Anonymität:

* Keine direkte Zuordnung von Stimme und Wähler in der Datenbank
* Für den Wähler wird ein Flag gesetzt, dass er gewählt hat
  + Authentifizierung notwendig
* Die Stimme wird mit den Eingaben erstellt und gespeichert

Authentifizierung:

* Zusatzinformation:
  + Geburtsdatum als TTMMYYYY
  + Name, Vorname, Gebursdatum als NVTTMMYYYY (mit definierten Stellen der beiden Namen)
* ID
  + Wird als Sequenz aufsteigend generiert
  + Nicht ideal, da Anzahl der Wahlberechtigten öffentlich bekannt und somit alle IDs erratbar
* Generierter Token pro Wahlberechtigter
  + Nicht erratbar
  + Muss extra gespeichert werden in elector oder als extra Tabelle
* Live-Generierung des Tokens aus der ID
  + Nicht erratbar bei kryptographischer Hash-Funktion (z.B. SHA 2)
  + Allerdings pro ID leicht berechenbar, wenn Berechnungsvorgang bekannt
* Live-Generierung des Tokens aus ID + Geburtsdatum als TTMMYYYY
  + Nicht erratbar bei kryptographischer Hash-Funktion (z.B. SHA 2)
  + Schwer berechenbar, da ID und Geburtsdatum bekannt sein müssen
* Anzahl von generierten Tokens pro Wahlkreis
  + Keine Zuordnung zum Wähler
  + Wird zufällig im Wahllokal ausgegeben
  + Jedes benutzte Token wird in der Datenbank abgehakt
  + Authentifizierung des Benutzers trotzdem nötig, um doppelte Wahlen zu verhindern
  + Nutzer-Daten müssen sowieso abgeschickt und verarbeitet werden

Vorgang:

* Der Wähler betritt das Wahllokal
* Der Wähler weist sich am Schalter aus (Personalausweis und Wahlbrief)
* Am Schalter wird nach obigen Methoden ein Token ausgegeben
* Der Wähler authentifiziert sich mit dem Token und persönlichen Zusatzinformationen, soweit nötig
* Der Wähler trifft seine Wahl und schickt den Stimmzettel ab
* Der Wähler wird ausgeloggt und verlässt das Wahllokal

Bewertung:

* Wahllokal für uns schlecht „simulierbar“, d.h. der Wähler muss sich **immer** auch gegenüber dem Wahlsystem authentifizieren
* Sichere Tokens alleine reichen also nicht, da persönliche Zusatzinformationen mitgeschickt werden müssen
* Tokens können/sollten also auch schon im Vorfeld dem Wähler in der Datenbank zugeordnet sein
* Verwendung von ID als Token + Authentifikation mit Zusatzinformation reicht aus
* IDs sind zwar erratbar, allerdings ist unbekannt, welchem Wähler genau die ID zugeordnet ist und insbesondere wie seine Zusatzinformation z.B. der Form NVTTMMYYYY lautet