



Erfahrungsbericht über die erste Common Criteria-Evaluierung eines Wahlsystems: dem Digitalen Wahlstift

Dr. Sönke Maseberg

CAST-Workshop „Elektronische Wahlen und Wahlmaschinen“

17. Oktober 2008



Agenda



- Hintergründe zum geplanten, aber nicht durchgeführten Einsatz des digitalen Wahlstiftsystems in Hamburg
 - Motivation
 - Funktionsweise des digitalen Wahlstifts
- Einblicke in die weltweit erste Evaluierung eines digitalen Wahlsystems
 - Common Criteria-Evaluierung
- Grenzen der Evaluierung

Motivation



- 13.06.2004 neues Wahlrecht:
 - 1 Stimme für die Landesliste und 5 Stimmen für die Wahlkreislisten
 - = 6 Stimmen je Wahl
 - Panachieren und Kumulieren

- Wahl 2008: Landtagswahl und Kommunalwahl.
 - 12 Stimmen pro Wähler

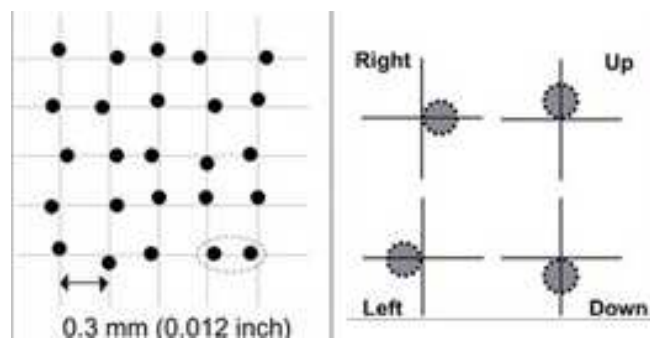
- Digitales Wahlstiftsystem



HAMBURG-WAHL 2008

1 A-Partei – A	
Gesamtliste – A	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
<i>Kandidatinnen und Kandidaten</i>	
1 Aramann, Jürgen, Stadtteil, 1935, Landwirt	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
2 Albers, Henning, Stadtteil, 1975, Jurist	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
3 Augustin, Christa, Stadtteil, 1942, Rentnerin	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
4 Arps, Matthias, Stadtteil, 1979, Student	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
5 Alan, Karin, Stadtteil, 1942, Hausfrau	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
6 Aukes, Norbert, Stadtteil, 1937, Pensionär	<input checked="" type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
7 Aven, Bernd Wilhelm, Stadtteil, 1950, Kaufmann	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
8 Atabaki, Holger, Stadtteil, 1968, Kaufmann	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
2 B-Partei – B	
Gesamtliste – B	<input checked="" type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
<i>Kandidatinnen und Kandidaten</i>	
1 Bitzer, Torsten, Stadtteil, 1981, Student	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
2 Bade, Rolf, Stadtteil, 1973, Angestellter	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
3 Brinck, Christoph, Stadtteil, 1942, Lehrer	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
4 Bauer, Murat, Stadtteil, 1972, Dipl.-Pädagoge	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>

Digitales Wahlstiftsystem I



1 A-Partei – A	
Gesamtliste – A	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<i>Kandidatinnen und Kandidaten</i>	
1 Aramann, Jürgen , Stadtteil, 1935, Landwirt	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2 Albers, Henning , Stadtteil, 1975, Jurist	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3 Augustin, Christa , Stadtteil, 1942, Rentnerin	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 Arps, Matthias , Stadtteil, 1979, Student	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5 Alan, Karin , Stadtteil, 1942, Hausfrau	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6 Aukes, Norbert , Stadtteil, 1937, Pensionär	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7 Axen, Bernd Wilhelm , Stadtteil, 1950, Kaufmann	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
8 Atabaki, Holger , Stadtteil, 1968, Kaufmann	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2 B-Partei – B	
Gesamtliste – B	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<i>Kandidatinnen und Kandidaten</i>	
1 Bitzer, Torsten , Stadtteil, 1981, Student	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2 Bade, Rolf , Stadtteil, 1973, Angestellter	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3 Brinck, Christoph , Stadtteil, 1942, Lehrer	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 Bauer, Murat , Stadtteil, 1972, Dipl.-Pädagoge	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>



Quellen der Graphiken: www.anoto.de, www.dotvote.de,
Freie und Hansestadt Hamburg

Digitales Wahlstiftsystem II



 **Ihre Wahl wurde registriert!**

Der Stift wurde geleert und Ihr Wahlvorgang ist abgeschlossen!

Ergebnisausdruck

Hauptbereich

Wahl zur XX. Bürgerschaft (Landesliste) am 30. September 2007
Ergebnismittlung

Wahlbezirk: 100

B	Wähler	0
B 1	davon mit Wahrschein	0
C	ungültige Stimmen	0
D	gültige Stimmen	0

Nr.	Partei / Wählergruppe	Stimmen
DO	CDU	0
DO	SPD	0
DO	GRÜNE/GAL	0
DO	PRO DM/SCHILL	0
DO	FDP	0

Aktuelle Seite: 1 | Seiten gesamt: 1 | Zoomfaktor: Seitenbreite

[Weiter >>](#)

Stimmzettelprüfung

Bezirksversammlungswahl (Wahlkreisliste)

Seite vor/zurück:  1 von 2

Stimmzettel 5 Anzeige mit Leerseite

Lebensmittelchemikern					
0312	Meier-Hedde, Felix, Bergedorf, 1968, EDV-Berater	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0313	Vollmer, Anette Helga, Bergedorf, 1967, Polit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0314	Richter-Hoops, Birgit, Bergedorf, 1959, EDV Kaufrau	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0315	Becker-Ewe, Ute, Lohbrügge, 1942, Versicherungskauffrau	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0316	Lentfer, Joachim, Bergedorf, 1957, Augenoptikermeister	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0317	Grabner, Silke, Bergedorf, 1963, Postbeamtin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0318	Fleige, Norbert, Bergedorf, 1955, Dipl.-Ing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0319	Hoops, Jessica, Bergedorf, 1984, Auszubildende	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0320	Müller-Kleßmann, Frank, Bergedorf, 1948, Studienrat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4 Freie Demokratische Partei – FDP

0400	Gesamtliste - FDP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0401	Barnatzki, Carsten, Bergedorf, 1960, Verleger	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	enwerder, 1936, Betriebswirt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	, Bergedorf, 1984, Student	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	n, Lohbrügge, 1938, Logistiker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Begründung zur Entscheidung **Grund 1** **Grund 2**

[Weiter >>](#)

 **Zweifelhafte Stimmzettel**
3

 **Der Stimmzettel kann nach "gültig" verschoben werden.**

 **Gültige entschiedene Stimmzettel**
3

 **Bitte geben Sie eine Begründung ein.**

 **Ungültige entschiedene Stimmzettel**
0

[Weiter >>](#)

datenschutz cert

Quellen der Graphiken: www.anoto.de, www.dotvote.de, Freie und Hansestadt Hamburg

Zulassungsvoraussetzungen



- Common Criteria-Evaluierung durch Prüfstelle
- Zertifizierung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik)
 - Basis der Evaluierung: Schutzprofil
- Prüfung der PTB (Physikalisch-technische Bundesanstalt)
- ULD-Datenschutz-Gütesiegel

Common Criteria-Evaluierung



- Schutzprofil
 - Anforderungen Innenbehörde Hamburg (Nutzung Common Criteria Teil 2)
- Sicherheitsvorgaben
 - Produktspezifische Anforderungen
→ definieren Sicherheitsmaßstab
- Prüfung des Produktes gegen diesen Sicherheitsmaßstab
- Prüftiefe/Vertrauenswürdigkeit (CC Teil 3)
- Zertifikat

Schutzprofil: Inhalt



Was beinhaltet das Schutzprofil?

- Beschreibung der Produktklasse „Wahlstiftsystem“ und der Einsatzumgebung
- Annahmen
- Bedrohungen
- Sicherheitserwartungen und -ziele
- Anforderungen
 - Funktionale Anforderungen (zum Erreichen der Sicherheitsziele)
 - Anforderungen an die Vertrauenswürdigkeit (EAL3+)

Schutzprofil: Abgrenzung I



Was gehört zum DWS?

- Anwendung zur Speicherung, Bewertung und Zählen der elektronischen Stimmen
- Digitale Stifte auf Grundlage der Anototechnologie, inklusive Stiffirmware und Dockingstationen



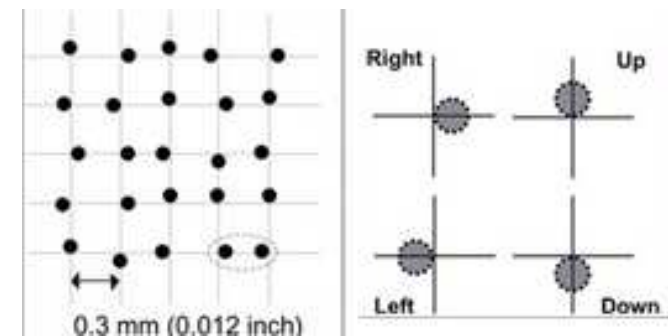
datenschutz cert

Schutzprofil: Abgrenzung II



Was gehört **nicht** zum DWS?

- Computer mit Betriebssystem
- Stimmzettel (das Anoto-Papier, Konfigurationsdaten)



datenschutz cert

Schutzprofil: Annahmen (Auszug)



- **A.Konfiguration:** Die für die Bewertung benötigten Stimmzetteldaten werden vor Beginn der Wahl vom Administrator ordnungsgemäß, vollständig und korrekt auf dem EVG installiert.
- **A.Personal:** Administrator und Wahlvorstand handeln nicht sorglos, nachlässig oder feindselig. Sie beachten und befolgen die von der Benutzer- und Systemverwalterdokumentation zur Verfügung gestellten Anweisungen.
- **A.Verbindung:** Alle Verbindungen zwischen den Geräten in der IT-Umgebung des EVG sind drahtgebunden und befinden sich innerhalb des Wahllokals. (...)

Schutzprofil: Bedrohungen



- T.Anonymität
- T.Beweis
- T.Betriebsstörung
- T.ManipulationStift
- T.ManipulationErgebnis
- T.Verzettbarkeit
- T.Wahlvorgang

Schutzprofil: Sicherheitsziele



- OT.Anonymität
- OT.Aufzeichnung
- OT.Auszählung
- OT.Bewertung
- OT.Ergebnisfeststellung
- OT.Protokollierung
- OT.Quittungsfreiheit
- OT.Robustheit
- OT.Unverkettbarkeit
- OT.Verifikation
- OT.Wahlhandlung
- OT.Wahlvorgang



FCS_COP.1 Cryptographic operation

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
- FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation]
- FCS_CKM.4 Cryptographic key destruction
- FMT_MSA.2 Secure security attributes

FCS_COP.1.1 **The TSF shall perform *{cryptographic checksum generation}* in accordance with a specified cryptographic algorithm *{SHA-256}* and cryptographic key sizes *{none}* that meet the following: *{FIPS180-2}*.**

Schutzprofil: Prüftiefe EAL3+



Assurance class	Assurance Family	Assurance Components by						
		Evaluation Assurance Level						
		EAL1	EAL2	EAL3+	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM			1	1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			3	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

CC-Evaluierung I



- ASE Sicherheitsvorgaben
 - Sicherheitsmaßstab konform zum Schutzprofil?
- ADV Entwicklungsdokumente
 - Werden die funktionalen Anforderungen umgesetzt?
 - FSP Funktionale Spezifikation
 - HLD High Level Design
 - SPM EVG-Sicherheitsmodell
- ATE Tests
 - Herstellertests
 - unabhängige Tests der Prüfstelle

CC-Evaluierung II



- Prüfung der Entwicklungsstandorte
 - ALC Lifecycle
 - ACM Konfigurationsmanagement
 - ADO Auslieferung
- AGD Handbücher
 - Wahlvorstand
 - Administrator (Installationsprozeduren)
 - Wähler
- AVA Schwachstellenanalyse
 - Stärke der Sicherheitsfunktionen
 - Möglichkeiten des Missbrauchs
 - offensichtliche Schwachstellen

Grenzen der Evaluierung



- Umfang/Tiefe der Evaluierung
 - Einsatz eines Laptops mit Standard-Betriebssystem
 - Innentäter
- vgl. Annahmen:
- organisatorische Maßnahmen an Administratoren und Wahlvorstand
 - korrekte Installation
 - keine Verbindungen
- Akzeptanz/Mitwirkung des Wählers
 - Angriffe auf Wahlstift, System und Stimmzettel

Fazit



- Weltweit erste Common Criteria-Evaluierung eines digitalen Wahlsystems
- Erfolgreiche Evaluierung des digitalen Wahlstiftsystems
- Common Criteria als Methodik grundsätzlich geeignet

Vielen Dank für Ihre Aufmerksamkeit



Dr. Sönke Maseberg

datenschutz cert GmbH

Barkhausenstr. 2

27568 Bremerhaven

Tel.: 0471 / 300 11-19

Fax.: 0471 / 300 11-11

smaseberg@datenschutz-cert.de

www.datenschutz-cert.de

