Standeskanzlei Graubünden
Chanzlia chantunala dal Grischun
Cancelleria dello Stato dei Grigioni

Stellungnahme zum Audit-Bericht

Unabhängige Überprüfung des Kantons Graubünden

7001 Chur, Reichsgasse 35, Tel. 081 257 22 23, Tel. direkt , 081 257 21 41, www.staka.gr.ch

Inhaltsverzeichnis

1 Einleitung 2

2 Stellungnahme 2

2.1 Art. 11 VEleS - Offenlegung Software für Erstellung der Stimmrechtsausweise 2

2.2 Ziff. 11.1 Anhang VEleS - Entschlüsselung am Samstag 3

2.3 Ziff. 15.1 Anhang VEleS - Verwaltung der Zertifikate 3

2.4 Ziff. 15.4 Anhang VEleS - Zertifikate gemäss ZertES 4

3 Schlussfolgerung 4

1 Einleitung

In Rahmen des Bewilligungsprozesses für den Einsatz der elektronischen Stimmabgabe wurden die Betriebsprozesse des Kantons Graubünden überprüft, um die Konformität der Prozesse 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 Mai und August 2023 durchgeführt. Dafür haben sie alle relevanten Dokumente erhalten, eine Simulation eines Urnengangs mitverfolgt und verschiedene Interviews mit den Kantonsvertreterinnen und Kantonsvertretern durchgeführt.

In Abstimmung mit der Bundeskanzlei fand keine erneute Überprüfung der Druckerei statt, die mit dem Druck und der Verpackung der E-Voting-Stimmrechtsausweise beauftragt ist. Die Druckerei wurde bereits im Rahmen des Bewilligungsverfahrens für die Grundbewilligung der Kantone St.Gallen und Basel-Stadt überprüft und die Prozesse sind nach Einschätzung der Experten konform zu den bundesrechtlichen Anforderungen. Für den Kanton Graubünden kommen keine Prozessanpassungen zur Anwendung.

2 Stellungnahme

Die Experten haben dem Kanton Graubünden ein sehr gutes Zeugnis ausgestellt. Lediglich drei Abweichungen aus rund 140 Prüfpunkten wurden festgestellt sowie eine Empfehlung ausgesprochen. Der Kanton hat, wo nötig, von der Möglichkeit Gebrauch gemacht, in begründeten Fällen Ausnahmen von den Bundesvorgaben zu beantragen (Art. 16 Abs. 2 VEleS).

2.1 Art. 11 VEleS - Offenlegung Software für Erstellung der Stimmrechtsausweise

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

Die Experten haben 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 canton should require the Post to publish the source code of the software used to generate the polling cards and publish the source code of the helper to enforce the principle of transparency.

Der Kanton stimmt der Einschätzung der Experten zu. Die folgenden Massnahmen wurden getroffen, um das Risiko zu minimieren (siehe Massnahme A.11 des Massnahmenkatalogs von Bund und Kantonen[1]):

- Der Kanton prüft im Betrieb per Stichprobe, dass die korrekten Codes ins PDF übernommen wurden.

[1] Massnahmenkatalog von Bund und Kantonen vom 04.08.2023 (https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsuebersicht.html)

- VCPS wird auf einem Laptop betrieben, für dessen Betrieb Ziffer 3 Anhang VEleS gilt und damit besonders geschützt ist. Insbesondere wird er ohne Netzwerkverbindung betrieben.
- Auf dem Laptop werden abgesehen von den Rohdaten für den Druck keine kritischen Daten nach Art. 2 Abs. 1 Bst. v VEleS geführt.

Das Restrisiko wird als gering eingeschätzt. Auf dieser Grundlage hat der Kanton Graubünden eine Ausnahme gemäss Art. 16 Abs. 2 VEleS beantragt.

Der Quellcode der Software des Kantons Graubünden (wird auch durch die Kantone Thurgau und Basel-Stadt eingesetzt) wird im Laufe des Jahres 2024 veröffentlicht.

2.2 Ziff. 11.1 Anhang VEleS - Entschlüsselung am Samstag

Ziffer 11.1 der VEleS legt fest, dass die Entschlüsselung der Stimmen und deren Auszählung frühestens am Abstimmungs- oder Wahlsonntag beginnen darf.

Die Experten haben festgestellt, dass der Kanton dies gemäss seiner Praxis nicht konform umsetzt:

Key	11.1
Finding	The decryption of the votes and the tallying begin before Polling Sunday.
Recommendation	The canton should decrypt and tally the vote on Polling Sunday or obtain a derogation from the Federal Chancellery to continue their current practice.

Die kantonalen Rechtsgrundlagen (Art. 31 Abs. 2 GPR; BR 150.100) ermöglichen es dem Kanton, mit der Auszählungsarbeit bereits am Samstag zu beginnen. Der Kanton Graubünden kann durch die Entschlüsselung am Samstagnachmittag die personellen Aufwände gleichmässiger auf das Abstimmungs- oder Wahlwochenende verteilen und mehr Vorlaufzeit für die Analyse von unvorhergesehenen Problemen bei der Entschlüsselung der Stimmen und der Überprüfung des Urnengangs erhalten.

Der Kanton Graubünden erachtet die Risiken, die mit dieser Nichtkonformität verbunden sind, als hinreichend gering. Nach seiner Einschätzung wird die Risikosituation dadurch sogar entschärft. Auf dieser Grundlage hat der Kanton Graubünden eine Ausnahme gemäss Art. 16 Abs. 2 VEleS beantragt.

2.3 Ziff. 15.1 Anhang VEleS - Verwaltung der Zertifikate

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

Die Experten empfehlen dem Kanton 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 described in detail (e.g., generation, distribution, protection of private keys, revocation, renewal, etc.)

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

2.4 Ziff. 15.4 Anhang 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 haben festgestellt, dass der Kanton dies nur teilweise konform umgesetzt hat:

Key	15.4
Finding	Although their security level may be equivalent, the certificates used in the direct trust model do not originate from a recognised supplier of certificate services under the ESigA.
Recommendation	The client should conduct discussions with the chancellery in order to obtain a waiver to the requirement to procure electronic certificates from a provider recognised 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 (Direct-Trust).

Aus sicherheitstechnischer Sicht ist diese Lösung zu bevorzugen. Die Massnahme B.14 aus dem Massnahmenkatalog von Bund und Kantonen[2] sieht eine Revision der Rechtsgrundlagen vor.

3 Schlussfolgerung

Der Kanton Graubünden bedankt sich bei den Experten für die Zusammenarbeit, die kritische Prüfung der Prozesse und deren Dokumentation sowie für die wertvollen Verbesserungsvorschläge.

Der Kanton hat bereits die notwendigen Massnahmen getroffen, um die Risiken gering zu halten. Die vollständige Behebung der Nichtkonformität "Offenlegung der Software für die Erstellung der Stimmrechtsausweise" ist für 2024 vorgesehen.

[2] Massnahmenkatalog von Bund und Kantonen vom 04.08.2023 (https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/versuchsuebersicht.html)