

# TruVote Software, Operating and Data Base System and System Security

## Overview

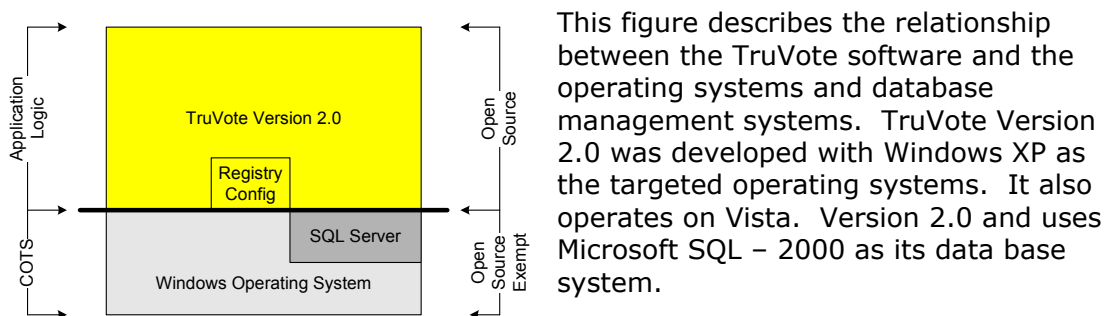
The requirements for voting used for United States general elections are defined in a set of guidelines produced by the United States Election Assistance Commission (EAC). ([www.eac.gov](http://www.eac.gov)) This commission was established by the Help America Vote Act of 2002 (HAVA) (<http://www.fec.gov/hava/hava.htm>). The guidelines are used by the states in generating requirements for voting systems they purchase and use. Voting equipment and systems must be certified against these guidelines to be accepted by the States. The 2005 Voluntary Voting System Guidelines (VVSG-2005) are currently in effect. TruVote 2.0 is conformant with these guidelines. The guidelines are available at <http://www.eac.gov/voting%20systems/voting-system-certification/2005-vvsg>

Existing voting equipment has not been certified to the VVSG-2005 guidelines. These system have been certified to the expired 2002 Voting System Guidelines (VVSG-2002). These systems must be upgraded to meet the standards of proposed legislation.

Several known deficiencies in VVSG-2005 have been addressed in newly proposed guidelines as developed by the EAC Technical Guidelines Development Committee as supported by the National Institute of Standards and Technology (NIST). These proposed guidelines were released in August 2007 (VVSG-August 2007) and are now in the public comment phase. The guidelines are available at <http://www.eac.gov/vvsg> The VVSG-2007 places a strong emphasis on election transparency (open), security, accuracy, paper records and audits. There is also emphasis on procedures required at the polling place. There requirements are also the emphasis of the TruVote 2.0 software which is conformant with VVSG-2005 and will be conformant with VVSG-August 2007 guidelines with few changes.

The TruVote Version 2.0 voting system software conforms with these requirements. Version 2.0 will be certified to VST-2005. A future release is planned which will be certified to VVSG-August 2007 as these guidelines are finalized and released by the EAC.

## Version 2.0 relationship to COTS software products



## “Open” Source

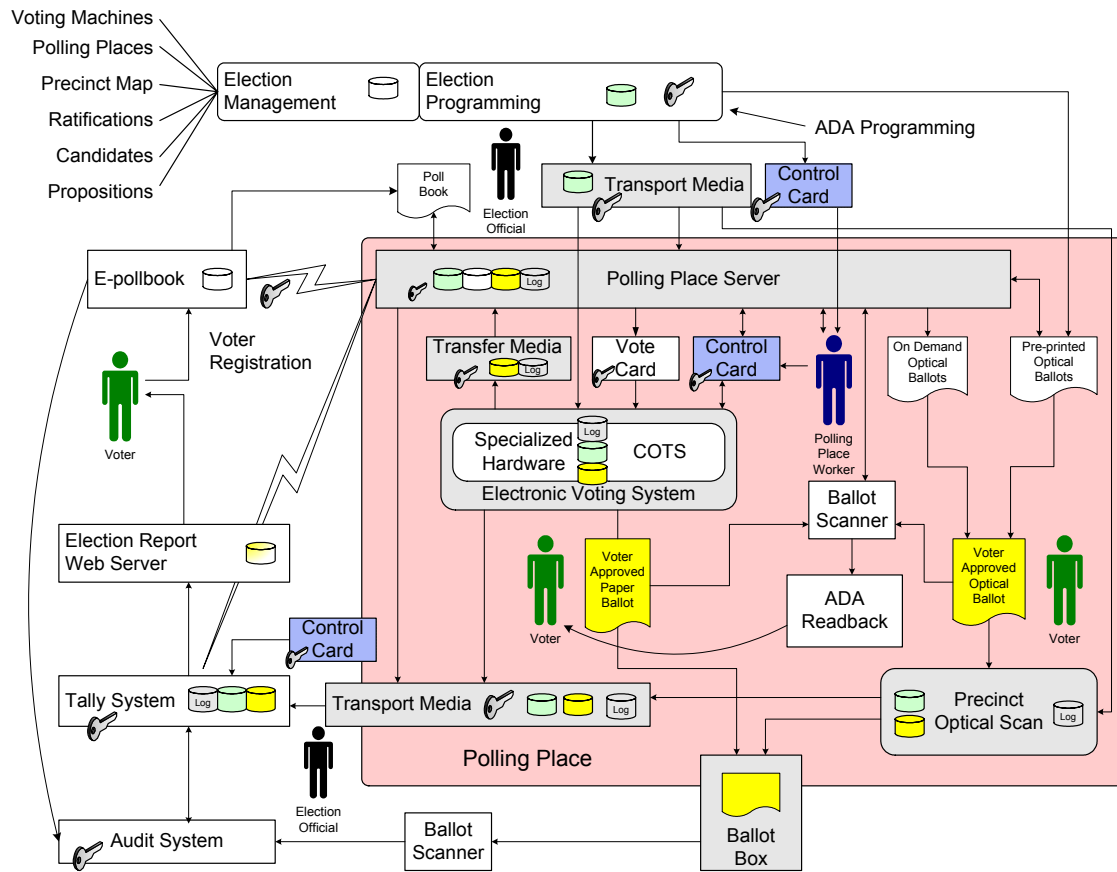
Currently some states require voting system software to be “open” and available for qualified review. TruVote intends to provide source of its software to an open environment. The VVSG-August 2007 does not require source to COTS software to be available as open source when off the shelf, commercially available versions are used. TruVote intends to meet these requirements.

## 2.7 Treatment of COTS in Voting System Testing

To clarify the treatment of components that are neither manufacturer-developed nor unmodified COTS (commercial off-the-shelf software/hardware) and to allow different levels of scrutiny to be applied depending on the sensitivity of the components being reviewed, different subdivisions of COTS have been identified, with various requirements scoped to the new terminology. For example, a COTS operating system may not require source code review, but configuration files that support the configuration of the operating system would require test lab review. The way in which COTS is tested has also changed; the manufacturer must deliver the system to test without the COTS installed, and the test lab must procure the COTS separately and integrate it. If the integration is successful, the COTS can safely be assumed to be unmodified. [VVSG-August 2007, page 60 The full document is available at <http://www.eac.gov/vvsg>]

## **Voting System Component Relationships**

Components of the TruVote Voting system are shown below.



## User Profiles

Voting systems operate in an environment of open public awareness. Multiple user types interact with the system and have different profiles.

**Voters** are the general public. Little or no computer experience is assumed, however, most voters have experience with ATM type touch screen systems.

**Polling Place Workers** are selected from the general public with little or no computer experience. Polling place workers receive some training in the use of the system

**Election Officials** have some computer experience, but have a focus on election procedures not computer systems

**Election programming** is often performed, under contract to the election jurisdictions by vendors who are training in computer systems and the programming, setup and operation of the various components of the election system.

## Election Management and Programming

A data base of the election information is generated and updated by election officials. This data base includes information about voting machines, precincts, maps, candidates races etc. Systems used for election management are usually Windows

client and server based with SQL as the database system of choice. Microsoft SQL will be used in the TruVote system.. Software is provided by voting equipment vendors or often in-house generated.

An important component of election management is the **Poll Book**. This is a list of registered voters and includes the polling place where they are to vote. Currently, most election jurisdictions print a copy of the poll book to be used at the polling place. This requires the voter vote at the location where they are listed in the poll book. Electronic poll books as being developed by Microsoft will allow for an on-line connection between the polling place and the poll book lists. This will allow voters to vote at any polling place of their convenience. On-line connections to voting machines are not allowed. Therefore, one of the function of the TruVote Polling place server is to provide on-line connections between the poll book data base and the polling place. The polling place server generates vote cards which are used by voters at the electronic voting machines.

### **Digital Keys**

All components of the TruVote election system software and data are digitally signed using a PKI key structure. Keys are shown in the figure. Private keys are transferred through the voting process using smart cards. All actions and data in the TruVote system are also authenticated by digital keys. Each record in the data base is signed and as the data base is ready for transfer, the entire data base is also signed. Physical security and accountability of key cards is part of the security model.

TruVote Version 2.0 software the Advanced Encryption Standard (AES) or Rijndael 256 bit encryption.

### **Transport Media**

Election data are transferred from the election management system using CD-ROMs. The CD-ROM is robust, permanent and write once. A corresponding control card is also generated for each polling place, signed for by the polling place judge and used to authorized all procedures at the polling place.

### **Polling Place Server**

The polling place server is unique to the TruVote system. It is a Microsoft Windows and SQL based system which support the TruVote Version 2.0 software. The polling place server manages security at the polling place, provides support for the electronic poll book and guides the polling place worker through the election process.

### **Electronic Voting System**

The TruVote Electronic voting system uses Microsoft Windows and SQL server as the foundation to the TruVote Version 2.0 software. Election data is transferred into the voting system using digitally signed transfer media (CD-ROM)

The polling place worker uses the control card to activate and control the voting system. Commands for the voting machine are generated by the polling place server and written to the digitally signed control card.

Each voter is given a vote card which identifies the correct ballot face the voting machine is to present. This vote card is also digitally signed, limited to use in the voting machines assigned to the polling place and is erased after each use. The vote card is returned to the polling place worker and reused.

## **Paper Records**

Proposed legislation <http://www.govtrack.us/congress/billtext.xpd?bill=h110-811>  
H.R.811: Voter Confidence and Increased Accessibility Act of 2007 – requires a paper record of each ballot cast to also be printed and approved by the voter before it is cast into the ballot box. There is a duplicate of the paper record in the electronic record maintained in the electronic voting machine. The paper record also contains an index number which links the paper record and the electronic records for audit. This index number is not associated with the voter but unique to the ballot.

The content of each paper ballot is encoded in a PDF 417 two-dimension bar code. The PDF 417 bar code contains check for each field in the code in addition to cross field checks. This insures the bar codes are complete and not modified.

The final security component of the voting system is an audit between the paper and electronic records.

## **ADA Considerations**

The proposed H.R. 811 legislation mandates disabled persons be able to have their paper record read back on a system which is not the electronic voting system. The polling place server provides this capability. Microsoft Accessibility and text to speech support as provided by Windows is a key component of this capability. The ballot bar code is scanned and used as input to the read-back process.

## **Election Reporting**

Election results are summarized at the polling place by the voting machines and the polling place server. Each record of the data is digitally signed as well as the entire data base being signed. Data are written to a CD. Election results are physically moved to election central for tally. Optionally the Polling Place server can electronically transport election results for tally.

## **Tally System**

The tally system links to the election data base and insures data are received from all polling places and voting machines. This system is a Microsoft Windows and SQL based system

## **Audit System**

The audit system provides for the scanning of paper records and compares their content with the contents of the tally system. This is a Microsoft Windows and SQL based system which is separate from the tally and election management systems.

## **Process Flow**

The process flow of the polling place is shown below.

