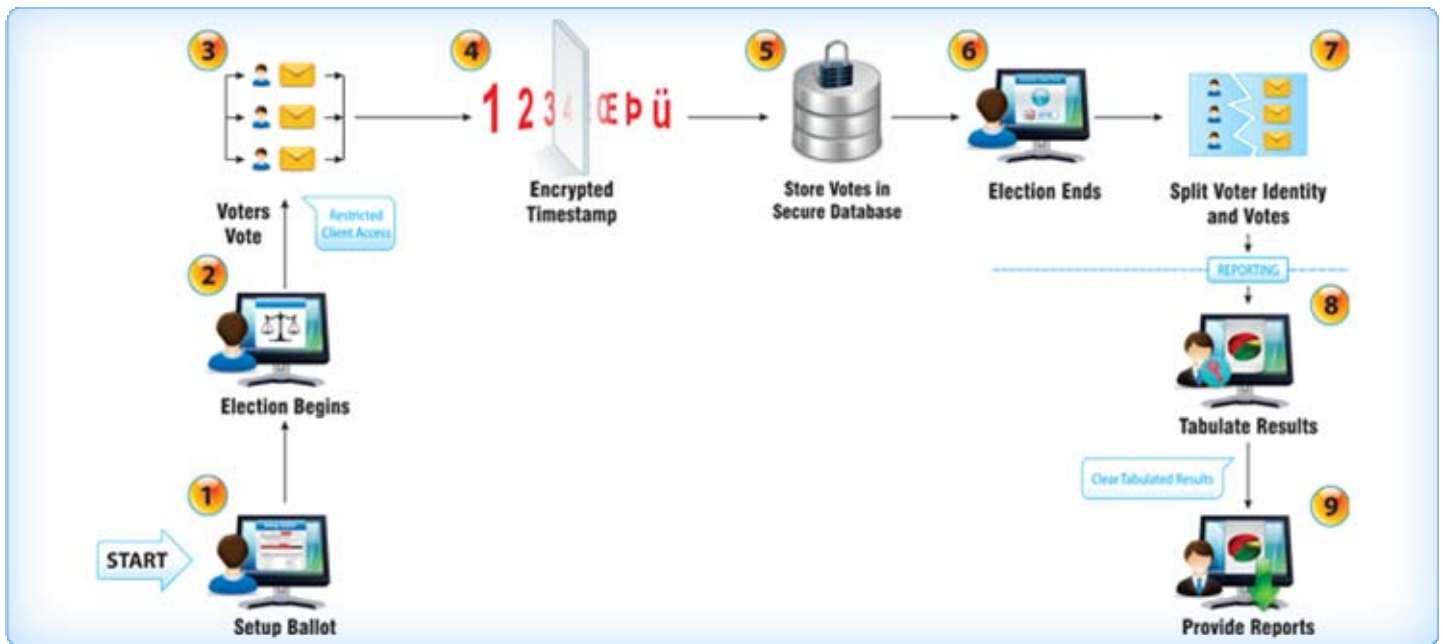


## Step by Step Explanation of Secure Online Voting for Unions



### Setup Ballot:

A Votenet Solutions election manager will set up the online ballot.



### Election Begins:

Ballots officially open based on time settings.

**Q: How is the encrypted key generated? Can technicians unlock it with the key or override it?**

**A:** We use a method known as “Public Key Encryption” to generate a pair of keys – a public key and a private key. The voting system will use the public key on the website to encrypt the timestamp data before it is stored in the database. There is no way for the website to decrypt the timestamp.

The private key will be stored at a separate physical location on the network. If fraud claims are made, the technology staff can decrypt the timestamp manually. This means that data must first be downloaded from the secure database and then a special program run to decrypt the data.

Also, the above process can only be done prior to the election being finalized. There is no way to decrypt any data once it is finalized.

---



#### Voters' Votes:

The online voting system is anonymous. This means that voters' identity is separated from the choices they make.

---



#### Encrypted Timestamp:

As ballots are passed in the database, timestamps will be encrypted. To the naked eye, it will be impossible to match-up two timestamps and match a voter and choices. This is a truly anonymous system where even the technicians cannot manipulate any votes or results.

**Q: Can the technician override the system?**

**A:** No. No one can override the system to stop encryption or decrypt "on the fly". Only the process outlined above exists.

**Q: Can the technician, because he/she built it, break it and see who voted for whom?**

**A:** No. The decryption password is stored separately from the election data, and a technician needs the system password to get the password and then know how to use the decryption tool to input the password. So merely knowing the decryption password is not enough.

---



#### Store Votes in Secure Database:

The Online voting system will have its own database. The timestamps and votes will be stored in encrypted format in secure databases.

---



#### Election Ends:

Once the election is complete, the administrators must "Finalize" it to view the results. Before an election is finalized, the reports and results are not available to administrators. This additional step further restricts administrator access to the system while the election is running. Since no reports are available while an election is in progress, the chance of fraud by administrators is further reduced.

---



### Split Voter Identity and Votes:

In addition to the encrypted timestamps, this phase of the process takes security one step further. Once an election is “finalized”, the encrypted timestamps are completely deleted, so there is no physical way to connect choices made to the voter.

**TIP: Why bother storing them in encrypted format if we’re going to delete them anyway?** This is done to provide an administrative “way out” in case the demand is made for a recount or if certain clients’ by-laws allow administrators to view votes prior to election results being closed. In this situation, before an election is finalized, it is possible to download a copy of the votes into a portable format (like Excel) and decrypt the timestamps. Note that timestamps cannot be decrypted in the database. These always remain encrypted. At cost, results can be downloaded to excel and then manually decrypted for inspection of the data to handle fraud claims.



### Tabulate Results:

The system will tabulate the votes and generate results.



### Provide Reports:

Results will be provided in downloaded and formatted report formats.

### Additional Information:

The public key encryption method will encrypt vote timestamps making it impossible to link a voter and his/her choices by mere observation. To make a successful link, the following must occur:

1. Technician downloads the data from secure database
2. Technician invokes a locally stored application program to decrypt data. Only this application can read the private key needed to unlock and decrypt the data.
3. Furthermore, merely having access to the private key and the decryption application does not grant access. The technicians must have physical access to the system to access the location where the passwords are stored.
4. Decrypted data is stored separately; visual observations made to find matching timestamps
5. This process is always “at a point in time” and up-to-the-minute data cannot be decrypted since there will always be a time-lag
6. This process can be done only during the time frame when an election is activated till it is finalized.

These six steps make it difficult for someone acting alone to tamper with or even view the data.