VOTING Stimmunterlagen Offline-Client

Benutzerhandbuch

Verfasser	Abraxas Informatik AG
Klassifizierung	öffentlich
Version	0.92 (Entwurf)
Datum	16. September 2024

Für die digitale Schweiz. Mit Sicherheit.

abraxas

Inhaltsverzeichnis

Abbildungsverzeichnis

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

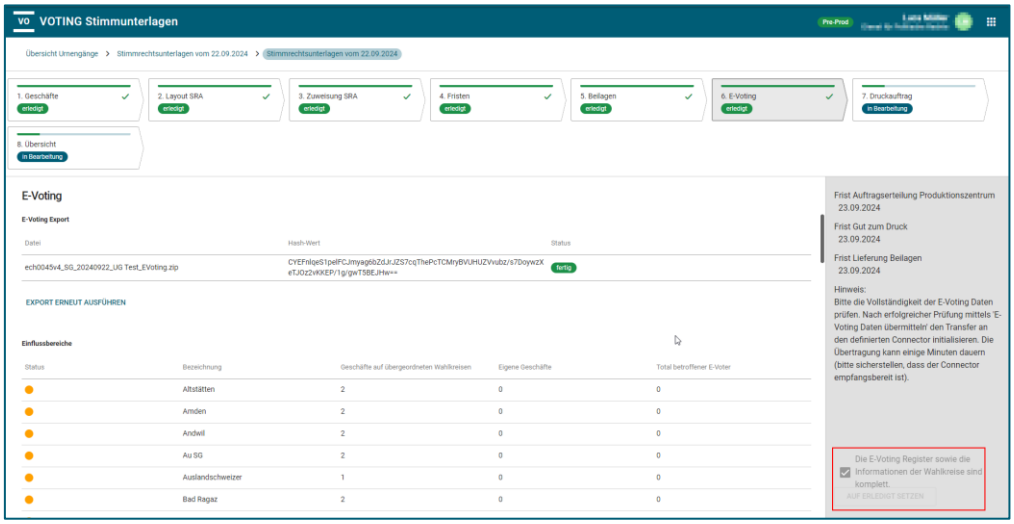

Abbildung 1: Bestätigung E-Voting VOTING Stimmunterlagen

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

Die aktuelle Version des Offline-Clients wird den Kunden jeweils durch die Abraxas Informatik AG zur Verfügung gestellt (via ShareFile) und auf GitHub publiziert (https://github.com/abraxas-labs?q=stimmunterlagen).

1.2 Start Offline-Client

Um den Offline-Client zu starten, muss das Zip, welches zuvor via ShareFile oder GitHub bezogen wurde (vgl. Kapitel 1.1), entpackt werden. Es wird empfohlen den Offline-Client lokal (z.B. Laufwerk C) zu entpacken, um die Performance zu verbessern.

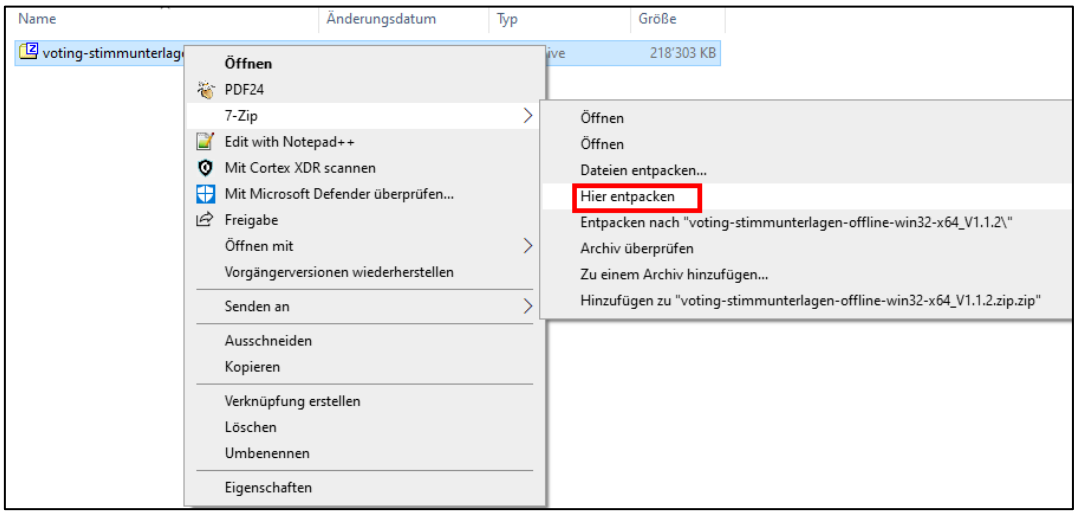

Abbildung 2: Offline-Client Zip entpacken

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

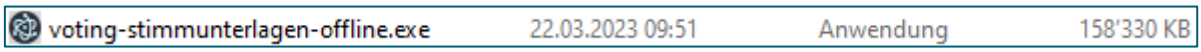

Abbildung 3: Offline-Client exe

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.

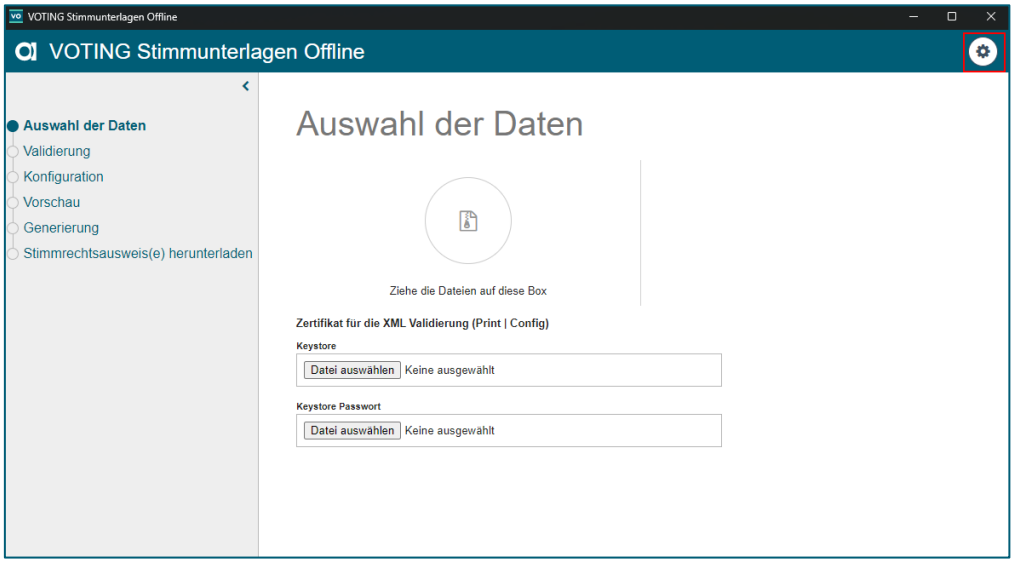

Abbildung 4: Aufruf Einstellungen

Neben der Auswahl der Sprache ist hier das sichere Löschen aller Daten möglich (vgl. Kapitel 4.1). Weiter können die Anzahl der angezeigten Stimmrechtsausweise in der Vorschau sowie die Anzahl Stimmrechtsausweise pro Job angepasst werden.

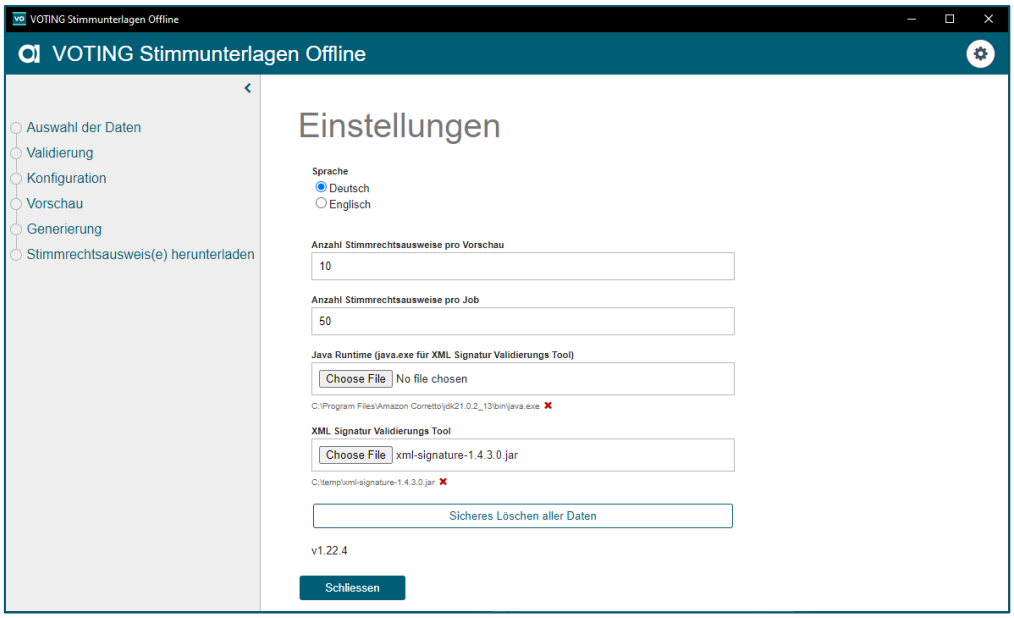

Abbildung 5: Einstellungen Offline-Client

Die Erfahrung zeigt, dass mit 500 Stimmrechtausweisen 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.

Weiter wird in den Einstellungen die 'Java Runtime' (lokale exe "java.exe") sowie das 'XML Signatur Validierungs Tool' (xml-signatur-x.x.x.x.jar) hinterlegt. Die Beiden Tools werden von der Post geliefert und gemäss Benutzeranleitung der Post installiert. Das Tool 'XML Signatur Validierungs Tool' erlaubt die Prüfung der digitalen Signaturen für die von der Post generierten Input-Dateien.
Für die Auswahl der beiden Tools jeweils auf 'Datei auswählen' klicken und das gewünschte Tool auswählen.

3. Stimmrechtsausweise generieren

3.1 Auswahl der Daten

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

- Post Druckdaten (print-*.xml) → Anlieferung durch E-Voting System
- Post Konfiguration (configuration.xml) → Anlieferung durch E-Voting-System
- Urnengangskonfiguration → Export-Datei von VOTING Stimmunterlagen (Online)

Optional kann auch das Stimmregister (eCH-0045.xml) übergegeben werden. Dieses ist nötig, wenn die Adresse der Auslandschweizerinnen und Auslandschweizer in den Extensions geliefert wird.

Zudem muss für die Validierung der Signatur der Post Druckdaten und Konfiguration jeweils der Keystore (Format .p12) mit den korrekten öffentlichen Schlüsseln und dem entsprechenden Passwort (in einer Text-Datei) hinterlegt werden. Diese können mittels 'Datei auswählen' ausgewählt und hinterlegt werden.

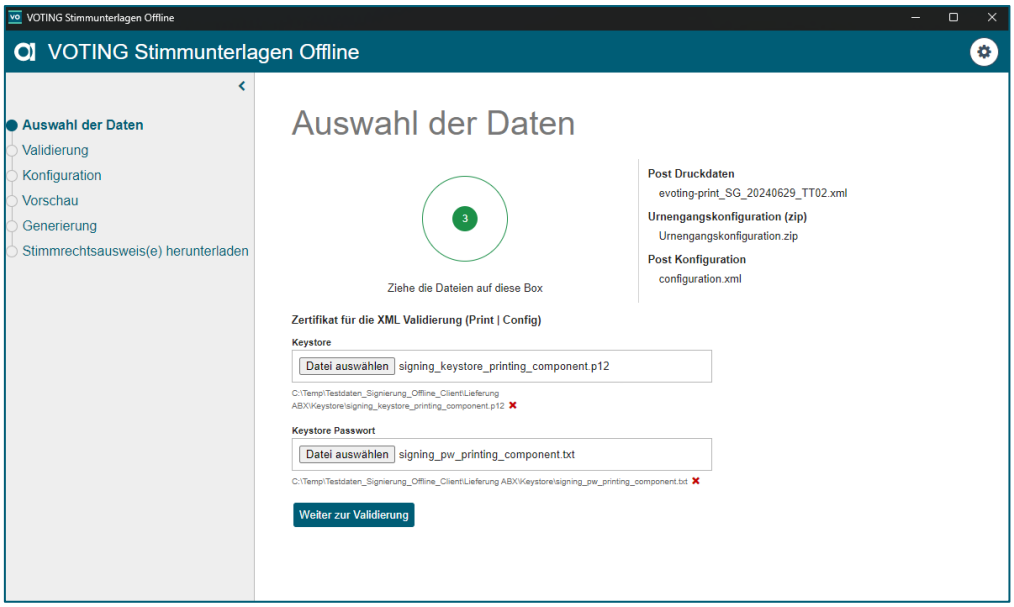

Abbildung 6: Auswahl der Input Daten

3.2 Validierung

Sind die korrekten Daten bereitgestellt, kann die Validierung gestartet werden. Dabei wird geprüft, ob für jede stimmberechtigte Person im Register bzw. in den 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. In diesem Falle muss eine korrekte Urnengangskonfiguration aus VOTING Stimmunterlagen online erstellt werden.

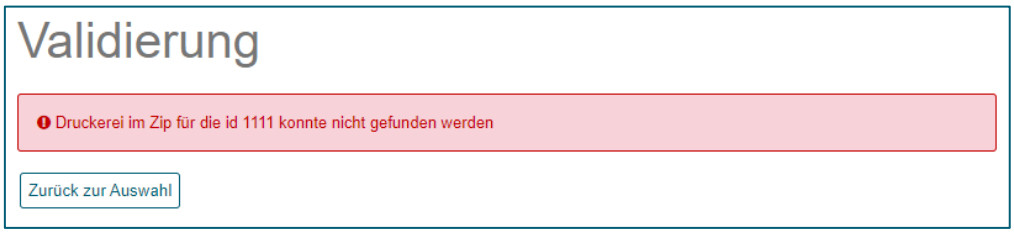

Abbildung 7: Fehlermeldung Validierung

Ebenfalls wird bei der Validierung eine Signaturprüfung durchgeführt. Sofern diese fehlschlägt oder nicht möglich ist (z.B. fehlende Konfiguration), wird dies in einer Warnmeldung ausgewiesen. In diesem Falle müssen gemäss Kapitel 2 korrekte Signaturdaten hinterlegt werden.

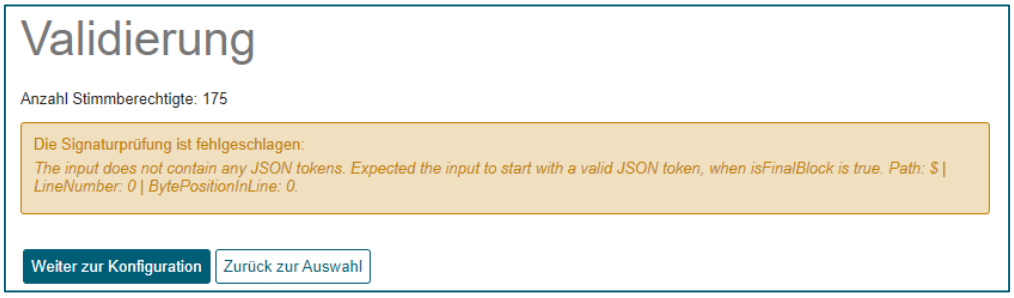

Abbildung 8: Warnmeldung Signaturprüfung

Wurde für alle stimmberechtigten Personen eine Konfiguration gefunden, so kann mit dem Schritt "Konfiguration" weitergemacht werden. Wenn die Signaturprüfung fehlschlägt, kann trotzdem fortgefahren werden.

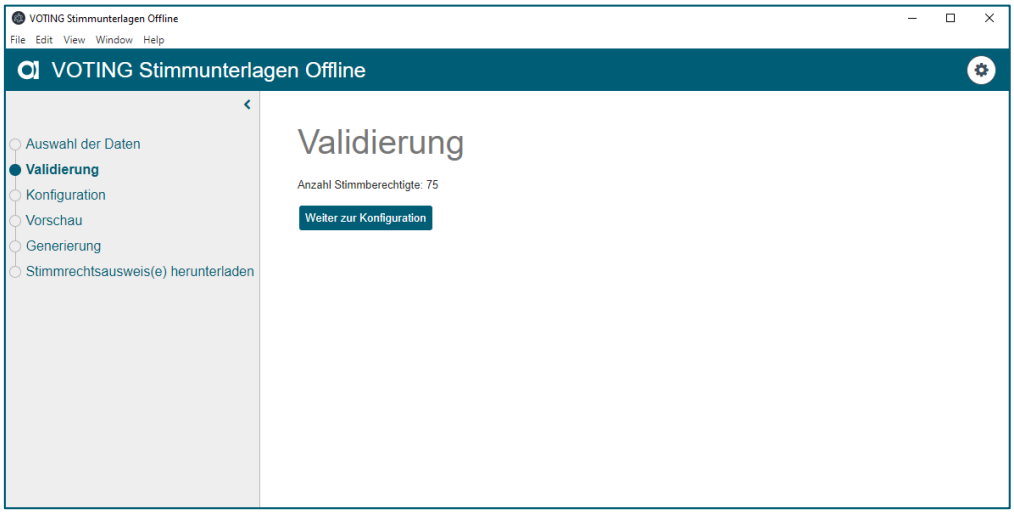

Abbildung 9: Erfolgreiche Validierung

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.

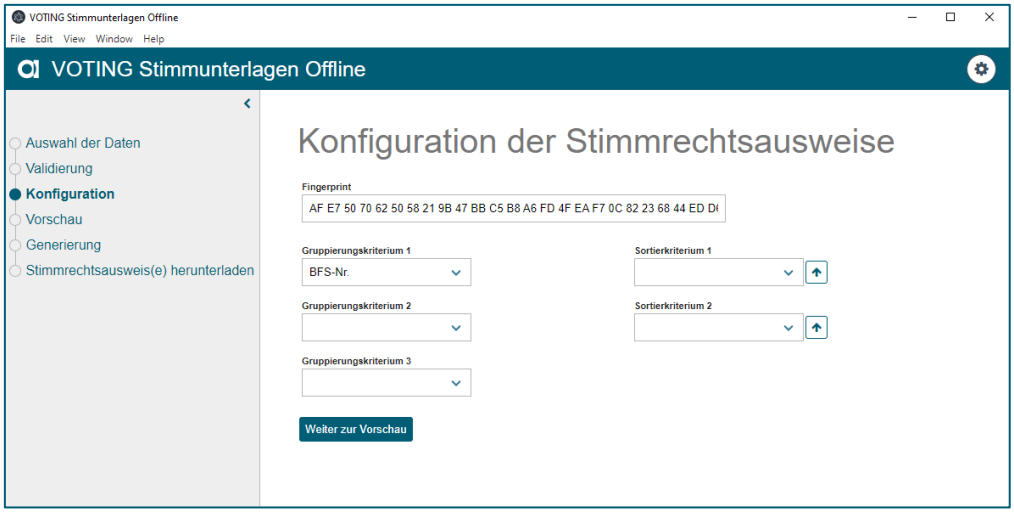

Abbildung 10: Konfiguration Stimmrechtsausweise

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.

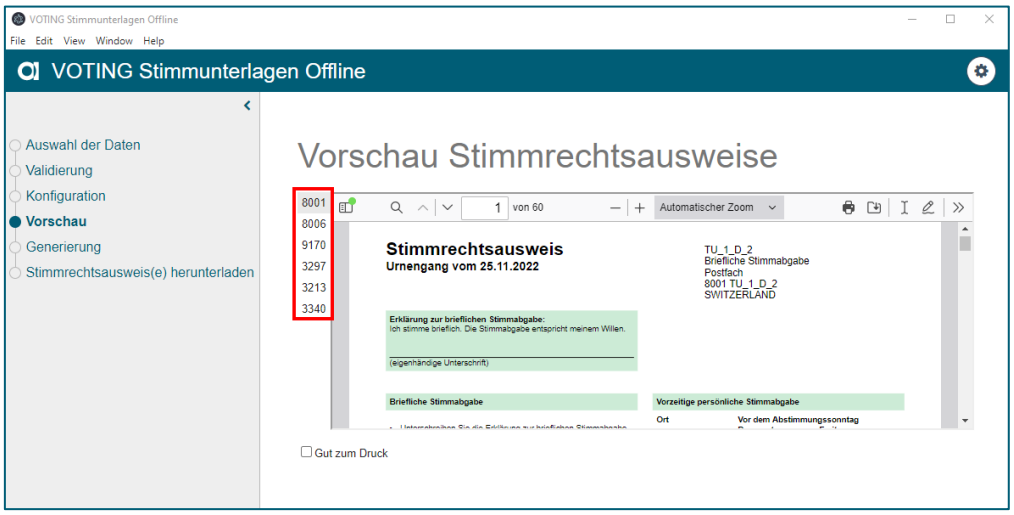

Abbildung 11: Vorschau Stimmrechtsausweise

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

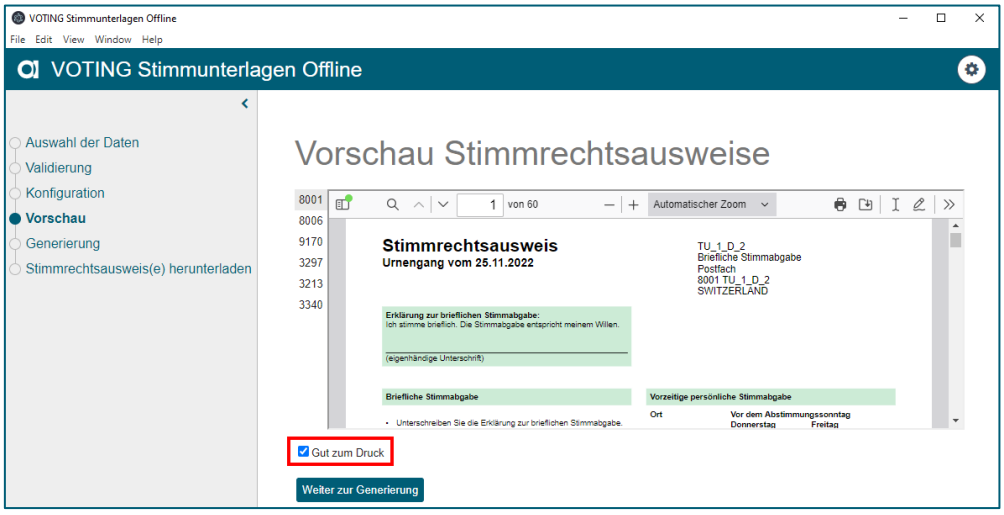

Abbildung 12: Erteilung Gut zum Druck

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.

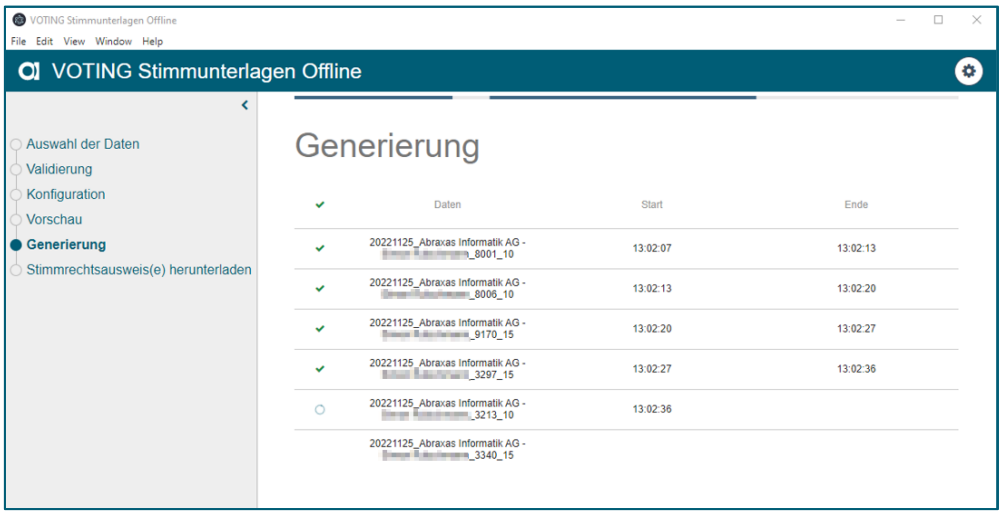

Abbildung 13: Generierung Stimmrechtsausweise

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.

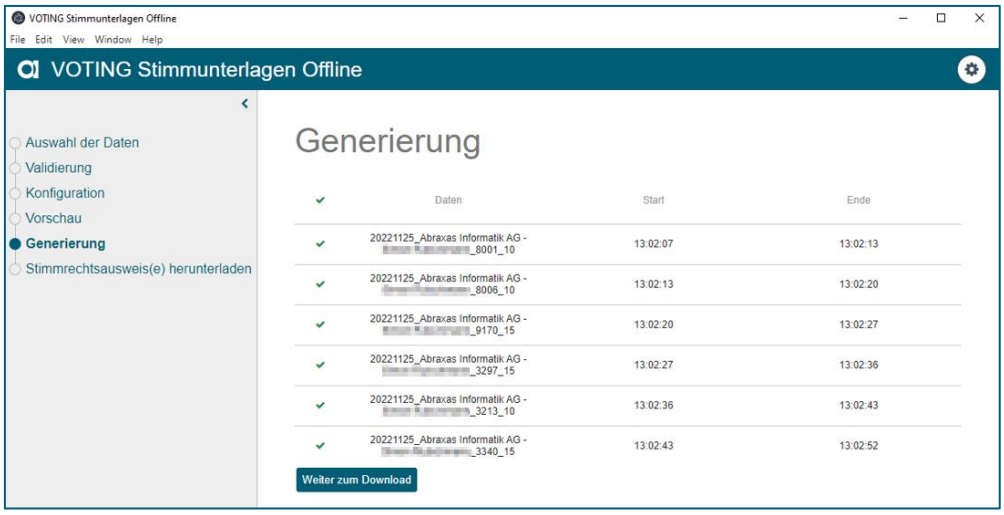

Abbildung 14: Erfolgreich generierte Stimmrechtsausweise

3.6 Download

Anschliessend können die fertigen Stimmrechtsausweise noch unverschlüsselt heruntergeladen werden.

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

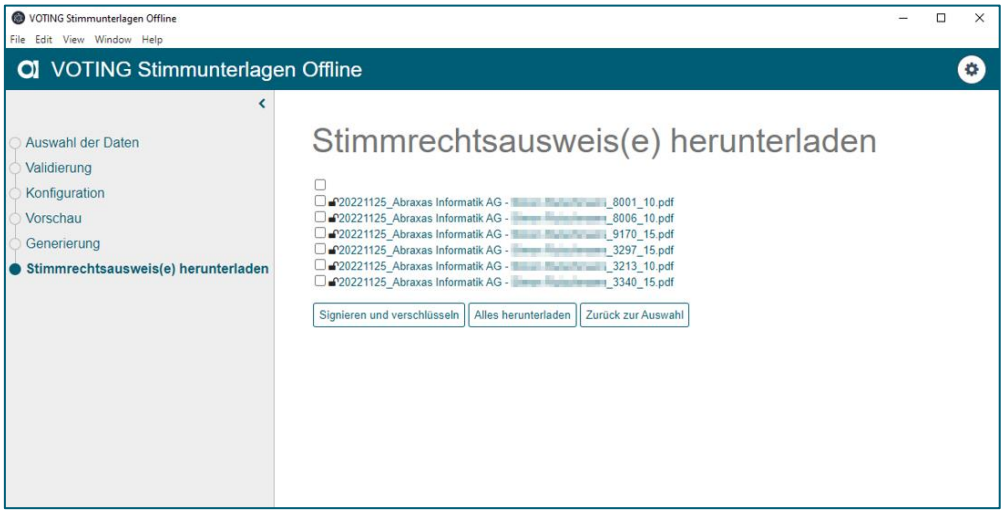

Abbildung 15: Übersicht Signierung und Verschlüsselung

3.7 Signieren und verschlüsseln

Für das Signieren der Dateien muss ein Zertifikat des Kantons verwendet werden.
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).

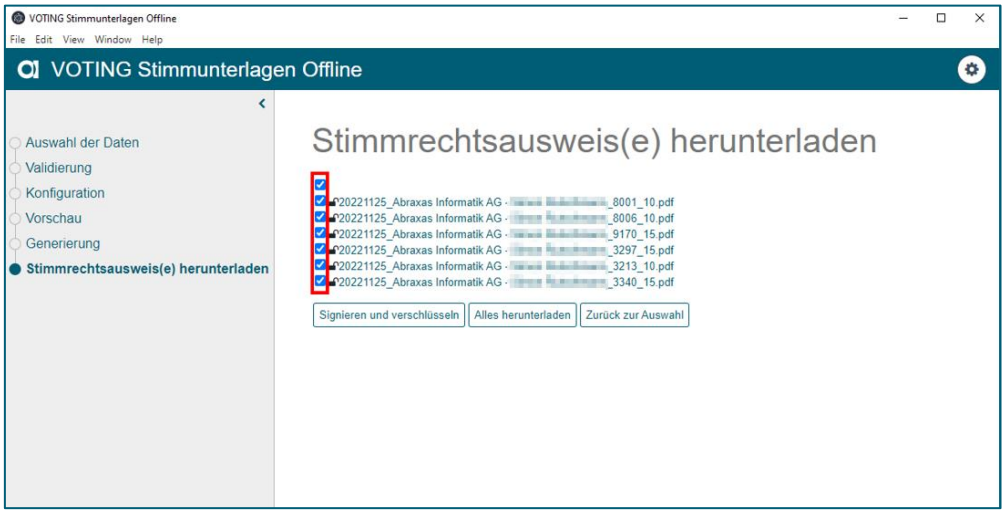

Abbildung 16: Auswahl zu signierende und verschlüsselnde Stimmrechtsausweise

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

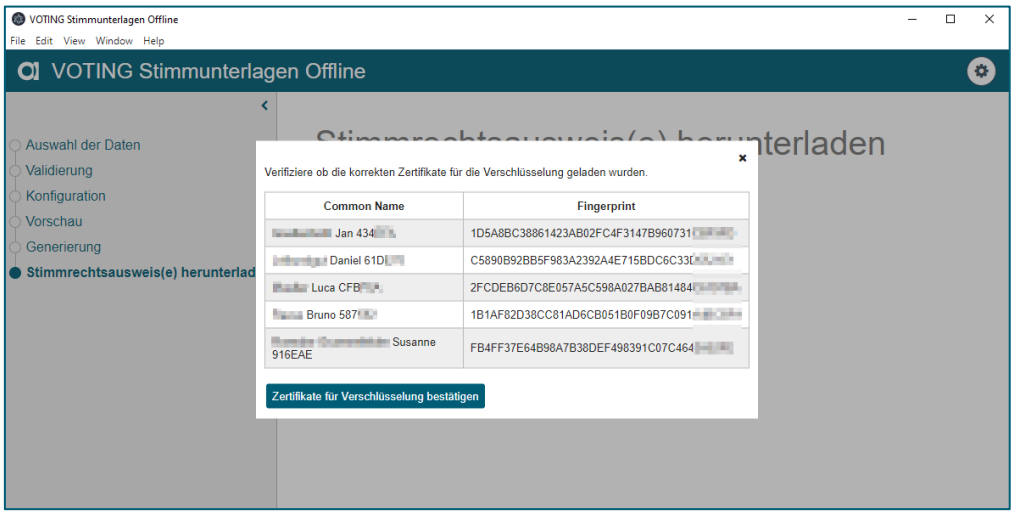

Abbildung 17: Bestätigung Zertifikate zur Verschlüsselung

Es werden alle in der Urnengangskonfiguration für die Verschlüsselung hinterlegten Zertifikate inklusive Fingerprint (SHA-1) angezeigt. Der Kanton kontrolliert, dass die Fingerprints anhand eines Austausch-Protokolls korrekt sind.

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

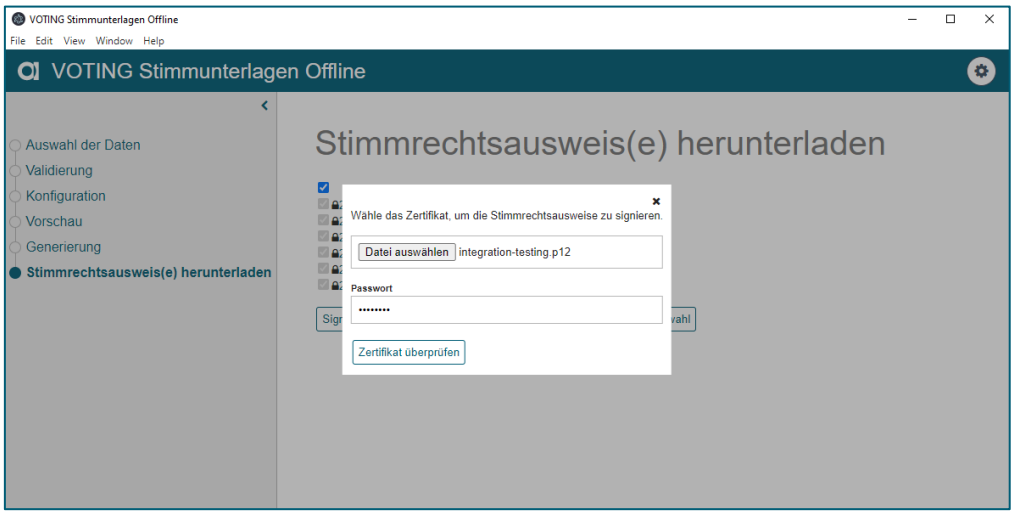

Abbildung 18: Auswahl Zertifikat für Signierung

Für die Signierung muss das Zertifikat im 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.

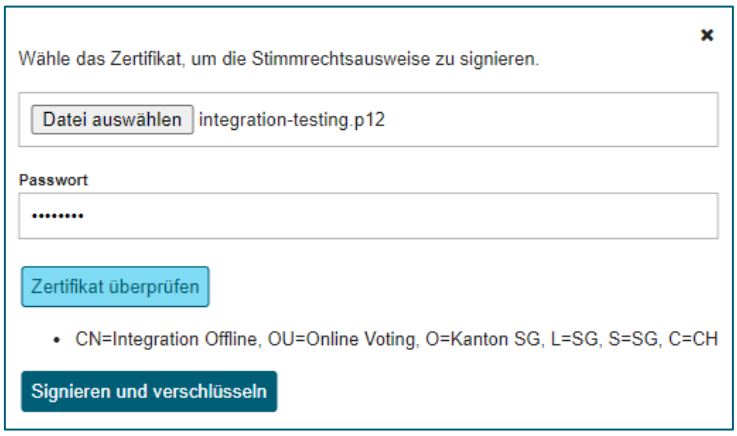

Abbildung 19: Start signieren und verschlüsseln

Das Schloss-Symbol vor den Dateien, die verschlüsselt wurden, ist jetzt geschlossen.
Nach dem Signierungs- und Verschlüsselungsvorgang werden die Daten erneut zum Download angeboten.

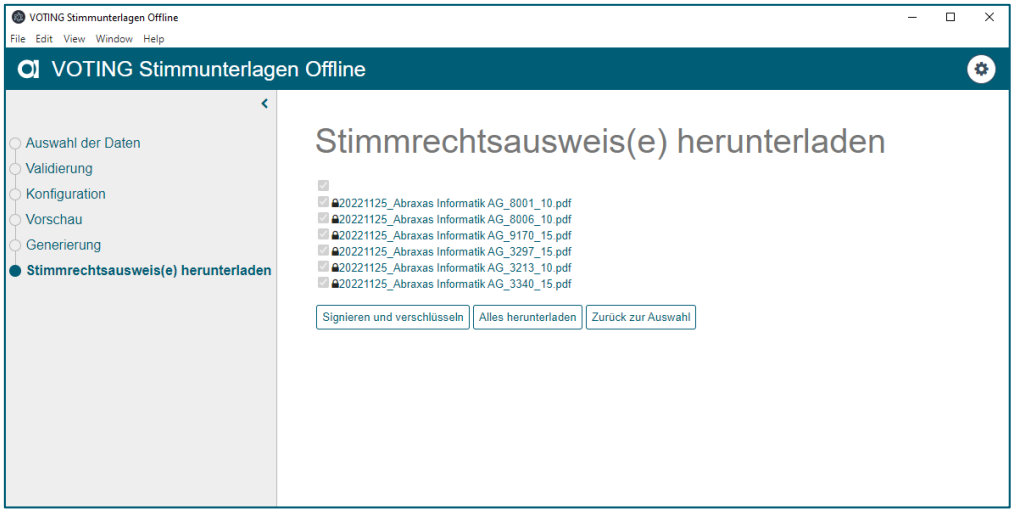

Abbildung 20: Download verschlüsselte Dateien

Durch einen 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.

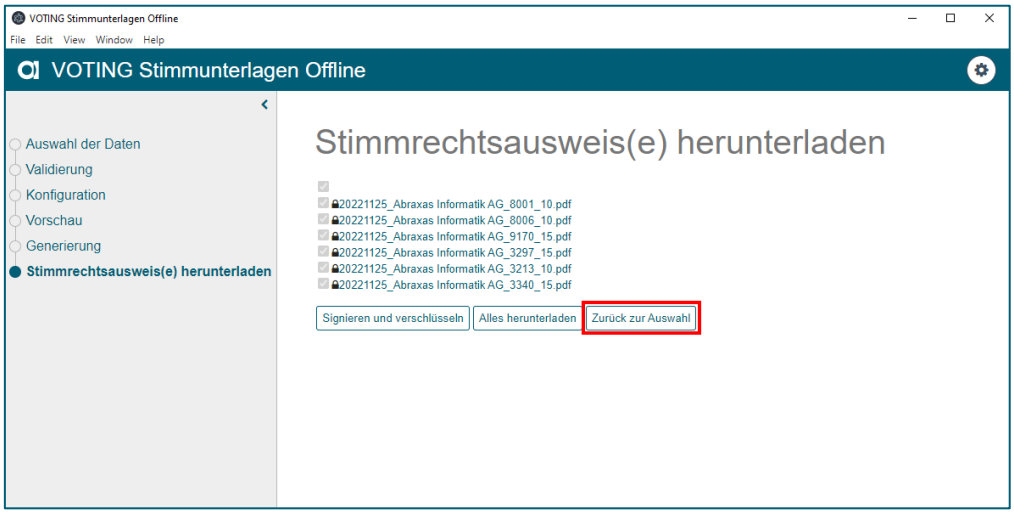

Abbildung 21: Löschen aller Daten mittels "Zurück zur Auswahl"

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

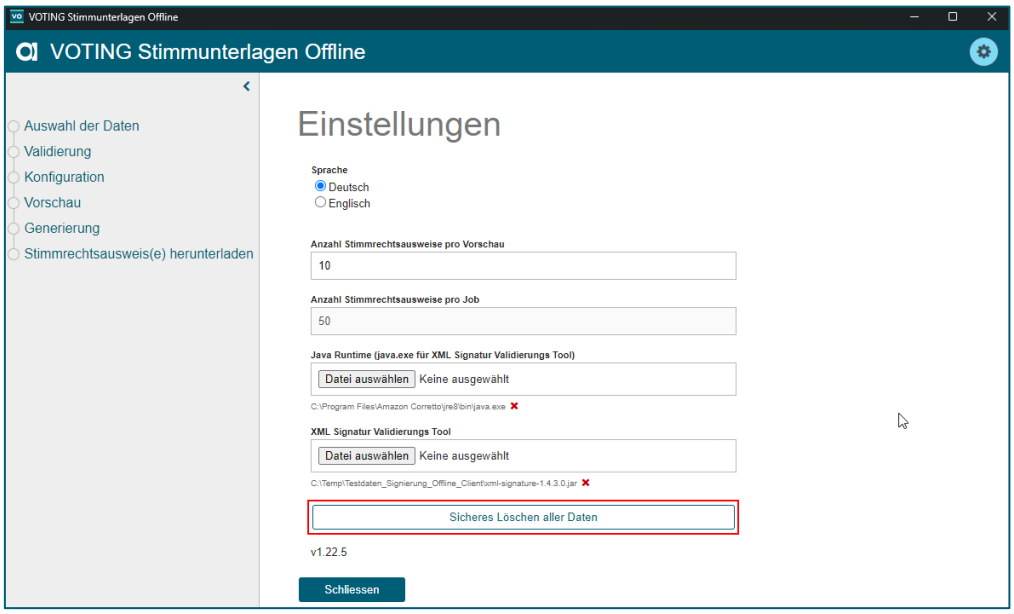

Abbildung 22:Löschen aller Daten mittels Einstellungen

Alle Dateien, welche währende 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 Zertifikat für die Verschlüsselung ist im Besitz eines Mitarbeitenden des Produktionszentrums der Abraxas Informatik AG, welcher 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 23: Zertifikat öffnen

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

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

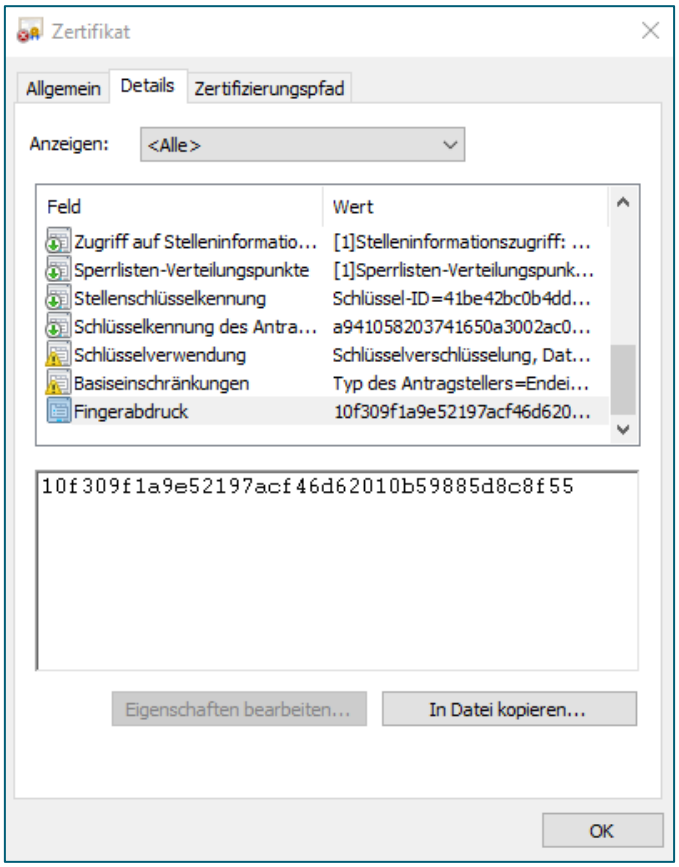

Abbildung 24: Fingerprint auslesen