Secure American Federal Elections (SAFE)

2020 Edition – Voting, Counting, Auditing and Architecture – Overview and Diagrams

Given the problems surrounding the 2020 election (ballot distribution, collection, counting and auditing), we have no choice but to design and implement a system that's efficient, transparent, auditable end-to-end and counts auditable by the public.

Election processes can be separated into three distinct areas:
- Voter registration and identification
- Ballots: creation, assignment, distribution and collection
- Elections: voting, counting and auditing

This document concentrates on ballot counting and auditing.

Many say they want manual counting. Manual counting isn't feasible when counting over 140,000,000 ballots. It's slow and prone to corruption and/or error. Given what's taken place in 2020, there's no way we'll ever trust electronic tabulation of election results as long as we try to process them while disconnected from the internet. Doing so requires manual processes, including movement of data, which increases the attack surface dramatically. It also removes the possibility of automated system validations. So, if we have to adopt a connected election infrastructure, do it properly; making sure it's secure, accessible and fully auditable.

To facilitate these goals efficiently and properly, all ballots "cast" are paper. If a state decides that electronic ballot preparation is desirable, that works, but that system doesn't inject votes into SAFE, it generates a paper ballot that can be cast, by the voter, using the same system as all other ballot preparation types. This concept separates ballot assignment, delivery and population from the "casting" counting and auditing processes/infrastructure.

Paper ballots are being employed because they provide a reliable audit source. Paper ballots are scanned and stored (for audit and recount purposes). The resulting ballot scans are read and processed by SAFE to perform automated counting and verification functions. Those images and data are stored, again for auditing, recount and voter verification purposes.

As stated earlier, the way to improve security, reliability and auditability is to have SAFE network/internet connected. This can be executed securely; we just need to treat the system with the level of importance and expertise it deserves. The resulting design will facilitate:
- Secure communications with mutual authentication and restricted network access
- Network analysis, logging and monitoring
- Firewalls/Web Application Firewalls protecting all servers
- Data store transaction logging
- Professional Identity and Access Management with Multi-factor authentication and logging, implemented for all but ballot casting operations.

Nothing will happen on/in the system without us knowing and being able to stop it and/or correct it.

Contents

Voter Experience

Voting

Arrive at polling location

If ballot has been prepared prior to arriving, proceed to "Cast your Ballot"

Check-in and receive ballot

Prepare ballot

Cast your Ballot

- Scan ballot
- Review voting selections
- If correct, select "Cast"
  - Votes are saved
  - Ballot images are stored
  - Receipt is printed, with Ballot ID and PIN
  - Confirm receipt delivery   (yes/no)
- If incorrect, select "Cancel"
  - Ballot is returned

Sample Receipt

Verifying Your Vote

Using Voting Receipt:
- Navigate to the identified URL
- Enter the ballot number
- Enter the PIN
- Enter permanent PIN (if not previously set)
- Your ballot selections are displayed

Auditing The Vote

The Audit Trail

- Registered Voters are issued Ballots with unique ballot IDs
- When cast, paper ballots are retained, images and voter pictures are processed
- The votes read from each ballot image are stored in the database, along with the ballot ID
- All ballot images are retained for public and secure audit purposes
- Votes in data can be confirmed against total counts
- Votes in data can be confirmed against images (or paper ballots)
- Images can be confirmed against ballots
- Ballots identify Voters, which can be verified
    - Ballot fingerprint and/or picture can be verified against voter registration data

Public Auditing

- Navigate to your state's election audit URL
  Sample: https://ElectionCenter.MI.gov/Audit
- Select the precinct that you'd like to audit
- All committed batches for that precinct are displayed, including the batch name/ID, committal timestamp, vote counts and a link to download the redacted ballot images included in that batch.
- Review each batch of ballot images, tallying votes, comparing counts against batch details.

Secure Auditing

- Voters are tied to ballots by associating each Ballot ID with the appropriate Voter Registration ID.
  This association is executed at the precinct level and retained at the state level.
- Each Voter Registration ID (or national VoterID) can be assigned to only one cast ballot.
  This can be determined at the state level via State Election data and/or at a national level via the Federal Election service. The possibility of multiple ballot submissions for one citizen needs to be impossible due to checks executed during the batch submission process/logic, and will be audited.
- Paper ballots are retained and can be used to verify/audit State Election data by Ballot ID.
  Paper ballots, scanned images and ballot data are all stored by/with precinct and batch information. Both images and ballot data can be verified against the paper ballots.
- Ballot Images, once audited, can also be used:
    - To verify State Election data.
      Images can be manually tallied by precinct and batch or ballot images could be reprocessed for automated counting.
    - Thumbprints and/or pictures can be verified against voter registration records.
      Note: This may not be feasible in the initial implementations.
- If any question exists as to manipulation, the voter can be contacted to gather additional information.

Definitions

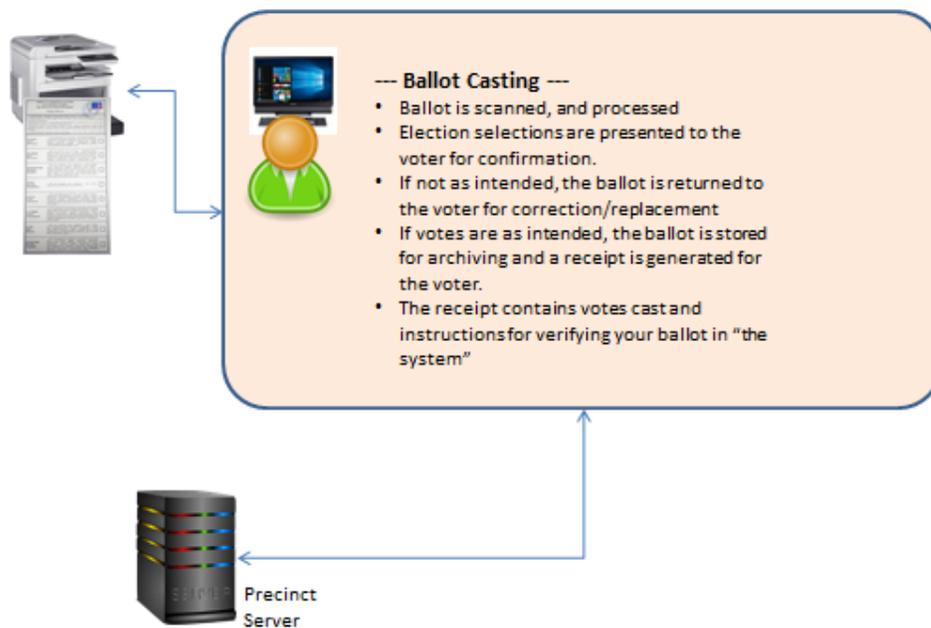| Casting a ballot	The act of submitting a ballot for counting

Diagrams

Ballot Flow – Voter Cast

--- **Ballot Casting** ---
- Ballot is scanned, and processed
- Election selections are presented to the voter for confirmation.
- If not as intended, the ballot is returned to the voter for correction/replacement
- If votes are as intended, the ballot is stored for archiving and a receipt is generated for the voter.
- The receipt contains votes cast and instructions for verifying your ballot in "the system"

Precinct Server

Ballot Flow – Mail-in

Note: Mail-in ballots are most prone to fraud and/or error.
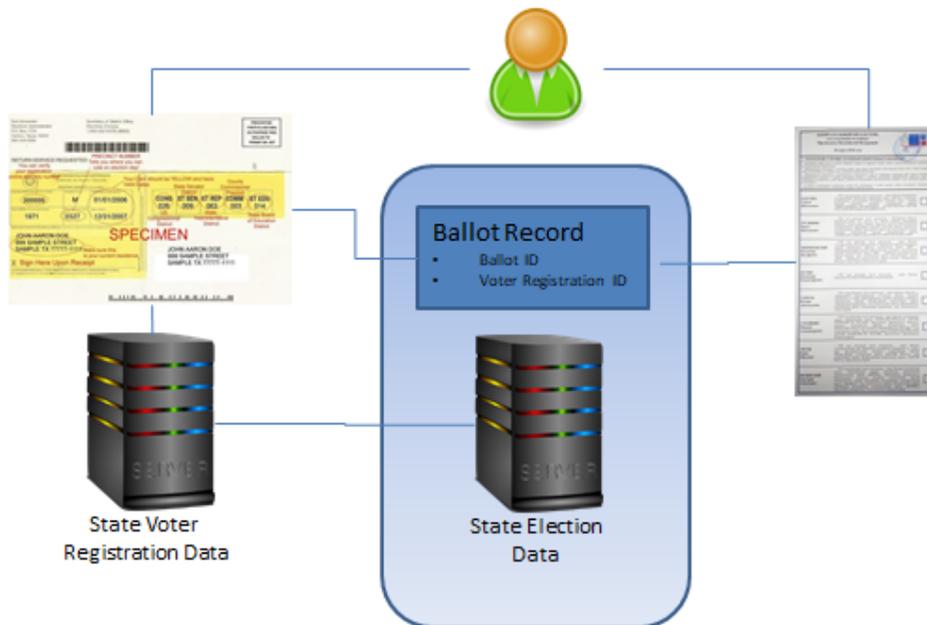*Their use should be limited to only when absolutely necessary.*
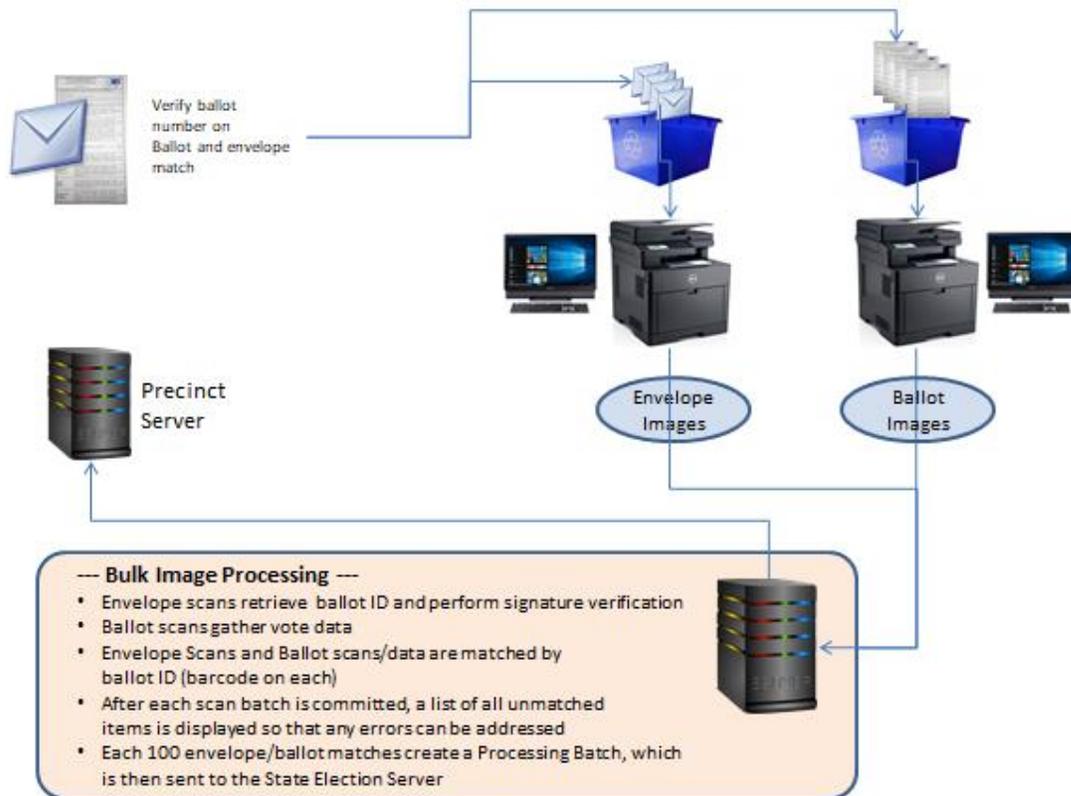
Voter / Voter Registration / Ballot Association

Voter Registration ID
- Points to voter information in the State Voter Registration data source
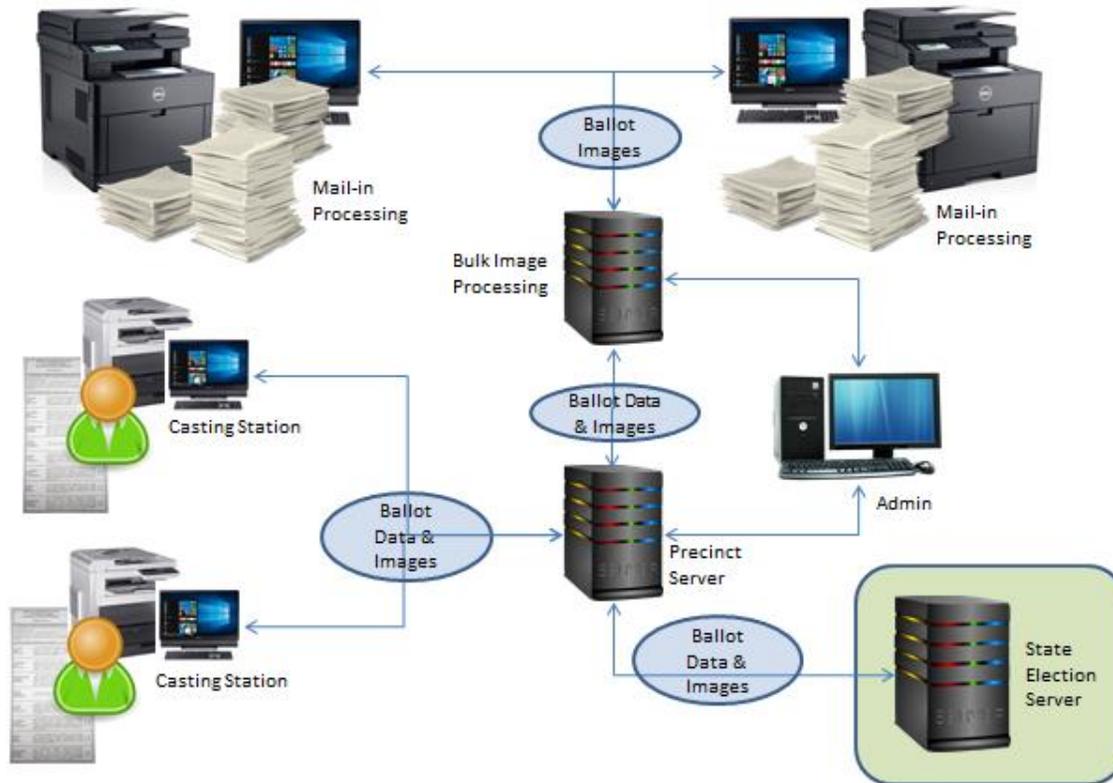- Points to the Ballot record in the State Election data source

Ballot ID
- Points to voter information in the State Voter Registration data source by getting the associated Voter Registration ID from the ballot record

Precinct Topology

System Topology

Version History

Date	Version	Description
12/02/2020	2020.O.0.5	• Added "The Audit Trail"
11/28/2020	2020.O.0.4	• Changed version format "O" = Overview • Moved requirements sections to a separate document • Expanded the introduction content
11/27/2020	2020.0.3	• A few clarifications in "Ballot Design and Processing" • Added "Voter / Voter Registration / Ballot Association" diagram
11/26/2020	2020.0.2	• Auditing The Vote • Added multiple "diagrams"
11/24/2020	2020.0.1	Initial layout • Voter Experience • Remainder – Stubs and Initial Rough Draft