

Digital Voting Process for Bavarian Elections

Overview

This document outlines the secure and anonymous digital voting mechanism designed for Bavaria elections. It utilizes a token-based system to ensure the integrity and confidentiality of the voting process, specifically designed to accommodate the unique aspects of Bavarian electoral procedures, including *Stimmkreis* allocation and the dual-vote system comprising *Erststimme* and *Zweitstimme*.

Token Generation and Registration

Step 1: Voter Registration

- **Voter Identification:** Each voter must provide their national ID number and the *Stimmkreis* (electoral district) where they are eligible to vote. This information is crucial for generating a unique voting token.
- **Token Creation:** A one-way hash function generates a secure token based on the voter's ID and *Stimmkreis*. This process ensures the token's uniqueness and anonymity.
- **Anti-Double Registration:** The system performs a check to verify that the voter is not already registered in any *Stimmkreis*. This safeguard prevents duplicate registrations and maintains the election's integrity.

Step 2: Secure Token Storage

- The generated tokens are securely and anonymously stored on a server. This measure protects voter identity and prevents unauthorized access to the voting tokens.

Voting Process

Step 1: Token Retrieval

- Voters enter their national ID and *Stimmkreis* into the user interface.
- If registered, the server returns the voter's unique token along with the *Erststimmzettel* (primary ballot) and *Zweitstimmzettel* (secondary ballot) corresponding to their *Stimmkreis*.

Step 2: Casting Votes

- Voters submit their choices for both *Erststimme* and *Zweitstimme*. The frontend sends the vote to the server through a secure communication channel, accompanied by their unique token.
- This method ensures that the vote remains anonymous and secure against potential interception by a man in the middle attack.

Step 3: Vote Confirmation and Token Invalidity

- Upon successful submission, the token is invalidated to prevent reuse, ensuring that each voter can only submit their vote once.
- The votes are then securely and anonymously stored in the database, maintaining the anonymity of the voter's selections.