Barcode/Encoding Use Case Analysis

This document discusses some of the various election use cases for barcodes/encoding. Below is detailed description of each barcode use case, relevant concerns, potential mitigations and related requirements.

Store Ballot Activation Information (e.g., ballot style) & Apply Voter Accessibility Options
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, transferred to a Ballot Marking Device, or printed on an on-demand ballot, then it may 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 necessary to read or parse the information contained in the barcode. A voter does not have full visibility or awareness of the information the barcode stores and transfers to the voting system. The barcode may include information that can identify a voter and be used to violate the principle of ballot secrecy as mentioned in the previous concern. Although the barcode may not include voter identifying information, the lack of transparency may cause a voter to suspect the violation of ballot secrecy and distrust the voting system.

Potential Mitigations

Inability to link Voters to Ballots/Ballot Selections
Ensure that the voting system does not receive any voter information that can be used to link a voter to their ballot selections. Below is one possible option:

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.

Provide Barcode + Human Readable Format
To increase transparency, a decoded human readable format is provided to the voter for visibility into the information stored in the barcode. One example is the human readable format displaying 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. This mitigation requires that each election jurisdiction provide a codebook or table and instructions for voters. Also, this mitigation assures the voting system has no way of linking a voter to their ballot selections by providing proof of what information is stored within the barcode.
Device and/or Application to Decode Barcode
Another option to increase transparency is the use of a separate device and/or application 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.

Pre-voting/Store Ballot Selections Prior to Entering Polling Place (e.g., Interactive Sample Ballot Transfer)
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 and that is then represented by the barcode. Voters can use the barcode to present the coercer with proof of their vote selections. A voter may also be provided a barcode by a coercer, perhaps on a sheet of paper just outside of the polling place. The coercer or someone in the polling place could observe whether the coerced voter is voting quickly by using the agreed upon barcode to determine the 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 also cause the voter to unknowingly download malware to their device. The malicious website/application may display the voter selecting one contest when they are actually selecting something else (clickjacking). As a result, the recorded barcode may not match the voter’s intent.

Additionally, malicious or faulty production of a barcode may present the voter with different information than what is interpreted by the machine.

Potential Mitigations
Enforce Ballot Secrecy through Universal Auditing
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. This mitigation requires auditing at each jurisdiction for each election to make sure the barcode does not include any information that could be linked to a voter. This would also require the ability for voters to decode the barcodes using code books and/or applications.

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.

To add on to this mitigation, a voter individually confirms each selection and is offered the opportunity to make a change before moving to the next selection. This assists with mitigating coercion as long as the coercer at a polling place cannot observe the coerced voter quickly accepting/changing the selections as determined by the barcode.

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.

Capture Ballot Selections at the Polling Place and Use for 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. However, with “remade” mail-in ballots the voter does not have the opportunity to review, modify or confirm their ballot selections before they are processed.
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 additional 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?
  - A discrepancy could be caused by a voter printing out their ballot using the barcode encoding of their selections and then hand marking their ballot to change their selections, for instance by filling out additional ovals.

Potential Mitigations

Enforce Ballot Secrecy through Universal Auditing
Ensure that barcodes do not contain any voter information that can be used to link a voter to their ballot selections. This mitigation requires audits to be performed in every jurisdiction for every election to ensure voter information is not included.

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. Such an audit depends on the regulations and diligence of the local jurisdiction. To ensure accuracy, audits would be needed in every jurisdiction to compare voters' mailed in ballots to the "remade" ballot and any post-election tabulation audit would have to use the original, voter verified ballots, not the remade ballot.

Application or Device to decode Barcode (does not apply to mail-in ballots)
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.

Documentation to Review Barcode (does not apply to mail-in ballots)
A reference implementation documentation is provided to allow a review to decode and replicate the barcode and verify its contents.
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

Store Ballot Identifier
Barcodes may be used to store a ballot identifier to match with cast vote records (CVRs).

Input CVR Data
In addition to the human readable information, a single QR or other standard 2D barcode is optionally printed on the paper CVR containing all the header information and foreign keys to
voter selections. The barcode may be used to assist auditors or election officials when manually transferring information from each VVPAT receipt into independent forms or spreadsheets for further analysis or verification. A handheld COTS keyboard wedge scanner could replace manual mouse clicks and keystrokes which are time consuming and prone to error. In both forms of data entry (manual or scanned) the transferred data is individually verified to match the human readable content.

**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.

**Malicious Input/Command Injection**
This concern applies to all uses of barcodes but was discussed during the Input of CVR Data use case. Barcode input is also thought to be the equivalent of keying in data or commands on a keyboard. In addition to the lack of transparency concerns mentioned previously, a barcode could potentially input malicious commands that modify data, inject malware, or give unauthorized access to election data.

**Mitigations**

**Enforce Ballot Secrecy through Universal Auditing**
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.

**Documentation to Review Barcode**
A reference implementation documentation is provided to allow a review to decode and replicate the barcode and verify its contents.
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.

Related requirements
2.5 - The voting system supports system processes and data with integrity.
2.5.3-D – Validate and filter input
The voting system must validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values.

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.

*Documentation to Review Barcode*
A reference implementation documentation is provided to allow a review to decode and replicate the barcode and verify its contents.

**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.

---

**Perform Redundancy Check**

*Human-readable text compared with ballot selections within Barcode*
A BMD may replicate a voter’s selections in human-readable form – either a ballot summary or marked full ballot. A barcode representation of voter selections can serve as a redundancy check to reduce the risk of error. Data read from a bar code could be used *both* to identify errors in interpretation of optical characters and also to identify potential calibration and ballot programing errors.

*Store digital signature value to notify of potential errors in human-readable interpretation*
The barcode in this scenario may not contain ballot selections but rather a value that is used to authenticate and verify that the information is from a valid BMD. Also, this barcode would
include a checksum to determine whether or not the human readable ballot information is interpreted correctly.

**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.

**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.
Store Encryption Data

Conveyance of Seed Data – E2E Verifiable System
A BMD provides each voter with a take-home receipt (or ballot tracker) that is based upon an encryption of the voter’s selections. This encryption should be randomized so that two ballots with the same selections do not produce identical encryptions. While it’s possible for the BMD to share its full encryption of each ballot, a more efficient and expedient approach would be for the BMD to convey its random seed data (also known as a nonce) to the election tabulation and reporting system. Possession of this nonce would allow back-end systems to reconstruct an identical encryption that could be used for E2E-verifiability. This nonce must be encrypted since providing it to voters would enable coercion.

Support for Privacy-Preserving, Transparent Ballot-Comparison Audits
In this scenario, the entire set of CVRs can be cryptographically committed and shown to be consistent with the tallies without full disclosure of CVRs. Selected CVRs can then be opened for auditing purposes. To protect CVRs from inappropriate disclosure, cryptographic keys or nonces which can be used to unseal selected CVRs should be encrypted (failure to encrypt these values provides a vector for coercion). The physical ballots can have a barcode that stores this encryption rather than maintaining them in electronic form.

Protection from Coercion, via Ballot Selfie
As cameras become ubiquitous, concerns grow about photography serving as a vector for coercion. In some scenarios, a mitigation to this risk can be established by offering voters an opportunity to create ballots which appear to be legitimate but are not eligible to be cast and counted. A cryptographic code could be placed on a ballot to indicate whether it is legitimate or faux. A barcode can serve as a compact and convenient means of conveying this cryptographic code.

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. Within these use cases the information stored is a nonce or other form of encryption data, that when provided in human-readable text, does not provide much meaning or value to the reader.

Misuse/Malware injection
Specific to the Protection from Coercion, via Ballot Selfie use case there are concerns that this would allow for additionally opportunities for malicious misuse. Allowing a voter to submit fake ballot brings up the concern of how to ensure only the cryptographically validated ballots are counted. Additionally, there are concerns that this allows for another avenue to inject malware into the voting system via a barcode/encoding.
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. In these use cases, the human readable information may not provide much value to the user if it is just a series of random letters/numbers/symbols that cannot be decoded by a codebook to inform the user what the encoded information means.
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

<table>
<thead>
<tr>
<th>1-Dimensional (1D) Barcodes</th>
<th>2-Dimensional (2D) Barcodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple and Linear</td>
<td>Complex</td>
</tr>
<tr>
<td>Data stored in one direction</td>
<td>Stacks – stacks of linear barcodes; Matrix – hexagonal, square, or circular</td>
</tr>
<tr>
<td>Stores small amounts of data</td>
<td>Stores more data</td>
</tr>
<tr>
<td></td>
<td>Often implements</td>
</tr>
</tbody>
</table>