Kurzgutachten zur Zertifizierung des Produkts Digitales Wahlstiftsystem dotVote® (Version 1.0)

im Auftrag der Behörde für Inneres, Hamburg

datenschutz nord GmbH

September 2008

Inhaltsverzeichnis

Kurzgutachten zur Zertifizierung des Produkts Digitales Wahlstiftsystem dotVote® (Version 1.0)

1. Zeitpunkt bzw. Zeitraum der Prüfung

Die Auditierung des Produkts „Digitales Wahlstiftsystem dotVote“ erstreckte sich auf den Zeitraum von September 2007 bis Juli 2008. Die Auditierung und abschließende Prüfung basiert auf einer konzeptionellen Analyse sowie einer – *im Rahmen einer parallel durchgeführten Evaluation nach dem Common Criteria-Standard (Stufe: EAL 3+)* - intensiven technischen Prüfung des Produkts.

2. Antragstellerin

Antragstellerin ist die

Innenbehörde des Landes Hamburg
Johanniswall 4
20095 Hamburg

Ansprechpartner ist Herr Thomas Steffens.

Hersteller des Produkts ist ein Konsortium der Firmen Diagramm Halbach (Schwerte) und WRS Softwareentwicklung (Hamm).

3. Sachverständiger/Prüfstelle

Prüfstelle ist die

datenschutz nord GmbH
Barkhausenstr. 2
27568 Bremerhaven.

Ansprechpartner sind Herr Dr. Maseberg, Herr von Rahden (Technik) und Herr Oliver Stutz (Recht).

4. Kurzbezeichnung des IT-Produkts

Digitales Wahlstiftsystem dotVote®, Version 1.0

5. Beschreibung des IT-Produkts, Zweck und Einsatzbereich

Das Digitale Wahlstift-System dotVote® ist ein Wahlgerät für die elektronische Abgabe, Speicherung, Bewertung und Auszählung von Stimmen. Es unterstützt die gleichzeitige Durchführung mehrerer Wahlen und erlaubt die schnelle Ermittlung der Wahlergebnisse, ohne dabei auf die papiergebundenen Stimmzettel verzichten zu müssen, d.h. das System verwendet immer auch die Papierversion eines Stimmzettels.

Hauptbestandteil des Produkts ist ein kugelschreiberähnlicher Stift, der zusätzlich zur herkömmlichen Kugelschreibermine eine Kamera, Prozessor und Speicher beinhaltet. Außerdem umfasst das System drei Dockingstationen, mit denen der Stift je nach Situation registriert, aktiviert oder zurückgesetzt wird bzw. mit denen die mit dem Stift abgegebenen Stimmen an den PC via USB-Schnittstelle übertragen werden. Softwareseitig wird das System durch die dotVote-Applikation und eine Datenbank ergänzt.

Die Stimmzettel haben einen speziell bedruckten Hintergrund (Raster), womit die Koordinaten zur Ermittlung der Stimmabgabe ermittelt werden. Der bzw. die

Stimmzettel (bei gleichzeitiger Durchführung mehrerer Wahlen an einem Wahltag werden mehr als ein Stimmzettel verwendet) sind als Konfigurationsdateien im Speicher des Wahlstifts hinterlegt, so dass der Stift bei Abgabe des „Kreuzchens“ stets „weiß“, wo auf dem Stimmzettel die Markierung gesetzt wird.

Nach dem Schluss der Wahlhandlung werden alle in den elektronischen Wahlurnen gespeicherten Stimmen von der dotVote-Software automatisch ausgewertet. Dabei erkennt die Software zweifelhafte Markierungen und zeigt sie dem Wahlvorstand an, dieser muss - wie bei einer herkömmlichen Papierwahl auch - die zweifelhaften Stimmen individuell dahingehend bewerten, ob der Wählerwille hinreichend deutlich kenntlich gemacht wurde. Die automatisch bewerteten Stimmzettel können vom Wahlvorstand eingesehen werden, auf diese Weise wird sichergestellt, dass der Wahlvorstand stets die letztendliche Entscheidung über die Gültigkeit der Stimme hat. Nach dem Abschluss der individuellen Bewertung der zweifelhaften Stimmzettel erfolgt die automatische Auszählung der Stimmen. Abschließend wird die elektronische Wahlurne „verschlossen“, d.h. mit einem elektronischen „Fingerprint“ versehen. Die Wahlergebnisse werden gemeinsam mit dem Fingerprint ausgedruckt und so das Ergebnis vor späteren Manipulationen geschützt.

6. Tools, die zur Herstellung des Produkts verwendet wurden

Das Digitale Wahlstift-System dotVote besteht aus folgenden Bestandteilen:

- --- Digitaler Wahlstift (Logitech IO2 BT, P/N 866142-1000) mit „dotVote“ Etikett,
- --- zugehörige USB Dockingstationen (Logitech P/N 866108-0000) mit Markierungsetiketten (DH67266 und DH67558),
- --- Block mit Anoto-Pattern für Funktionstest (TC: 4665.508.67283 V110607),
- --- Firmware des Digitalen Wahlstifts (FW U44.53),
- --- dotVote® Applikation Version 1.0 (Software).

7. Voraussetzungen für den Einsatz des DWS

Grundsätzlich ist das DWS für den Einsatz bei unterschiedlichsten Wahlen geeignet, da – im Gegensatz zu Wahlcomputern - die elektronischen Stimmen stets anhand der ebenfalls vorhandenen Papierstimmen kontrolliert werden können. Soweit das System für Landtagswahlen eingesetzt werden soll, muss zuvor sicher gestellt sein, dass Wahlgesetz und Wahlordnung diese Art der Stimmabgabe zulassen. In Schleswig-Holstein ermöglicht das Landeswahlgesetz Schleswig-Holstein mit der offenen Formulierung des § 39 Abs. 2 LWahlG

> *Die Wählerin oder der Wähler gibt [...]*
>
> *ihre oder seine Zweitstimme in der Weise ab, daß sie oder er durch ein auf den Stimmzettel gesetztes Kreuz oder auf andere Weise eindeutig kenntlich macht, welcher Landesliste sie gelten soll.*

grundsätzlich auch die Nutzung alternativer Wahlsysteme wie des DWS.

In § 39 Absatz 3 LWahlG wird darüber hinaus deutlich gemacht, dass für die Durchführung der Wahl zwar auch alternative Wahlverfahren (sog. Stimmenzählgeräte -

z.B. das DWS) angewendet werden dürfen, dies muss jedoch zuvor durch das zuständige Innenministerium zugelassen werden, d.h. hierzu bedarf es einer Ergänzung bzw. Änderung der Wahlordnung. Eine solche muss auch Regelungen dafür vorsehen, wie mit Abweichungen zwischen Papierstimme und elektronischer Stimme umzugehen ist.

Soweit eine solche Zulassung erfolgt, wäre der Einsatz des DWS somit auch in Schleswig-Holstein nach dem Wahlgesetz zulässig.

8. Besondere Sicherheitsvorkehrungen für den Einsatz des Produkts

Aus technischer Sicht erfüllt das DWS alle datenschutzrechtlichen Anforderungen, insbesondere die Eigenschaft einer geheimen Wahl. Es wird vom DWS sichergestellt, dass eine Zuordnung von Stimme zum Wähler nicht möglich ist, auch nicht unter Zuhilfenahme von Zeit-Informationen. Vergleiche hierzu die Common Criteria Zertifizierung, Zertifikatsnummer „BSI-DSZ-CC-0444-2008“.

Damit die Funktion des DWS im vollen Umfang gewährleistet ist, müssen zum einen die Annahmen an die Umgebung (Kapitel 3.1.2 der Sicherheitsvorgaben) erfüllt sein. Der Wahlveranstalter hat diese zu erfüllen, um das DWS zertifikatskonform einzusetzen. Hierzu gehört u.a., dass das DWS keine Verbindungen von/nach außerhalb des Wahllokals zulässt, alle Verbindungen kabelgebunden und auf die in den Sicherheitsvorgaben definierten beschränkt sind.

Zum anderen ist die Integrität des DWS im Wahllokal sicherzustellen, Zu diesem Zweck sind vom Hersteller detaillierte Auslieferungsprozeduren festgelegt worden, die die Integrität des DWS in jeder Phase der Auslieferung schützen:

Phase 1: Übergabe und Installation der dotVote® Applikation (ohne Konfiguration und daher nicht betriebsbereit)

Phase 2: Übergabe der Hardware (Digitale Wahlstifte mit installierter dotVote® Firmware und Zubehör sowie Bedienungsanleitungen)

Phase 3: Übergabe und Installation der wahlspezifischen dotVote® Konfiguration (für die Herstellung der Betriebsbereitschaft)

Phase 4: Bereitstellung des DWS und seiner Betriebsumgebung in den Wahllokalen

Phase 5: Inbetriebnahme des DWS und seiner Komponenten

In Phase 1 wird eine eindeutig gekennzeichnete Master-Copy-CD per Kurier an den Wahlveranstalter (bzw. den beauftragten Dienstleister) übergeben. Dieser muss mit Hilfe von zur Verfügung gestellten Hilfsmitteln die Integrität und Authentizität des Inhalts auf der CD überprüfen. Für den Zeitraum ab Erhalt des DWS bis zum Einsatz im Wahllokal hat der Wahlveranstalter sicherzustellen, dass keine Unbefugten Zugang zu den Systemen haben. Die Installation des DWS ist im 4-Augen-Prinzip durchzuführen.

In Phase 2 wird die vom DWS verwendete Hardware in versiegelter Form ausgeliefert. Bei Empfang hat der Wahlveranstalter die Vollständigkeit der Lieferung nach Frachtpapieren und die Unversehrtheit der Lieferung, insbesondere der Siegel, zu

bestätigen. Für den Fall von Unvollständigkeit oder Beschädigung sind Konsequenzen eindeutig definiert, um die Sicherheit des DWS weiterhin zu gewährleisten.

In Phase 3 werden die Konfigurationsdaten, d.h. die Wahllisten und die Konfiguration der zugehörigen Stimmzettel sowie die Liste der zugelassenen Wahlstifte auf die gleiche Weise wie in Phase 1 ausgeliefert.

In Phase 4 wird das DWS in den Wahllokalen bereitgestellt. Hierfür sind vom Hersteller Vorgaben und Mechanismen bereitgestellt, die dem Wahlvorstand bei Inbetriebnahme des DWS ermöglichen, festzustellen, ob das DWS unversehrt ist. Er hat die Anweisung, bei Verdacht auf Manipulation des DWS ein neues DWS anzufordern.

In Phase 5 wird das DWS vom Wahlvorstand in Betrieb genommen. Ab diesem Zeitpunkt steht es unter Kontrolle und ständiger Aufsicht durch den Wahlvorstand. Mit Hilfe des gut verständlichen Benutzerhandbuchs und der bereitgestellten Kennzeichnungsetiketten ist der Wahlvorstand in der Lage das DWS korrekt in Betrieb zu nehmen und, auch für den Wähler sichtbar, korrekt zu bedienen.

Insgesamt stellen die bei der Auslieferung getroffenen Maßnahmen sicher, dass das DWS unverändert zum Einsatz kommt.

9. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 1.2

10. Zusammenfassung der Prüfergebnisse

Anforderung	Stimmdatensätze	Konfigurationsdaten
Zulässigkeit	zulässig	
Technikgestaltung		
Datensparsamkeit	vorbildlich	adäquat
Löschen, Anonymisierung, Pseudonymisierung	vorbildlich	vorbildlich
Transparenz und Produktbeschreibung	vorbildlich	vorbildlich
T/O-Maßnahmen		
Unbefugten Zugang verhindern	vorbildlich	vorbildlich
Unbefugte Verarbeitung oder Kenntnisnahme verhindern	vorbildlich	n.a.
Angemessene Protokollierung	n.a.	Vorbildlich
Betroffenenrechte		

Aufklärung/Benachrichtigung	n.a.
Auskunft	
Berichtigung/Sperrung/Löschung, Widerruf	

11. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Soweit die Bewertung „Förderung des Datenschutzes“ als Instrument zur Verhinderung rechtlich unzulässiger Verarbeitung personenbezogener Daten zu verstehen ist, können dem Wahlstiftsystem dotVote hervorragende Eigenschaften bescheinigt werden: Mit diversen, sehr durchdachten Funktionen wird sichergestellt, dass das grundrechtlich geschützte Wahlgeheimnis - letztlich ein explizites verfassungsrechtliches Verbot personenbezogener Datenverarbeitung - in allen Ausprägungen gewahrt wird. Personenbezogene Daten werden mit dem System somit überhaupt nicht erhoben oder verarbeitet. Zusätzlich bestehen aufgrund der systemimmanenten Funktionen zur Sicherstellung der Anonymität der Stimmabgabe mit der Verwendung des dotVote-Systems weniger Missbrauchsmöglichkeiten (zur Fälschung von Wahlergebnissen), als bei Verwendung herkömmlicher Stimmzettel.

Im Hinblick auf die getroffenen technisch-organisatorischen Sicherheitsmaßnahmen sind sämtliche Vorkehrungen für denkbare Angriffsszenarien getroffen worden. Dies wird nicht zuletzt durch die erfolgreiche, parallele Zertifizierung nach dem CommonCriteria-Standard (EAL 3+) verdeutlicht. Auf die Ergebnisse dieser Zertifizierung wird hier zur Vermeidung von Wiederholungen verwiesen:

http://www.hamburg.de/servlet/contentblob/349886/BSi_Zertifikat_2008/data.pdf