Stellungnahme zum Audit-Bericht

Unabhängige Prüfung der Kantone Basel-Stadt, St.Gallen und Thurgau

Inhaltsverzeichnis

1 Einleitung

In Rahmen des Bewilligungsprozesses für den Einsatz der elektronischen Stimmabgabe wurden die Betriebsprozesse der Kantone Basel-Stadt, St. Gallen und Thurgau überprüft, um die Konformität der Prozesse in den Kantonen im Hinblick auf die Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) einzuschätzen.

Stéphane Adamiste von SCRT und Philippe Oechslin von Objectif Securité haben im Auftrag der Bundeskanzlei das Audit zwischen Juni und September 2022 durchgeführt. Dafür haben sie alle relevanten Dokumente erhalten, eine Simulation eines Urnengangs mitverfolgt und verschiedene Interviews mit den Kantonsvertreterinnen und Kantonsvertretern durchgeführt.

Parallel wurden die beiden Druckereien, die mit dem Druck und der Verpackung der E-Voting-Stimmrechtsausweise beauftragt sind, auditiert. Die Druckereien erfüllen alle Anforderungen vollumfänglich. Die Berichte der Druckereien weisen keine Nicht-Konformitäten aus.

2 Stellungnahme

Die Experten haben den Kantonen ein sehr gutes Zeugnis ausgestellt. Lediglich drei Abweichungen aus rund 130 Prüfpunkten wurden festgestellt sowie eine Empfehlung ausgesprochen. Die Kantone haben wo nötig von der Möglichkeit Gebrauch gemacht, in begründeten Fällen Ausnahmen von den Bundesvorgaben zu beantragen (Art. 16 Abs. 2 VEleS).

Zwei der Abweichungen (Offenlegung der Software für die Erstellung der Stimmrechtsausweise; Ausstellung sämtlicher Zertifikate durch ZertES-anerkannte Anbieter) sowie die Empfehlung zur Verwaltung der Zertifikate sollen noch im Verlaufe des Jahres 2023 behoben bzw. überprüft werden. Sie werden in diesem Kapitel ausgeführt. Die vierte Abweichung betrifft die Entschlüsselung der elektronischen Urne, die am Abstimmungssamstag am Mittag um 12 Uhr schliesst. Die Entschlüsselung und Auswertung erfolgt gemäss Bundesrecht am Sonntag. Allerdings werden in Basel-Stadt und St. Gallen die brieflichen Stimmabgaben bereits am Samstag ausgezählt. Die Auswertung der elektronischen Urne soll terminlich gleich gehandhabt werden wie die Auswertung der brieflichen Stimmabgaben. Die Entschlüsselung der elektronischen Urne lässt sich am Samstagnachmittag am besten in die Abläufe von Wahlen und Abstimmungen integrieren und entlastet so den terminlich bereits vollgepackten Abstimmungssonntag.

2.1 Art. 11 VEleS – Veröffentlichung

Artikel 11 der VEleS legt fest, dass der Quellcode der Software des Systems einschliesslich der Dateien mit relevanten Parametern offengelegt werden.

Die Experten habe festgestellt, dass dies nicht für alle Softwareteile umgesetzt wurde, die den Hauptprozess unterstützen:

Key	Art. 11
Finding	The source code of the software used to generate the polling cards and of the helper scripts is not published.
Recommendation	The source code of the software used to generate the polling cards and of the helper scripts should be published to enforce the principle of transparency.

Die Kantone stimmen der Einschätzung der Experten zu. Die folgenden Massnahmen wurden getroffen, um das Risiko zu minimieren:

- Wichtige Helper-Skripts werden vor der Inbetriebnahme veröffentlicht;
- Der Quellcode der Software des Kantons St. Gallen für die Generierung der Stimmrechtsausweise wird vor der Inbetriebnahme veröffentlicht;
- Der Quellcode der Software der Kantone Thurgau und Basel-Stadt wird im Laufe des Jahres 2024 veröffentlicht. Die beiden Kantone haben operative Massnahmen getroffen. Dazu hat die Firma Objectif Sécurité beide Programme im Auftrag der Bundeskanzlei auditiert und die geringen Risiken beim Einsatz bestätigt.

Das Restrisiko wird als gering eingeschätzt. Auf dieser Grundlage haben alle Kantone eine Ausnahme gemäss Art. 16 Abs. 2 VEleS beantragt.

2.2 Ziffer. 15.4 VEleS – Zertifikate gemäss ZertES

Ziffer 15.4 der VEleS legt fest, dass die elektronische Signatur die Anforderungen an eine fortgeschrittene elektronische Signatur gemäss Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES) zu erfüllen hat.

Die Experten habe festgestellt, dass die Kantone dies nur teilweise konform ungesetzt haben:

Key	15.4
Finding	The examiners did not receive any evidence that the electronic certificates used for data signature originate from a recognised supplier of certificate services under the ESigA.
Recommendation	The cantons should ensure that the certificates they use for data signature are sourced from a recognised supplier of certificate services under the ESigA.

Einzelne Zertifikate, die im E Voting-Prozess verwendet werden, sind nicht von einem nach dem Bundesgesetz über die elektronische Signatur (ZertES; SR 943.03) anerkannten Anbieter ausgestellt (vgl. VEleS Anhang Ziff. 15.4 Satz 3), sondern von den Kantonen oder der Post. Die Authentizität dieser Zertifikate wird durch den physischen Austausch ihrer Fingerprints sichergestellt.

Aus sicherheitstechnischer Sicht ist das die bessere Lösung. Auf dieser Grundlage haben alle Kantone eine Ausnahme gemäss Art. 16 Abs. 2 VEleS beantragt.

2.3 Ziffer. 15.1 VEleS – Verwaltung der Zertifikate

Ziffer 15.1 der VEleS legt fest, dass elektronische Zertifikate nach besten Praktiken verwaltet werden.

Die Experten empfehlen allen drei Kantonen folgende Verbesserungsmöglichkeit:

Key	15.1
Finding	The cantons do not provide any detail regarding the “best practices” in place to manage certificates used on the informational cantonal websites dedicated to e-voting.
Recommendation	The best practices regarding the management of the said certificates should be detailed (e.g., generation, distribution, protection of private keys, revocation, renewal, etc.)

Die betroffenen Zertifikate werden ausserhalb des Betriebs der elektronischen Stimmabgabe verwaltet. Die Internetseite der Kantone gehören zur Standard-IT-Infrastruktur der Kantone, bei welcher der Grundschutz angewendet wird.

3 Schlussfolgerung

Die Kantone bedanken sich bei den Experten für die Zusammenarbeit, die kritische Prüfung der Prozesse und deren Dokumentation sowie für die wertvollen Verbesserungsvorschläge.

Die Kantone haben bereits die notwendigen Massnahmen getroffen, um das Risiko gering zu halten. Die vollständige Behebung der Nicht-Konformitäten ist für 2023 und 2024 vorgesehen.