Stephan Neumann, Melanie Volkamer, Johannes Buchmann

Tauglichkeit von Common Criteria-Schutzprofilen für Internetwahlen in Deutschland

Dieser Artikel erscheint in der Zeitschrift Datenschutz und Datensicherheit.

Die Common Criteria und insbesondere das Konzept der Schutzprofile haben sich als internationaler Standard zur Spezifikation von Sicherheitsanforderungen an Produktgruppen sowie zur Evaluation von spezifischen Produkten nach diesen Schutzprofilen bewährt. Die zunehmende Entwicklung von elektronischen Wahlsystemen sowie deren praktischer Einsatz für politische Wahlen (z.B. in Estland, Norwegen, Schweiz und den USA) motivieren den Entwurf von Schutzprofilen für die unterschiedlichen elektronischen Wahlsysteme wie Wahlgeräte, digitale Wahlstifte und Internetwahlsysteme. Dieser Artikel untersucht die Tauglichkeit von Common Criteria Schutzprofilen mit Hinblick auf parlamentarische Internetwahlen in der Bundesrepublik Deutschland. Das Ergebnis dieser Untersuchung zeigt, dass das Konzept der Common Criteria Schutzprofile nur sehr eingeschränkt geeignet ist. Aus den gewonnenen Erkenntnissen werden erste Empfehlungen für die Weiterentwicklung und Etablierung eines geeigneteren Standards gegeben.

1 Einleitung

Die Common Criteria sind ein international entwickelter Sicherheitsstandard der Informationstechnologie, der seit 1999 im ISO Standard 15408 festgehalten ist. Ein zentrales Konzept des Standards sind so genannte *Schutzprofile*, domänenspezifische, produktunabhängige Sicherheitsanforderungen an einen abstrakten Evaluierungsgegenstand, die Herstellern ermöglichen auf etablierte Sicherheitsanforderungen zurückzugreifen und die helfen das Vertrauen der Benutzer in entsprechend zertifizierte Produkte zu steigern. Zahlreiche Schutzprofile wurden entwickelt, so beispielsweise für Signaturverfahren, hoheitliche Dokumente und Produkte des Gesundheitswesens. Die Common Criteria wird und wurde bereits für eine Vielzahl von Produktevaluierungen eingesetzt. Mit der weiteren Verbreitung der Common Criteria und dem steigenden Interesse an elektronischen Wahlen[1], ist es nicht erstaunlich, dass bereits mehrere Schutzprofile für elektronische Wahlsysteme entwickelt wurden. Jedoch adressiert keines der bisher entwickelten Schutzprofile Internetwahlen für parlamentarische Wahlen in der Bundesrepublik Deutschland. In dieser Arbeit wird die Tauglichkeit des Konzepts der Common Criteria Schutzprofile zur Integration verfassungsrechtlicher Vorgaben an Internetwahlsysteme zur Durchführung parlamentarischer Wahlen in der Bundesrepublik Deutschland untersucht.

Im nächsten Abschnitt wird zunächst eine kurze Übersicht über die Common Criteria und insbesondere das Konzept der Schutzprofile gegeben. Danach werden Schutzprofile für elektronische Wahlsysteme der Literatur aufgeführt, sowie deren Bezug zu dieser Arbeit dargestellt. Im weiteren Verlauf werden drei Herausforderungen mit Hinblick auf die Tauglichkeit von Schutzprofilen zur Evaluation von Internetwahlsystemen für parlamentarische Wahlen in der Bundesrepublik Deutschland herausgearbeitet. Der darauf folgende Abschnitt stellt Lösungsansätze für diese Herausforderungen dar. Im letzten Teil des Artikels kann ein Fazit gezogen werden und es können Richtungen für zukünftige Forschungsarbeiten gewiesen werden.

[1] So belegt eine von Microsoft Deutschland in Auftrag gegebene Forsa Umfrage von Januar 2013, dass mehr als 50% der deutschen Wahlberechtigten ihre Stimme bei der Bundestagswahl 2013 online abgegeben hätten. (http://www.microsoft.com/de-de/news/pressemitteilung.aspx?id=533684)

2 Common Criteria

Die Entwicklung der Common Criteria (kurz: CC)[2] wird von den Staaten Australien/Neuseeland, Kanada, Frankreich, Deutschland, Japan, den Niederlanden, Spanien, dem Vereinigten Königreich und den Vereinigten Staaten von Amerika mitgetragen. Version 1.0 der Common Criteria wurde 1996 veröffentlicht. Die aktuelle Common Criteria Version ist 3.1 Release 4. Die Common Criteria sind ein Standard zur Evaluation von Produkten der Informationstechnologie Sicherheit und als solcher im ISO Standard 15408 [8] festgehalten. Die Common Criteria unterscheiden zwei generelle Konzepte: *Schutzprofile* und *Security Targets*. Schutzprofile sind im Vergleich zu Security Targets eher abstrakt und unabhängig von einem konkreten Produkt. Sie adressieren daher ganze Produktgruppen. Schutzprofile werden dementsprechend zumeist stellvertretend aus Sicht der Endnutzergruppe verfasst. Darin werden auf einem geeigneten Abstraktionslevel die sicherheitsspezifischen Anforderungen an ein generisches Endprodukt spezifiziert. Ein Schutzprofil beinhaltetet: Sicherheitsproblemdefinitionen (engl. security problem definition), Sicherheitsziele (engl. security objectives) funktionale Sicherheitsanforderungen (engl. security functional requirements) und Anforderungen an die Vertrauenswürdigkeit (engl. security assurance requirements). Die Common Criteria stellen diese Anforderungen in den entsprechenden Katalogen Part 2: Security functional components und Part 3: Security assurance components bereit. Die dort definierten Komponenten unterteilen sich in Klassen und Familien, die dazu genutzt werden können, Sicherheitsziele strukturiert durch eine entsprechende Konkretisierung in Anforderungen zu überführen.

Im Gegensatz zu den Schutzprofilen stellen Security Targets den herstellerseitigen Gegenpart dar. Security Targets entsprechen einer konkreten Produktspezifikation eines Herstellers, die in weiten Teilen den entsprechenden Abschnitten eines Schutzprofils entspricht. Hinzu kommt eine Beschreibung, wie das konkrete Produkt die Anforderungen erfüllt. Ein Security Target kann sich auch direkt auf ein Schutzprofil beziehen. Es dient dem CC Evaluator als Grundlage für die CC Evaluation.

Bis heute wurden zahlreiche Produktzertifizierungen nach entsprechenden Schutzprofilen durchgeführt[3]. Insbesondere hat sich eine derartige Zertifizierung in den Bereichen der hoheitlichen Dokumente, der digitalen Signaturen und des Gesundheitswesens etabliert. Im Bereich der hoheitlichen Dokumente sei hier die STARCOS 3.5 ID GCC C2 der Firma Giesecke & Devrient GmbH erwähnt, die nach dem Schutzprofil BSI-CC-PP-0061-2009 der Stufe EAL4+ evaluiert und zertifiziert wurde. Das Produkt STARCOS 3.4 Health HBA C1 der Firma Giesecke & Devrient GmbH wurde nach dem Schutzprofil für Health Professional Card (PP-HPC) with SSCD Functionality BSI-CC-PP-0018-V3-2009 für Stufe EAL4+ evaluiert und zertifiziert. Als sichere Signaturerstellungseinheit wurde das Produkt STARCOS 3.5 ID ECC C1R des Unternehmens Giesecke & Devrient GmbH nach dem Schutzprofil BSI-CC-PP-0059-2009-MA-01 der Stufe EAL4+ evaluiert und zertifiziert.

[2] http://www.commoncriteriaportal.org/cc/

[3] vgl. hierzu: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/ZertifizierteProdukte/zertifizierteprodukte_node.html

3 Common Criteria Schutzprofile für elektronische Wahlsysteme

Die gesamtgesellschaftliche Bedeutung von Wahlen sowie die zunehmende Verbreitung elektronischer Wahlsysteme resultierten bis zum heutigen Tag in einer Vielzahl von Schutzprofilen und Entwürfen für Schutzprofile für verschiedenartige, elektronische Wahlsysteme. So gibt es einerseits eine Reihe von Schutzprofilen für Wahlgeräte, z.B. PP-CIVIS [16], IEEE P1583 [6] und Lee et al. [12] sowie für den digitalen Wahlstift [5]. Es existiert außerdem ein Schutzprofil für Internetwahlsysteme BSI-PP-0037 [2]. Dieses steckt seinen nicht rechtsverbindlichen Rahmen bereits eingangs ab, wie der folgende Auszug belegt:

> *"Zur sicheren Durchführung von Online-Wahlen mit höherem Angriffspotential, wie etwa Betriebsratswahlen oder parlamentarische Wahlen, sind weitere Sicherheitsanforderungen zu formulieren und mit nachweisbaren Maßnahmen durchzusetzen, um die Annahmen über die Anwendungsumgebungen, wie sie hier beschrieben sind, zu erfüllen."* BSI-PP-0037

Diese Schutzprofile wurden grundsätzlich hinsichtlich ihrer Eignung als Basis für ein Schutzprofil für Internetwahlen bei parlamentarische Wahlen untersucht: Zunächst stellt sich die Frage, inwieweit diese Schutzprofile systematisch aus rechtlichen Vorgaben abgeleitet wurden. Den Autoren dieses Aufsatzes ist für keines dieser Schutzprofile eine Dokumentation des systematischen Ableitens von Sicherheitsproblemdefinitionen aus rechtlichen Vorgaben bekannt. Es scheint als hätten Techniker nach bestem Wissen diese Sicherheitsproblemdefinition verfasst.

Außerdem stellt sich die Frage, inwieweit alle in ModIWa 2[4] abgeleiteten technischen Ziele (siehe Tabelle 1) grundsätzlich abgedeckt sind. Dabei hat sich gezeigt, dass mit Ausnahme des Entwurfs von Karokola, Kowalski und Yngström [11] und des Entwurfs von Lee et al. [12] eine Betrachtung der Individuellen Verifizierbarkeit (die aus dem Öffentlichkeitsgrundsatz der Wahl aus Art. 38 Abs. 1 Satz 1 GG in Verbindung mit Art. 20 Abs. 1 und Abs. 2 GG folgt) fehlt. Dabei ist zu beachten, dass Karokola, Kowalski und Yngström [11] Verifizierbarkeit als grundlegende Sicherheitsanforderung zwar betrachten, diese Anforderung in der späteren Sicherheitsproblemdefinition, aus für die Autoren dieser Arbeit nicht ersichtlichen Gründen, jedoch nicht mehr einbeziehen. Aus der Tatsache heraus, dass es sich bei den Common Criteria um einen Sicherheitsstandard handelt, ist nicht überraschend, dass die meisten anderen technischen Ziele nicht adressiert werden.

[4] https://www.secuso.informatik.tu-darmstadt.de/de/research/projects/#c13061

Letztlich wurde untersucht, ob diese Schutzprofile ausschließlich auf existierenden funktionalen Sicherheitsanforderungen (engl. functional security requirements) und Anforderungen an die Vertrauenswürdigkeit (engl. security assurance requirements) aufbauen oder diese erweitern. Letzteres hätte Nachteile hinsichtlich einer internationalen Anerkennung. Lee et al. schließen individuelle Verifizierbarkeit in die Sicherheitsproblemdefinition mit ein, erweitern dazu jedoch die Anforderungen an die Vertrauenswürdigkeit des Common Criteria Standards. Zwar erweitern die Autoren die funktionalen Sicherheitsanforderungen nicht, geben aber keine Beziehung (engl. rationale) zwischen Sicherheitszielen und Sicherheitsanforderungen an.

Technisches Ziel	Sicherheit	Funktional
Benutzbarkeit		X
Stimmenintegrität	X	
Zugänglichkeit		X
Systemerreichbarkeit	X	
Wählererreichbarkeit	X	
Wahlberechtigung	X	
Einmaligkeit	X	
Systemneutralität		X
Fairness	X	
Geheimhaltung	X	
Anonymität	X	
Individuelle Verifizierbarkeit	X	
Verantwortlichkeit		X
Archivierung	X	
Universelle Verifizierbarkeit	X	
Verständlichkeit		X
Systemintegrität	X	

Tabelle 1: In ModIWa 2 abgeleitete, technische Ziele. Diese Ziele unterteilen sich in funktionale Ziele und Sicherheitsziele.

Ergebnis dieser ersten Untersuchung ist, dass selbst für die abgeleiteten technischen Sicherheitsziele keines der existierenden Schutzprofile direkt übernommen oder angepasst werden kann.

4 Die Common Criteria und Internetwahlsysteme - Herausforderungen und Fragestellungen

Bei dem Versuch entsprechend ein neues Schutzprofil für parlamentarische Internetwahlen zu schreiben, hat sich schnell ein grundsätzliches Problem gezeigt: Die Umsetzung elektronischer Wahlsysteme, und hier insbesondere Internetwahlsysteme, für parlamentarische Wahlen geht mit einer besonderen verfassungsrechtlichen Gegebenheit einher. So können die verschiedenen verfassungsrechtlichen Vorgaben, und deren Konkretisierung, wie zum Beispiel Geheimhaltung (mit und ohne Zutun des Wählers) und die individuelle sowie universelle Verifizierbarkeit aufgrund der zum Teil widerstreitenden Zielsetzungen nicht bedingungslos umgesetzt werden. Bei der konkreten Ausgestaltung der verfassungsrechtlichen Vorgaben ist dem Gesetzgeber ein gesetzlicher Gestaltungsspielraum gegeben, innerhalb dem es erlaubt ist die Umsetzung individueller Wahlrechtsgrundsätze zugunsten der Gleichmäßigkeit des gesamten Wahlsystems, zu reduzieren[5] [13,14]. Zusammengefasst führt dies zu der Erkenntnis, dass

1. mehrere Ausprägungen möglich und zulässig sind und somit mehrere Möglichkeiten einer Ausgestaltung des Schutzprofils existieren. Denkbar wäre, dass in einem Fall die geheime Wahl stärker gefordert wird, in dem anderen Fall die individuelle Verifizierbarkeit.
2. mögliche Ausprägungen nicht ausschließlich auf Ebene der Sicherheitsziele festgelegt werden können, sondern auch andere technische Ziele einfließen, welche in einem Schutzprofil (derzeit) nicht formuliert werden können. Dies erweist sich insbesondere insoweit als kritisch, als dass z.B. Produkte zertifiziert werden können, deren zugrunde liegendes kryptographisches Protokoll (im Falle von Internetwahlsystemen) die Anforderungen des Schutzprofils adäquat umsetzt sowie die Anforderungen an die Umgebung auf einem rechtlich akzeptablen Level hält, jedoch bereits auf Protokollebene derart starke Einschränkungen an die Benutzbarkeit impliziert, dass das voll funktionsfähige Produkt nicht den verfassungsrechtlichen Vorgaben genügen kann. Beispielhaft sei hier auf das Helios Wahlprotokoll verwiesen [1], indem die Integrität der Stimmen ohne Vertrauen an die Wahlumgebung umgesetzt ist, der Wähler dafür jedoch eine zufällige Anzahl von Verschlüsselungsvorgängen (manuell) durchlaufen muss[6].
3. mögliche Ausprägungen nicht festgelegt werden können, da in einem Schutzprofil Annahmen an die Einsatzumgebung (engl. security objective for the operational environment), wie etwa ein vertrauenswürdiger Wahlserver, gemacht werden, deren Umsetzung jedoch rein über eine Common Criteria Evaluierung nicht sichergestellt ist.

Die hier ausgeführten Probleme belegen, dass Common Criteria Schutzprofile in ihrer jetzigen Form kein geeignetes Mittel zur Evaluation von Internetwahlsystemen für deren Einsatz für parlamentarische Wahlen in der Bundesrepublik Deutschland bieten.

[5] BVerfGE, 59, 119 (124 f):1981

[6] Man könnte sich vorstellen diesen Prozess zu automatisieren. Jedoch darf die entsprechende Anzahl an Wiederholungen ausschließlich dem Wähler bekannt sein, da Manipulationsangriffe durch Kenntnis dieses Wertes möglich sind.

5 Integration von Standards zur ganzheitlichen Evaluation von Internetwahlsystemen

Die dargelegten Probleme bezüglich der derzeitigen Untauglichkeit von Common Criteria-Schutzprofilen für Internetwahlen in Deutschland lassen sich auf verschiedene Wege adressieren.

Problem - Verifizierbarkeit. Es stellt sich heraus, dass keine geeigneten Komponenten in Form der Sicherheitsanforderungen zur Verfügung stehen, die die Öffentlichkeit der Wahl umzusetzen vermögen, vorliegen. Das Hinzufügen von funktionalen Sicherheitsanforderungen ist zwar möglich, liegt aber außerhalb des Common Criteria Standards und macht eine internationale Anerkennung schwierig. Daher wurde nach anderen Möglichkeiten in Bezug auf das CC Schutzprofil für Internetwahlen gesucht. Hier könnte alternativ entschieden werden, die individuelle Verifizierbarkeit durch das Entfernen entsprechender Annahmen aus dem BSI-PP-0037 Schutzprofil wie zum Beispiel der folgenden Annahme indirekt einzufordern:

"A.Endgerät: Der Wähler nimmt seine Verantwortung zur Sicherung des Endgerätes wahr. Es wird angenommen, dass der clientseitige EVG, falls erforderlich, vom Wähler so installiert bzw. benutzt wird, dass das Endgerät den Vorgang der Stimmabgabe weder beobachten noch beeinflussen kann. Dazu gehört auch, dass der Wähler sein Endgerät nicht absichtlich für solche Zwecke manipuliert. Das Endgerät ist in der Lage, den Stimmzettel korrekt anzuzeigen, die Eingaben des Wählers korrekt an den Wahlserver zu übertragen und die Stimme nach der Wahlhandlung zu löschen." BSI-PP-0037

Fällt diese Annahme weg, existieren derzeit keine anderen technischen Möglichkeiten das technische Ziel der Stimmenintegrität umzusetzen, außer mit Hilfe individueller Verifizierbarkeit. Somit wird diese, durch die genannte Änderung am Schutzprofil, indirekt gefordert.

Problem - Annahmen an die Einsatzumgebung. Eine Möglichkeit das Problem mit den Annahmen an die Einsatzumgebung zu adressieren besteht in der Etablierung eines ganzheitlichen Sicherheitsstandards. Ein solcher Standard sollte es einerseits erlauben den eigentlichen Evaluierungsgegenstand, zum Beispiel das kryptographische Protokoll eines Internetwahlsystems, auf Grundlage eines Schutzprofils, andererseits im Schutzprofil getroffene Annahmen an die Einsatzumgebung auf Grundlage des IT-Grundschutzstandards [3] nach ISO Standard 27001 [10] zu evaluieren. Eine entsprechende Methodik, die einzelnen Standards zu verbinden wurde in Roßnagel et al. [15] aufgezeigt. Die Autoren schlagen auch vor grundsätzlich zwischen Sicherheitszielen an die Umgebung zu unterscheiden, die aus rechtlicher Sicht umzusetzen sind und solchen Zielen, die aus rechtlicher Sicht nicht weiter durchgesetzt werden müssen. Sicherheitsziele an die Umgebung, die umzusetzen sind, müssen im weiteren Verlauf der beschriebenen Methodik durch entsprechende Schutzmaßnahmen des IT-Grundschutz Maßnahmenkatalogs umgesetzt werden.
Die Etablierung eines solchen allgemeinen Sicherheitsstandards kann letztendlich nicht nur für elektronische Wahlen von großer Bedeutung sein, sondern kann ebenso eine direkte Unterstützung bei der Identifikation und Beseitigung systemischer Schwachstellen sein und somit die Entwicklung ganzheitlich evaluierter, sicherheitskritischer Systeme vorantreiben. Der von Roßnagel et al. [15] angestoßene Prozess stellt den ersten Schritt in diese Richtung dar, weitere Schritte müssen zur Fertigstellung und Etablierung eines solchen Standards jedoch folgen. Der Integrationsprozess verschiedener IT-Sicherheitsstandards kann eine wesentliche Stütze bei der Etablierung ganzheitlich sicherer Systeme, darstellen.

Problem - weitere technische Ziele. Um auch technische Ziele wie Benutzbarkeit, (politische) Systemneutralität (engl. *system neutrality*) und Zugänglichkeit (engl. *accessibility*) integrieren zu können, müsste die zuvor angesprochene Erweiterung auch um diese technischen Ziele erweitert werden. Es existieren Standards zur individualisierten Umsetzung und Evaluierung einiger dieser Anforderungen, so zum Beispiel der Standard ISO 9241-11 [7] mit Richtlinien zur Umsetzung von Benutzbarkeit und der Standard ISO 9241-171 [9] mit Richtlinien zur Umsetzung von Zugänglichkeit. Diese sollten in den erweiterten Sicherheitsstandard einfließen. Von einer derartigen Integration können weitaus mehr Produktgruppen als Wahlsysteme profitieren, was auch die Überlegungen Aspekte der benutzbaren Sicherheit (engl. usable security) in die Common Criteria zu integrieren [4] zeigen. Da dies nicht für alle technischen Ziele möglich oder sinnvoll ist (ggf. zu speziell, wie Systemneutralität), bleibt offen, wie diese in einen solchen Standard integriert werden können.

Problem - Gestaltungsspielraum. Mit Hinblick auf die wahlspezifische Gegebenheit des gesetzlichen Gestaltungsspielraums bleibt offen, wie diese verfassungsrechtliche Besonderheit mit einem ganzheitlichen Standard zur Evaluation von Internetwahlsystemen in Einklang gebracht werden kann. Es reicht mit Hinblick auf elektronische Wahlsysteme und damit auch für Internetwahlsysteme bei parlamentarischen Wahlen demnach nicht aus, individuelle Standards mit Fokus Sicherheit bzw. Funktionalität zu integrieren, sondern vielmehr muss bereits an dieser Stelle eine adäquate Modellierung des gesetzlichen Gestaltungsspielraums bedacht werden. Es bleibt in weiteren Forschungsarbeiten zu erörtern, inwieweit ein derart flexibles Konstrukt wie der gesetzliche Gestaltungsspielraum in einen ganzheitlichen Standard zur Bewertung von elektronischen Internetwahlsystemen aufgenommen werden kann bzw. soll.

6 Fazit und Ausblick

Die Common Criteria bieten mit dem Konzept von Schutzprofilen einen etablierten Standard zur produktunabhän-

gigen Spezifikation von Sicherheitsanforderungen an eine definierte Produktgruppe sowie die produktspezifische Evaluation nach Schutzprofilen. Damit können die Common Criteria als Standard zur Beschreibung der Sicherheitsanforderungen für Internetwahlsysteme im Zusammenhang mit parlamentarischen Wahlen in Deutschland in Betracht gezogen werden. In dieser Arbeit haben wir uns der Fragestellung angenommen, inwieweit Common Criteria Schutzprofile das Mittel der Wahl zur Bewertung und Evaluation von Internetwahlsystemen im Rahmen von parlamentarischen Wahlen in der Bundesrepublik Deutschland sein können. Es konnte die Erkenntnis gewonnen werden, dass das Konzept der Schutzprofile derzeit nicht adäquat erscheint, verfassungsrechtliche Vorgaben auszudrücken. So fehlen einerseits Sicherheitsanforderungen (security functional requirements & security assurance requirements) zur Umsetzung des Öffentlichkeitsgrundsatz der Wahl, andererseits können Annahmen durch die kontrollierte Definition des Evaluierungsgegenstandes nach Belieben ausgelagert werden, so dass andere Sicherheitsstandards zwar ansetzen können, deren Durchsetzung jedoch nicht evaluiert werden kann. Des Weiteren zeigt sich, dass auch solche Anforderungen durch die Verfassung definiert werden, die über die reine Sicherheit des eigentlichen Systems hinausgehen. Letztlich kann der gesetzliche Gestaltungsspielraum, der dem Gesetzgeber die Freiheit bei der Ausgestaltung der verfassungsrechtlichen Vorgaben gibt, nicht in CC Schutzprofilen abgebildet werden.
Schlussendlich führen uns die hier erarbeiteten Ergebnisse zu der Erkenntnis, dass das Bestreben Sicherheitsstandards zu integrieren [15] ein Schritt in die richtige Richtung sind. In Zukunft werden derartige Standards um funktional orientierte Standards zu erweitern sein. Abschließend wird die Etablierung eines solchen Standards unumgänglich mit einer adäquaten Betrachtung des gesetzlichen Gestaltungsspielraums einhergehen. Die vorliegende Arbeit befasst sich ausschließlich mit parlamentarischen Internetwahlen in der Bundesrepublik Deutschland. Es bleibt in zukünftigen Arbeiten zu erörtern, inwieweit die hier identifizierten Herausforderungen und Lösungsansätze für andere Wahlszenarien relevant sind.

Literatur

[1] Adida, B. (2008). *Helios: Web-based Open-Audit Voting*. USENIX Security Symposium (pp. 335-348), USENIX Association.

[2] Bundesamt für Sicherheit in der Informationstechnik (2008). *BSI-CC-PP-0037: Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte.* http://www.commoncriteriaportal.org/files/ppfiles/pp0037b.pdf

[3] Bundesamt für Sicherheit in der Informationstechnik (2008). *BSI Standard 100-2: IT-Grundschutz-Vorgehensweise*

[4] Church, L., Kreeger, M.N., Streets, M. (2008). *Introducing Usability to the Common Criteria.* 9th International Common Criteria Conference (ICCC).

[5] Freie und Hansestadt Hamburg (2007). *BSI-PP-0031: Digitales Wahlstift-System*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/PP0031b_pdf.pdf?__blob=publicationFile

[6] IEEE (2005). *P1583 SCC 38, IEEE P1583TM/D5.0 Draft standard for the Evaluation of Voting Equipment.*

[7] International Organization for Standardization (1998). *ISO 9241: Part 11: Guidance on usability*

[8] International Organization for Standardization (1999). *ISO/IEC 15408: Information technology -- Security techniques -- Evaluation criteria for IT security.*

[9] International Organization for Standardization (2008). *ISO 9241: Part 171: Guidance on software accessibility*

[10] International Organization for Standardization (2013). *ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems – Requirements*

[11] Karokola, G. R., Kowalski, S., Yngström, L. (2012). *Secure e-Government services: Protection Profile for Electronic Voting - A Case of Tanzania*. IST-Africa 2012 Conference Proceedings. Paper presented at Regional Impact of Information Society Technologies Conference, IST-Africa. IIMC International Information Management Corporation.

[12] Lee, K.-W., Lee, Y., Won, D., Kim, S. (2010). *Protection Profile for Secure E-Voting Systems*. ISPEC (pp. 386-397), Springer.

[13] Neumann, S., Kahlert, A., Henning, M., Jonker, H., Volkamer, M. (2013). *Informatische Modellierung der Prinzipien des gesetzlichen Gestaltungsspielraums im Hinblick auf Wahlsysteme.* Internationales Rechtsinformatik Symposion (IRIS 2013) (pp. 277-284), Weblaw.ch.

[14] Neumann, S., Kahlert, A., Henning, M., Richter, P., Jonker, H., Volkamer, M. (2013). *Modeling the German Legal Latitude Principles.* Fifth International Conference on eParticipations (ePart) (pp. 49-56), Springer.

[15] Roßnagel, A., Richter, P., Kahlert, A., Volkamer, M., Neumann, S., Grimm, R., Simic-Draws, D. (2013): *Holistic and Law compatbile IT Security Evaluation*. Angenommen zur Publikation in International Journal on Information Security and Privacy.

[16] Secrétariat général de la défense nationale (2006). *Protection Profile: Machine a voter (PP-CIVIS)*. http://www.commoncriteriaportal.org/files/ppfiles/pp0604.pdf