Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612

BESCHEINIGUNG NACH § 34 ABS. 6 HSG 1998[1]

Client und Wahlserversoftware: pnyx-austria 2.0.4.

Hersteller:
SCYTL Secure Electronic Voting, S.A.
Tuset 20
08006 Barcelona, Spanien

Antragsteller:
Bundesministerium für Wissenschaft und Forschung
Minoritenplatz 5
1014 Wien

Bescheinigung ausgestellt am: 27.3.2009
Referenznummer A-SIT-1.078

1. Beschreibung der zu bescheinigenden Komponenten

Gemäß HSWO 2005[2] sind der Client[3] und die Wahlserversoftware[4] des elektronischen Wahlsystems[5] von einer Bestätigungsstelle gemäß § 34 Abs. 6 HSG 1998 zu bescheinigen.

Client:

Als Client kommt ein Java-Applet zum Einsatz, das von den Wählerinnen und Wählern über das Internet-Portal des elektronischen Wahlsystems bezogen wird. Die Authentizität des Clients kann von den Wählerinnen und Wählern an Hand einer elektronischen Signatur überprüft werden.

Über den Client erfolgt:

- Die Identifikation (unter Verwendung der Bürgerkarte gemäß E-GovG[6]) und Authentifizierung der Wählerinnen und Wähler sowie die Überprüfung der Wahlberechtigungen durch Kommunikation mit dem Voting-Service über den Voting-Proxy.

[1] Bundesgesetz über die Vertretung der Studierenden (Hochschülerinnen- und Hochschülerschaftsgesetz 1998 – HSG 1988), BGBl. I Nr. 22/1999 zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 2/2008.
[2] Verordnung der Bundesministerin für Bildung, Wissenschaft und Kultur, mit der die Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 - HSWO 2005 erlassen wird, BGBl. II Nr. 91/2005 zuletzt geändert durch die Verordnung BGBl. II Nr. 351/2008
[3] Definition laut § 1 Z. 5 HSWO 2005: „Client: Lokales Softwaresystem bei der Wählerin oder dem Wähler zur Stimmabgabe mittels E-Voting;“
[4] Definition laut § 1 Z. 4 HSWO 2005: „Wahlserversoftware: Programm, das im Rahmen von E-Voting von der Wahlkommission zur Wahrnehmung ihrer Aufgaben herangezogen wird;“
[5] Definition laut § 1 Z. 3 HSWO 2005: „Elektronisches Wahlsystem: Hardware- und Softwaresystem zur Durchführung von E-Voting;“
[6] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), BGBl. I Nr. 10/2004, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 59/2008

- Das Ausfüllen der elektronischen Stimmzettel durch die Wählerinnen und Wähler sowie die Anzeige der getroffenen Wahloptionen vor der Stimmabgabe.
- Die Verschlüsselung der elektronischen Stimmzettel.
- Die Anforderung eines von der Wählerin oder dem Wähler überprüfbaren Prüfcodes und eines zugehörigen vom Voting-Service signierten Bestätigungscodes.
- Die Berechnung eines Hashwerts aus dem Prüfcode und dem verschlüsselten Stimmzettel. Diese Hashwerte werden mit dem Text einer eidesstattlichen Erklärung durch die Wählerinnen und Wähler, dass die Stimmabgabe persönlich, unbeobachtet und unbeeinflusst erfolgt ist, an die Bürgerkartenumgebung zur qualifizierten Signatur übergeben. Die Signatur und der verschlüsselte Stimmzettel werden dann vom Client an das Voting-Service übermittelt.
- Nach der Stimmabgabe und erfolgreicher Verifikation der Signatur durch das Voting-Service die Anzeige des Prüfcodes und des zugehörigen vom Voting-Service signierten Bestätigungscodes.

Zum Nachweis der Identität der Wählerinnen und Wähler unter Verwendung der Bürgerkarte gemäß E-GovG bzw. zum Auslösen von qualifizierten elektronischen Signaturen verwendet der Client eine Bürgerkartenumgebung, die die Applikationsschnittstelle Security-Layer[7] zur österreichischen Bürgerkarte implementiert. Die Sicherheit und Verwendung der Bürgerkarte sind im SigG[8] bzw. E-GovG geregelt und es sind daher die Elemente Bürgerkarte und Bürgerkartenumgebung nicht Gegenstand dieser Bescheinigung.

Wahlserversoftware:

Die Wahlserversoftware besteht aus den folgenden Kernkomponenten:

- Voting-Service:

  Komponente zur Entgegennahme (über den Voting-Proxy) und Verwahrung der verschlüsselten Stimmen vom Client. Auf das Voting-Service kann nicht direkt vom Internet aus zugegriffen werden.

- Voting-Proxy

  Komponente zur Abwicklung der Kommunikation zwischen Client und Voting-Service. Zur Identifizierung und Authentifizierung der Wählerinnen und Wähler sowie zur Prüfung von Signaturen werden vom Voting-Proxy entsprechende Module genutzt.

- Administration-Service

  Komponente zur Konfiguration und Administration des Voting-Services und des Mixing-Services. Mit dieser Komponente werden u.a. Beginn- und Endzeiten der elektronischen Wahl festgelegt und der Schlüssel der Bundeswahlkommission generiert und auf Teilkomponenten verteilt, die auf SmartCards gespeichert werden.

- Mixing-Service

  Komponente zur Entschlüsselung und Anonymisierung der Stimmen. Die verschlüsselten Stimmen werden zuerst durch Prüfung der Signaturen verifiziert und dann nach Rekonstruktion des Schlüssels der Bundeswahlkommission aus den Teilkomponenten entschlüsselt. Im Zuge des Entschlüsselungsvorgangs werden die Stimmen so vermischt, dass danach keine Zuordnung mehr zwischen der Reihenfolge der Stimmen vor und nach dem Mixing-Prozess und damit auch keine Zusammenführung der Identität der Wählerin oder des Wählers mit ihrem oder seinem Wahlverhalten mehr möglich ist. Das Mixing-Service generiert für jede elektronische Wahlurne neben einer Liste der anonymisierten abgegeben Stimmen

[7] Siehe: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/
[8] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999) zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 8/2008.

auch eine Liste, die die IDs der Stimmzettel enthält, die am Mixing-Prozess teilgenommen haben.

Für das Administration-Service und Mixing-Service ist der Betrieb auf einem isolierten System, dessen Installation und Initialisierung unter einem unabhängigen Audit stattfindet vorgesehen. Nach dem Ablauf der Wahlen ist eine gesicherte Verwahrung der verwendeten sicherheitsrelevanen Komponenten vorgesehen.

Die gesamte Software (Client und Wahlserversoftware) wird vom Hersteller als Quellcode an das Bundesministerium für Wissenschaft und Forschung übergeben und von diesem (bzw. dessen Dienstleister) compiliert. Für die Installation des Systems zur Compilierung, den Compilierungsvorgang selbst sowie die Installation der erzeugten Programme ist ein unabhängiges Audit vorgesehen.

2. Erfüllung der Anforderungen des HSG 1998 und der HSWO 2005

Der Client und die Wahlserversoftware erfüllen unter nachstehenden Einsatzbedingungen die Sicherheitsanforderungen des § 34 HSG 1998 sowie des § 64 HSWO 2005.

Die Erfüllung der Sicherheitsanforderungen wurde durch die Bestätigungsstelle unter Heranziehung der Empfehlung des Ministerkomitees des Europarates an die Mitgliedsstaaten Nr. Rec2004(11) vom 30. September 2004 zu den rechtlichen, operationalen und technischen Standards von E-Voting („Legal, Operational and Technical Standards for E-Voting“), erlassen gemäß Art. 15 Abs. b Satzung des Europarates, BGBl. Nr. 121/1956, idgF, überprüft.

3. Geltungsbereich

Die Überprüfung der bescheinigten Komponenten und Verfahren erfolgte unter den Randbedingungen des HSG 1998 und der HSWO 2005 in der jeweiligen zum Zeitpunkt der Ausstellung dieser Bescheinigung gültigen Fassung. Diese Bescheinigung ist daher ausschließlich im Anwendungsbereich dieser Rechtsgrundlagen gültig.

4. Einsatzbedingungen

Die Gültigkeit dieser Bescheinigung ist an die im Folgenden angeführten Einsatzbedingungen gebunden:

(1) Schlüssellängen:

Client und Wahlserversoftware sind so zu konfigurieren, dass Schlüssellängen für die verwendeten kryptographischen Algorithmen so gewählt werden, dass diese dem aktuellen Stand der Technik entsprechen und das bei qualifizierten elektronischen Signaturen erforderliche Sicherheitsniveau erreichen.

(2) Client:

Für die sichere Nutzung des Clients ist vorauszusetzen, dass der jeweilige von den Wählerinnen und Wählern verwendete Rechner frei von Software ist, die den Client in seiner korrekten Funktion beeinflussen oder beobachten kann. Über das Internet-Portal[9] sind daher entsprechende Sicherheitshinweise vorzusehen, die den Wählerinnen und Wählern vor Abgabe der Stimme angezeigt werden. Insbesondere ist auch darzustellen, wie sie die Echtheit des Clients überprüfen können und dass sie verhindern können, dass Restinformationen am Clientrechner gespeichert bleiben.

(3) Wahlserversoftware:

Für den sicheren Betrieb der Wahlserversoftware ist vorauszusetzen, dass diese auf vertrauenswürdigen Systemen compiliert und installiert wird. Die im Zuge der Bescheinigung

[9] Definition laut § 1 Z. 2 HSWO 2005: „Internet-Portal: Präsenz im Internet, die als zentraler Einstiegspunkt für die Benutzerinnen und Benutzer dient, die sich über E-Voting informieren oder ihre Stimme mittels E-Voting abgeben wollen;“. Das Internet-Portal ist nicht Gegenstand dieser Bescheinigung.

vorgelegten Konzepte zur Compilierung und Installation sind daher strikt einzuhalten und die durchgeführten Schritte zu protokollieren. Für Systeme, die bei der Generierung von sicherheitsrelevanten Schlüsseln verwendet werden, sind sichere Verfahren anzuwenden, die ein nachträgliches Auffinden von Restinformationen zu den generierten Schlüsseln verlässlich verhindern.

(4) Elektronische Wahlurne und Schlüssel der Wahlkommission:

Die elektronische Wahlurne und die Teilkomponenten des privaten Schlüssels der Wahlkommission sind nach der Auszählung der Stimmen auf gesicherte Weise und unter einem unabhängigen Audit nachweisbar sicher zu löschen bzw. zu vernichten. Die involvierten Systeme und Daten sind über den gesamten Lebenszyklus einschließlich aller Komponenten und Datenelemente kontrolliert und protokolliert so zu betreiben bzw. zu speichern, dass eine Manipulation oder ein Datentransfer nach außen auch organisatorisch ausgeschlossen ist.

Sollte aus rechtlichen Überlegungen eine Löschung nicht möglich sein, ist sicherzustellen, dass die Inhaber der Teilkomponenten des privaten Schlüssels der Wahlkommission keinen Zugriff auf die elektronische Wahlurne haben und ein Öffnen der elektronischen Wahlurne (für eine etwaige erneute Durchführung des Mixing-Prozesses) nur unter den gleichen sicheren Voraussetzungen wie im Zuge der Wahl durchgeführt wird. Bei einer Aufbewahrung der elektronischen Wahlurne ist des Weiteren zu beachten, dass wenn die zur Verschlüsselung verwendeten Schlüssellängen nicht mehr das bei qualifizierten elektronischen Signaturen erforderliche Sicherheitsniveau erreichen, eine zusätzliche Verschlüsselung der elektronischen Wahlurne vorzusehen ist. Die Infrastruktur und die Verschlüsselungsverfahren müssen dabei der technischen und organisatorischen Kontrolle innerhalb des Lebenszyklus der Komponenten und Datenelemente unterliegen. Die dabei verwendeten Schlüssel sind unter den gleichen sicheren Voraussetzungen wie im Zuge der Wahl zu generieren, auf Teilkomponenten aufzuteilen und an die oder den Vorsitzenden der Wahlkommission sowie weitere Mitglieder der Wahlkommission zu übergeben.

Wenn innerhalb des Lebenszyklus der Teilkomponenten des privaten Schlüssels der Wahlkommission, eine Inhaberin oder ein Inhaber einer Teilkomponente ihre oder seine Funktion im Sinne des HSG 1998 bzw. der HSWO 2005 nicht mehr ausüben sollte, ist für eine gesicherte Übergabe der Teilkomponente an ein Mitglied der Wahlkommission, das keine weitere Teilkomponente verwahrt, Sorge zu tragen.

(5) CA der Wahlschlüssel:

Das Sicherheits- und Betriebskonzept der Zertifizierungsstelle („Election-CA“), die die Zertifikate für die Schlüssel der Wahlsoftware ausstellen wird, muss nachweislich den Sicherheitsanforderungen der elektronischen Wahl im Sinne des HSG 1998 entsprechen.

5. Prüfbericht

Die dieser Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-1.078 dokumentiert.

Unterschriften:

Signaturwert	rxE7bTsRUAZVQ14ItmtmXhTw6IfMO8a+AOYmWsNRlVUmRg4c99h5IrYsRftHxveP	
	Unterzeichner	Manfred Holzbach, geschäftsführender Vorstand
	Datum/Zeit-UTC	2009-03-27T15:29:47Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	261828
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1238167787-349828@27573-20840-0-1342-5148
Prüfhinweis	Prüfinformation finden Sie unter: https://www.buergerkarte.at/signature-verification	

Signaturwert	WSlPee/1wzQCvkwxqGDgykw0h/DHDMjYDIEspXrwvVJtC6rZAg9stSIx7THRWeV/	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2009-03-27T18:41:18Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	193264
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1238175698-539917473@463887-463887-0-463887-463887
Prüfhinweis	Prüfservice: https://www.buergerkarte.at/signature-verification/	