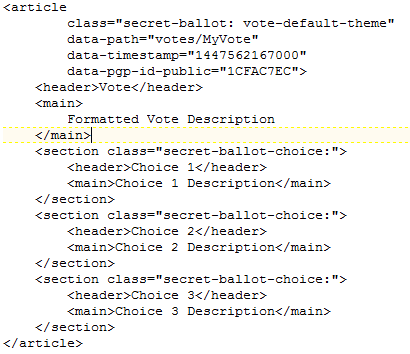
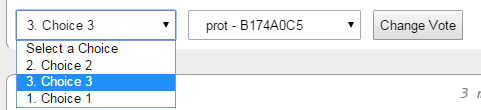
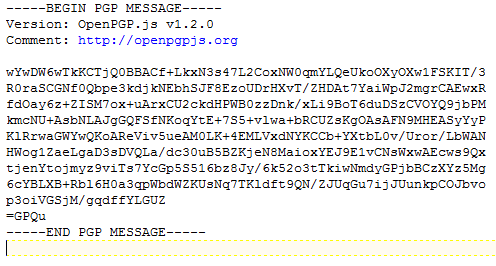
Relay In Depth: Secret Ballots

(Rough Draft)

1. Creating a Secret Ballot
   1. Anyone that uses relay can create a Secret Ballot.
   2. A Ballot Host creates a new Secret Ballot as an entry in their *KeySpace* and publishes it to the Relay Network. This is accomplished by generating the code using a *Secret Ballot Form Wizard* or writing the vote from scratch in HTML. Relay Clients interpret the votes as soon as they appear.
   3. The Relayer may customize the layout and descriptions of the vote before signing it as KeySpace Content. Once Signed, a vote must publish a newly signed revision if further changes are necessary.
   4. The Relayer that created a secret ballot is also the Host of that ballot and may periodically publish tally reports by decrypting their PGP Private Key.
   5. An (unsigned) HTML5 Secret Ballot generated by the Secret Ballot Form Wizard looks similar to this:  
      
2. Submit Votes
   1. Relayers on the network that view the vote may submit a 1-click, PGP encrypted vote request that only the Host can decrypt.



* 1. The Ballot Host automatically collects votes associated with their vote and decryptable by their PGP Private Key
  2. Relayers may view their own vote, along with a complete copy of the most recent ballot tally at any time. They may also use the tally sheet to verify the value and total value of the secret ballot. This happens automatically once authorized by the Relay Voter’s PGP Private Key
  3. Relayers may change their vote at any time.
  4. Example Encrypted Vote Value *(as seen by the rest of the network)*:  
     

1. Tally Reports and Verification
   1. When requested, Relay prints to the KeySpace the most recent Tally Report, as well as the means for each voter to validate their vote against the tally grand total.
   2. The Verification List consists of a one-per-vote entry list of hash strings. Each hash is a string of characters and numbers of indeterminate length that, when combined by the client with information inside the encrypted vote message, validates the vote without exposing the value or identity to the network. This can happen automatically once the voter’s PGP Private key is authorized.
2. Protection against Double-Voting and Fraud
   1. Double-Voting may occur when a user attempts to vote more than once with different PGP Identities registered on the network.
   2. Relay Secret Ballots combat fraud by identifying it after-the-fact during Verification. Old vote tallies may be updated and revalidated with newer fraud scrubbing (via software updates) at any time.
   3. Vote tallies may be adjusted as fraud is identified.
   4. Optional Methods for identifying fraud
      1. Meta Tags - Optional meta tags can be requested of voters asking for real name, address, and other data while encrypting any sensitive. Only the Host may decrypt the optional tags during Verification
      2. Fraud Scrubbing - occurs on the network in relation to the *Reputation* of each PGP Identity. If an Identity is flagged for abuse, it may fail to qualify for votes.
      3. Voter Registration - Optional voter registration ensures a secure pool of voters without exposing the identities or relationships between Relayers. Registration is accomplished when a registered Relayer authorizes a non-registered Relayer to vote. Registering a pool of Relayers creates a Reputation Tree where each Relayer is responsible for any Relayers they register. If fraud occurs on a registered account, that account and all accounts it registered may no longer be qualified to vote.
      4. Real ID verification. Any method that proves the real-world identity of a voter may be used to authorize a PGP Identity for voting. An example would be a $0.01 charge to a credit card.
3. Secret Ballot
   1. Relay maintains the secrecy of the voter’s identity and vote value using PGP Encryption.
   2. Ballots tallies may be set to *Periodical* to protect any chance of determining vote values and identities (theoretically by correlating changes to the grand total with voter activity). Otherwise, ballots are updated whenever the Host PGP Private Key authorizes a new tally. This can happen in real-time
   3. PGP Identities are not revealed in PGP Encryption. Users who vote or engage in voting only provide a portion of their PGP Fingerprint known as a Key ID. Votes can be tallied without revealing the identity of the voter.
4. Reputation
   1. Each vote created has a single point of failure: The Host. The only entity able to tally and publish results is that which controls the PGP Private Key. This also means the *legitimacy* of the vote is bound to that PGP Identity. A public vote will only be as good as the *reputation* it carries with the community.
   2. Allegations of tampering can be independently verified by using the Tally Reports history available publically on the network. Conversely, best practice and full disclosure are the primary means for building a community *reputation.*