



## Security Overview

### Safe, secure, and reliable

Everyone Counts uses military-grade encryption to encode each ballot. No ballot can be read until decrypted using the election judges' keys. Even the authors of the software or the Internet Service Provider cannot read or alter the ballots on their way to be counted.

Only Everyone Counts uses a completely open software system. All of the computer code handling the ballots is available for audit and inspection by independent reviewers. And we build the whole system on open-source software and industry-standard hardware. There is no hidden technology, so you and your auditors know exactly what the Everyone Counts system is doing.

We use a multi-key system to secure our votes. The first key locks the vote up at casting time (the sealed ballot box) and at counting time the second set of keys unlocks the vote (checking and breaking the seal on the ballot box). Even a single election official can't access the votes. Like a nuclear missile, the Everyone Counts ballot box cannot be accessed until multiple authorized officials enter their coded keys.

### So tough, even the security experts use it

Everyone Counts has been chosen for secure voting by the Australian Defence Forces on their secure military network.

Top auditing/accounting firms like KPMG use Everyone Counts for their own internal board elections.

The US Democratic Party chose Everyone Counts for overseas voters in the 2008 primary election, one of the most highly scrutinized primaries in recent history.

### More secure than direct-recording electronic (DRE) machines

Unlike DRE machines, Everyone Counts immediately encrypts each ballot with a different key and sends it off to a remote, secure ballot box instantly, so ballot records cannot be lost or misplaced.

Unlike DRE machines, the computer code handling the voting and ballots is transparent: completely available for inspection and audit. There is no "black box" to hide mysteries.

Unlike DRE machines, Everyone Counts takes votes on standard PC hardware which has not been altered.

## Bringing confidence to the voter

Everyone Counts uses state-of-the-art computer security to ensure that each person's vote gets counted as intended.

Prevents discarding of ballots. Each ballot receives a unique code based on a secret word the voter chooses. When the election closes, the voter can go to the election website and see this unique code to prove that the ballot was received.

Prevents alteration of ballot. At the moment the user presses the final button to cast his/her vote, the computer encodes the ballot using digital encryption. From this moment forward, until received and decoded by election judges using their secret keys, the ballot looks like a long series of meaningless numbers. Without the keys, even a Ph.D. mathematician with a top-of-the-line computer lab cannot unscramble even one ballot enough to alter it and put it back together again.

Provides verification that ballot was delivered intact. Optionally, each ballot can be wrapped in a "digital envelope" marked with a secret phrase chosen by the voter. The voter can visit the election site on the Internet. The secret phrase verifies that his or her sealed envelope was delivered correctly to the counting station.

Prevents unauthorized viewing of votes. Before transmission, each ballot is encrypted (put into digital code) so that no one but the authorized election judges can read it using their digital keys. Even the Internet service provider cannot read the ballot without these keys, which are unique to each election.

Prevents "mystery software". One of the concerns about electronic voting machines is their secret, proprietary software. Independent inspections have found errors and unacceptable quality problems in that software. Because the Everyone Counts system is based on open-source software and is open to 100% inspection, there is no secret software to hide biases, defects, or other problems.

Prevents "rogue software". Another concern in traditional electronic voting machines is the difficulty of detecting altered software. Everyone Counts uses crypto digest technology and public-key signature technology to ensure that the software running on a machine is exactly the software chosen for the present election, with no additions or alterations.

Prevents abusive third-party intervention. Voters with disabilities often rely on a third party to execute a ballot for them, opening the door for interference and lack of privacy.

Prevents identifying marks. Every ballot submitted by the Everyone Counts voting station contains only the data constituting a valid ballot. Software prevents any addition or alteration outside the rules set by election officials.

Prevents "mystery hardware". Everyone Counts voting runs on an industry-standard computer chosen by the polling place or by the actual voter. There is no proprietary computer doing who-knows-what. Open software running on open computers – that's the Everyone Counts way.