|  |  |
| --- | --- |
|  | Government Blockchain Association  Series of Voting Standards |

**App-Based Cell Phone and Tablet Vote Selection and Vote Registration**

Standard Number: GBA-2000

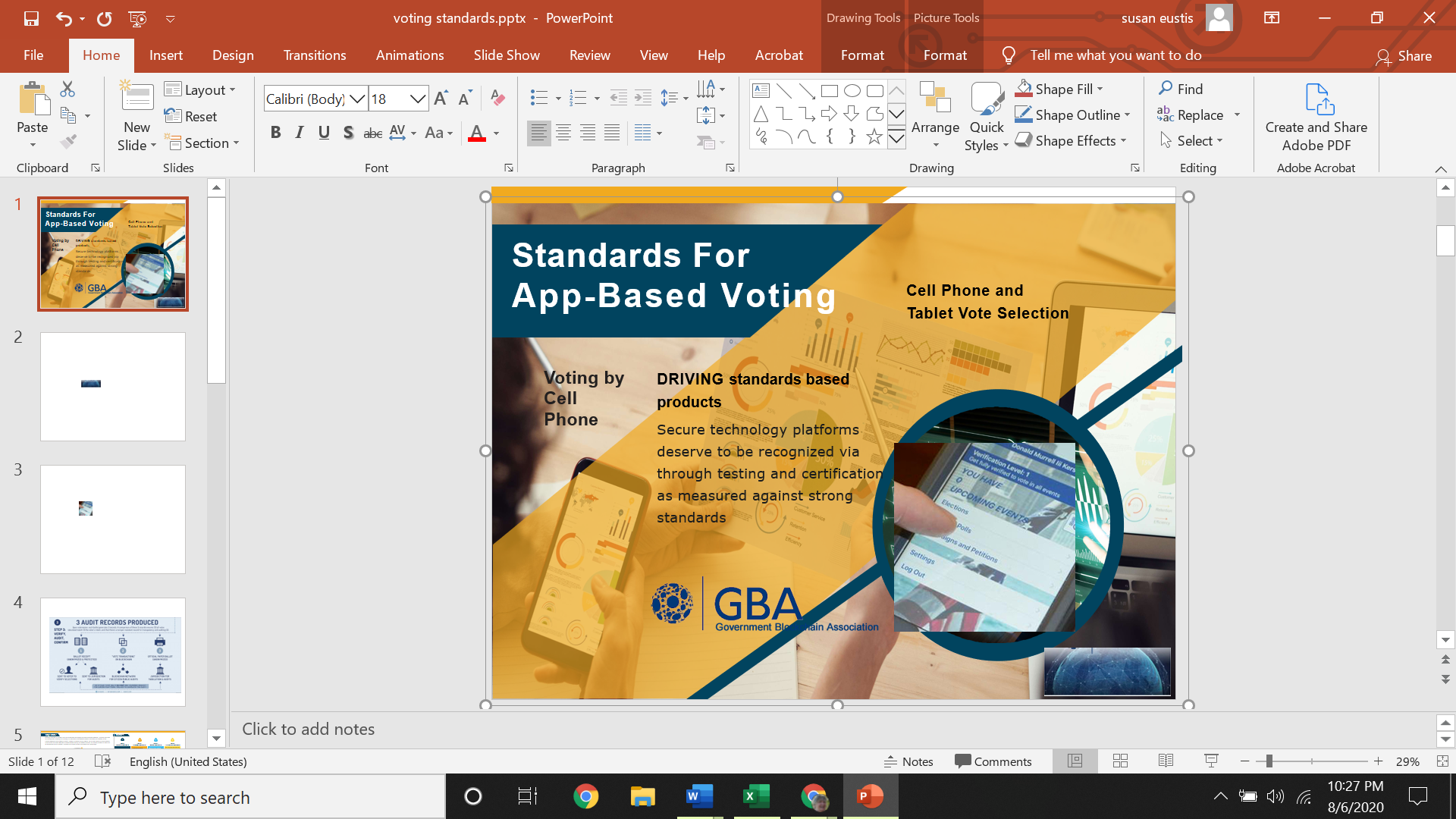
Date: September 15, 2020

Version 0.09

Status: Draft

**Gerard Dache: Executive Director.**

This paper is a product of the Government Blockchain Association (GBA) Voting Working Group. It is intended to be used as a means of capturing ideas and suggestions. It does not contain any official position, intent, or commitment by any individual or group associated with the GBA. It is purely informative and not declarative in any manner. Any declarative statements do not contain the authority or approval of any member or contributor. While every attempt to maintain accuracy is made, the GBA organization takes no responsibility for mistakes. All information is provided on a best efforts basis, with contributions from senior experts in the voting and security industry.



# Introduction

This family of process standards is being developed by the Government Blockchain Association (GBA) for the purpose of serving government officials and their constituents. The GBA is a global organization of public and private blockchain professionals dedicated to implementing government processes that have integrity in both process and outcome.

## Purpose

The purpose of this family of standards is to define an election process that can be verified against defined standards to assure the integrity of the process and the outcome.

Democracy is dependent of counting votes with integrity. Secure election systems provide a basic tenant of democracy. All aspects of the election process, from voter registration, to presentation of ballots, to voter selection protection against spoiling a ballot, to letting voters change their minds, and to counting votes by machine, are fundamental to the conduct of democracy.

A robust infrastructure to protect the process needs to be in place. State regulation and independent certifications are core to the process. Computer security is an essential part of the smart phone ballot transmission process. Ballots are transmitted from the registration check in server to the voter for marking.

Systems as certified support voters casting a ballot marked on a cell phone. There is a system in place that makes fraud detectable and permits poll workers from opposing parties to monitor procedures at all times, this set of standards portends ot extend that system to smart phone voting.

Note on Use of Standards Document:  
Most of the topics are described as lists. These lists are meant to serve as checklists for a certification. A product either meets the criteria shown on the list or does not. The technician running the certification issues a pass or fail based on the quality of the offering as determined by its ability to meet the requirements presented in this standards document.

No product can meet all the requirements, this is a given, it is too early in the market cycle to have mature products offered to the market, but our requirements document is meant to be stringent enough to provide a guide towards progress.

## Scope

The scope of this document applies to any jurisdiction that seeks to demonstrate compliance to an international voting standard and that seeks to have an election process and its results validated by blockchain technology.

Elections can be large, complex logistical government operations. Smart phone election solutions are positioned to reduce risks and costs, maximize productivity, increase efficiency, and enhance transparency. These standards seek to define how to easily configure the smart phone voting app so it can address the visual, audio, language, physical and cognitive needs of the user.

## Terms

This document includes Italicized words that are defined in the document glossary (Appendix A).

## Process Overview

This family of process standards serves to account for the following election phases along with different modalities:

The expectations of each phase are defined in subsequent sections of this document. Below is the proposed classification schema for this family of standards:

### Sample Standards Number: GBA-2110

The 2 stands for Voting, 1 stand for Election Administration, 1 stands for in-person voting, and the last zero is a place holder for more detailed classification (as needed).

Election Cycle Standards Classification with corresponding voting modalities:

Standards Number: GBA-2100 (Election Administration)

Standards Number: GBA-2110 (Election Administration for in-person voting)

Standards Number: GBA-2120 (Election Administration for mail voting)

Standards Number: GBA-2130 (Election Administration for cell phone voting)

Standards Number: GBA-2140 (Election Administration for web application voting)

## References

To be added soon.

## Process Validation

The single most important validation of an election process is reflected by the confidence that the stakeholders have in the integrity of the election process and results. Following this family of standards results in data that allows the members of the jurisdiction to fully assess the integrity of the election process.

## Process Overview

This family of process standards serve to account for the following election phases along with different modalities: Venues can vary for voting. There are two main election venues noted below:

* In-person
* Remote

Voting Venues

Remote

In-Person

**Voting Technology Requirements**

Ballot Generation & Distribution

Candidate Registration

Voter Registration

Casting Votes

Vote Counting

Result Certification

Election Administration

* Ballot received
* Ballot marked
* Ballot returned
* Ballot receipt confirmed
* Ballot validated and authenticated
* Ballot counted
* Ballot paper copy printed
* Ballot rejection process:

-Resubmit

request

-Rejection

queue

* Ballot not submitted alert
* Reconciliation of voters voting equals ballots counted plus ballots rejected (both electronic and paper)
* For DLT – voter confirms vote:

Cast as

intended

Recorded as

cast

* Voter or counting dispute recording and resolution
* Final Vote count reported to election authority.
* Approved Ballot generation
* Ballot Delivery (one per registered voter requesting vote)
* Voter Application
* Voter Approval
* Voter Application records and audit
* Candidate Application
* Candidate Approval
* Candidate Application records and audit
* Candidate publication & notification

**Election Admin**:

* Ballot format and content preparation
* Ballot format and content preparation
* Election authorities to approve candidates, voters, election staff
* Voter eligibility definition
* Voter registration process – forms, controls etc.
* Ballot authentication, acceptance & rejection standards and controls
* Election definition e.g. roles, issues, timing, standards etc.
* Candidate eligibility definition.
* Voting process, methods, roles, administration, standards oversight definition
* Vote total count reporting and aggregation process.
* Local, State and Federal or National Government laws & regulations compliance.

The primary aspects of voting are shown above in the diagram illustrated. Result Certification is at the end of the election cycle (as needed) In the event of a close election that goes to court, after the hand recount has perhaps changed the outcome, it is likely that the court will order that the parties go back to the blockchain to achieve an electronic audit of the actual votes cast. (The last sentence here should perhaps be a recommendation rather than a prediction. Also, in the recommendation it can be explained why it is a recommendation – immutable record.)

Additional Requirements –

**Voter Registration Distributed Ledger Roles Responsibilities**

(To be defined)

* Voter Registration Application
* Voter Registration Application accepted
* DLT “Voter Registration” Transaction Generation (Note: could include encrypted or hashed data for the immutable record)
* Voter Registration proposed to immutable ledger
* Voter Registration confirmed to immutable ledger
* Confidential voter receipt issued
* Confidential record of ballot delivered when voting during election

**Voting Distributed Ledger Roles Responsibilities**

(To be defined)

* Ballot Delivery
* Voter - Ballot Marking
* Voter - Ballot Return
* Ballot Return receiver – DLT “Vote” Transaction Generation
* Ballot Validation (Potential for Public validation and also Public witness to Ballot Validation process)
* Ballot Counting
* Ballot proposed to immutable ledger
* Ballot confirmed to immutable ledger
* Ballot receipt for voter
* Ballot counting / vote reporting after voting ends

**Control Relationships:**

* Confidential Voter registration to Voter Ballot link
* Confidential reconciliation of registered voters voting to votes cast
* Confidential receipt for voter to confirm
  + Vote cast as intended and
  + Recorded as cast

# Blockchain Voting Infrastructure: Government Business Blockchain Platform

The Government Business Blockchain Platform (GBBP or SERVER) is a multi-blockchain platform that allows any vendor blockchain data to be connected to this platform. The GBBP or SERVER performs verification and integrity check. It ensures that data that is recorded to the GBBP or SERVER may not be changed or altered without detection. It provides viability of data in accordance with established permissions. The GBA administers the GBBP or SERVER certification that tests the system for security and transmission functionality, looking for protection of the integrity of each ballot in every case.

## Specific Election Technology

Each election shall use a tool suite that is comprised of components that satisfy the following criteria.

### Administration Interface Technology

Election Administration data shall interface with the GBBP OR SERVER Election Ledger. All Election data is written to the GBBP OR SERVER in an append only mode. This means that information may be added. But no electronic data can be deleted or changed. Data includes:

• Election workers identity, roles, and assignments

• Candidate information

• Voter registration data

### Election Administration Central and Polling Station App-Based Voting Interface Technology

Polling station and voter-app technology shall:

• Read voter registration data from the GBBP OR SERVER

• Receive messages from voters

• Ask voter to present ID electronically

• Validate voter eligibility against voter registration data

• Avoid use of the Internet during this process, rely instead on the cell phone app and the cell phone network, imbedded codes in the app

• Issue an electronic voting entry code associated with the name listed on the voter registration rolls

• Imbed the matching code in the voter app on the voter phone

• Imbed multiple matching codes matching multiple voters to a single tablet selection device. In the voter app on the voting tablet authorization codes need to be imbedded in the device in the case of nursing home and similar uses of the selection devices – Should be optional and not mandatory to achieve certification or achieve standards.

• Give election administrator control panel access to newly issued electronic voting entry code

• Provide opposing party representatives the ability to observe the election administrator control panel in the same manner the election administrator can do so in traditional election venues

• Continuous observation needs to be supported

• Work with representatives of the press to allow reporting on voting process and outcomes

• Secure transmission interfaces (see details later in document)

• Secure API connectivity between system interconnects

• Support to store, record the vote physically and electronically

• Distribute physical copies of the vote to the Election Admin and representative of each candidate in the election.

• Record election results onto the GBBP OR SERVER.

## Voter Interface Technology

The voting application requirements include:

• Identifying users with requirements similar to opening a bank account

• Identifying users consistent with internationally recognized Know Your Customer (KYC) requirements

• Reading the candidate and election information from the GBBP OR SERVER

• Sending a secure message from the voter to the Polling Station (Does the platform need to send messages? Or is submitting a vote sufficient for compliance?)

# Voting Lifecyle

## Election Administration (GBA-2100)

Local election administration is one key to safeguarding the integrity of the voting process. Allowing observation of every step of the process, all testing being open to view by the opposing political parties is another step of the process. Freedom of the press, existence of an independent press organization is fundamental to election administration of fair elections.

### Election Technology

The Election Administrator (Admin) is a member of the jurisdiction. That group of people selects, acquires, installs, configures and commissions an election technology that satisfies the following requirements:

### Media

• All votes are recorded physically on an electronic media resistant to alteration. Use of a blockchain storage vault for the individual voter ballots represents a storage media where an alteration would be detectable. The reason to make fraud detectable is that all systems are vulnerable to hacking and the fundamental protection of a fair election is to have opposing parties participate in the process and watch always for fraud. The presence of an independent press is protection that helps make fraud detectable.

* Electronic totals are captured at the polling station.

• Vote totals from polling stations are recorded on a blockchain that may be part of the Government Business Blockchain Platform (GBBP) or server or any other certifiable public or private blockchain.

## Election Preparation

The Election Administrator (Admin) shall:

• Assign roles to individuals representing the candidates that are participating in the election. The roles are defined in Appendix B.

• Assign roles to election workers who have permission to access the election technology.

• Ensures that the Voter Registry is fully and accurately copied to the GBBP OR SERVER

### Remote

Remote voting requires special attention to the ballot preparation and to the location of the voter names on the server.

### Ballot Layout

App-based voting depends on content management used for building ballots all over the country.

250 ballot style components are used to put together a ballot on the phone (or tablet) screen (These 250 ballot components are defined in appendix A following)

Each component haves a metadata tag

Font, placement, vertical/horizontal, image have different tag variations

Tags that are different denote office, candidate, questions, slate

A metadata controller (MDC) is a type of data control used over a storage area network (SAN). As the clients are given block-level access to the physical level of data a MDC controller is needed to manage rapidly accessing the same block.

MDC is used to lock files, move and allocate data space, and give authorization to clients for different block levels. MDCs are only used on high-end servers and are never found on user computers.

One of the most difficult aspects of building and managing an election for smart phone voting is managing the meta data. Meta controllers of ballot data categories relate to ballot formatting, ballot presentation, ballot fonts, and selection codes. Meta data controllers relating to setup of the app with software modules that permit verifying ballot selections is used to let voters change their mind, to prevent voter error.

Certification looks at the stability and the viability of the meta data controllers for ballot formation and for user error checking.

### Ballot Generation & Distribution (GBA-2400), Protection of ballot

The putting together of these screen configuration components is used to create a coherent ballot that can be displayed on a screen. This will take significant expertise. The names of the offices and candidates will differ by location, and the number of offices and questions will differ by district, the basic format can be assembled by this expert team, and the local districts can be supported to build their own ballots and make them ready for handing out to individual voters in individual districts.

The ballot information and the preparation of the ballots needs to scale and the distribution of ballots needs to scale in such a manner that each voter always receives one and only one ballot, and votes once and only once.

An election database is used to build electronic ballots. The database is used to construct ballots and support tabulation systems. Standards require that the database architecture conforms to fundamental database design principles (See Appendix B). Industry standards for ensuring accurate data are needed to build ballots accurately.

## Candidate Registration (GBA-2200)

The Election Admin defines the process, criteria, and schedule for candidates to be added to the election ballot is the same whether the voting is conducted in person or remotely.

# Voter Registration (GBA-2300)

## Standards for Voter ID

### Remote ID

Appropriate personal ID image, facial recognition, name and address, all these are used for voter ID. Other standards are emerging that are more secure. Use of vote by mail scenarios.

Standards for Voter ID and requirements vary by jurisdiction depending upon local laws and standards. In cases where picture ID is required, government issued IDs and facial recognition technology can be combined to fulfill this requirement. In jurisdictions where photo ID is not required, a combination of personal information and two or three factor identification can be used to verify identity of a voter.

# Casting Votes (GBA-2500)

The sections below describe the requirements to ensure that votes are cast as intended, and recorded as cast. It describes the requirements in several modalities including in-person and remote voting. These requirements are defined in GBA-2500 (Casting Votes).

### Remote: Cell Phone / Tablet

Votes cast using cell phone devices shall satisfy the following criteria:

* End-to-end security that ensures that the votes are received by the election administrator as cast by the voter without any monitoring, tampering or compromise
* Voters must authenticate by at least one of the following methods:
* Biometric credentials
* Check in process can be similar to what is done for vote by mail.
* After check-in a code is generated for that voter and attached electronically to the name on the voter registration list. The code is then sent to the voter by embedding it in the app that is on the voter’s phone
* In order to vote, the voter merely needs to call into the voter registration rolls, app recognizes and matches the code embedded into the app and sends the voter the correct ballot automatically.
* Check-in using a remote video technology possible
* Ballots may not be accessed, or viewed by any party other that the voter and election officials

• All votes are recorded on a blockchain that includes nodes hosted by all parties of the election. (Do we define who holds nodes? Would this preclude commercial blockchains like fabric from being used?)

• Cast ballots are sent to the voter via automated process to verify the correct recording of the vote with an option to correct any errors.

Alternatively, cell phone check-in can occur virtually using the code that has been assigned to the voter during the request for the ballot. With the code imbedded into the app, then an app request for voting will automatically send the ballot to the voter for marketing and casting of the market ballot, placing the completed ballot in the block chain automatically.

Ballot tracking to assure integrity of ballot transmission is a significant aspect of the casting votes cycle. Not every voter needs to track their ballot to ensure the system maintains its integrity. Even with the ability of 1% of voters check that their ballots are correctly encrypted and tallied, there is a monitor of election security. The way the encrypted votes are tallied need to be able to be checked by anyone to make sure that each candidate gets the correct number of votes.

Ballot security solutions simplify logistics and reduce cost. By eliminating the need to pre-print, scan, and manage paper ballots, a more efficient voting system can be implemented. Reading and reporting results is fast and secure. Security is assured with redundant electronic and physical measures.

# Vote Counting (GBA-2600)

Vote counting and tabulation depends on access to a paper or electronic ballot. The tabulation equipment must be able to continuously scan and intelligently sort ballots with high-speed digital image processing, saving election staff valuable time when tabulating results.

Security safeguards are designed to make tampering detectable. They alert election officials to unauthorized access. While the tabulation unit is in storage, transport, preparation, and operation protections need to be in place to make systems tampering evident.

In order to overwrite or change the election definition or system firmware, the attempt to change is noted in the log. These standards call for each jurisdiction to lay out local procedures to enforce checking the log.

Tabulation accumulates and transmits votes directly from the polling place to a central vote consolidation place. For paper ballots, the tabulation equipment must process a variety of ballot sizes and designs, from 11 to 19 inches. Tabulation equipment needs to be lightweight, compact, and easy to set up and use in the polling place. It may include extra USB ports and expandable memory to accommodate evolving Election Assistance Commission (EAC) standards.

Intelligent Mark Recognition (IMR™) technology helps determine a ballot mark for a candidate.

Software needs to allow users to select and sort ballots that need to be reviewed; over-votes, under-votes, blank ballots, blank contests, marginal marks, and write-ins can be reviewed. Manual, automated or digital out-stacking can be reviewed:

## Blockchain Procedures

Vote counting shall be:

• counted at polling stations.

• performed in real-time as votes are cast

• validated by representatives of all parties in the election

Vote totals must be agreed by election workers assigned to vote counting from each party in the election.

### Remote: Cell Phone

Vote counting via cell phones shall meet the following criteria:

• Vote totals are recorded to a blockchain. The details recorded allow the voter to recognize their own vote while preventing anyone else to know who voted for a particular candidate or ballot option.

• Votes recorded include a date/time stamp and other meta data to help identify potential fraudulent fake votes

• Each voter’s meta-data is published to the voting administration dashboard.

• Metadata management must preclude anyone from being able to trace a ballot or see how anyone voted.

• Votes recorded on a blockchain may be audited by any person or organization by counting the votes on a blockchain using the audit process detailed under the law and used for a recount or court review. Electronic tallying is not precluded.

# Result Certification (GBA-2600)

### Remote Cell Phone

 The designated local election authority is responsible for result certification, backed by the appropriate oversight agency. (Do we want this to be a US standard or a global standard? If global then terminology should be more general.)

# Remote App-Based Voting: 5 Types of Security

Secure transmission

Secure storage

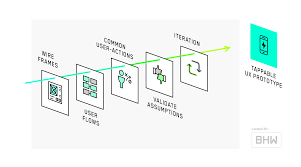
Authentication (are you who you say you are)

Authorization (are you allowed to do this)

Non-repudiation (you can't deny you did this)

The app-based voting products need to have documented drawings and descriptions that illustrate adherence to standard development practice illustrated in Figure 1.

Wire Frame App-Based Voting Development Diagram



Source: BWH

The wire diagram below illustrates standard industry practice for metrics, error detection, performance monitoring, tracking, and reporting requirements. App-based voting needs to comply with standard industry practice with regard to these device characteristics.

Wire Diagram of App-Based Voting Metrics, Error Detection, Performance Monitoring, Tracking, and Reporting Requirements



Source: BWH

(Note need permission from BWH to reproduce their drawings with source attribution)

Smart phone voting products are expected to embrace security as a system. Rather than offering individual security solutions they are expected to be constructed to adapt easily to future changes in security technologies or protocols.

### 8.1 Secure ID

Voter anonymity needs to be secured. A voter's selections must be known to the voter and anyone he/she willingly shares them with. There must be no means for anyone to obtain the identity of the voter who cast an individual vote or ballot, or to tie an individual ballot to an individual voter.

**Non-repudiation (you can't deny you did this)**

**Blockchain makes ballot manipulation detectable**

Aim is to make all fraud detectable

Illustrated step by step procedure manuals are useful for poll watchers from opposing parties

Voter uses one phone; number is entered ahead of time on voter registration rolls

The election authority creates a code that identifies that voter with that name on the voter rolls, the voter registration list

Voter gets code, limit SMS for delivery of code, need asynchronous highly secure messaging and app containers (Standard two factor authentication uses SMS).

Transmission needs to perform validation and coherence checks. Eliminating intermediate tasks during transmission is important. Recording and transmitting data at the Vote Processing Centre (VPC), speeding up the recording of information in the system is important. It reduces the number of errors detected in the data transmission chain.

Systems need to validate the vote totals gathered at polling stations.

**Need end to end authentication via encryption at every step of the transmission chain**

**Design Document App Based Cell Phone Voting**

**Security Rules:**

No Internet

No SMS – secure message based

End to end encryption built in

No browser

All communication in an app container

Mission critical, asynchronous messaging

End to end encryption for messages

2 or 3 factor identification

Ability to support facial recognition

Blockchain holds ballots after cast vote is selected

App not implemented in blockchain, too slow, will not scale

Voting process must be simple and intuitive for voters

Voters may be of various cognitive abilities

Design with cultural sensitivity

Voters must be able to negotiate the ballot marking process without making mistakes

Variability of ballot presentations supported

Voter must be provided the opportunity to verify the voting system

**Secure transmission:**

Identify all paths of transmission where secure transmission is needed

Avoid all SMS - Use secure transmission instead

Secure transmission

- once and only once delivery

- asynchronous, guaranteed delivery of data transmitted

- from server to phone screen

- from selection, server to blockchain

- from blockchain to the tabulation center

- are those the only time the ballot moves?

**Secure storage**

- Of voter registration list that has access codes associated with name and the number of the cell phone

- For working servers while voter marking ballot

- Use blockchain for immutable ballot

- Once and only once messaging for ballot delivery to blockchain

- Asynchronous messaging for ballot transport

**Authentication (are you who you say you are)**

-Voter registration list has code and phone secure ID; voter sends code to match what is shown on the voter list

Voter Authorization Code Embedded in Voter Registration List and In Voter App - They must Match

-Voter registration list could have the phone secure ID for two or more people, but a different code for that registered voter, with the code next to the voter name and phone ID #

-Use the ID required by that election jurisdiction name, address, assigned code, maybe image recognition, picture of license

Need to check in to get ballot and check out

Check-in to check-out 10-minute process

Cast as intended generates proof to the voter that the voting system has correctly handled the ballot

**Authorization (are you allowed to do this)**

Election official checks in voter prior to or on Election Day by

1. Adding the cell phone unique # to the voter’s name on the voting list

2. Generating a unique code that is associated with the voter name on the voter registration list

3. Specifically authorizing the voter to cast a ballot via app-based selection mechanism means election official generates the code and by generating an authorization code it gets added to the app and to the voter registration roll

Facial recognition is possible to use

Voter credentials – check-in and check-out at desks for voter are automated using the secure code contained in the app

Management of lines of voters needs to be in place

Election official credentials – representatives of opposing parties monitor all actions by election officials

For poll site, precinct, mail ballot duties, voting place duties election officials sworn in

Individuals from opposing parties performing duties together always (Global standards would use more generic terms for political parties. Many will have more than two.)

Need to make fraud detectable

One Person One Vote Goal

In democratic elections, each voter's vote has equal weight with every other

One voter's vote has the same weight

A secret ballot election is fundamental to a voting process

Voters feel they have the freedom to vote their true conviction

# GBA Certification of App-Based Voting Products

Certification of app-based voting products is accomplished through examination of how the election process is protected in accordance with the law and with common practice in the various localities. The standards provided above generally instantiate the tradition of elections security. These standards provide a basis for certification of app-based voting products.

The conduct of elections is governed as much by the rule of explicit law as it is by tradition, the rule of common law, this is how we have always done it. The wardens and the clerks that run the poll sites stay in their jobs for years and train their replacements who then stay in their jobs for many, many more years. In this manner elections traditions are upheld in the conduct of elections. (Manuals and instructions should be documented to ensure adherence to standards and ensure succession.)

Running an election has become a way to see your neighbors, to participate in the democratic process. The more that app-based voting can preserve tradition, the better.

Security becomes paramount in an app-based election process. The GBA app-based voting security certification is carried out in a non-partisan manner, done in a way that protects the integrity of the voting process from end to end.

End to end authentication via encryption and secure ID is a fundamental requirement for systems certification. Testing of products to see they meet these standards is fundamental to the process of launching app-based voting at scale.

Test Cycle

**Source: GBA**

Smart phone voting certification is positioned to address issues with the Platform (Hardware and Operating System on Device and in the cloud). Certification seeks to verify that systems designs are secure enough to assure the nation someone cannot penetrate them. Security standards above are poised to provide guidance to laboratories so they can test against to ensure the smart phone voting application is secure.

**This is the critical challenge the certification authority must address: We seek to work from the premise that certification provides a stamp of approval addressing the needs of all the people participating in the election. The “threats” are varied and difficult. If we want the certification to serve the needs of the entity holding the election, then the potential for state actors to seek to infiltrate is enormous and must be addressed by the voting standards.**

**Questions Regarding Managing Each Election District Separately**

Are there different processing servers for different election districts?

How do you spin the virtual servers securely?

How do you track them?

How do you keep them separate on the various local dashboards?

How is that managed? Does AWS spin a virtual server each time?

What about erasing the blockchains at the end of their useful life?

What about keeping the virtual servers going until they can legally be erased?

Are there different blockchains for different election districts?

Are there merely different blockchain segments for different election districts?

How is that segmentation managed?

Are there different voter registration servers for different election districts

How is that managed?

How do we keep the info in the servers inviolate until the recount is complete?

How do we conduct recounts?

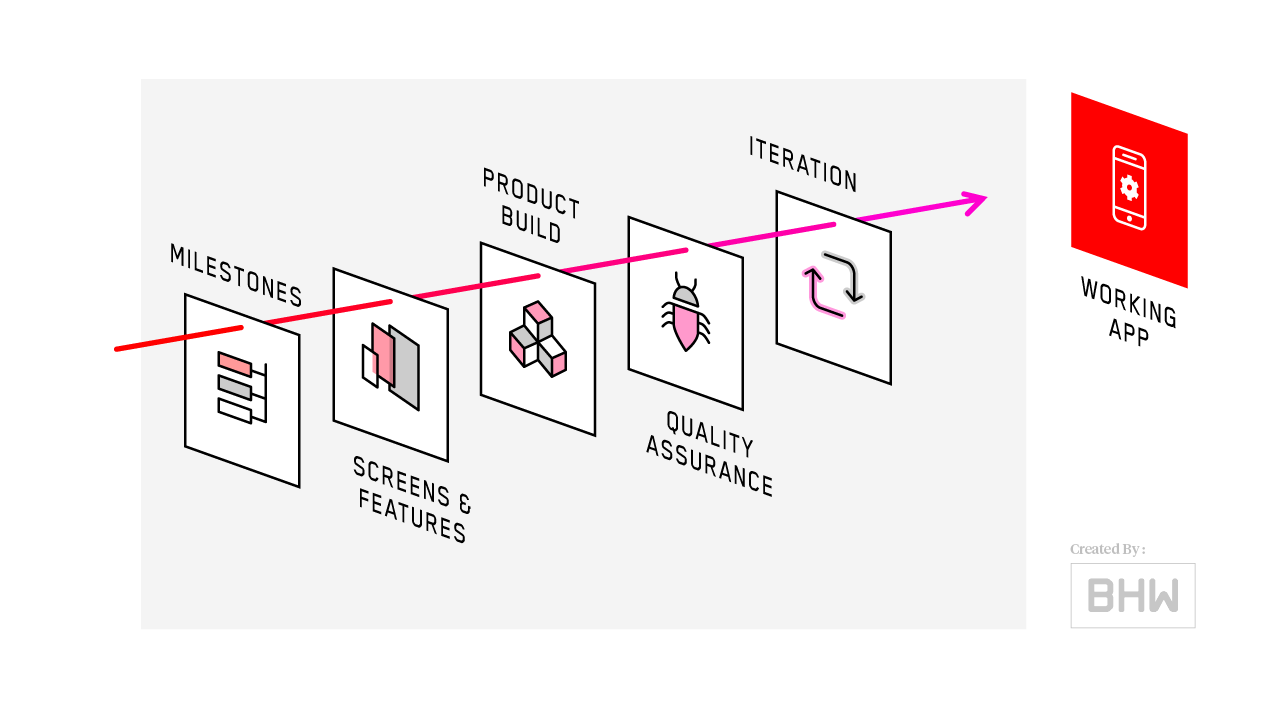
These are the questions that need to be addressed by each vendor. Certification depends on vendors having the ability to answer these questions in a straightforward manner that reflects deep thought about adhering to strong security standards.

(For creation of true, defendable standards, there needs to be an absolute answer to each question. The questions above should be formatted in a check yes or no standard for compliance checks.)

# Mobile App Development Process

The mobile app development process depends on management of the backend transport layer, the front-end ballot display layer, and the blockchain. Secure transmission ties the entire device together.

Mobile App Development Process – Wire Diagram



Source: BWH

## Cyber Security

Cyber security is an essential aspect of the app-based voting. World-class security experts & tools previously only available to large enterprises and federal governments. Banks and financial organizations are the owners of the most sophisticated and logically coherent security suites. The banking industry provides cyber security protection for every business.

The ability of the various app-based voting companies to leverage technology available to the banking industry is what certification organizations need to look at. Is this company providing the best cyber security available in banking and copying that?

(Is there an industry-accepted standard that could be applied from banking or other cyber-security?)

All data generated during the election needs to be encrypted and digitally signed. Hash validations are used to protect data. Integrity of the system is significant; the voting machines need to remain intact once they have been set up for the election. The smart phone voting systems needs to generate a signed data key. Should unauthorized access of a unit occur, no other units can be affected through data transfer

Computer security is achieved by making fraud detectable. Once fraud and hacking are detectable, secure election services can be implemented.

Encryption is fundamental. Symmetric and asymmetric encryption needs to be used. Transparency is achieved through end-to-end system auditability. Integrated ballot security features include many different varieties of encryption. Extensive internal security monitoring ensures data integrity.

Homomorphic encryption is used to ensure that nobody can tell how a person voted. Even the voter cannot use the tracking code to prove how they voted. They are able to prove that their vote was not changed.

A prioritized and prescriptive set of safeguards mitigate the most common cyber-attacks against systems and networks. They mitigate 83% of all attack techniques found in the Mitre Att&Ck Framework.

An adversarial tactics, techniques, and common knowledge) framework describes how data sources are used to support the mapping to specific controls and their associated sub-controls. Safeguards against specific attack patterns mitigate the effects of: web-application hacking, insider intrusion, privilege misuse, malware, ransomware, and targeted intrusions.

Systems must embrace the standard **CIS** Safeguards Against Specific Attack Patterns

Malware: Implementing IG1 of the CIS Controls can mitigate 79% of malware attack pattern techniques. Implementing IG1 is the definition of Basic Cyber Hygiene.

Web-Application Hacking: 100% of instances of web-application hacking techniques can be defended against by implementing all of the CIS Controls.

Insider Privilege & Misuse: 100% of the techniques can be defended against by properly implementing the CIS Sub-Controls in IG1.

Targeted Intrusion: 80% of targeted intrusion techniques can be defended against by implementing all of the CIS Controls.

--

--

## Election Administrator Dashboard

The election administrator dashboard is used for picking the ballots from various locations. Picking the ballot configuration for each ballot depends on having a good strong content management module behind the dashboard, one that can scale quickly. The election administrator dashboard is used for managing selections, managing ballot configurations, managing aspects of cyber security.

Election administrators use the dashboard to manage ballot request, ballot selection, time left, the cell phone. The dashboard needs to be able to tell the time the ballot hit the various servers in the blockchain, and record the fact that the ballot is stored. Time stamp, time to process time to arrive at blockchain full election process are available on the election administrator dashboard. No one touches the ballot between the time it leaves the phone and the time it touches the blockchain.

The election administrator dashboard needs functionality that shows that each ballot has left and arrived at its destination, it needs to show ballots stuck along the way.

Election audit trail

Capture and send ballot

Works under current laws that govern voting

Electronic voting app hack prevention via visibility

Premise is anything can be hacked

Make it detectable

Messaging once and only once ballot provisions

Ballot provisioning

ID provisioning

Visibility back to registration system

Once done block chain has record of ballots

Mail in ballot

Data on dashboard gets shared always with the poll watchers

Have enough screens for all the poll watchers

Control x # poll sites

Show active voters by precinct and polling location

Cell number is entered on the voting rolls

Allow navigation of the poll watcher screens to different polling locations

Activate callback to any voter

## Tablets for Voting in Nursing Homes

(This section could use some rewording. Perhaps something like – Voting for voters without access to personal mobile device. – Ensure that there is a method for voters without access to individual mobile devices. Then list several options.)

Allow use of tablets for voting in nursing homes

Multiple users on same device

Appropriate number of poll workers from opposing parties for the site and set up polling there

Create a virtual poll site

Notify election administration ahead of time people want to vote by phone

Manage challenged ballots

Show consecutive list of who is voting

## Voter Registration List

Supports absentee voting

Supports Election Day app-based voting

Supports Election Day registration with app-based voting (Not always required)

Separate list on server to be accessed by voting system

Support virtual voter check-in and voter check-out using the code assigned to the voter when they sign up for app-based voting

Checkout can be automated, check-in controlled by poll workers at the time the voter signs up to use app-based voting - need poll workers from opposing parties to observe process as it happens (should be inline with signing up for absentee voting. Doesn’t always require opposing poll workers. Process should however be auditable.)

Give person 10 minutes to vote (Can require more time if person is doing research or if ballot is long and has a lot of questions. Perhaps have each jurisdiction set the time limit.)

Implement some kind of time limit

Track the progress of ballots

Send reminders to people who have stuck ballots (Best practice but not required for certification.)

Dashboard shows all active voters

Send messages to voters through the app if time expires

Let voter request more time

Then make them start over or press continue button

## User Interface Design

Show evidence of having studies the variety of user interfaces available (e.g.)

<https://www.mockplus.com/blog/post/mobile-ui-design-inspiration-dribbble>

Simplicity and consistency of the user interface

Voter registration list has phone ID to be used next to voter name

Support more than one person using same phone (I don’t believe this is necessary but is a great feature to have.)

(Separate codes on the voter registration list)

Multiple codes for one phone can be used if the registration list has the name of the voter, the unique phone #, and the code all embedded next to each other

## Specification for App Based Cell Phone Voting

Description of App Operations for Cell Phone Voting

How the app works is as follows.

The ballot consists of some fixed number of positions, (say 400 numbered positions)

Sometimes there are duplicate, triplicate, or even more numbering schemes for the positions, those the app uses and those indicating a display sequence. The selection boxes are numbered from 1 to 400 but the candidates may be labeled

1A, 2A nA to represent all the candidates from one party.

Then the second party of candidates may be numbered 1B, 2B, nB to indicate a different party.

The software looks at the ballot positions sequentially, looking at every element in the list in the same order and taking action based on the rules associated with that element. The list of elements is above, the associated actions are described below.

The ballot is loaded onto the screen one office at a time. The app goes through the ballot looking for the first OF or Q and performs all the operations associated with that office or question. It is at this point that the office or question is put on the screen and that the voter now gets a chance to make selections based on what is presented on the screen.

All the CEs and Qs associated with that first OF are what it takes to display and register selections. At the next OF or Q in sequence, the app processes the selection spaces in sequence.

Generally, during the display process, the app stops when it gets to an OF or Q designation. This indicates the start of the office or question to be displayed. Everything in that office gets displayed.

As the app is processing through an office after an OF it increments a counter as to how many VFs votes for are set for this office. Thus, there is no single counter to count the number of votes for, it is a function of the processing of the locations. So, an office that has 35 candidates and vote for 15 will have 15 VFs set sequentially. This permits greater flexibility in changing the ballot setup. A counter can be used but it is more cumbersome.

Ballot preparation

List offices on excel sheet

Office name in column A

Candidates in column B

Codes for presentation control in columns C-Z (See appendix A)

B Ballot

Each voter receives a unique ballot upon which he or she can make selections.

Partial List of Voting Machine Ballot Constraints Managed by the App

EE Enable election button

CV Cast votes button

Election Test Button

Election Set-up Passed Test

PRE-Primary enable setting

NPE Nonpartisan enable setting

CE Candidate enable

WI write-in enable

OF office enable marks the beginning of an office,

IL Office Interlock

SE slate enable

ECE Endorsed candidate enable

VE Vote Enable

PE Primary enable

Protected Counter

Votes Cast counter

End of Election Lock 2

QE Question enable

NCE No candidate enables, skip a space on the ballot

NP Go to Next Page

NPOF Nonpartisan office, skip this office for some candidates

System Error Messages

Set-up

No CE after WI

No Write-ins in a question office

Voter Error Messages

You pushed cast votes too soon, no candidates are selected yet.

Need to handle loss of network etc.

EOB End of ballot designation

SMO Show more offices at a time, not just one

B ballot

Each voter receives a unique ballot upon which he or she can make selections. The ballot always has 400 locations in the

Partial List of Voting Machine App Constraints

EE Enable election button

CV Cast votes button, have to be careful that the whole ballot is selected or that the voter indicates he or she is done. Most frequently people try to push this after selecting in each office, but that is mistake and spoils the ballot

Election Test Button We have elaborate test scenarios.

Election Set-up Passed Test, this tests all the vote for mind makes sure you can select only the number of voters to be allowed and not select too many. An overvote spoils the ballot for that office, makes the votes not count so the app does not permit that mistake.

PRE-Primary enable setting Here we put the label for the ballot presented in a primary, the name of the party to be voted for.

NPE Nonpartisan enable setting

CE Candidate enable This lets the voter make a selection at this ballot position.

CN Candidate Name

WI write-in enable Every office has as many write-in capabilities as there are votes for. As with the VF, there can be reference to the counter for the number of votes for, or as many WIs as needed to permit writing in for every candidate allowed for.

OF office enable marks the beginning of an office. This is one of the most significant elements, probably the first to be processed as this divides the ballot into one office at a time to be presented.

VF, indicates the cumulative number to be selected in the office, it can be implemented as a counter associated with the OF, or as a separate element to be set in the boxes for, i.e. President vote for 1, Selectperson vote for 5, City Council vote for 15, etc.

IL Office Interlock This sets the interlock for the office, prevents voting for more than the designated number of candidates in an office

SE slate enable, this enables the ballot to contain slates sometimes there are as many as 15 slates of candidates on a ballot. When a slate button is pushed by the voter, the candidates on that slate are all selected automatically. After a slate is selected, the voter can go back and change his or her mind to vote for fewer candidates or vote for candidates on another slate.

ECE Endorsed candidate enable

VE Vote Enable

PE Primary enable, this sets the ballot to a condition whereby different ballots can be presented for different parties in a primary. Voters from one party are not allowed to vote for candidates in another party, they must select one party or the other. Requirements are different, sometimes the voter selects the party after they go into the ballots, sometimes they must declare a parry ahead of time and the election official distributes the correct ballot.

Protected Counter cumulative for the life of the system throughout elections

Votes Cast counter counts number of voters

End of Election Lock 2, trips a switch after the polls close lock system against further voting, after everyone in line has finished voting, need line management so voters can schedule vote or get call back when their place in line comes up

QE Question enable, this always has two selection boxes, but for layout reasons they may not be contiguous. There may be some empty spaces between the Yes and The No on the presentations, and those empty spaces can be designated with a

QT Question Text, this has the text of the issue.

NCE No candidate enables, skip a space on the ballot.

NP Go to Next Page This is used at the end of an office, and its existence permits more than one office to be displayed on a page.

NPOF Nonpartisan office, skip this office for some candidates, this is used with voters who may or may not be able to vote in a school district election

NCE No candidate in this position, this is used at the end of the ballot to lock out unused positions and is used to create spaces in the ballot presentation when needed

EOB End of ballot designation When a candidate position is given this designation, the program should automatically fill in the remaining ballot positions (from the 400 locations) with an NCE No candidate in this position.

Ballot, voter makes selections on ballot, selections collected and sent to back end that sends the ballot to the blockchain.

## Description of Pre-Election Ballot Setup

Get List of Candidates and Questions to be Voted

Ballot set up master is reused in each poll site with the changes for that poll site

Embedded content management structure for each numbered square

Master has some offices and candidates staying the same

Top of the ticket is entered first

Questions that are for the whole election district are entered

Candidate and questions change for different subdistricts are entered

Entry in logical sequence.

Check the ballot a lot of times to get it right.

400 sequentially numbered positions for use as office designation

Can increase of decrease voter selection positions on the ballot

Should remain permanent after optimum size determined

Each numbered position must have a designation

Not used positions still have a designation

## Description of Back End Operations for Cell Phone Voting

Accept the request for a check in against the voter registration list

Accept the request for a ballot

Gather location info, locate type of ballot to be handed to voter

Check to see what poll site the voter is located in

Check the ID to be sure requester is on the voting rolls

Check voter off the vote roll

Hand voter the ballot on the cell phone using virtual controls, automated

Once the code from the app is matched, pass the ballot automatically

## Presentation of Ballot

**Do not use SMS**

**Do not use SMS for ballot presentation**

Show offices sequentially

Show candidates sequentially

Provide selection box for each candidate

Prevent overvoting

Show questions sequentially

Allow yes of no vote for questions

Prevent overvoting

Allow voter to navigate up and down ballot

Put in controls to prevent voting for single office and by mistake push cast vote

Allow voting for one office only if desired but make sure not a mistake

Support slate voting

Support primaries

## Before the Election

Voters have to sign up on the registration list that they are going to vote by phone

Need verification process it is them

Give voters a code to use when they call in (Call in?? I think this may be left over from the previous idea of phone in polling locations)

No reason there could not be 2 or 3 codes allowed for husband wife and mother (once again, this is a suggestion. Some systems may use one device one voter as a security measure.)

Associated with the phone # phone unique identifier

Need a server with that list

Is dynamic because people will use during Election Day

## Conduct of the Election

Dashboard purpose is to get the poll clerks and the election administrators working together

Check the dashboard is complete, use checklist

Testing of election equipment prior to Election Day

Step by step procedures for opening polls

Use procedure for challenged ballots

Use procedure for dropped calls

Voter assigned to ballot associated with a poll site (voter registration rather than “poll site”)

Indicates ballot to be voted on

Voter given # to call when time to cast ballot (Once again, left over from phone voting, not app voting.)

Clerk has ability to call back when time to check in voter Once again, left over from phone voting, not app voting.)

No waiting in line - no busy signals need capacity to handle calls

Polling site clerk takes trouble calls in due course

Set up virtual poll sites to manage phone voting Once again, left over from phone voting, not app voting.)

Poll workers can work from home to staff virtual poll site

Voter app automatically enters code that matches code on registration list

App needs to allow navigation to text messages from the app (Should be feature, not necessary for certification)

Virtual pool site able to send text messages (Should be feature suggested)

Needs to be simple, ease of access to ballot, no complicated codes

Voter receives ballot sent by clerk to match voter polling site (proper voter jurisdiction rather than voter polling site)

## Messaging

Ballot transmission handled with modern once and only once messaging

Messaging patterns include Queue, Stream, Pub/Sub and RPC

Diversified messaging patterns, enable flexibility

Different microservices software depends on messaging

Kubernetes Message Queue

Enterprise-grade message broker and message queue, scalable, HA and secured

Kubernetes native solution in a lightweight container deployed in one minute.

Enterprise grade assurance

Certification, and enterprise support.

KubeMQ is a Kubernetes Message Queue Broker

Enterprise-grade message broker and message queue, scalable, high available and secured.

A Kubernetes native solution in a lightweight container, deployed in just one minute.

Ballot image auditing capability make it possible for jurisdictions to retain a secure digital image of every ballot cast.

## Auditability

The auditability challenge is asymmetric. Local U.S., elections run by counties and by townships are faced with coping with attack from large international organizations. Attackers can be nation states. It is simply not reasonable to expect a small county government to withstand an attack from a nation-state attacker. Because attacks cannot always be prevented, it is vital that they are detected and protected against by a large government entity capable of deterring sophisticated cyber-attacks. In this manner, voters know if the result can be trusted. That requires stringent auditing.

Election monitors carry out spot checks on individual ballots in risk-limiting audits. A comprehensive audit is achieved by providing end-to-end verifiability. Each vote is encrypted and given a unique identifier. The voter is given a tracking code that lets them check that their vote goes through the system unchanged and ends up in the final tally.

Not every voter needs to track their ballot to ensure the system maintains its integrity. If 1% of voters nationally check that their ballots are correctly encrypted and tallied, it would be a good monitor of election security. At the same time, the way the encrypted votes are tallied can be checked by anyone to make sure that each candidate gets the correct number of votes.

Secret ballots protect the privacy of each ballot.

Spot checks and administrative audits can be carried out by the members of the existing canvassing boards who currently decide on whether ballots are eligible or spoiled, with built-in safeguards to make sure no individual can either disrupt or influence the verification process.

A fundamental principle of auditability security is to provide means to check whether ballots as submitted are valid. Every single voter has the ability to verify their own vote. Checking can occur on public websites set up by election boards or local authorities. Observers from opposing parties can use a verification program to check the final tallies. The election officials can implement procedural checks using their dashboard.

## Phone Navigation, Ballot Tabulation, and Ballot Counting

After done voting voter checks out with poll worker (left over from phone rather than app voting)

Cast vote button for checkout

Must checkout with same code checked in with; App should make it available

Need to be able to navigate to look at text messages without losing ballot

Need to be able to navigate to take calls without losing ballot

Every step of way needs to be able to reconnect and continue from where left off during voting process

After checkout - ballot goes to ballot box which is blockchain vault

At this point, after ballot reaches the blockchain, the voter is considered to have cast the ballot- if the rest of the process (PDF, Printing) does not work, ballot still counts

Need electronic count from the blockchain as unofficial result

Should correlate with the tabulation of the paper ballots

Ballot goes to server for PDF printout

Marked ballot comes back to voter on the cell phone

Voter can check the marked ballot on the phone before it leaves the phone

If not ok, there needs to be appeal process

Ballot goes to server at tabulator according to current process for in person voting

Process for mitigation of claims of “not how I voted”

Challenged ballot procedures end to end encryption

Must mix ballots as deposited in blockchain and server so cannot tell how someone voted

Here a built-in delay is good, use a trigger on moment cast votes button is pushed by the first voter to initiate random number generator algorithm that mixes the first 3 ballots – 3 ballot mixing is sufficient -3 ballot mixing continues throughout the election. Delay makes the system work. Do not scrabble in manner that leaves ballots able to be detected, i.e. lay first ballot in first.

Need to adhere to secret ballot rule – not tell how someone voted

Blockchain works like a ballot box, called a vault

Only use for blockchain

Blockchain immutable just for one election, whatever the law says about how long the ballots have to be stored, then wiped out. Blockchain is used for only one election

Election administrator responsibilities

Set up registration list

Maintain backups of registration list

Set up ballots for each poll site (jurisdiction rather than poll site)

Have phone banks available to take voter calls

May accommodate early voting in some jurisdictions

Assign votes code to enter that validates eligibility to receive cell phone ballot

Have ability to send ballot to eligible voter after voter checked off registration list and after voter enters the right code

Mechanism to deal with lost voter codes

## Voter Procedures for Cell Phone Voting

Voter receives ballot sent by clerk to match voter poll site (jurisdiction)

Voter marks ballot

App prevents making a mistake to spoil ballot by preventing overvotes

Voter can change mind and navigate through ballot

Supports slate voting, endorsed candidates, write-in for every office (where a write in candidate is or can qualify)

Every office has as many write-ins as there are votes-for in that office

No write-ins on questions, just yes or no vote

When done voting, voter pushes cast votes button

App asks “Are you sure? (some voters will try to push cast vote after completing selections for one office – most common problem)

App needs to make the point you must make choices for desired candidates

Before exiting voting

Make clear this is the final step

App must ask, “Did you make all desired selections?”

Voter registers to vote by cell phone

Voter assigned to poll site / Poll site (Their voter registration should do this for them)

Indicates ballot to be voted on

Voter given # to call when time to cast ballot (Is this for app based voting?? Or phone voting?? Different standards)

Voter given # to call when time to cast ballot

Clerk has ability to call back when time to check in voter

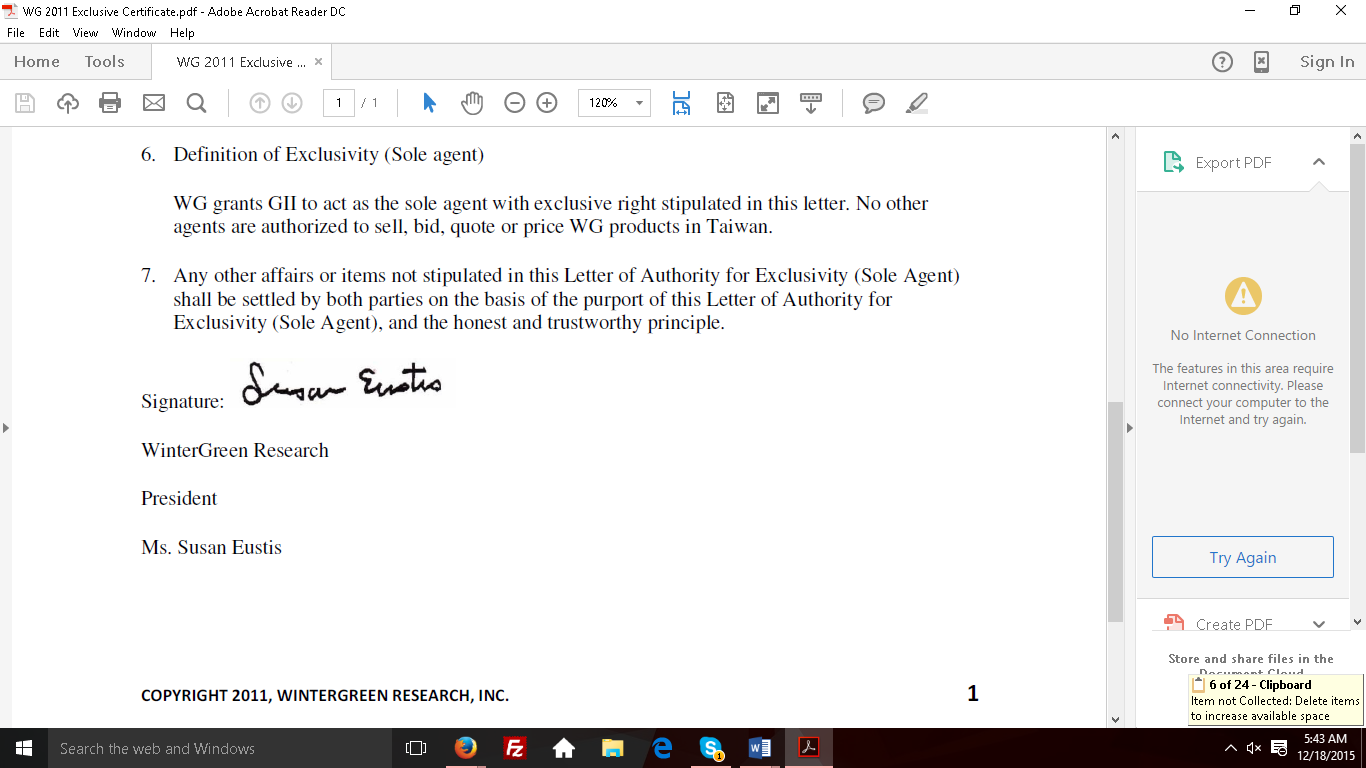
No waiting in line - no busy signals need capacity to handle calls

Polling site Clerk takes call in due course

**Respectfully Submitted,**

Susan Eustis

Leader GBA Voting Working Group



Appendix A: Glossary

|  |  |
| --- | --- |
| **Ballot** | **The physical and electronic representation of the options that may be selected in an election.** |
| **Election Administrator (Admin)** | The person responsible for the planning and conduct of an election and the reporting the election results. |
| **Election Worker** | Anyone assigned a roll by the Election Admin or a Party Lead |
| **Government Business Blockchain Platform (GBBP or server)** | The GBBP or server is a multi-blockchain platform that connects to public and private blockchains. It allows governments to maintain private blockchain connected to a global network that validates the integrity of allowed information. May be any server used for election processing and ballot storage, preferably blockchain |
| **Jurisdiction** | The organization such as a city, state, province, or any other public or private organization conducting an election. |
| **Polling Station** | The physical location where the votes are cast. |
| **Voter Registry** | The database of authorized voters in a jurisdiction. It is maintained by the jurisdiction. |

Need to add precinct or voting jurisdiction as in the unit that votes are grouped into for ballot creation.

Appendix B: Roles

The table below identifies the permissions and restrictions for all roles associated with a blockchain based election process. However, no role listed or otherwise may have permission to view or change and individual vote.

|  |  |  |  |
| --- | --- | --- | --- |
| Role | View | Permissions | Restrictions |
| Election Administrator (Admin) | All role assignments | Assign party leads |  |
| Party Lead | All role assignments | Add candidates  Add Election Workers |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Appendix X: Acknowledgements

Gerard Dache has been a capable leader through this entire standards process definition. We are so grateful for his capable leadership and his untiring integrity.