



AN OPEN SUITE OF ELECTION TECHNOLOGY SYSTEMS & SERVICES

Preliminary White Paper
v 1.0

Gregory Miller
gam@osdv.org

E. John Sebes
jsebes@osdv.org



ABSTRACT

The mission of the Open Source Digital Voting (OSDV) Foundation mission is to work to restore trust in the cornerstone of American democracy—the process of fair and free elections—through the design and development of open source, transparent, high-assurance election and voting technology, freely available for adoption and deployment by any state, jurisdiction, or precinct.

The first step toward achieving that goal is to lay the foundation for a new elections technology platform built on open processes, open data, and open standards. Such a foundation is described in the high level overview provided in this White Paper.

This paper represents the first substantive results to be presented to the real stakeholders in American election systems—the States’ elections officials charged with determining, deploying, operating, and managing the systems and services used to ensure fair public elections.

This paper will be used as the root for subsequent development of all work product of the OSDV Foundation’s TrustTheVote Project including, but not limited to Request for Comments (RFCs), Design Specifications, prototypes, and open source reference implementations of election systems and services. While through transparency of the non-profit OSDV Foundation any and all content is readily and freely available once published, the intended audience for this White Paper is primarily States’ elections directors who’ve taken an interest in the work of the OSDV Foundation and the TrustTheVote Project. This version of the White Paper is considered “draft” and comments and feedback are invited and welcome.

INTRODUCTION

This is the initial document to describe, in summary manner, the core work of the OSDV Foundation's TrustTheVote Project. This document provides the initial footing for all Request for Comments, Design Specifications, and ancillary content. It is the first public release of an organized description of a “system” comprising a suite of devices and services, which taken together, create an open source, high-assurance, transparent, and certifiable voting system architecture or blueprint for the American public benefit.

This White Paper presents a draft system that is the result of investigation and research on “best practices” voting systems in the United States conducted by the OSDV Foundation between January 2007 and January 2009. The following observations can be made from that investigative period:

Over the months, many approaches, architectures, and designs were considered.

Thorough consideration included hundreds of hours of online and offline interactions with [a] elections officials at state and federal levels, [b] leading voting systems experts, [c] computer scientists, and [d] election law and public policy specialists.

The outcome of that research resulted in the conclusion that current elections processes represent the best and most likely basis for “requirements” and operational preferences for any new voting system design intended to improve reliability, ease operation, and restore trust in elections technology.

Certainly, there are opportunities for innovation, however, a base architecture must be established and proven first, which fully accounts for the desires, requirements, and political preferences as they stand today.

Therefore, this draft White Paper describes what the TrustTheVote Project Core Technology Team (“CoreTeam”) believes to be the best case solution to address the challenges of restoring trust in voting systems and providing a transparent system to do so. It is only an initial draft presented to the first line stakeholders: the States’ elections directors, officials, and staff for review, advice, and comment.

The TTV Suite of Election Technology Systems and Services will be designed and developed to provide a broad range of transparent, high assurance elections technology to meet current and emerging needs of IT automation of election processes as best understood and articulated by our stakeholder community of States’ election directors and their designates (the “Design Congress” or “DesCon community”). What follows is a high-level description of the envisioned suite, with a summary of each component.

1.0 TTV SUITE

1.1 Two Types of Components

The TTV Suite is composed of two types of components:

- Services applications delivered via a Web browser user experience, preferably using a “Browser Appliance”
- Application-specific, single-purpose, dedicated devices

First, the TTV Suite includes **Election Data Management** (EDM) Services. These three applications, shown in Figure 1, provide services for data management of election-related information concerning:

- voter registration (the **Registrar**);
- election management (the **Election Manager**); and
- ballot composition (the **Ballot Design Studio**).

Each of these is built for data-center deployment using standard platforms and software stacks like Linux, Apache, and MySQL, or commercial products of a similar nature.

To best deliver these three services, the TTV Suite includes a specialized utility called a “**Browser Appliance**” that provides election officials with a high-integrity, dedicated, web browser-like alternative to access EDM Services. Certainly, one can use common Web browsers on existing commodity-based personal computing systems and workstations to access these services, but there are distinct benefits of using a dedicated browser experience to minimize, if not outright prevent, the introduction of variable conditions, unwanted data, or errant operations. (More detail in **Section 2.4**).

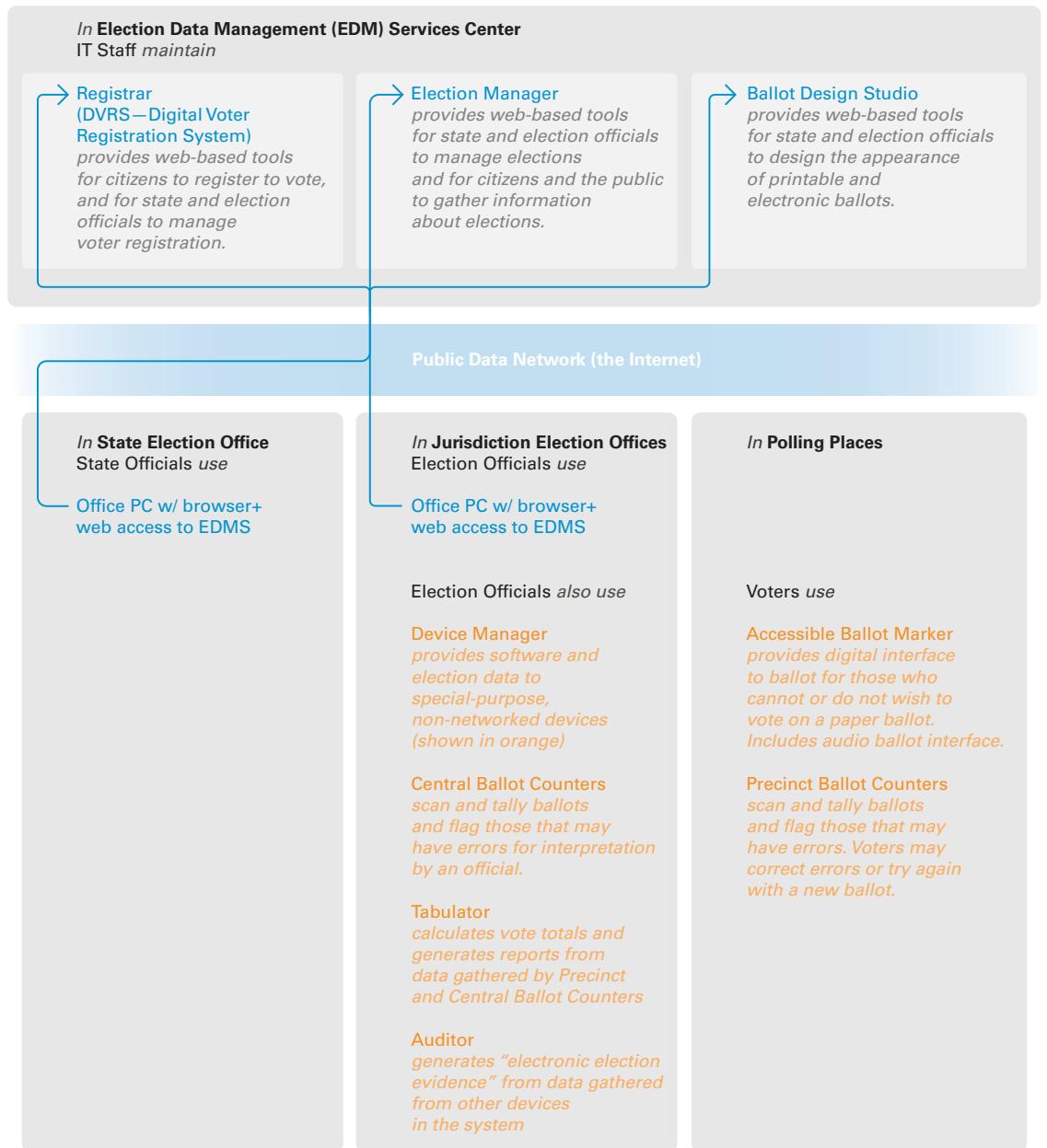
The TTV Suite also includes a **Voting System**, which is comprised of five single-purpose, un-modifiable, dedicated devices, each performing a single function solely by local (non-networked) computing. The devices include:

- **Precinct Ballot Counter**
- **Accessible Ballot Marker**
- **Central Ballot Counter**
- **Tabulator**
- **Auditor**

The **Auditor** consolidates all the log records and audit data of an election cycle, and provides features useful for election audits.

THE TTV ELECTION TECHNOLOGY SYSTEM

Figure 1



2.0 TTV ELECTION DATA MANAGEMENT

2.1 Registrar

The TTV Suite's **Registrar** provides all the functions of a typical state-level voter digital voter registration system (DVRS), both general features, and a capability for localizing features to specific state's needs.

The high-level concept of operation of the Registrar is:

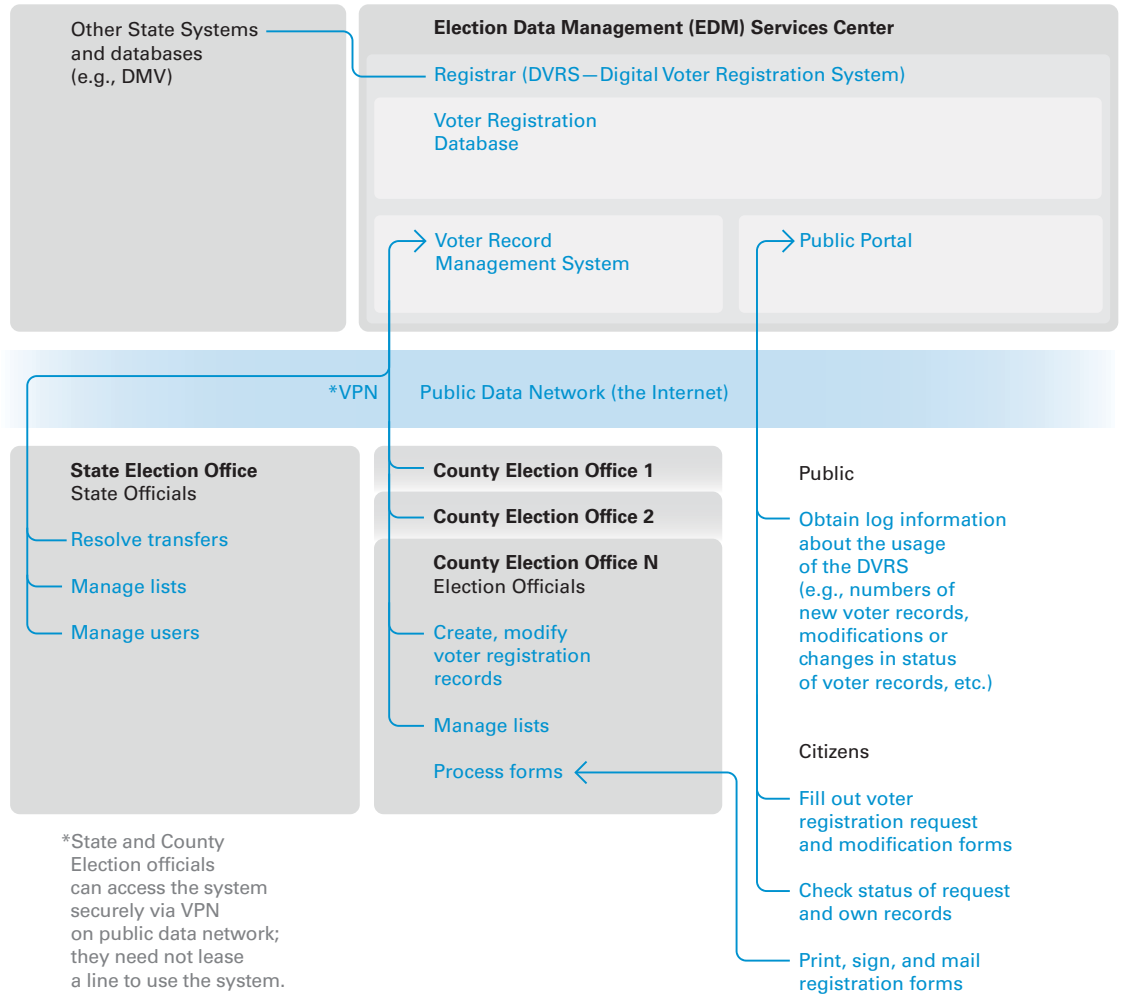
- Citizens use the public portal of the Registrar to create registration request forms and registration modification forms (to be printed, signed, and mailed to a jurisdictional elections office), and to track the status of requests, and of their records.
- Jurisdictional elections officials process these forms, creating and modifying voter registration records, and also perform other jurisdictional functions including list management.
- State elections officials perform state functions such as transfer resolution, list management, voter wheel preparation, and user management of the TTV Registrar system itself.
- Members of the public at large use the public portal to obtain log information about the usage of the DVRS (e.g., numbers of new voter records, modifications or changes in status of voter records, etc.)

Figure 2 illustrates the Registrar, a group of Web-based applications that are accessed by both citizens and state elections officials. Public (citizen) access is achieved using ordinary Internet-connected PCs to communicate with the TTV Registrar system deployed in a State authorized or owned and operated data center. Jurisdictional and state elections officials access the Registrar either via a public data network, or private networks of dedicated communication links.

Figure 2 also shows (at the label "VPN" in the center left), deployment of the TTV Registrar using Virtual Private Network technology to create an access-controlled link between the data center and each local network at a state or jurisdiction election office. The Registrar supports the use of standard Web security protocols SSL and HTTPS to authenticate individual election officials' access to the system.

PUBLIC DATA NETWORKS CAN INCREASE REGISTRATION TRANSPARENCY AND EFFICIENCY

Figure 2



2.2 Election Manager

The TTV Suite's **Election Manager** is a data management application for managing election data including jurisdiction and district extents and boundaries, precincts, election definitions, contents, candidates, etc. **Figure 1** illustrates the Election Manager as an EDM service similar to the Registrar. In other words, the Election Manager is a Web-based application that is accessed by both citizens and election officials in the same way as the **Registrar**. The high-level concept of operation of the Election Manager is:

- Between election cycles, election officials use the Election Manager to modify and manage the definitions of districts, jurisdictions, precincts, etc.
- In the early phases of an election cycle, elections officials create election contests in the Election Manager, populating them with information about candidates, measures, etc.
- After the contest qualification period is over, and the deadline for ballot definition nears, jurisdictional election officials pull from the Election Manager the full set of contests in the jurisdiction for the election, as well as the data that defines each ballot style. These are used as part of the ballot design process (see below). These ballot design styles include jurisdiction-specific factors such as candidate rotation.
- After the voter registration process is closed, jurisdictional election officials pull from the Election Manager the data that represents poll books for each precinct, including a printable form. (To create the poll book data, the Election Manager cross-references precinct records with voter registration records pulled from the Registrar.)
- Members of the public access the public portal to obtain log information about the usage of the Election Manager, e.g., precinct/address and precinct/district relations, current state of contests in the upcoming election, etc.

2.3 Ballot Design Studio

The TTV Suite's **Ballot Design Studio** (BDS) is the third EDM service, to be deployed and accessed as a Web-based application, also illustrated in **Figure 1**. The Ballot Design Studio is an **AIGA** Ballot Design Guidelines Standard (1) tool for jurisdictional elections officials to create ballot definitions that are used by the various components of the TTV **Voting System** (described later). Ballot style definition data from the TTV **EMS** is used as the starting point for the design of each ballot style.

The BDS automatically creates drafts of printable ballot images for each style, using existing national ballot design guidelines, and applying constraints or requirements as specified by state election codes. Election officials can then perform modifications of the draft ballot images (e.g., changing the default order of contests). In addition to completing all of the individual ballot style designs, election officials use the BDS to apply global modification (e.g., jurisdiction-specific instructions, in order to finalize the ballot definitions.)

Electronic visual ballot representations are derived from the paper ballot images. Electronic audio ballot representations must be provided for each unit of the electronic visual representation.

When the ballot design process is complete, election officials pull from the BDS the various data that will be used by the TTV Voting System, including printable ballot images, ballot meta-data used by ballot counting devices (e.g., contest/candidate/ target-mark-zone relations), and electronic ballot representation (image and audio) and meta-data to be used by electronic balloting devices.

¹ The American Institute of Graphic Artists (AIGA) was commissioned by the Federal Elections Assistance Commission (EAC) to develop a set of standard ballot design guidelines. See generally: <http://bit.ly/VUh7W>

2.3 Browser Appliance

The TTV EDM Services are implemented as a set of Web-based applications as described earlier. Elections officials can certainly access the EDM Services using any Web browser on typical personal computing devices. However, the TTV Suite includes a **Browser Appliance** which election officials can use for dedicated access to the EDM Services, with all the application configuration and security settings pre-populated and unmodifiable. In other words, this application interface has all of the look, feel, and user interaction experience of any World Wide Web browser; however, its capabilities and utility are restricted to the EDM services it is accessing “across the cloud.”

To achieve this, the Browser Appliance uses the election officials’ existing PC hardware, but not any of the software or data stored on that PC (e.g., no other ancillary software, applets, bookmarks, cookies, or utilities). Instead, the Browser Appliance is a “bootable system image” (2) delivered on a write-once medium such as CD-ROM media. Use of the Browser Appliance begins by starting (“booting”) the PC hardware with such a media (disk). This action results in the user presented with what appears to be typical Web browser application experience, but pre-configured for access to the EDM Services in a manner that is error-free and higher assurance (with respect to software errors and “malware.”)

² A system image in computing is the state of a computer or software system stored in some non-volatile form. The form of storage is often a file. A system is said to be capable of using (or dumping) system images if it can be closed down and later restored to exactly the same state. See generally: http://en.wikipedia.org/wiki/System_image

3.0 TTV VOTING SYSTEM

3.1 Device Manager

The entire TTV Voting System is comprised of the dedicated devices illustrated in **Figure 1**. The **Device Manager** is the component of the overall system that manages all other system devices, using election-specific data and information. Election-specific data from the TTV Ballot Design Studio is supplied to the Device Manager as its input for its operation during a specific election cycle. In fact, the Device Manager supplies all the information required by the TTV Voting System for an election cycle.

The Device Manager is a special-purpose, non-networked device, which like all the devices, runs on existing PC hardware (but without using any software or data stored on the PC), booting from a write-once media such as CD-ROM disk. Once launched, the Device Manager obtains its input from another such medium (disk), created by another computer, interacting with the Ballot Design Studio to download the requisite information and “burn” it to disk. The Device Manager has no electronic connection to other systems because it is non-networked. Of course, operation does rely on a manual means (as just described) of transferring data from the TTV Election Data Management services, as a step towards assured integrity. (3)

The Device Manager’s principal function is to create “boot images,” on write-once media (e.g., CD-ROM disk), for each of the other components of the TTV Voting System. Each of these boot images contains the software for the specific component (which is fixed, not changing between elections), and the election-specific data and configurations for each device. For example, the two ballot counting devices’ configuration includes data that defines where on a marked paper ballot image the ballot counting software should look for marks, and what each mark means in terms of contest and selection.

The Device Manager is intended to be operated in a jurisdiction’s Elections Office, and used as part of the officials’ preparation for an election as a “best practices” implementation.

³ This is sometimes referred to affectionately as “sneaker net” on the basis that an individual walks the data transfer from device to device by way of a disk media.

3.2 PRECINCT BALLOT COUNTER

The **Precinct Ballot Counter** (PBC) device is used in a polling place, to scan a paper ballot for errors (e.g., over-votes, possible under-votes), and if error-free to retain the data from the ballot, for tabulation (since typically a scanned ballot goes immediately into a secured ballot box.)

The PBC device is comprised of [a] application-specific software (contained on a boot disk created by the Device Manager) and [b] hardware that includes a commercial off-the-shelf (“COTS”) optical scanning device. The PBC uses a COTS scanner to provide the functions of a conventional Precinct Count Optical Scan (PCOS) device. Each “duty cycle” of the PBC software begins when the scanner provides a ballot image to be processed. The PBC software performs digital image processing to find marks in target areas (specified in the election-specific configuration data) and maps the marks to election-specific interpretations of contests, candidate, choices, etc. Apparent over-votes and under-votes are identified and handled in a typical manner for PCOS systems.

At the end of session (typically a full election day of service in a precinct or voting center or early voting center), the PBC produces vote tallies for each contest, and audit logs that include each ballot image and the interpretation of the image, together with records of over/under-votes, under-vote overrides, etc.

All of this information is written out on write-once removable media that, together with the paper ballots, comprise the election evidence from the precinct that is subject to chain of custody requirements. No election information is retained on the hardware; just as the hardware starts out empty before the system is started from the boot disk, the hardware remains empty after the PBC software has finished executing.

3.3 CENTRAL BALLOT COUNTER

The Central Ballot Counter (CBC) device is used by an election official to do bulk scanning and interpretation of ballots. Interpretation is required for ballots that have apparent errors (e.g., possible over- or under-votes or stray marks) that are detected by the scanning software. The CBC is comprised of CBC software (contained on a boot disk created by the Device Manager) designed to work with a commercial off-the-shelf (COTS) high-speed optical scanning device, in order to provide the functions of a conventional Central Count Optical Scan (CCOS) device. Unlike the PBC, however, the CBC software does not interact directly with the COTS scanner on a ballot-by-ballot basis; rather, a scanner is used to bulk scan a batch of ballots, creating a dataset of ballot images that the CBC software analyzes. Typically, each dataset will be a batch of ballots from a particular precinct. The CBC software's "duty cycle" begins when such a batch of ballot images is provided. The CBC software then performs digital image processing on each ballot, in a manner similar to the PBC software.

However, the CBC's user interface is more complex, and intended for use by election officials. The CBC software finds ballot images with apparent under votes, over votes, stray marks, or other irregularities; each of these ballot images and automatic assessments are presented for human interpretation. The processing of the batch is not complete until an election official has interpreted each such ballot, confirming or overriding the automatic assessment.

At the end of a session, the CBC vote tallies for each contest, and produces audit logs that include each ballot image and the interpretation of the image, together with records the election officials' decisions about apparent ballot irregularities identified by the CBC software.

As with the PBC, all of the information is written to write-once removable media, and no election information is retained on the hardware.

3.4 ACCESSIBLE BALLOT MARKER

The **Accessible Ballot Marker** (ABM) provides a digital interface so that ballot choices can be indicated by voters who:

- require “enhanced access” in order to vote unassisted, or
- prefer a digital on-screen ballot marking experience.

The ABM software provides video and audio access to ballot information, and uses hardware that supports a variety of enhanced-access user input/output devices. At the end of a duty cycle of serving a single voter, the ABD prints a paper ballot in the same format as the unmarked paper ballots used in the precinct or voting center, but with automatically generated marks that indicate the voter’s choices. The intent is that these digitally marked paper ballots will be counted by being scanned in the polling place, just as are the hand-marked paper ballots.

At the end of the session (typically a full election day of service in a precinct or voting center or early voting center), the ABM produces audit logs that include the finished set of digitally marked ballot choices of each “vote caster” and the series of vote caster actions that led to it.

The benefit of the ABM is to support enhanced access and to provide a digital means for marking a ballot that can deliver an improved, more error-free user experience strictly from the standpoint of making ballot marks.

3.5 TABULATOR

The **Tabulator** provides the critical service of tabulating vote totals for each contest in a jurisdiction in an election. The inputs to the Tabulator are:

- The master list of all contests for the jurisdiction, and
- The vote tally data sets that were produced by several Ballot Counter devices.

The Tabulator produces a variety of outputs:

- A tabular listing of tallies from all devices, which can be used to independently confirm the results of tabulation;
- A variety of simple report documents that describe election results, precinct-level totals, etc.;
- Log data about the operator and operation of the Tabulator.

3.6 AUDITOR

The Auditor is used by election officials to extract the log entries and other auditable information from the TTV Voting System components, and consolidate them into a complete set of “electronic election evidence” that can be used by election officials to assist in election audits, and aid in public disclosure and transparency of information about an election’s operations at the level of a jurisdiction.