

VOTING Stimmunterlagen Offline-Client

Benutzerhandbuch

Verfasser	Abraxas Informatik AG
Klassifizierung	öffentlich
Version	0.91 (Entwurf)
Datum	31. März 2023

Inhaltsverzeichnis

1.	Einrichten Offline Client	4
1.1	Bezug Client und Konfiguration	4
1.2	Start Offline-Client.....	4
2.	Einstellungen Offline-Client	5
3.	Stimmrechtsausweise generieren	6
3.1	Auswahl der Daten	6
3.2	Validierung	6
3.3	Konfiguration	7
3.4	Vorschau	8
3.5	Generierung	9
3.6	Download	10
3.7	Signieren und verschlüsseln	11
4.	Beenden des Programms	13
4.1	Sicheres Löschen der Daten	13
5.	Anhang	15
5.1	Übermittlung Fingerprint.....	15
5.2	Kontrolle der Vertrauenswürdigkeit des Verschlüsselungszertifikates	15

Abbildungsverzeichnis

Abbildung 1: Offline-Client Zip entpacken	4
Abbildung 2: Offline-Client exe.....	4
Abbildung 3: Aufruf Einstellungen	5
Abbildung 4: Einstellungen Offline-Client	5
Abbildung 5: Auswahl der Input Daten	6
Abbildung 6: Fehlermeldung Validierung	6
Abbildung 7: Erfolgreiche Validierung	7
Abbildung 8: Konfiguration Stimmrechtsausweise	8
Abbildung 9: Vorschau Stimmrechtsausweise	8
Abbildung 10: Erteilung Gut zum Druck	9
Abbildung 11: Generierung Stimmrechtsausweise	9
Abbildung 12: Erfolgreich generierte Stimmrechtsausweise	10
Abbildung 13: Übersicht Signierung und Verschlüsselung	10
Abbildung 14: Auswahl zu signierende und verschlüsselnde Stimmrechtsausweise	11
Abbildung 15: Bestätigung Zertifikate zur Verschlüsselung	11
Abbildung 16: Auswahl Zertifikat für Signierung	12
Abbildung 17: Start signieren und verschlüsseln	12
Abbildung 18: Download verschlüsselte Dateien	13
Abbildung 19: Löschen aller Daten mittels "Zurück zur Auswahl"	14
Abbildung 20: Löschen aller Daten mittels Einstellungen	14
Abbildung 21: Zertifikat öffnen.....	15
Abbildung 22: Fingerprint auslesen	16

1. Einrichten Offline Client

1.1 Bezug Client und Konfiguration

Für die Verwendung des VOTING Stimmunterlagen Offline-Client wird die Nutzung von VOTING Stimmunterlagen (Online) vorausgesetzt. Wird der E-Voting Tab im online Teil bestätigt so startet der Download der Urnengangskonfiguration. Diese wird für die Generierung der Stimmrechtsausweise benötigt und als Zip-Datei zur Verfügung gestellt.

Im E-Voting Tab wird der Fingerprint des zur Signierung der Urnengangskonfiguration verwendeten Zertifikats angezeigt. Die Kontrolle des Fingerprints erfolgt manuell (siehe Anhang).

Die aktuellste Version des Offline-Clients wird den Kunden jeweils durch die Abraxas zur Verfügung gestellt.

1.2 Start Offline-Client

Um den Offline-Client zu starten muss das Zip entpackt werden. Es wird empfohlen den Offline-Client Lokal (z.B. Laufwerk C) zu entpacken um die Performance zu verbessern.

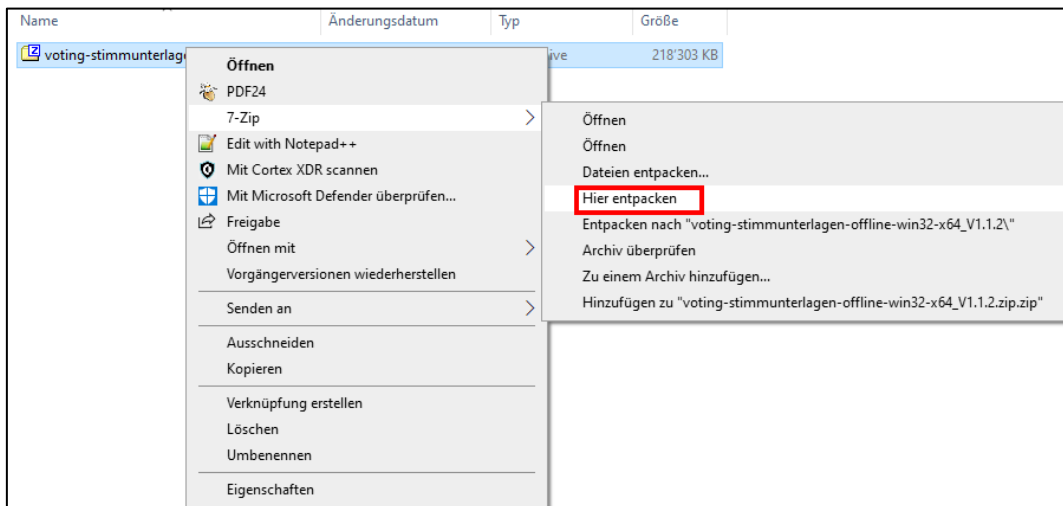


Abbildung 1: Offline-Client Zip entpacken

Nach dem entpacken kann der Offline-Client mittels Doppelklick auf die Datei "voting-stimmunterlagen-offline.exe" gestartet werden.



Abbildung 2: Offline-Client exe

2. Einstellungen Offline-Client

Es können diverse Einstellungen am Offline-Client vorgenommen werden. Dazu kann die Einstellungs-Seite mit dem Zahnrad oben rechts aufgerufen werden.

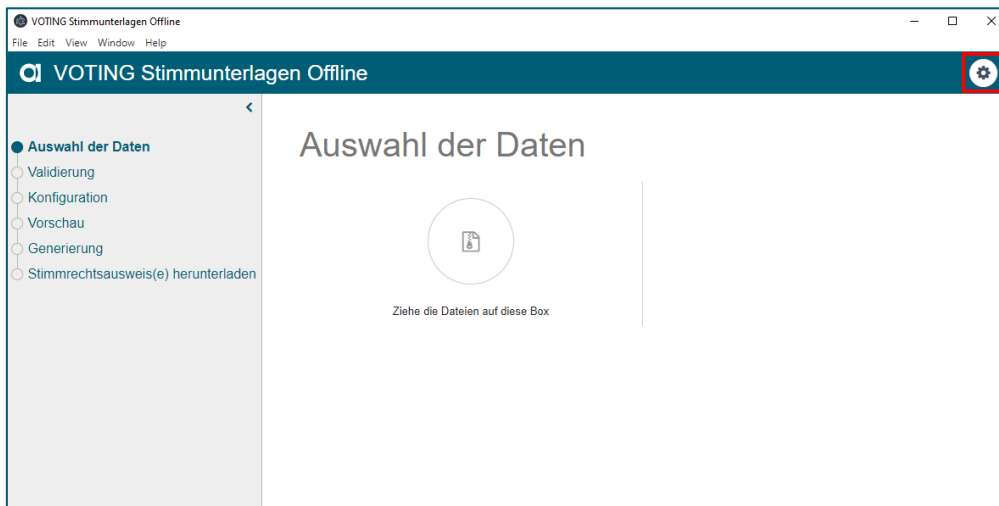


Abbildung 3: Aufruf Einstellungen

Neben der Auswahl der Sprache ist hier das sichere Löschen aller Daten möglich. Weiter können die Anzahl der angezeigten Stimmrechtsausweise in der Vorschau sowie die Anzahl Stimmrechtsausweise pro Job angepasst werden.

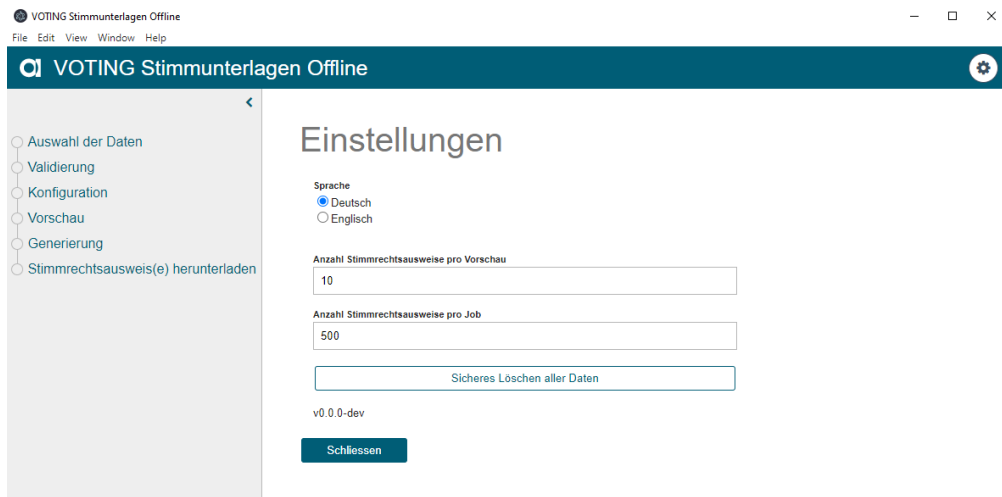


Abbildung 4: Einstellungen Offline-Client

Mit diversen Messungen konnte festgestellt werden, dass mit 500 Stimmrechtsausweise pro Job ein gutes Ressource-Performance Verhältnis erreicht werden kann. Eine grössere Anzahl verbessert die Performance nur unwesentlich, benötigt aber zusätzlichen Arbeitsspeicher auf dem Endgerät.

3. Stimmrechtsausweise generieren

3.1 Auswahl der Daten

Für die Generierung der E-Voting Stimmrechtsausweise müssen dem Offline Client 3 Dateien via Drag and Drop übergeben werden:

- Post Druckdaten → Anlieferung durch E-Voting System
- Post Konfiguration → Anlieferung durch E-Voting System
- Urnengangskonfiguration → Export-Datei von VONTING Stimmunterlagen (Online)

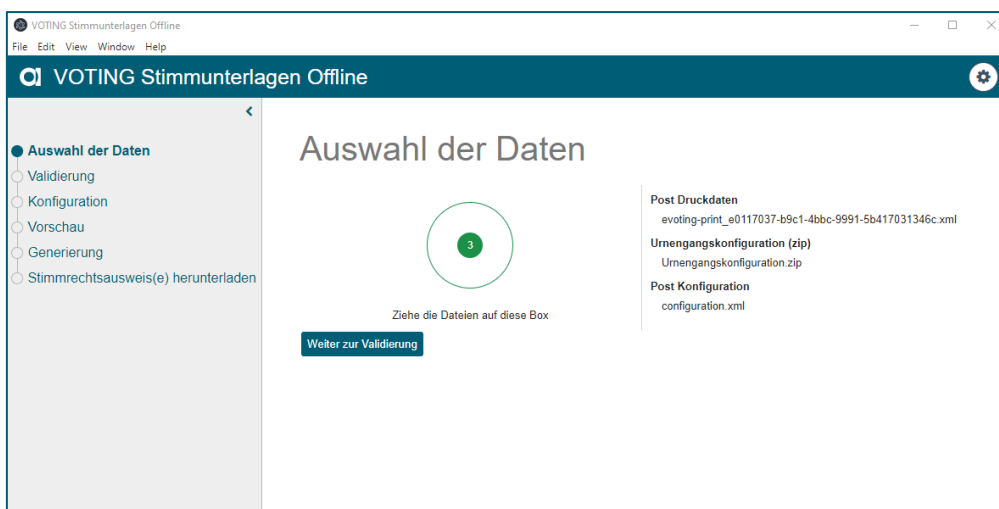


Abbildung 5: Auswahl der Input Daten

Bei der Erstellung der Urnengangskonfiguration werden mehrere Verschlüsselungszertifikate hinterlegt. Somit können mehrere Personen im Produktionszentrum der Abraxas die Entschlüsselung und Weiterverarbeitung der Stimmrechtsausweise vornehmen.

3.2 Validierung

Sind die korrekten Daten bereitgestellt, kann die Validierung gestartet werden. Dabei wird geprüft, ob für jeden Stimmberechtigten im Register bzw. E-Voting Konfigurationsdateien ein Konfigurations-Eintrag in der Urnengangs-Konfiguration vorhanden ist. Wenn es im Stimmregister Personen gibt, für welche kein entsprechender Eintrag in der Urnengangs-Konfiguration gefunden wird, kann die Erstellung nicht weitergeführt werden.

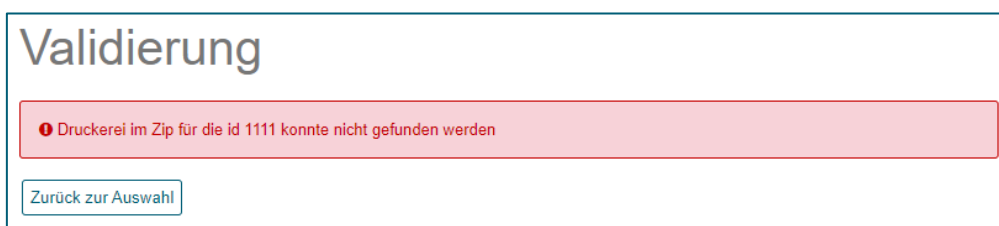


Abbildung 6: Fehlermeldung Validierung

Wurde für alle Stimmberechtigten eine Konfiguration gefunden, so kann mit dem Schritt "Konfiguration" weitergemacht werden.

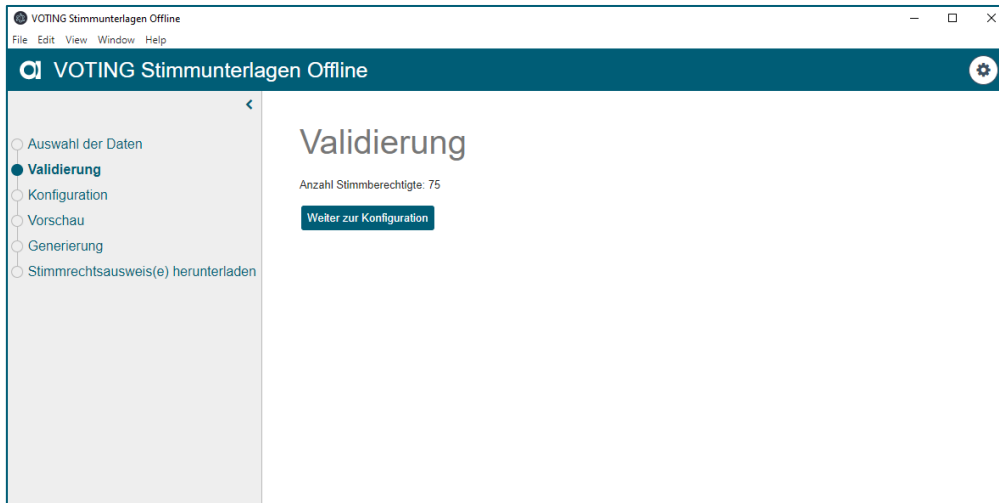


Abbildung 7: Erfolgreiche Validierung

3.3 Konfiguration

Der Fingerprint der E-Voting Webseite kann im Eingabefeld "Fingerprint" eingefügt werden. Dieser wird anschliessend an der entsprechenden Stelle auf dem Stimmrechtsausweis aufgeführt. Mit dem Fingerprint kann die abstimmende Person verifizieren, ob sie sich effektiv auf der E-Voting Website befindet.

Weiter kann im Schritt Konfiguration die Erstellung der Stimmrechtsausweise in verschiedene Dateien gruppiert werden. Beispielsweise kann für jede Gemeinde (BfS-Nummer) und Korrespondenz-Sprache eine eigenständige PDF-Datei erstellt werden. Zusätzlich kann auch die Versandregion unterschieden werden.

Die Sortierung kann dann sinnvoll sein, wenn die Stimmregister-Daten nicht vorsortiert sind. Dies hat Vorteile bei der Postaufgabe. Es kann z.B. nach Versandregion (entspricht dem Land und Postleitzahl) sowie der Strasse mit Hausnummer sortiert werden. Dadurch können unter Umständen die Kosten bei der Postaufgabe reduziert werden. Ohne die Sortierungs-Angaben werden die Stimmrechts-Ausweise in der Reihenfolge des Stimmregisters aufbereitet.

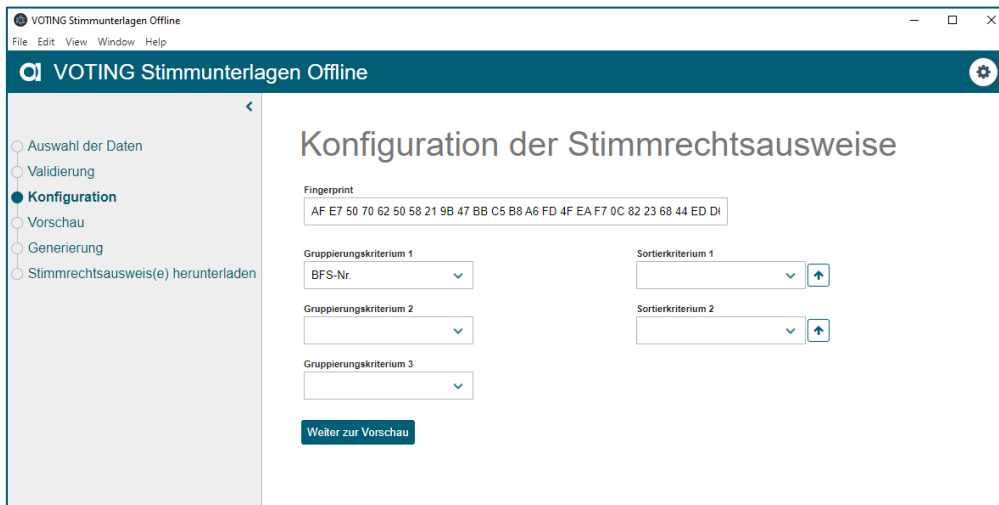


Abbildung 8: Konfiguration Stimmrechtsausweise

3.4 Vorschau

Bevor nun alle Stimmrechtsausweise erstellt werden, kann eine Vorschau für jede Gruppe angezeigt werden. Damit lässt sich überprüfen, ob die PDF-Dateien korrekt erstellt werden. Links neben der PDF-Vorschau kann zwischen den einzelnen Gruppen gewechselt werden.

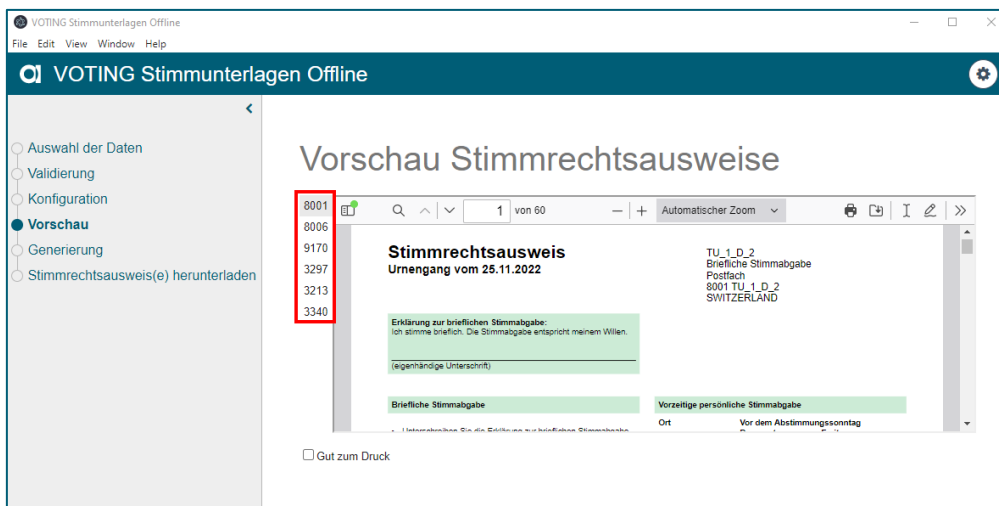


Abbildung 9: Vorschau Stimmrechtsausweise

Mit der Auswahl "Gut zum Druck" kann der Generierungs-Schritt aktiviert werden.

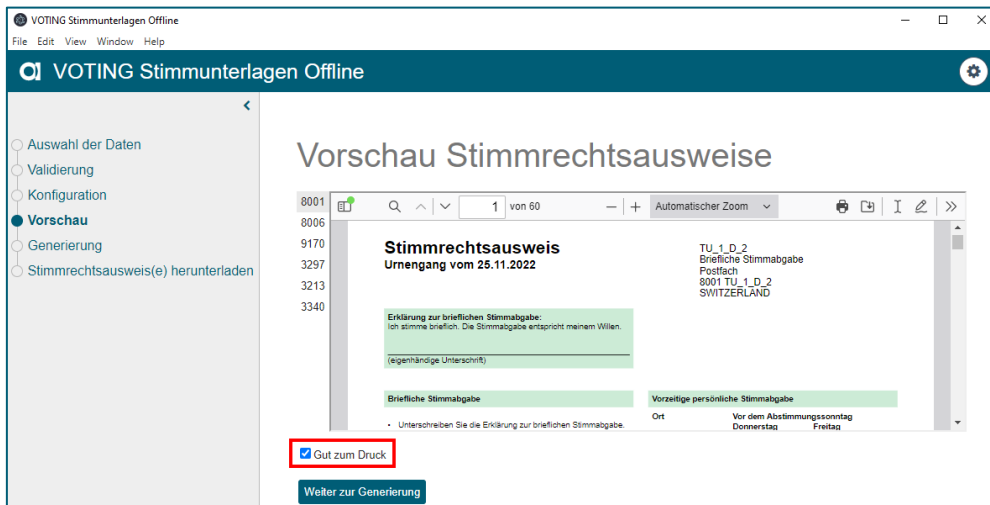


Abbildung 10: Erteilung Gut zum Druck

3.5 Generierung

Wurde die Generierung aktiviert, so startet die finale Aufbereitung der Stimmrechtsausweise. Jede Gruppe wird nacheinander erstellt. In der Ansicht kann der Fortschritt der einzelnen Gruppen überwacht werden.

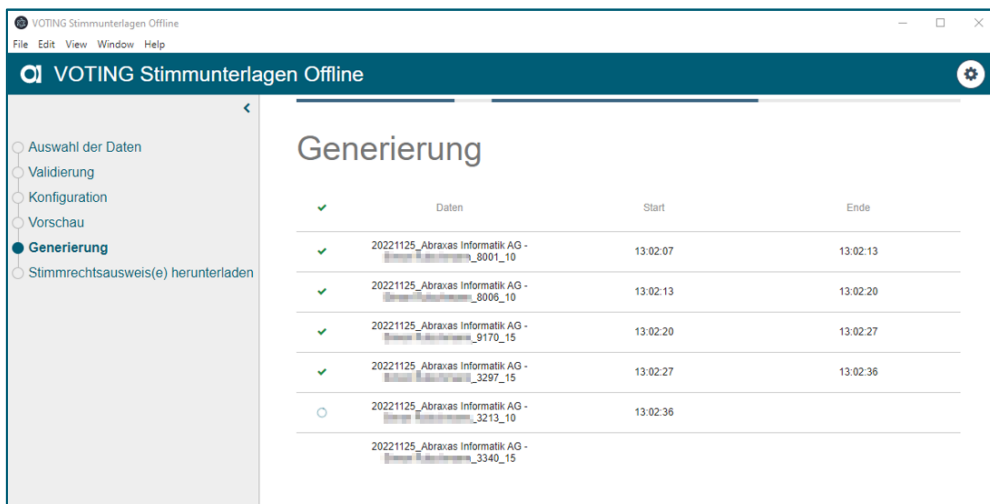


Abbildung 11: Generierung Stimmrechtsausweise

Mittels Klick auf die einzelnen Gruppen werden die einzelnen Jobs angezeigt. Je nach Einstellung und Anzahl Stimmberechtigte werden unterschiedlich viele Jobs für die Erstellung durchgeführt. Sobald alle Jobs einer Gruppe fertig gelaufen sind, startet die Generierung der nächsten Gruppe.

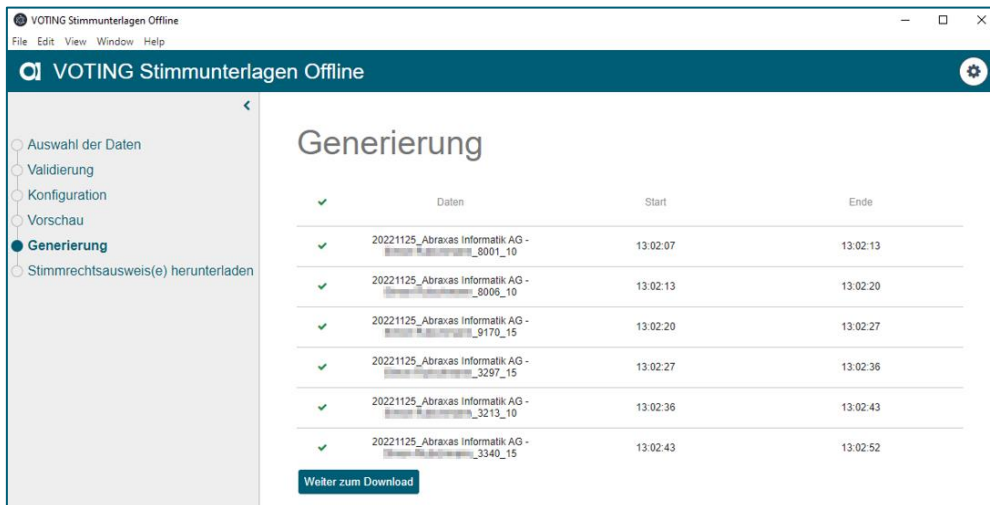


Abbildung 12: Erfolgreich generierte Stimmrechtsausweise

3.6 Download

Anschließend können die fertigen Stimmrechtsausweise noch unverschlüsselt heruntergeladen werden.

Hierbei kann eine einzelne Datei zum Download ausgewählt werden, oder alle Dateien können in einem ausgewählten Verzeichnis abgelegt werden.

Mit Klick auf "Alles herunterladen" wird der Prozess gestartet.

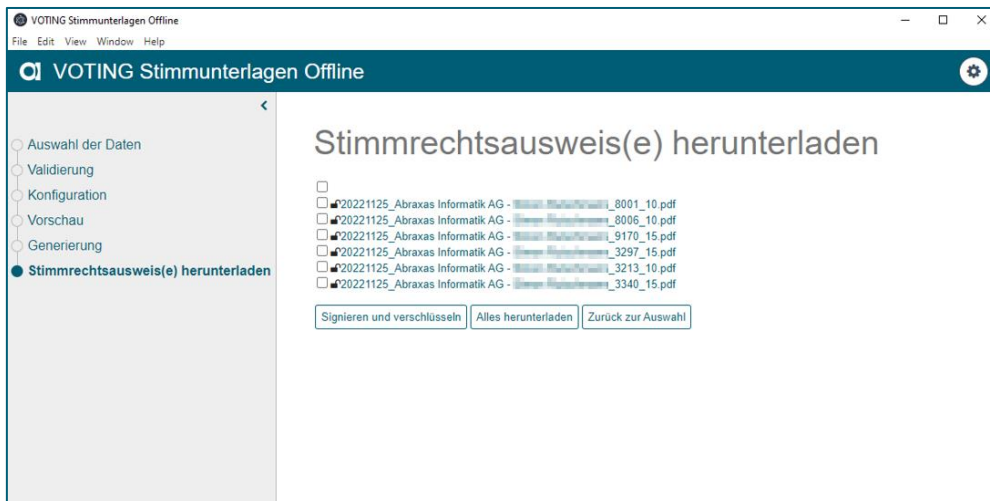


Abbildung 13: Übersicht Signierung und Verschlüsselung

3.7 Signieren und verschlüsseln

Für das Signieren der Dateien muss eine SmartCard der "Swiss Government PKI" verwendet werden. Das entsprechende Zertifikat kann ausgewählt werden. Üblicherweise beinhaltet eine SmartCard aber nur ein Zertifikat für die Signierung der Daten.

Das Verschlüsselungs-Zertifikat des Empfängers kann nicht ausgewählt werden, es wurde als Bestandteil der Konfigurationsdatei bereits für jeden Kanton festgelegt und kann nicht geändert werden.

Es können entweder einzelne oder sämtliche PDF Dateien gemeinsam signiert und verschlüsselt werden (Auswahl mittels Checkbox).

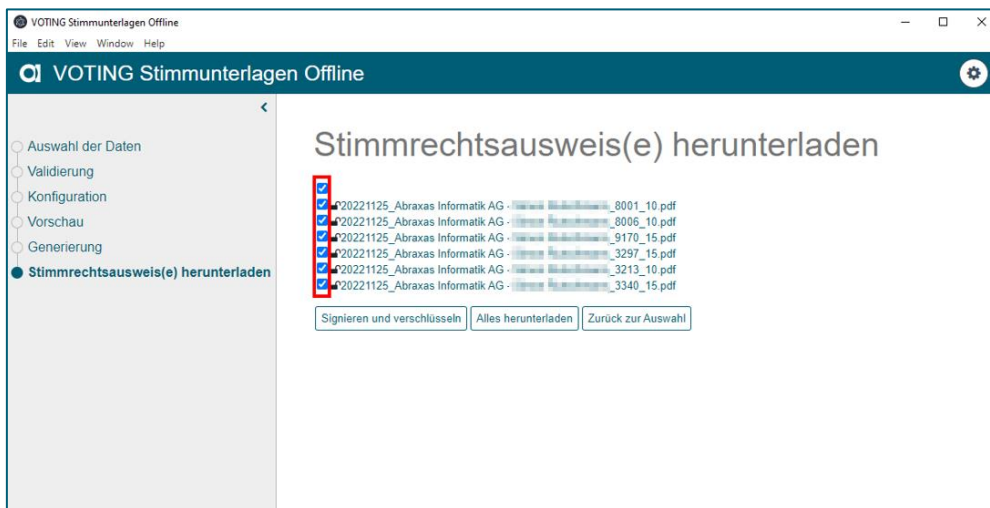


Abbildung 14: Auswahl zu signierende und verschlüsselnde Stimmrechtsausweise

Nach einem Klick auf "Signieren und verschlüsseln" wird der Dialog zur Bestätigung der Verschlüsselungszertifikate angezeigt.

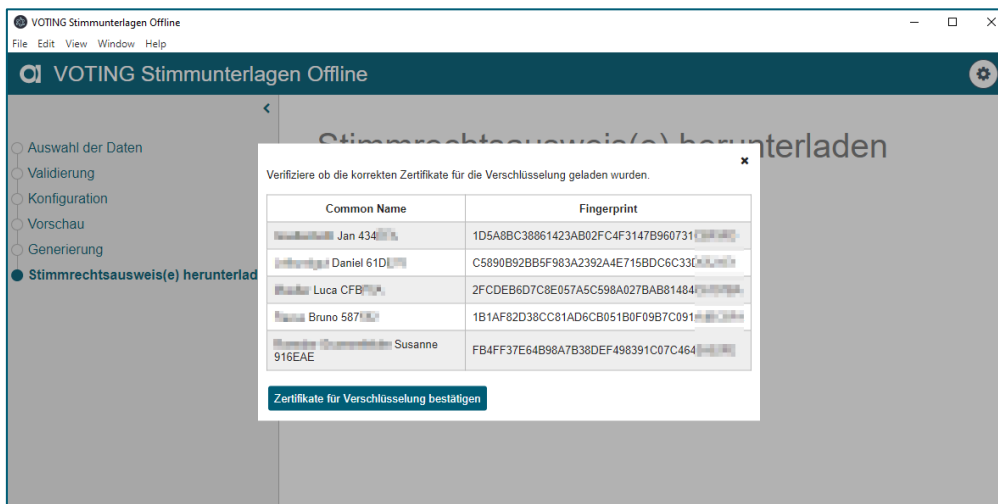


Abbildung 15: Bestätigung Zertifikate zur Verschlüsselung

Es werden alle in der Urnengangskonfiguration für die Verschlüsselung hinterlegten Zertifikate inklusive Fingerprint angezeigt.

Nach der Bestätigung der Verschlüsselungszertifikate erscheint der Dialog zur Auswahl des Zertifikates für die Signierung der Stimmrechtsausweise.

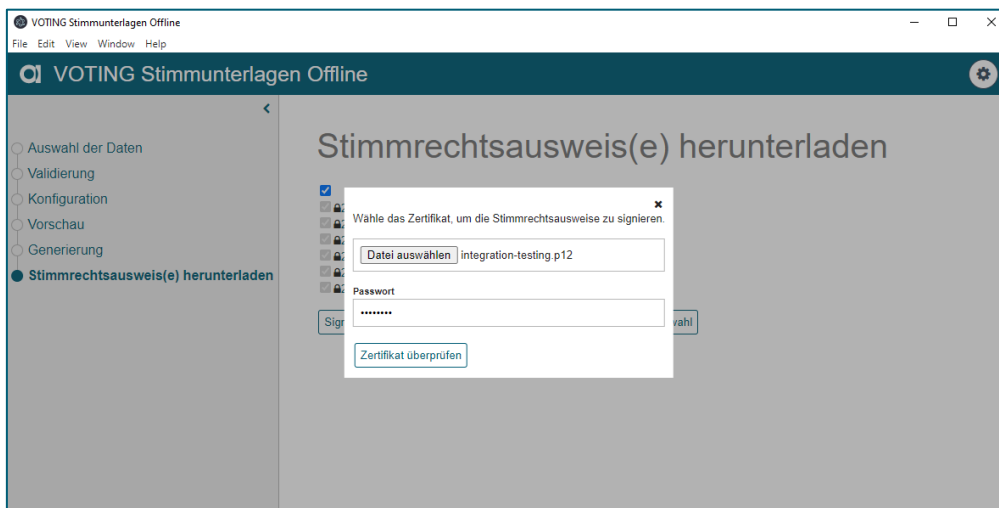


Abbildung 16: Auswahl Zertifikat für Signierung

Für die Signierung muss das Zertifikat mit Format .p12 (PKCS#12) mit dem Privaten-Schlüssel verwendet werden.

Nach einem Klick auf "Zertifikat überprüfen" kann im nächsten Schritt die Signierung und Verschlüsselung der Stimmrechtsausweise ausgelöst werden.

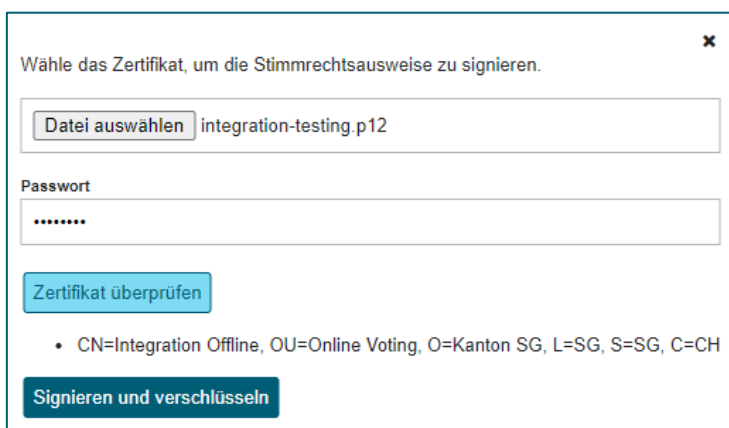


Abbildung 17: Start signieren und verschlüsseln

Das Schloss-Symbol vor den Dateien ist jetzt geschlossen, die Dateien sind verschlüsselt.

Nach dem Signierungs- und Verschlüsselungsvorgang werden die Daten erneut zum Download angeboten.

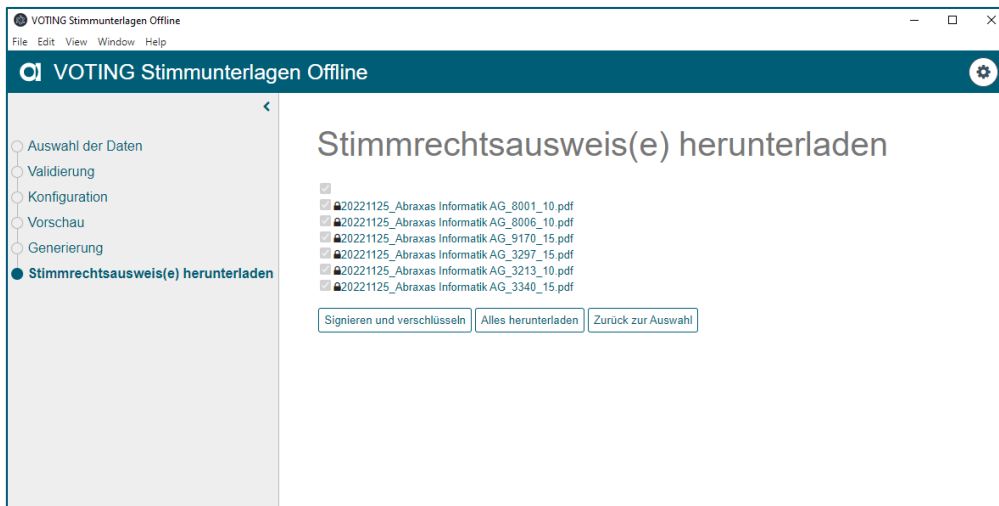


Abbildung 18: Download verschlüsselte Dateien

Bei einem Klick auf "Alles herunterladen" öffnet sich der Datenexplorer und das gewünschte Verzeichnis für den Download kann ausgewählt werden.

Für die Verschlüsselung wird AES mit dem Modus Cipher Block Chaining und dem Padding PKCS#7 verwendet.

Für die Signierung wird RSA mit dem Hash Algorithmus SHA512 und dem Padding PKCS#1 v1.5 verwendet.

4. Beenden des Programms

4.1 Sicheres Löschen der Daten

Der Offline-Client speichert den aktuellen Datenstand fortlaufend. Nach dem Herunterladen der PDF-Dateien gibt es zwei Möglichkeiten den Datenstand sicher zu löschen:

Mittels Klick auf "Zurück zur Auswahl" kommt man zurück zum ersten Arbeitsschritt "Auswahl der Daten". Im Zuge dessen werden sämtliche Daten sicher gelöscht.

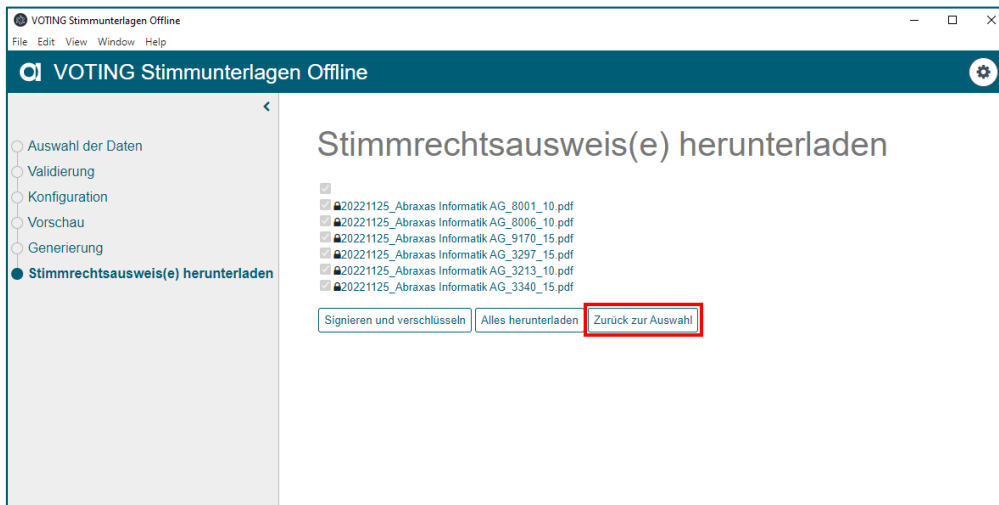


Abbildung 19: Löschen aller Daten mittels "Zurück zur Auswahl"

Die zweite Möglichkeit zur sicheren Datenlöschung ist die Schaltfläche "Sicheres Löschen aller Daten" in den Einstellungen.

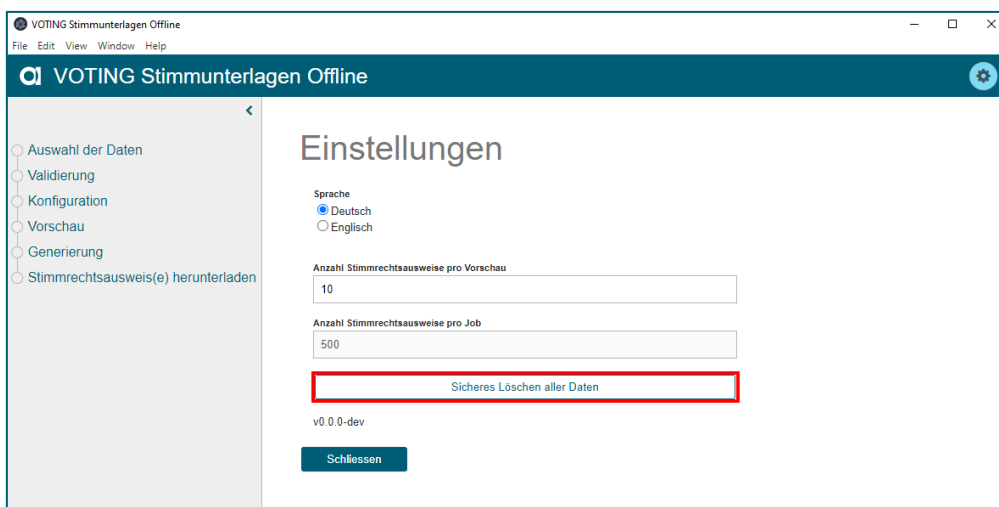


Abbildung 20: Löschen aller Daten mittels Einstellungen

Alle Dateien, welche während der Generierung auf der Festplatte angelegt wurden, werden mittels [sdelete](#) (Windows Sysinternals) gelöscht.

5. Anhang

5.1 Übermittlung Fingerprint

Die Übermittlung des Fingerprints des für die Verschlüsselung, sowie für die Signierung verwendeten Zertifikates wird mittels eines telefonischen oder physischen Meetings zwischen den Zertifikatsinhabern sichergestellt. Sofern ein relevantes Zertifikat abläuft, muss das Meeting wiederholt werden, sobald ein neues Zertifikat ausgestellt wurde.

5.2 Kontrolle der Vertrauenswürdigkeit des Verschlüsselungszertifikates

Das Zertifikate für die Verschlüsselung ist im Besitz eines Mitarbeitenden des Produktionszentrums der Abraxas Informatik AG, welche die Datei entschlüsseln darf. Es muss geprüft werden, dass das Zertifikat vertrauenswürdig ist.

Das Zertifikat ist in der Zip-Konfigurationsdatei im Ordner "certificates" zu finden. Beispielsweise die Datei "Mustermann Max 9207R2.cer".

Das Zertifikat öffnen (nicht installieren):



Abbildung 21: Zertifikat öffnen

Der Name der Person "Ausgestellt für" muss jener Person entsprechen, welche die Stimmrechtsausweise entschlüsseln wird (gemäss Prozess-Dokumentation der Druckerei).

Im zweiten Reiter muss der Fingerprint (Fingerabdruck) mit dem vom Produktionszentrum gelieferten Fingerabdruck abgeglichen werden:

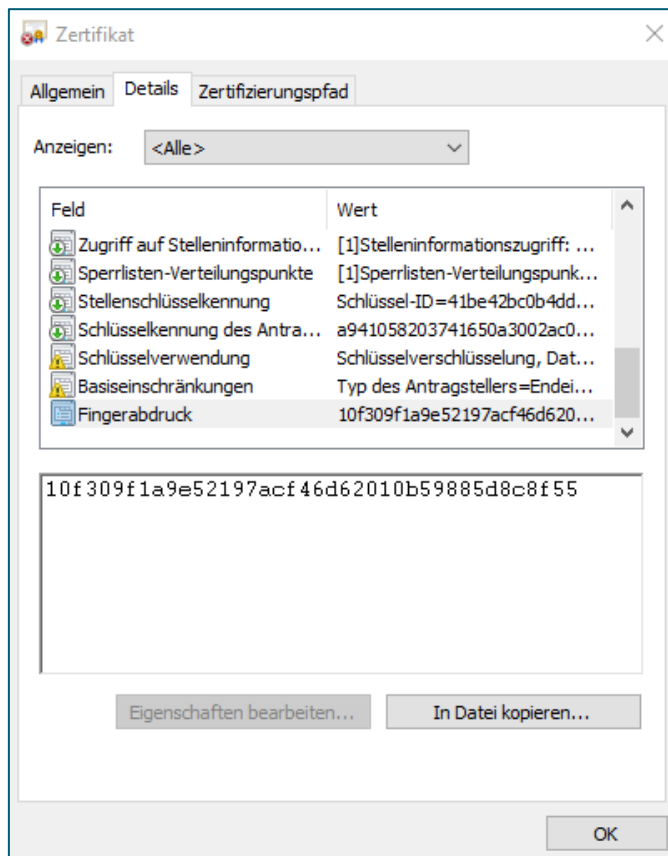


Abbildung 22: Fingerprint auslesen