Voting process

Pre-voting

Citizen table defines all citizens

CitizenRegistration defines in what Direktwahlbezirk a citizen may vote

hasVoted defines whether a citizen has voted already for the current year (can be initialized via initalizeHasVoted(year))

Citizens get a PIN to authenticate themselves at the voting machine. This could authentication could alternatively be done by a local assistant. For the purpose of having the election potentially human-free and online-voting-capable, we decided for the former approach.

Requesting to vote

Using their PIN, citizens authenticate themselves at the machine. Should they have voted already, they are informed of this and the voting process cannot continue.

In case they have not voted yet, a random yet unique token is generated for the citizen. Upon token generation the hasvoted flag is set for the given citizen. These two actions are done in a single transaction as to prevent the hasvoted flag being set and the token not generated or vice versa due to an error. The token is stored as a cookie on the machine.

At this point the citizen can vote only with the just generated token and on that local machine (by having the IP stored with the token) for his Direktwahlbezirk. Aside from that only statistical information (age, gender) are retained.

Voting

The citizens enter his vote and submits it.

If all choices are acceptable (invalid or a candidate / party votable for this citizen) the Vote is entered into the database alongside its statistical information. At the same time and in the same transaction, the token entry is deleted. This is again to prevent one of the two happening while the other aborts due to an error, thus preventing multiple votes or the loss of votes.

Last the cookie storing the token is removed from the voting machine to remove that association as well.

Drawbacks

With token generation being in the transaction of setting the hasvoted, which is associated with a ID number, and token deletion being in the transaction of entering the vote, an reasonably safe assumption can be made as to the association between ID number and vote, based on the timestamps of both transactions in the log files. However, having someone unauthorized or malicious access the log files is a security issue in itself and must be resolved at the level of file system access control.