eingeführt).

- Medium: Die Verifizierung kann manuell auf der Basis von Papierstimmzetteln oder mathematisch auf der Basis kryptographischer Verfahren mit technischen Hilfsmitteln erfolgen.

- Stärke: Die Verifizierungsfunktionen können unterschiedlich stark implementiert werden: Im Fall der individuellen Verifizierbarkeit wird unterschieden, ob der Wähler (a) nur feststellen kann, ob seine Stimme berücksichtigt wurde, oder (b) zusätzlich feststellen kann, dass sie so gezählt wurde wie abgegeben. Durch die stärkere Variante wird sichergestellt, dass Stimmen weder unbemerkt entfernt noch verändert werden können. Im Fall der universellen Verifizierbarkeit wird unterschieden, (a) ob es lediglich möglich ist, die Stimmen „selber“/erneut auszuzählen oder (b) ob zusätzlich geprüft werden kann, ob im Ergebnis nur Stimmen von berechtigten Wählern berücksichtigt werden. Wenn in beiden Fällen die stärkere Verifizierungsfunktion implementiert ist, wird sichergestellt, dass alle autorisierten Stimmen und nur solche korrekt ausgezählt werden.

- Beweiskraft: Hinsichtlich der Beweiskraft kann zwischen drei Klassen individueller Verifizierbarkeit unterschieden werden: (a) der Wähler kann zwar feststellen, dass seine Stimme nicht oder falsch ins Ergebnis eingegangen ist, er kann dies aber nicht beweisen; (b) er kann die Manipulation erkennen und auch nachweisen, allerdings nur unter Preisgabe seiner Stimme[1]; (c) der Wähler kann die Manipulation aufdecken, ohne seine Stimme offenzulegen. Hinsichtlich der Beweiskraft bei der universellen Verifizierbarkeit kann zwischen zwei Klassen unterschieden werden: (a) es kann festgestellt werden, dass das Wahlergebnis falsch ist, allerdings kann dieser Integritätsverlust nicht nachgewiesen werden oder (b) der Fehler kann aufgedeckt und auch bewiesen werden.

[1]-Hierbei kann unterschieden werden, ob dieser Nachweis gegenüber einer beliebigen Person erfolgen kann oder nur gegenüber eine bestimmten Gruppe.

- Vertrauensbasis: Hier wird unterschieden, ob der durch die Verifizierungsfunktion gelieferte Nachweis auf dem Vertrauen in einzelne Komponenten des Systems beruht oder nicht.

Der einfache Hinweis in Form einer entsprechenden Meldung an den Wähler, dass seine Stimme erfolgreich gespeichert wurde und im Ergebnis berücksichtigt wird – entweder als Abschluss der Wahlhandlung oder nach erneutem Anmelden am System – wird in diesem Zusammenhang nicht als individuelle Verifizierbarkeit bezeichnet. Analog wird die Möglichkeit, am Ende der Wahl die Anzahl der laut Wählerverzeichnis abgegebenen Stimmen mit der Anzahl der Stimmen in der elektronischen Urne zu vergleichen, in diesem Zusammenhang nicht als universelle Verifizierbarkeit sondern als *Plausibilitätscheck* bezeichnet. Laut eines Urteils des Bundesverfassungsgerichtes [BVG09 Absatz 119/120] bieten diese Maßnahmen keine hinreichende Kontrolle. Im Urteil wird darüber hinaus nicht festgelegt welche der hier vorgestellten Form der Verifizierbarkeit gefordert wird; im Gegenteil; es wird dem Gesetzgeber auferlegt „zu regeln, wie die Nachvollziehbarkeit [..] sichergestellt wird“[BVG009 Absatz 115]. Dazu ist unter anderem zu überlegen, was unter die mehrfach geforderte „zuverlässige“ Nachvollziehbarkeit fällt. Allerdings bleibt zu prüfen, ob die Verifizierung mittels technischen Hilfsmitteln mit dem Urteil vereinbar ist, das eine Überprüfbarkeit „ohne besondere Sachkenntnis“ [BVG09 Absatz 118], „nähere computertechnische Kenntnisse“ [BVG09 Absatz 119] und „besonderes technisches Vorwissen“ [BVG09 Absatz 122] fordert. Dafür spricht, dass im Urteil betont wird, dass die Verifizierung zuverlässig sein muss. Die Ausgestaltung der Verifizierung nach dem Urteil stellt noch eine ungelöste Forschungsfrage dar.

Individuelle Verifizierbarkeit kann kryptographisch durch blinde Signaturen umgesetzt werden [BM03]. Geeignete Maßnahmen zur Umsetzung universeller Verifizierbarkeit sind Mix-Netze, Benalohs Modell, homomorphe Verschlüsselung sowie Zero-Knowledge-Beweise [BM03]. Verifizierungt auf der Basis eines Papierstimmzettels bietet beispielsweise der digitale Wahlstift.

3 Vor- und Nachteile beider Ansätze

In diesem Abschnitt werden die Vor- und Nachteile der Evaluation/Zertifizierung und der Verifizierung untersucht. Dabei ist zu beachten, dass die genannten Vor- und Nachteile für die unterschiedlichen Implementierungen von Verifizierbarkeit unterschiedlich stark gelten.

3.1 Evaluation und Zertifizierung

Vorteile: Der Wähler kann sich auf die Sicherheit des Wahlgerätes verlassen, da diese von einer qualifizierten Stelle überprüft wird. Der Wähler selbst bedarf daher keiner qualifizierten Kenntnisse und keines Aufwands, um die Sicherheit des Gerätes einzuschätzen. Die Evaluation und Zertifizierung eines Wahlsystems ermöglicht dem Wähler so, auf für ihn einfache und komfortable Weise ein sicheres Wahlgerät zu nutzen. Die Evaluation und Zertifizierung eines Wahlsystems kann alle Sicherheitsanforderungen an das Wahlgerät prüfen. Diese Prüfung kann nach Bedarf auf einer formalen Verifikation beruhen.

Nachteile: Ein Zertifikat stellt keine Garantie für eine korrekte Wahl dar. Durch die Evaluation/Zertifizierung steigert man lediglich die Vertrauenswürdigkeit des Wahlsystems, der tatsächliche Ablauf einer konkreten Wahl wird allein durch die Evaluation und Zertifizierung nicht überprüft. Ein mathematischer Nachweis, dass ein System die gewünschten Eigenschaften erfüllt, ist zwar theoretisch i.d.R. möglich (mittels formaler Verifikation), in der Praxis aber zu aufwendig und teuer (dabei ist noch zu prüfen, ob dies für alle Anforderungen möglich ist). Eine Evaluation / Zertifizierung dauert in der Regel mehrere Monate und muss immer erneuert werden, wenn sich etwas an der Software / Hardware / Konfiguration ändert. Dadurch kann nur sehr unbefriedigend auf kurzfristig auftretende neue Bedrohungen reagiert werden. Des Weiteren besteht die Gefahr, dass das eingesetzte Wahlgerät nicht mit dem geprüften übereinstimmt. Außerdem muss dem Hersteller, der evaluierenden und zertifizierenden Instanz vertraut werden.

3.2 Verifizierung

Vorteile: Mit der Kombination aus individueller und universeller Verifizierbarkeit kann nachgewiesen werden, dass die Integrität des Wahlergebnisses gewährleistet ist. Dadurch bieten elektronische Wahlen sogar mehr Sicherheit als Papierwahlen. Der Wähler hat selbst die Möglichkeit, sich von der korrekten Durchführung der Wahl zu überzeugen. Die Überprüfung ist ggf. unabhängig von dritten Stellen und basiert somit nicht auf Vertrauen.

Nachteile: Individuelle Verifizierbarkeit bedeutet für den Wähler eine Änderung im Wahlablauf und in der Regel wird ein zusätzlicher Schritt für den Wähler eingeführt – ggf. mit Medienbruch. Wenn der Wähler die universelle Verifizierbarkeitseigenschaft selber nutzen möchte, kommt noch ein weiterer Schritt hinzu. Die Durchführung der Verifizierung verlangt vom Wähler häufig ein Grundverständnis des Wahlsystems und seiner Prozesse. Die damit notwendige Auseinandersetzung des Wählers mit dem Wahlsystem macht die Durchführung der Wahl für den Wähler aufwändiger und komplizierter.

Die Sicherheit und Vertrauenswürdigkeit des Wahlgerätes basiert auf der Nutzung der Verifizierung. Es ist aus soziologischer Sicht problematisch, dem Wähler zu erklären, dass die Korrektheit und Integrität der durchgeführten Wahl davon abhängt, dass die Wähler von der individuellen Verifizierbarkeit Gebrauch machen.

Ein entscheidender Nachteil ist auch die Tatsache, dass die Verifizierbarkeit nur die Integrität des Wahlergebnisses (d.h., das alle autorisierten Stimmen und nur solche richtig ausgezählt werden) adressiert aber keine weiteren Eigenschaften – wie etwas das Wahlgeheimnis. Durch die Integration von Verifizierungsmechanismen werden die zugrunde liegenden Wahlprotokolle komplexer und damit fehleranfälliger. Es muss sichergestellt werden, dass die Verifizierbarkeit nicht das Wahlgeheimnis, die Unzwingbarkeit und die Quittungsfreiheit gefährdet.

4 Synthese

Nach der Definition und der Diskussion über die Vor- und Nachteile beider oft kontrovers diskutierter Ansätze zur Ermöglichung einer sicheren elektronischen Wahl mit Wahlgeräten wird in diesem Abschnitt ein Vorschlag für eine Kombination beider Ansätze vorgeschlagen.

Es wird vorgeschlagen, zum Schutz der Integrität der Stimmabgabe/-speicherung und des Wahlergebnisses individuelle bzw. universelle Verifizierbarkeit einzusetzen. Die verschiedenen Anforderungskataloge (wie die Empfehlungen des Europarates [CoE04]) weisen neben der Sicherstellung der Integrität noch eine ganze Reihe von weiteren Anforderungen auf. Hierzu zählt vor allem die Sicherstellung des Wahlgeheimnisses. Da diese Eigenschaften weder durch individuelle noch durch universelle Verifizierbarkeit adressiert werden, wird vorgeschlagen, ihre Erfüllung durch eine Evaluation und Zertifizierung des elektronischen Wahlgerätes nachzuweisen. Dies kann in Abhängigkeit von der Anforderung beispielsweise mittels Common Criteria oder FIPS 140-1/2-Criteria nachgewiesen werden.

Nun bleibt zu überlegen, ob die Anforderungen an die Integrität, die durch die Verifizierung abgedeckt werden, trotzdem Teil der Evaluation sind oder auf eine entsprechende Prüfung verzichtet werden kann. Für den Fall, dass die Verifizierungsfunktionen auf dem Vertrauen in einzelne Komponenten des Wahlgerätes beruhen, kann offensichtlich nicht auf die Evaluation dieser Anforderung verzichten werden. Was ist aber, wenn die Verifizierungsfunktionen nicht auf dem Vertrauen in einzelne Komponenten beruhen?

Im Fall der universellen Verifizierbarkeit, könnte argumentiert werden, dass eine entsprechende Evaluation entfallen kann, da Fehler im Auszählungsalgorithmus durch die universelle Verifizierbarkeit aufgedeckt werden. Mögliche Fehler und Schwachstellen möchte man bereits vor dem Realbetrieb beseitigt haben, da das Aufdecken bei der universellen Verifizierbarkeit für ein negatives Bild für elektronische Wahlen sorgen würde und die Wahl ggf. wiederholt werden müsste – was mit hohen Kosten verbunden ist. Daher wird vorgeschlagen auch diese Anforderungen im Rahmen der Evaluation/Zertifizierung zu prüfen, die bereits durch die universelle Verifizierbarkeit abgedeckt werden.

Bei der individuellen Verifizierbarkeit kann prinzipiell das gleiche Argument vorgebracht werden. Allerdings kommt hier noch erschwerend hinzu, dass nur im Rahmen der Evaluation/Zertifizierung geprüft werden kann, ob die hierzu implementierten Mechanismen nicht im Widerspruch zum Wahlgeheimnis stehen. Kurzum, die Evaluierung/Zertifizierung kann nicht abgekürzt werden, sondern wird im Gegenteil eher aufwändiger, weil die Wahlprotokolle i.d.R. komplexer sind, wenn sie individuelle und universelle Verifizierbarkeit umsetzen.

Das Vertrauen der Wähler in ein elektronisches Wahlsystem sollte neben Evaluation/Zertifizierung und Verifizierungsmechanismen noch durch einen dritten Pfeiler gestützt werden: Transparenz. Dies gilt für den Entscheidungsprozess, aber auch für den Entwicklungsprozess, die Prüfmethoden und -ergebnisse sowie für den Source Code und andere Entwicklungsdokumente. Dies kann aber nur unterstützend eingesetzt werden, denn das Urteil hat in [BVG09 Absatz 125] festgelegt, dass solche Maßnahmen nicht zur Sicherstellung der Kontrollierbarkeit beitragen.

5 Diskussion des Vorschlages

In diesem Abschnitt wird der Vorschlag, zusätzlich zur Evaluation/Zertifizierung Verifizierungsfunktionen zur Sicherung der Integrität des Wahlergebnisses zu implementierten, diskutiert: Hierzu wird zunächst der Fall betrachtet, dass die Verifizierungsfunktionen auf Vertrauen in einzelne Komponenten des elektronischen Wahlsystems basieren. Es stellt sich die Frage, warum man diesen Komponenten bzgl. einer zur Verifizierung erforderlichen Eigenschaft vertrauen sollte, wenn dieses Vertrauen nicht generell bzgl. der Ergebnisberechnung der Fall ist. In erster Linie scheint das nur eine Verlagerung des Problems zu sein. Zwar sinkt die Komplexität der vertrauenswürdigen Komponente, so dass die Korrektheit einfacher nachgewiesen werden kann, aber die Nachteile und Probleme einer Evaluation und Zertifizierung bleiben. Daraus kann gefolgert werden, dass das Urteil nur eine Verifizierung fordert, die nicht auf einer Vertrauensbasis in einzelne Komponenten aufbaut.

Im Fall, dass die Verifizierungsfunktion nicht auf das Vertrauen in einzelne Komponenten stellt sich aber auch noch eine Frage. Warum kann dem System hinsichtlich der Gewährleistung des Wahlgeheimnisses nach der Zertifizierung vertraut werden, wenn hinsichtlich der Integrität des Wahlergebnisses zusätzliche Mechanismen gefordert werden. Ist das Wahlgeheimnis weniger wichtig? Im traditionellen Verfahren gilt dies nicht, denn da kann der Wähler sich davon überzeugen, dass eine Wahlurne verwendet wird, die die Wahrung des Wahlgeheimnisses sicherstellen.

Ein anderes Argument, was in Erwägung gezogen werden könnte, liegt im unterschiedlichen Angreifermodell: Um das Wahlgeheimnis mittels Wahlgerät brechen zu können, muss nicht nur das Wahlgerät über entsprechend unerwünschte Funktionen verfügen, sondern der Angreifer muss zusätzlich im Wahllokal notieren, wer wann, bzw. in welcher Reihenfolge seine Stimme abgegeben hat. Um diesen Angriff in der Breite durchführen zu können, ist also eine Reihe von Leuten erforderlich. Ob diese Begründung juristisch zulässig ist, wird von den Autoren bezweifelt werden.

Wenn beide Argumente nicht gelten, bleiben zwei Folgerungen offen: Entweder muss auch die Sicherstellung des Wahlgeheimnisses von einem verfassungskonformen Wahlgerät für den Wähler nachvollziehbar und kontrollierbar implementiert werden oder es wird analog zur Papierwahl argumentiert. Theoretisch könnte man auch hier den Wahlhelfern vertrauen, dass sie die Wahl korrekt durchführen. Dennoch hat der Wähler das Recht, sich durch seine Anwesenheit im Wahllokal davon zu überzeugen. Analog kann man auch der Zertifizierung vertrauen, aber zusätzlich bekommt der Wähler noch die Möglichkeit zur Verifizierung. Dies stellt aber noch eine offene Forschungsfrage dar.

6 Fazit und Zusammenfassung

Motiviert durch das Urteil des Bundesverfassungsgerichtes diskutiert dieser Beitrag zwei unterschiedliche Ansätze zur Sicherstellung, dass Wahlen mittels elektronischer Wahlgeräte genauso sicher ablaufen wie bisherige papierbasierte Wahlen im Wahllokal: Evaluation/Zertifizierung versus Verifizierung. Dazu werden zunächst beide Ansätze definiert. Es werden insbesondere die verschiedenen Implementierungsformen für die Verifizierung vorgestellt und festgehalten, dass das Urteil die Ausgestaltung offen lässt. Anschließend werden Vor- und Nachteile beider Ansätze diskutiert. Aufbauend auf dieser Einführung wird ein Vorschlag für die Kombination aus beiden gemacht. Dabei wird begründet, dass die individuelle und universelle Verifizierbarkeit nur einen Teil der Anforderungen an Wahlgeräte abdeckt und insbesondere nicht sicherstellt, dass das Gerät das Wahlgeheimnis sichert. Daher ist es mindestens für diese Anforderungen erforderlich, das Wahlgerät außerdem zu zertifizieren.

In der Diskussion dieses Vorschlages wird die Frage aufgeworfen, wie begründet werden kann, dass der Zertifizierung hinsichtlich des Wahlgeheimnisses vertraut werden soll, wenn dies nicht für die Integrität des Wahlergebnisses gilt. Eine mögliche Antwort könnte die Forderung nach Verifizierungsfunktionen für das Wahlgeheimnis sein. Dieses Thema stellt eine offene Forschungsfrage dar, die nicht abschließend geklärt wurde. Allerdings wird dieses Thema auch weitere Forschungsfragen auf, beispielsweise hinsichtlich der Ausgestaltung der Verifizierungsfunktionen und deren Benutzerfreundlichkeit.

Acknowledgement. This work was supported by CASED (www.cased.de).

Literaturverzeichnis

[BM03] Burmester, M.; Magkos, E.: Towards Secure and Practical e-Elections in the New Era. In: Gritzalis, D. (Ed.), Advances in Information Security, Vol. 7, Kluwer Academic Publishers, 2003.

[BVG09] Zweiter Senat des Bundesverfassungsgerichts: Urteil n den Verfahren über die Wahlprüfungsbeschwerden: http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html; 2009.

[BWGV99]Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland (Bundeswahlgeräteverordnung), 1975. BGBl I 1975, 2459, Zuletzt geändert durch Art. 1 V v. 20. 4.1999 I 749.

[CoE04] Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe and explanatory memorandum. Council of Europe Publishing, http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e%2Dvoting/01_recommendation/Rec(2004)11_Eng_Evoting_and_Expl_Memo.pdf;2004.

[CC3.1] Common Criteria for Information Technology Security Evaluation. Version 3.1, http://www.commoncriteriaportal.org/thecc.html; Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf; 2006.

[FIP140] National Institute of Standards and Technology: Security Requirements for Cryptographic Modules; http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf and http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf; 2002.

[NSW05]Naveen, K., Sastry, N., Wagner, D. Cryptographic Voting Protocols: A Systems Perspective: In USENIX Security Symposium, number 3444 in Lecture Notes in Computer Science

[SK95] Sako K, Killian J. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In: Advances in cryptology – EUROCRYPT '95. LNCS, vol. 921. Springer-Verlag; 1995. p. 393–403.

[SP06] Sampigethaya, K.Poovendran, R.: A framework and taxonomy for comparison of electronic voting schemes, Computers & Security, volume 25, no. 2, pp 137-153; 2006.

[VK06] Volkamer, M.,Krimmer, R.: Ver- / Misstrauen schaffende Maßnahme beim e-Voting. In Informatik 2006 - Informatik für Menschen, Band 1, Beiträge der 36. Jahrestagung der Gesellschaft für Informatik e.V. (GI), volume 93 of LNI, pages 418-425, Bonn, 2006. Gesellschaft für Informatik; 2006.