Discussion of Barcode Issues

This document highlights the discussion around the use of barcodes by a voting system. There are requirements within the Voluntary Voting System Guidelines (VVSG) 2.0 that are specific to barcodes or encoded information produced by a voting system. Barcodes are noted as an open area for the standard due to concerns around transparency, auditability, interoperability and ballot secrecy. This document curates potential use cases of barcodes, identifies the threat concerns, and discusses current VVSG 2.0 related requirements.

Overview

Use Cases

Ballot Activation
Apply Voter Accessibility Options
Interactive Sample Ballot Transfer
Capture Ballot Selections
Tabulation
Process Mail-In Ballots
Store Audit Identifiers
Store Digital Signatures
Transfer Unofficial Tabulation Results

Primary Concerns

Transparency
Interoperability
Ballot Secrecy
Auditability

Residual Risk of Not Having Barcodes

States may choose not use the federal certification program
States may need to purchase new voting systems.
Voting systems may be less accessible to voters
There may be increased wait times at precincts
There may be increased time spent completing tabulation, audit, or recount

Barcode Analysis

This section steps through a list of barcode uses cases that are relevant to scope of the VVSG requirements. Each use case is followed by concerns, suggested mitigations and related requirements.

Ballot Activation

A barcode is scanned to present a voter with the correct ballot style for their particular political party and/or location. The barcode may also be used to apply a voter's accessibility options to a ballot marking device (e.g., audio and visual settings).

Concerns

Ballot Secrecy Violation

The activation data encoded in the barcode may uniquely identify the voter. If this information is recorded in the e-pollbook as well as the Ballot Marking Device, then it would be possible to link the identity of voters to their voted ballots.

Lack of Transparency

Information within barcodes is not human-readable. Special hardware and software may be needed to read the barcode or parse the information contained in the barcode. Due to this, a voter does not have full visibility or awareness of the information stored in the barcode and being transferred into the voting system. The encoded information may include information that can identify a voter.

Mitigations

Ensure Unlinkability of Ballots

Ensure that the voting system does not receive any voter information that can be used to link a voter to their ballot selections. Below are two possible options:

1. The ballot activation data should not contain any unique identifiers that can be associated with a voter. For example, the barcode may only contain an identifier for the ballot style.

2. The activation data might be specific to a voter but is not included on the marked ballots or stored in any way that could be associated to a particular ballot.

Provide Barcode + Human Readable Format

To increase transparency, a decoded human readable format is provided to give the voter visibility of the information stored in the barcode. One option for this solution, is the human readable format will display the activation code that is stored in the barcode. The voter can then reference a codebook or a table that displays their ballot style based on the activation code.

Device and/or Application to Decode Barcode
A separate device and/or application is provided to the voter to decode the barcode and verify its contents. This requires the voter to trust the results displayed by the device/application.

Provide Human Readable Format Only
To give full transparency, do not encode information in a barcode and only provide human readable information. In this scenario, the voting system would be required to read information from the pre-voting slip using optical character recognition (OCR).

Related Requirements
10.2-L – Activation device records
This requirement is found under the ballot secrecy principle and restricts activation devices from including information that can be used to expose a voter's identity.
`
3.3-Transparency Guideline
This guideline under the Transparency principle states that the public must be able to understand and verify voting system operations throughout the election process.

4.1 Interoperability Guideline
This guideline under the Interoperability Principle requires voting system data, such as barcode information, to be imported and exported in an interoperable format. Interoperability allows barcode data to be interpreted the same way across different types of voting system.

4.2 Interoperability Guideline
This guideline requires that barcode implementation use a standard publicly available format.

Interactive Sample Ballot Transfer (i.e., Pre-Voting)

A voter uses their personal device to record their selections, which are then presented or stored in a barcode. The voter takes the barcode to a polling place and scans the barcode to automatically populate the voter's ballot selections. This technique provides additional usability and accessibility value. For example, voters with low literacy or cognitive disabilities are able to vote at their own speed. Blind voters have the opportunity to avoid the slow BMD audio interface.

Concerns
Ballot Secrecy Violation/Lack of Transparency
Information within barcodes is not readily understandable to the human eye and require additional technology to translate the encoded information. Due to the encoding, a voter does not have full visibility or awareness of the information stored in the barcode and transferred into the voting system. The encoded information may include more than just the voter's ballot selections and may inadvertently identify a voter.

Voter Coercion/Vote Buying
Prior to entering the polling place a voter is coerced into filling out their sample ballot in a manner that goes against their own opinion. Voters can use the barcode to present the coercer with proof of their vote selections. Voters may also be offered a reward to vote a specific way and required to provide proof to receive the reward.

Presentation/Spoofing Attack
A malicious website/application masquerades as a legitimate election service and presents a voter with the option to complete their ballot. The malicious website/application may display the voter selecting one contest when they are actually selecting something else (clickjacking). Additionally, malicious or faulty production of a barcode may present the voter with different information than what is interpreted by the machine.

Mitigations
Enforce Ballot Secrecy
Ensure that the voting system does not receive any voter information from the barcode that can be used to link a voter to their ballot selections.

Give the Opportunity for Voter Verification/Modification
At the polling place, the voter has the opportunity to review, modify, and confirm their choices before printing their selections. This mitigates against any coercion/vote buying that may occur prior to the voter casting their ballot.

Application or Device to decode Barcode
A separate device and/or application is provided to the voter to decode the barcode and verify its contents. This requires the voter to trust the results displayed by the device/application.

Provide Barcode + Human Readable Format
To increase transparency, a decoded human readable format is provided to give the voter visibility of the information stored in the barcode. For this use case, the barcode would contain

Provide Human Readable Format Only
To give full transparency, do not encode information in a barcode and only provide human readable information. This would require a voter to print a full ballot with their ballot selections rather than just a barcode. The voting system would then read information directly from the printed ballot using OCR.

Related requirements
9.1.3-A – Records for voter verification
This requirement states the voting system must produce a record that allows the voter to verify their selections were correctly interpreted.

9.1.3-B – Identification of errors

This requirement states that the voting system must provide the voter with the opportunity to identify any errors in their selections before submitting their ballot for tabulation.

9.1.5-C – Paper record intelligibility
This requirement implies that a voting system must print a record that represents the voter's ballot selections in a manner understandable by the voter. If a barcode is used to capture ballot selections, an additional human readable format must also be available.

3.3-Transparency Guideline
This guideline under the Transparency principle states that the public must be able to understand and verify voting system operations throughout the election process.

4.1 Interoperability Guideline
This guideline under the Interoperability Principle requires voting system data, such as barcode information, to be imported and exported in an interoperable format. Interoperability allows barcode data to be interpreted across different types of voting system.

4.2 Interoperability Guideline
This guideline requires that barcode implementation use a standard publicly available format.

Ballot Selections/Tabulation

A ballot marking device prints a barcode on a ballot that stores a voter's ballot selections. This barcode is scanned to include a voter's ballot selections in the tabulation.

Process Mail-In Ballots

Mail-in ballots may not be printed on the paper size/type necessary to be fed into a tabulation system. Similar to *Interactive Sample Ballots*, the code on the ballot can be used to "remake" the ballot onto a standard ballot card, perhaps using a ballot on demand (BoD) system.

Concerns
Ballot Secrecy Violation/Lack of Transparency
Encoded information in barcodes is not readily understandable by the voter. This leaves voters unaware of any voter identifying data that may link them to their cast ballots, such as unique identifiers, sequential identifiers, or timestamps.

Presentation/Spoofing Attack
If barcodes are the primary tool used for tabulation of cast ballots, it is important that the barcode information matches the voter's ballot selections. Some key concerns include:

- How can a voter be sure their ballot selections match the information captured in the barcode?

- How can discrepancies be detected? How to handle issues of mismatching information?

Mitigations

Enforce Ballot Secrecy

Ensure that barcodes do not contain any voter information that can be used to link a voter to their ballot selections.

Provide Barcode + Human Readable Format

To increase transparency, a decoded human readable format is provided to give the voter visibility of the information stored in the barcode. The printed ballot would include a barcode and a print-out of the information stored in the barcode. The voting system would take in information through the barcode and the voter can reference the human readable format on the printed ballot.

Give the Opportunity for Election Official Verification/Correction

When processing mail-in ballots, the election official has the opportunity to review, correct, and confirm the choices are accurately captured when the ballot is remade.

Application or Device to decode Barcode

A separate device and/or application is provided to the voter to decode the barcode and verify its contents. This requires the voter to trust the results displayed by the device/application.

Require Identical Information

Barcodes are often used to encode information in a minimized format. To avoid any misinterpretations of the data, the barcodes would capture all the data verbatim.

Provide Human Readable Format Only

This option does not use a barcode and instead reads in information using OCR. The printed ballot would only contain human readable information.

Related requirements

9.1.1-A – Software independent

This requirement states that voting systems must be software independent.

9.1.5-C – Paper record intelligibility

9.1.5-D – Matching selections

This requirement states that any representation of the selections to match the selections chosen by the voter.

3.3-Transparency Guideline

This guideline under the Transparency principle states that the public must be able to understand and verify voting system operations throughout the election process.

4.1 Interoperability Guideline
This guideline under the Interoperability Principle requires voting system data, such as barcode information, to be imported and exported in an interoperable format. Interoperability allows barcode data to be interpreted across different types of voting system.

4.2 - A Standard Formats
This requirement states that a barcode implementation must use a standard, publicly available and publicly documented format. The discussion sections specifically calls out barcodes.

7.3 Marked, Verified, and Cast As Intended Guideline
Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Store Audit Information

Barcodes may be used to store a ballot identifier to match with cast vote records (CVRs). Additionally, barcodes can store digital signatures that may be used to verify the integrity and authenticity of barcode information, such as the ballot identifier.

Concerns

Ballot Secrecy Violation
The information within the identifier is a concern if the identifier includes the order in which a ballot is cast. An example is if the identifier includes a timestamp. The timestamp could potentially be used to correlate a voter's ballot with the time their ballot was cast.

> *Lack of Transparency*
> Information within barcodes is not readily understandable to the human eye and require additional technology to translate the encoded information. Due to the encoding, a voter does not have full visibility or awareness of the information stored in the barcode and being transferred into the voting system. The encoded information may include information that can identify a voter.

Mitigations

Enforce Ballot Secrecy
Ensure that all identifiers do not include any voter related information, including information that may capture the sequence in which a ballot was cast.

Provide Barcode + Human Readable Format
To increase transparency, a decoded human readable format is provided to give the voter visibility of the information stored in the barcode. The printed barcode would also include the

human readable representation of the information stored in the barcode. The voter would be able to read the identifier.

Provide Human Readable Format Only
This option would print the identifier instead of encoding the identifier in a barcode. The identifier would be read-in through OCR to match with the identifier on the CVR.

Related requirements
10.2-D – Prohibition on voter record order information
10.2-E – Identifying information in voter record file names
10.2-H – Aggregation and ordering
These requirements state that voter record data or metadata must not include information that can be used to determine the order in which a voter cast their ballot.

Transfer Unofficial Tabulation Results

The voting system produces the final tabulation results for a polling station and stores the results in a barcode. The barcode is scanned by a cellular device and the tabulation results are transferred to the central tabulation center over the cellular network.

Concerns
Lack of Transparency
Information within barcodes is not readily understandable to the human eye and require additional technology to translate the encoded information. Due to the encoding, the election worker does not have full visibility or awareness of the information stored in the barcode and the information that is being transferred. The encoded information may include more than just the tabulation results.

Malware/Presentation/Spoofing Attack
The compromised application used to transfer the tabulation results may make modifications to the data without the user being aware.

Eavesdropping/Data modification
This information may be sent using public telecommunication networks via a cellular modem or wirelessly over the cellular network (e.g., LTE). Data transferred through these means touch the internet and may be vulnerable to interception and modification of the data in transit. This may result in an unauthorized user gaining access to the tabulation results and/or modifying the tabulation results before they reach their destination.

Mitigations
Application or Device to decode Barcode
A separate device and/or application is provided to the election worker to decode the barcode and verify its contents. This requires the election worker to trust the results displayed by the device/application.

Provide Barcode + Human Readable Format
To increase transparency, a decoded human readable format is provided to give the election worker visibility of the information stored in the barcode. For this use case, the barcode would contain

Provide Human Readable Format Only
To give full transparency, do not encode information in a barcode and only provide human readable information. This would require a phone to scan the human readable tabulation results printed from the voting system rather than produce a barcode.

Related requirements
3.3-Transparency Guideline
This guideline under the Transparency principle states that the public must be able to understand and verify voting system operations throughout the election process.

4.1 Interoperability Guideline
This guideline under the Interoperability Principle requires voting system data, such as barcode information, to be imported and exported in an interoperable format. Interoperability allows barcode data to be interpreted across different types of voting system.

4.2 Interoperability Guideline
This guideline requires that barcode implementation use a standard publicly available format.

Related Requirements

7.3 Marked, Verified, and Cast As Intended Guideline

Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

9.1-B.1– Voter verification

Tamper-evident records must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections.

9.1.1-A – Software independent

The voting system must be software independent

Discussion

Software independence means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. All voting systems need to be software independent in order to conform to the VVSG.

There are essentially two issues behind the concept of software independence:

- it is be possible to audit voting systems to verify that ballots are being recorded correctly, and
- testing software is so difficult that audits of voting system correctness cannot rely on the software itself being correct.

Therefore, voting systems need to be 'software independent' so that the audits do not have to trust that the voting system's software is correct. The voting system will provide proof that the ballots have been recorded correctly, ,that is, voting records will be produced in ways in which their accuracy does not rely on the correctness of the voting system's software.

This is a major change from previous versions of the VVSG, because previous versions permitted voting systems that are software dependent, that is, voting systems whose audits rely on the correctness of the software. One example of a software dependent voting system is the DRE, which is now non-conformant to this version of the VVSG.

There are currently two methods specified in the VVSG for achieving independence:

- through the use of independent voter-verifiable paper records, and
- E2E cryptographic voting systems.

9.1.3-A – Records for voter verification

Tamper-evident records must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections.

Discussion

Precinct-based voting systems are the only way to meet this requirement. Entirely separate voting channels, such as remote postal voting, do not offer this opportunity to the voter.

Applies to: Vote Capture Devices

9.1.3-B – Identification of errors

The voting system must offer voters the opportunity to identify ballot errors before it is cast.

Applies to: Paper-based system architectures
Cryptographic E2E system architectures

9.1.5-C – Paper record intelligibility

The recorded ballot selection must be presented in a way the voter can understand.

Applies to: Paper-based system architectures

9.1.5-D – Matching selections

All representations of a voter's ballot selections produced by the voting system must agree with the selections made by the voter.

Applies to: Paper-based system architectures

9.1.5-E– Mandatory ballot availability

The voting system must make available all encoded ballots for public posting.

Applies to: Cryptographic E2E system architectures

9.1.5-F – Verification of encoded votes

Voters must have the opportunity to verify that their ballots are included within the tabulation results.

Applies to: Cryptographic E2E system architectures

9.1.5-G – Sufficient information for verification

The receipt must provide sufficient information for voters to verify that their cast ballots are uniquely contained within the publicly available list of encoded ballots.

Applies to: Cryptographic E2E system architectures

10.2-D – Prohibition on voter record order information

The voting system must not contain data or metadata associated with the CVR and ballot image files which can be used to determine the order in which votes are cast.

10.2-E – Identifying information in voter record file names

CVR and ballot image names must not include any information identifying a voter.

Discussion

This helps to ensure that information that could accidently be used to reference a voter is not used within a file name.

10.2-H – Aggregation and ordering

Aggregated and final totals must not contain voter specific information, and must not be able to recreate the order in which the ballots were cast.

10.2-J – Voting information with receipts

Receipts produced by a voting system must not contain voter information.

10.2-L – Activation device records

Activation devices must not create or retain information that can be used to identify a voter's ballot, including the order and time at which a voter uses the voting system.

Discussion

The activation device must not create or retain any information that could be used for the purposes of identifying a voter's ballot, or the time the voter arrived at the polls, or the specific vote-capture device used by the voter.

10.2-O – Ballot secrecy for receipts

The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

Applies to: E2E voting system architectures

Barcode Types

1-Dimensional (1D) Barcodes	2-Dimensional (2D) Barcodes

Simple and Linear	Complex
Data stored in one direction	Stacks – stacks of linear barcodes; Matrix – hexagonal, square, or circular
Stores small amounts of data	Stores more data