Voting by Mail: The Impact of Signature Identity Verification for Voters with Disabilities

November 2023

Lynn Baumeister
Whitney Quesenbery
Center for Civic Design

Sharon Laskowski
National Institute of Standards and Technology

This is a pre-publication draft of material created for the NIST Voting Technology Series

Abstract

Voters with disabilities experience a gap in turnout compared to the overall US population. That gap has been shrinking, supported in part by changes in election administration under the Help America Vote Act (HAVA) and the requirements that voters with disabilities be able to vote privately and independently. A major effect of HAVA has been in making in-person polling places and voting systems accessible. Voting by mail (also called absentee voting) has long been offered as an option, but recently it has grown from an exception for older voters, voters with disabilities, and those out of their usual district on Election Day to a widely used method of voting. In many states, a signature is used to confirm the identity of the person returning the ballot and ensuring that ballots are being cast by the voter themselves. However, many people with a variety of disabilities cannot produce a consistent signature that can be used for verifying their identity. This includes voters who face challenges in making a wet signature or handling paper. This report examines how signatures and signature comparison are used in elections, explores the uses and types of signatures in other contexts, and discusses alternatives being developed that might – and might not – be appropriate for use in elections.

Keywords

accessible voting; accessible vote by mail; signatures; remote identity verification; election administration; print disabilities; vote by mail; VBM; electronic return

Table of Contents

Executive Summary

Voters with disabilities experience a gap in turnout compared to the overall US population. That gap has been shrinking, supported in part by changes in election administration under the Help America Vote Act (HAVA) [1] and the requirements that voters with disabilities be able to vote privately and independently. A major effect of HAVA has been in making in-person polling places and voting systems accessible.

Voting by mail (also called absentee voting) has long been offered as an option but recently it has grown from an exception for older voters, voters with disabilities, and those out of their usual district on Election Day to a widely used method of voting.

This expansion has made voting easier for many, but also brings some challenges for voters with disabilities. In many states, a signature is used to confirm the identity of the person returning the ballot and ensure that ballots are being cast by the voter themselves. Unfortunately, many people with a variety of disabilities cannot produce a consistent signature that can be used for verifying their identity. This includes:

- Blind and low vision voters who cannot visually confirm a hand-written signature for consistency and may not be able to place it on the form in the correct location.
- Voters whose signature has changed over time, especially due to age-related dexterity disabilities.
- Voters who rely on digital assistive technology for communication

It is also a general challenge that has increased with the growth of voting by mail and the general shift to more online and digital transactions. Many credit card companies, for example, no longer rely on a signature, even for in-person transactions. It is not clear, however, whether these new methods of authentication fit the current ways of administering elections.

Although research shows that instances voter fraud through in-person impersonation of a voter is "vanishingly rare," [2] it is much more of a challenge at a distance. This is partly true because it is not possible to observe the signature being made — in other words, there is not a close identification between the signature itself and the person. The remote nature of voting by mail also makes it impossible to ask for alternative sources of identification easily. (Many states have implemented a process known as "curing the ballot" in which voters are given a second chance to authenticate their mail-in ballot. The fact that this often happens after Election Day extends the schedule for announcing official results.)

This report examines how signatures and signature comparison are used in elections, explores the uses and types of signatures in other contexts, and discusses alternatives being developed that might – and might not – be appropriate for use in elections.

Section 1: Voter authentication and signatures in elections lays the groundwork, starting with the impact on voters with disabilities and then reviewing relevant aspects of the voter registration process and voter identification.

Section 2: Signature collection & comparison looks at how voter signatures are collected, signature comparison methods, and ways to reduce false mismatches.

Section 3: Remote identity verification considers other ways to authenticate voters' identity in order to reduce the number of rejected mail-in ballots from eligible voters, particularly voters with print disabilities.

Section 4: Future looks forward, discussing alternatives as well as constraints and challenges for election offices seeking to implement new methods.

Section 1: Voter authentication and signatures in elections

This section provides context for this of the report. It is a broad overview of how and where signatures fit into elections (rather than a state-by-state analysis) in order to lay the groundwork for discussions later in this report.

Private and independent voting - closing the turnout gap

The mandates in HAVA have made substantial improvements in the ability of people with disabilities to vote privately and independently. These modernizations have gone a long way to closing the turnout gap between voters with and without disabilities. In their research over several years, Lisa Schur and Doug Kruse report that the gap has fallen from 7.3% in 2008 to 3.6% in 2020 [3]. Notably, response to the pandemic in 2020 brought many features of elections, including expanded voting by mail, more return options, and the opportunity to "cure" signatures, that benefitted all voters.

Although implementations vary by state, today:

- All but 6 states have online voter registration [4].
- Accessible voting systems are required for all in-person voting due to HAVA.
- Early voting (in-person voting before Election Day) and vote centers (voting locations that allow voters a choice of where to go to vote in person) add options for when and where to vote in person. For voters with disabilities, these options can reduce barriers caused by mobility and transportation challenges as well as allowing them to choose days and times to vote that work with daily changes in health or support.
- When voting by mail requires an excuse, disability is almost always one of the allowed excuses. Wider availability of voting by mail makes it easier for all voters – including voters with disabilities – to choose this option without stigma or proof of disability.
- Accessible vote by mail systems, available in approximately half of the states in 2022, make it possible for people with print disabilities to mark an absentee ballot at home using their own accessible technology.

Voting from home also reduced the mobility barriers many voters with disabilities face and allowed them to receive assistance from trusted individuals, if they wish, more easily.

These changes in elections also take place in the context of changes in other interactions with government and daily life. The use of both new general use technologies, such as ride sharing and online banking, and improved assistive technologies, making independent living easier for people with disabilities, are now commonplace. This changes the baseline of expectations about the accessibility of elections.

Barriers to voting caused by signatures

The need for voter signatures in election

ns is still a barrier for many voters with disabilities. The NIST report "Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities" written in response to Executive Order (EO) 14019 Promoting Access to Voting identified several barriers for people with disabilities [5]:

- [...] Voters unable to sign their names consistently or at all would have increased independence if alternative identity verification methods existed to provide a signature on both paper forms and online documents.
- Voters with disabilities may not be able to complete the registration process online if there is no alternative to using a state Department of Motor Vehicles (DMV) driver's license or identification (ID) to provide a signature.
- [...], some voters with print disabilities may be unable to provide a consistent wet signature or provide a wet signature at all; [...]
- Some voters with print disabilities are unable to make a consistent handwritten (or "wet") signature that is needed for their application to be verified to receive their vote by mail ballot in some states. [...]

These issues can be identified by the capabilities needed and how they affect voters with different disabilities as shown in Table 1.

Table 1: *Barriers to using signatures*

	Blind, low vision	**Manual dexterity**	**Cognitive disabilities**
Holding a pen		×	
Finding where to sign	×		×
Signing in a small, restricted area (a signature box)	×	×	
Drawing the letters needed for signature	×	×	
Making a consistent signature	×	×	×

Voter registration - collecting the first signature sample

Voter authentication begins with the voter registration process. Voters registering in person or by mail provide a signature on the paper form, along with other information such as their address and asserting their eligibility to vote.

One of the most common ways to register to vote is through a transaction at a state motor vehicles office (DMV). Getting a new driver's license requires identification that can prove eligibility to vote as a citizen, a photograph, and a signature. The National Voter Registration Act (NVRA) [A] (also known as the Motor Voter Act) gives people the opportunity to use the information in their driver's license application for voter registration, either through an opt-in or more automatic process. Through agreements between the state DMV and elections offices, the driver's license number can also be used as authentication for online voter

registration. In either case, the signature is entered into the voter's registration record and used as the reference sample for comparison in the future.

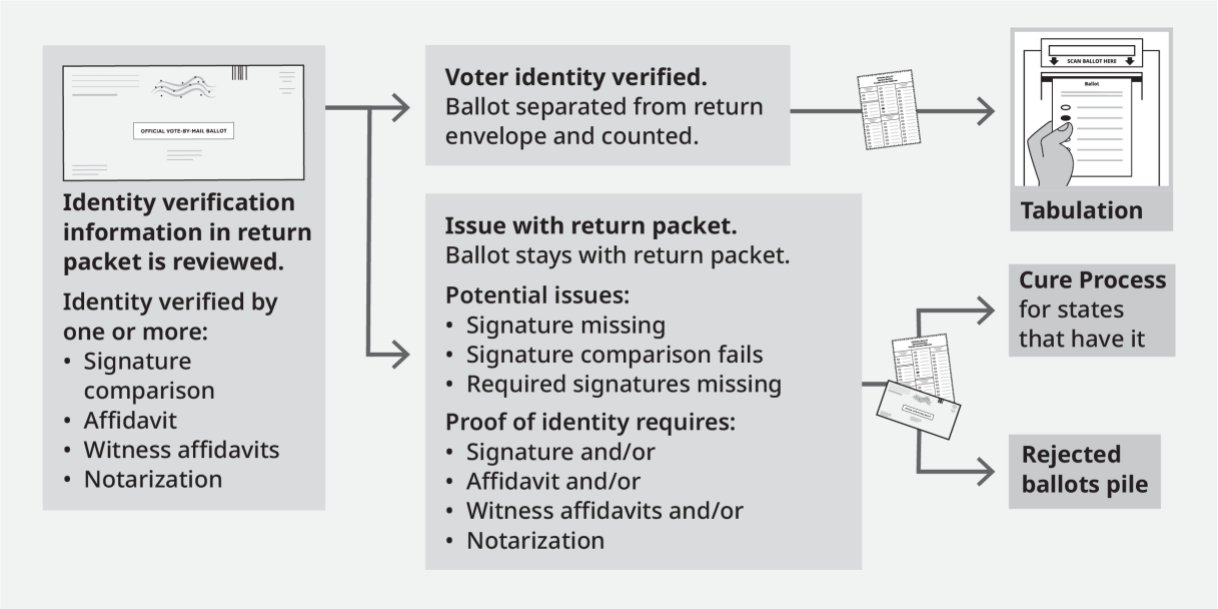
When a new voter has not provided a signature or other documentation required in the state, they are asked to do so when they vote for the first time–whether in-person or by mail.

Confirming voter identity and eligibility

With in-person voting, the voter is physically present during the check-in process. The check-in process differs from state to state; it may be as simple as stating your name and address or it may require presentation of official identification. Whatever the process, the purpose is the same - to establish that the person who showed up to vote is the person listed in the pollbook as an eligible voter.

The VBM check-in process, in contrast, happens without the voter physically present, based information in the ballot return packet. Although the process and the format of the ballot return package varies, they all have a method for keeping return package together and ballot secret until the voter's identity has been confirmed. Only when the voter is authenticated are the voter identification and ballot are separated and the ballot added to the stream of ballots to be counted. (See Figure 1.)

Figure 1: *Identity verified before ballot is separated from the return packet*



Signature comparison - comparing the signature in the mail-in ballot return packet with a previously collected signature from the voter – is an important method of authenticating mail-in ballots. Half the states rely on signature matching. Other states rely on witnessing or notarization of signed affidavits.

Concern over the growing number of mismatches as the use of voting by mail has increased, although this phenomenon may not be due to fraud, but to the proportionally larger number of voters whose signatures have changed over time, or where the difference between a signature made on a touchpad and on paper make accurate comparison harder.

Additionally, there is concern that the number of voters whose ballots are rejected for signature mismatches may disproportionately affect not just voter with disabilities but many others. For example, in a lawsuit in

California, the “Court found that between 33,000 to 45,000 voters had gone uncounted” [7] without evidence of voter fraud, identifying not just voters with disabilities, but also those whose first language does not use the English alphabet, or whose signatures had changed over time. This resulted in California adding mismatched signatures to an existing process that allowed voters an opportunity to provide missing signatures.

There are also broader social changes in common transactions such as paying with a credit card. Almost all credit card transactions used to require a signature–usually a wet signature on a receipt saved by the merchant. The rise of online purchases and use of cards containing chips means that fewer and fewer require a signature at all. Even those that do may not require a well-formed signature for comparison, accepting any squiggle on a point-of-sale touch pad.

Signature verification in vote by mail

Historically the use of absentee voting or vote by mail (VBM) was limited. It was allowed for individuals unable to get to their polling place on election day, people with disabilities that inhibited their mobility, people traveling on election day, or people working the polls.

VBM has grown, accounting for almost 40 million ballots in the November 2022 election – approximately 35% of all ballots cast [8]. This includes “no excuse” vote by mail, where any voter can request a mail-in ballot, as well as nine states VBM is the default voting method, with ballots mailed to all voters. The result is that elections offices have a larger volume of mail-in ballots to process, authenticating the voter and opening and counting their mail-in ballot.

The most common method for verifying the voter’s identity is signature comparison (comparing the voter’s signature in the return packet with a signature already on file). Although signatures match for most mail-in return packets, as shown by the national average of only 0.26% of mail and absentee ballots rejected for all reasons from 2012 – 2020 [9], the comparison process can flag false mismatches (the signatures are from the same voter but fail in the comparison process).

Each false mismatch means a rejected ballot from an eligible voter, unless the state has a process for following up with the voter to gather a new signature or otherwise confirm the voter’s identity. This is often referred to as a “cure” process. It is used in combination with signature verification as a way to meet the need to prevent election fraud, while not over-burdening voting by mail for most voters.

Accessible Vote by Mail (AVBM) - a partial solution for voters with disabilities

Some states provide voters with disabilities the option to use accessible vote by mail (AVBM), where the voter can mark their ballot digitally using their own assistive technology (screen reader, sip and puff mouse, etc.) rather than marking a paper ballot with a pen [10]. These systems are an important step in making voting by mail accessible as its use grows.

However, the final step in most AVBM procedures is for the voter to print their digitally marked ballot, sign the return packet, and mail the return packet to the election office.

A voter that successfully marked their ballot digitally may not be able to handle printed paper, locate the position where the signature must be placed, make a signature at all, or make a signature with sufficient consistency for signature comparison. This can lead to higher rates of ballot rejections due to signature problems for voters with disabilities, even with a robust cure process.

Section 2: Signature comparison

To understand the challenges of using signatures in elections, it's important to review the different ways that signatures are collected and the meaning they have in different kinds of transactions. This chapter also reviews some of the reasons why signatures may not match and methods used to reduce the number of ballots rejected because of a mismatch.

What we mean by a "signature"

Signatures have a long history as a way to identify the person who approved a document or completed a transaction. Historically, a signature was a name written in cursive using a pen on paper, or a special mark for the same person used by some people with disabilities. The signature functioned as a stand-in for the person themselves. This kind of signature is sometimes called a **"wet" signature,** one that a person has signed - in ink - on a unique piece of paper.

Technology, and the need to make it possible to provide a signature remotely, means there are now many more options [1]. There are two ways to directly produce electronic signatures.

- **Hand-drawn digitized electronic signatures** that can be either an image of a wet signature or one made using an electronic capture method such as a touch pad. These methods require the signer to complete the action of producing a signature. The quality of the signature produced depends on the physical properties of the capture method as well as the dexterity of the voter.
- **Typed electronic signatures**, in which the person's name is typed rather than formed by hand. These signatures are most often used as ceremonial "handshake" at the end of a transaction in which the identify of both parties has already been established.
  There are differences in how these signatures are displayed, but they **can not** be used for signature matching.

All of the electronic signature types shown in Table 2 are typically verified through visual examination and comparison to a reference version. Banks, for example, store a copy of depositors' signatures to validate checks.

Table 2: *Types of electronic signatures*

Hand-drawn signatures: Methods of producing an electronic version of a wet signature	
Digitized hand-drawn signature	Electronic version of a wet signature For example:

[1] There are also cryptographic signatures which are outside the scope of this report. These are not signatures in the traditional sense, but a mathematical scheme for verifying the authenticity of digital messages or documents. Readers of a document signed with a cryptographic signature can both be assured of the identity of the signer and that the contents have not been altered since it was signed.

	• A scan or image of the paper and signature inserted into a document • A document sent by fax
Entry pad signature	Signature drawn using finger or stylus on a signature capture pad. For example: • A point-of-sale payment tablet • A small signature pad, often a separate device for this purpose with minimal interactivity.
Computer mouse signature	Signature drawn using finger on computer touchpad or handheld mouse attached to computer.
Mobile screen signature	Signature drawn on phone or tablet touch screen using a finger.
Typed signatures: Signatures based on typed characters	
Typed signature	A name typed into a field and accepted as a signature. For example, used at conclusion of an agreement, often including assertions related to the transaction or accepting the digital signature as valid
Cursive facsimile -	A typed signature transformed into a visual equivalent using a font. Similar to a typed signature, but with the addition of font selection as a secondary identification.

Why signatures may not match

Signatures - especially wet signatures - made in different ways may not match even when they are genuinely from the same person. Reasons they may not match include:

- The signatures being compared may have been made at different times. The voter's signature may be changing due to age-related infirmities (such as developing hand tremors) or due to maturity (the voter no longer puts a little heart on top of their "i" or a swish under everything).
- The two signatures may have been captured on different devices. For example, some screens are harder to write on than others.
- One of the signatures may have been made on a signature pad or a mobile screen with poor resolution.
- One of the signatures may be a pro-forma wiggle rather than a careful signature, especially if it was captured in a setting where it was not being used for identification.

These problems affect all voters, not just voters with disabilities, but also those with physical challenges due to age.

Best practices to reduce mistakenly rejected signatures

Comparing signatures is complex; it requires looking at several characteristics:

- Overall proportions and style
- Hesitations
- Spacing between names
- Slant of the letters
- Slant of the entire signature
- Spacing between letters
- Size of the letters
- Distinguishing features (loops, cross points)
- Pen lifts
- Beginning and ending strokes

Better processes for signature comparison can reduce the number of incorrect mismatches in which a signature is rejected even though it has been signed by the correct voter. Some ways to improve ballot processing to reduce the number of ballots that cannot be counted include:

- Retain signatures from multiple touch points with government services in order to have more than one to compare against.

  For example, the signature from the voter's paper voter registration form, the signature from the voter's driver's license, the signature from the voter's last service as a juror, the voter's signature from their request for a mail-in ballot, the voter's signature from last year when their mail-in ballot needed to be cured. Ideally retaining multiple signatures will provide signatures captured through different methods (e.g., wet signature, signature pad). There will be fewer signatures for newer residents of since they will likely have had fewer interactions with government agencies, but the signatures of newer residents will be recent ones.

- Compare with more than one signature on file.

  Set policies establishing which signature is the primary signature to be compared with and the order other signatures should be considered.

- Use automated signature comparison software for the first review.

  Software has the benefit that the same examination parameters will be objectively applied to each signature pair.

- Conduct a manual bipartisan review of signatures that are flagged as mismatches by the software.

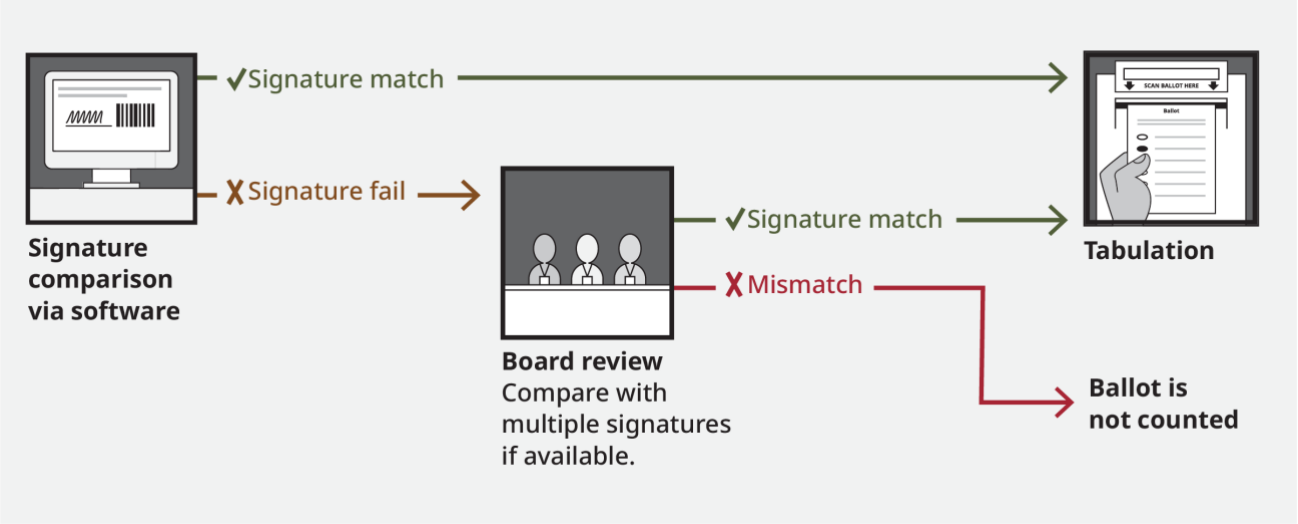
  Train the people doing the signature comparisons in signature forensics.

  Establish consistent policies for evaluating the signature pairs.

- Accept signatures that are outside of the designated signature location, for example allow them anywhere on the return envelope or affidavit form. This will accommodate voters that have difficulty locating the precise location to sign or can't fit their signature into the limited space.
- Give voters with disabilities ways to formally register and use a signature stamp or other consistent indicator chosen by the voter as a stand-in for their signature.

Figure 2 shows how the signature matching can either direct ballots to tabulation (ballot box / scanner) or to a secondary review.

Figure 2: *Signature comparison flow*



Section 3: Remote identity verification

The mitigations discussed in Chapter 2 can reduce the number of false mismatches, thereby minimizing the number of valid mail-in ballots that are rejected or must go through a cure process, but do not address the barriers faced by people with disabilities who cannot make a wet signature or who can't reproduce the same signature consistently.

Technology has the potential to assist elections offices by providing methods for voters with disabilities to validate their identity. Online (remote) identity verification method used for elections will need to strike a balance between how onerous the steps are, sometimes referred as how much friction the process has, and the risk of letting bad actors (individuals claiming an identity that is not their own or fictional) slip through.

Multi-factor authentication

One commonly used method is multi-factor authentication (MFA). Multi-factor authentication requires a person to present a combination of two or more different authenticators to verify their right to access an online system. The authenticators are a combination of:

- **Something the person knows:** a PIN, passcode, keyboard pattern, answers to "secret" questions the person set up. These can be items chosen by the person or supplied by an authenticator app.
- **Something the person has:** a hardware token such as a fob or personal identity verification (PIV) card, smartphone, email address (verified with information from or sent to the device)
- **Something the person is:** biometrics such as fingerprint, voice pattern, facial characteristics, palm or finger vein patterns.

Two-factor authentication (2FA) is a subset of multifactor authentication that uses a passcode entered on one system with a secondary identification provided by another system. For example, providing login ID and password in addition to a secondary authentication code from an authenticator application. Many government systems use 2FA to confirm legitimate access to their online systems after ownership and right-to-access have been established (login.gov, irs.gov, ssa.gov).

Current mobile phone security combines possession of the device itself (*something the person has)* with either a passcode or gesture pattern (*something the person knows*) or a biometric (*something the person is*) such as face or fingerprint to allow access. People choose the identification method for their phones. The ability to choose the identification method is important for people with disabilities as it allows them to pick based on what works for their situation. For example, someone with hand tremors may choose face recognition instead of a gesture pattern.

Multi-factor authentication may be stringent enough for elections, requiring a combination of things the voter knows and has. For example, submitting their full name, date of birth, and address, corroborating ID numbers from a government agency (their drivers license number, state voter identification number, last 4-digits of their Social Security number), a PIN number they received from the elections office, or other information that can be matched to the voter registration record.

Other authentication methods - hardware and vaults

Multi-factor authentication is not the only identity verification method that elections can consider. Other digital tools are also tackling the issue of how to control access in a usable way and may provide the combination of accessibility and security needed in elections.

- **Digital wallets and a digital election vault**

  A more futuristic approach looks to methods being used in financial domains - the technology and concept behind digital wallets. A digital wallet provides a place for a person to store digital equivalents of credit cards. What can be stored in a digital wallet is not limited to financial information, depending on the digital wallet application, they can store a host of other information (such as metro cards, boarding passes, or travel documents.). Information in the device can be selectively released (transmitted) by the wallet's owner, for example by opening the wallet app, authenticating according to the wallet's requirements, selecting the information to be released, and releasing it.

  A digital voter-vault could contain information relevant to elections, such as the information used for proof of identity and residency for the voter (photo ID, voter ID, signature or mark, utility bills showing residency – whatever is required for the state the voter is in). With the voter's permission, identification information from their vault could be released as needed to verify their identity that is, a voter identity certificate.

  A digital election vault would not work for everyone, but it is a method that could assist voters with disabilities who own and are comfortable using their smart phone.

- **Tangible "keys"**

  Physical multiple protocol security keys such as a Yubikey combine physical possession of the key (something you have) with additional security layers (something you know). This kind of technology has the potential to be a remote identity verification solution for a subset of people, particularly for blind and low-vision voters.

- **End-to-end verification**

  The U.S. requirements for a secret ballot – that is, one in which the identity of the voter cannot be connected to the ballot after it is cast - creates challenges for managing identity verification electronically that cannot be solved by election procedures alone.

  The idea of using cryptography to protect ballots was first introduced in the EAC's Technical Guidelines Development Committee as early as 2006 as a means to achieve software independence, defined as:

  > A voting system is s*oftware independent* if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome.

  Since then, security researchers have explored ways to use what is known as end-to-end verification (E2E-V) in elections. Nine leading researchers produced a summary of the field in 2017 in a paper, *Public Evidence from Secret Ballots* [11].

  More recently, a collaboration among researchers and voting systems vendors, ElectionGuard [11], has run pilot elections testing the use of the cryptographic system in real elections. The focus of these pilots

was both the capability for individual voters to confirm that their ballot was counted and independent verification that the election results are correct.

Although early use of E2E-V has focused on the ensuring that ballots are counted accurately, another use for cryptography might be in accessible voting by mail.

Inadequate verification

There are a number of pseudo identity verification methods that are used in low risk situations, such as setting up an account for storing videos that are inadequate and not appropriate for elections. Pseudo identity verification methods are relatively frictionless, requiring few steps and little effort.

- **Simply establishing personhood**

  The lowest level of verification seeks to establish that a person, not an automatic form filler (a "robot") is interacting with the website. "Completely Automated Public Turing test to tell Computers and Humans Apart" (CAPTCHA) is a prevalent example as is the "I am not a robot" checkbox at the end of a form. Social platforms such as dating apps may establish personhood by requiring a selfie taken in a particular pose, such as the right hand on top of the head.

- **Voice acceptance of conditions**

  Voice acceptance recordings are an example of a ceremony – providing a way for a person to indicate understanding and acceptance remotely. In these situations, the information is read aloud on a recorded line; with the listener being asked to verbally indicate acceptance after the information has been verbally delivered. This is not the same as using the person's voice pattern (a biometric) to positively identify the person.

- **Confirmation through access to an email or messaging account**

  Setting up an online account often simply confirms that the person providing the email address or mobile phone number, has access to that email or mobile number. This is not the same as confirming the identity of the person.

- **Third party verification**

  There are third-party companies that provide identity verification by validating ID cards, face recognition, and other biometrics. These services can be used for signature curing. This is typically done through a website that voters connect to through after being notified by mail. Although in use in a few states these systems raise questions of equivalent access (because they require use of a computer or mobile device) and privacy (because voter data is being managed by a commercial entity).

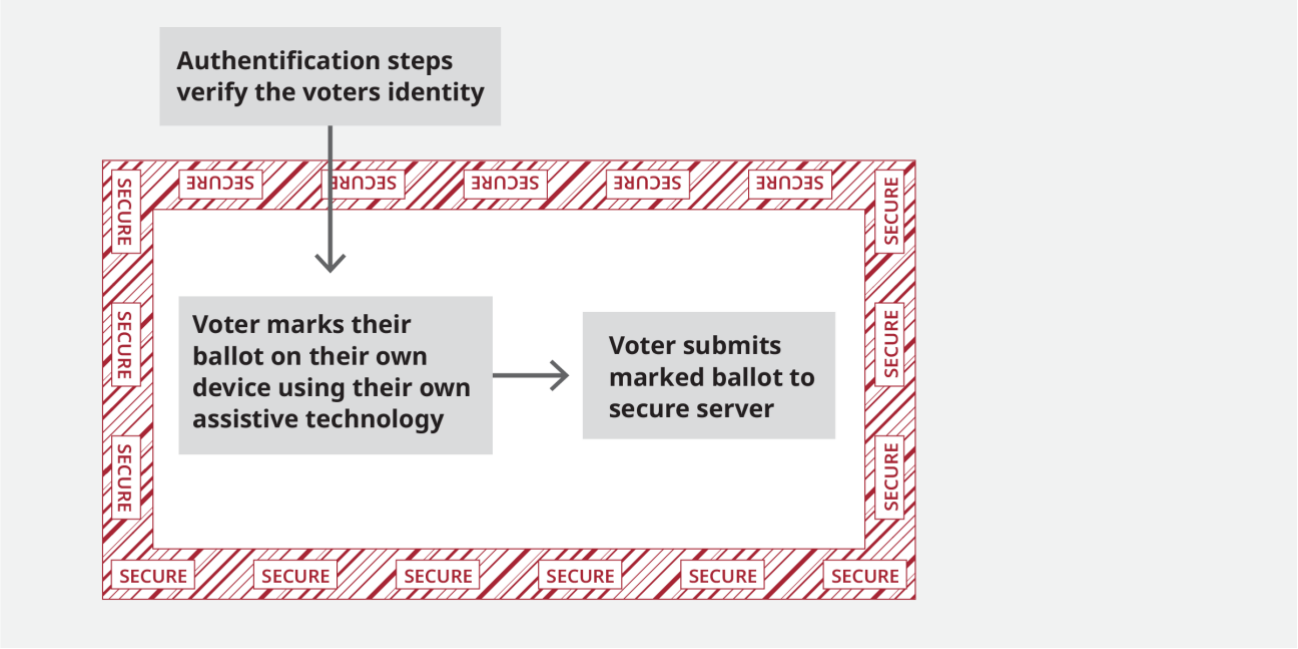
Section 4: Future

Strong identity verification methods allow electronic interactions

With AVBM, a voter receives and marks their ballot digitally rather than filling in ovals with a pen on a piece of paper. This allows the voter to use their own assistive technology (e.g., screen reader, text-to-speech, sip and puff mouse). **But the final step in the majority of states with AVBM requires the voter to print their marked ballot, provide a wet signature on the oath form or the envelope, and pack it in an envelope.**

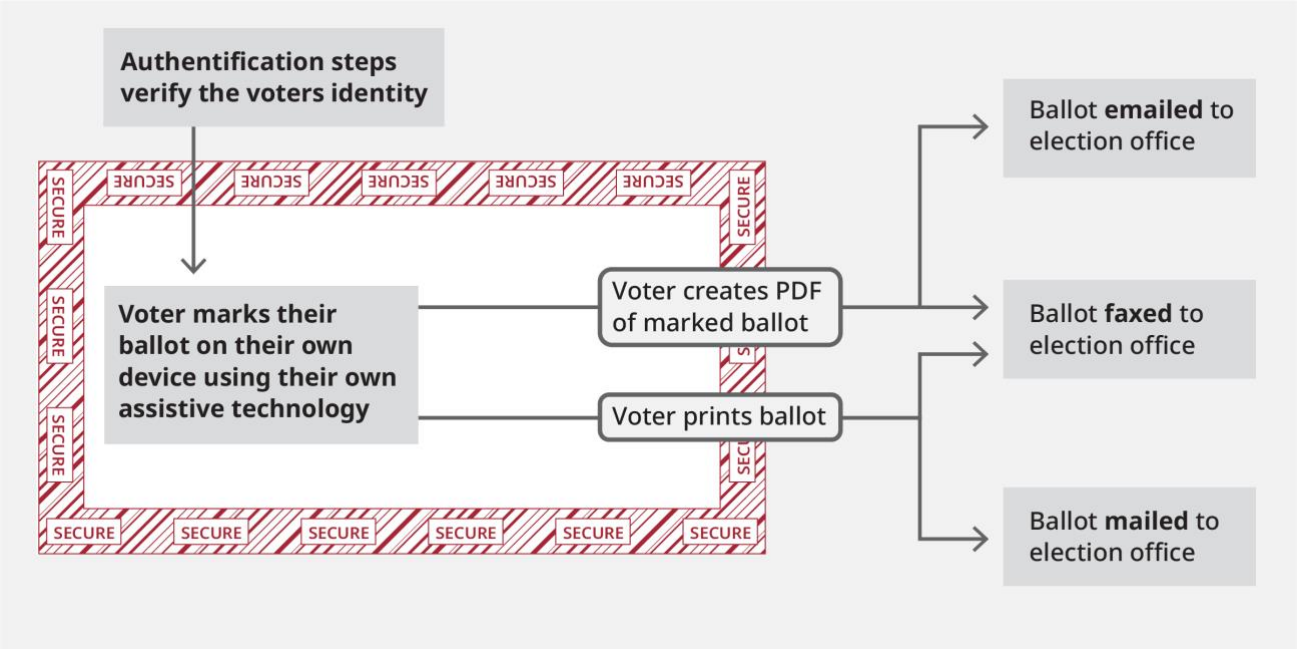
Electronic return through a secure portal removes paper-handling and signature making barriers by providing a return method that doesn't require the voter to handle paper and make a wet signature. If a signature is required to comply with state voting regulations, there are some new options if the voter has already been authenticated. They include a typed signature or linking to the signature on file in the voter registration system. In some ways, this is an electronic equivalent of what happens with in-person voting. At a polling place the voter's identity is verified at check-in and after that the voter marks their ballot and casts it without further checking of their identity within the polling place.

Figure 3: *Ballot submission from within secure area*



There is an important distinction between electronic return via fax or email and electronic return through a secure portal. When an AVBM ballot is saved as an external file (in order to be faxed, emailed, or mailed to the elections office), the ballot leaves the authenticated area. Those returned ballots must go through the same voter verification process (such as comparing signatures) as other mail-in ballots before the ballot can be counted.

Figure 4: *Return via mail - fax - email - breaks the circle of trust*



Conclusion: Supporting voters with print disabilities

Going beyond signature verification and offering a range of identity verification options will help voters with disabilities find a solution that fits with their circumstances. A voter with dexterity challenges might use the electronic signature because they can't shape a signature. A blind voter might opt for a solution that uses a tangible physical key and tapping in a PIN sent by the elections office. Offering these options to all voters can help reduce the number of vote by mail ballots that are rejected due to false signature mismatches. More transactions are going digital; the question is which of those can find a place in elections, offering the right balance of ease and security.

Are we there yet?

Elections offices across the country are currently exploring new options including electronic signature curing and ballot return along with tools and procedures for more robust identity verification. However, any discussion of offering more options to voters must also consider election administration and the need for new technical skills, staff resources, and funding for the tools and training as new methods are adopted [13]. Elections are critical infrastructure for democracy, so there are good reasons to be cautious when introducing new technology. They also have a unique need for security, usability, privacy, and access for everyone eligible to vote. Even promising new technologies in use in commerce and personal lives may not be "election-ready." The challenges include:

- **Cybersecurity.** The technical platforms must be secure from malicious attacks that could interfere with running the election, including both undetected attacks and catastrophic failures.
- **Ballot secrecy.** The verification system cannot create a connection between the identity of a voter and how they voted.
- **Equitable access to the system.** The system for verifying mailed-in ballots must be available to all voters, without relying on their having access to specific technology.

- **Privacy.** The procedures must protect a voter's private information beyond the public voter registration record. This might include a requirement to create an account that stores additional personal preferences that can reveal language or accessibility options.
- **Accessibility and language access.** The system must meet requirements for accessibility for people with disabilities (both in voting system standards and legal requirements for digital accessibility) and support for language access requirements.

References

[1] Help America Vote Act of 2002 (HAVA), Pub. L. No. 107-252, 116 Stat. 1666- 1730. Available at https://www.govinfo.gov/content/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf

[2] Morris, K., Dunphy, P. (2019) *AVR Impact on State Voter Registration New Brennan Center Report Finds Significant Gains in Voter Rolls*. (Brennan Center for Justice, NY, NY). Available at https://www.brennancenter.org/sites/default/files/201908/Report_AVR_Impact_State_Voter_Registration.pdf

[3] Schur, L., Kruse, D. (n.d.) *Voter Turnout and Voting Accessibility*. (Rutgers University Program for Disability Research, NJ). Available at https://smlr.rutgers.edu/faculty-research-engagement/program-disability-research/disability-and-voting

[4] National Conference of State Legislatures (2022) *Online Voter Registration*. (NCSL, Washington, D.C.) Available at https://www.ncsl.org/elections-and-campaigns/online-voter-registration

[5] Buchanan, K.E., Mangold, K.C., Laskowski, S. J. (2022). *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities*. NIST Special Publication (NIST SP) 1273 - Executive Order on Promoting Access to Voting. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1273.pdf

[6] The National Voter Registration Act of 1993 (NVRA), Pub. L. No. 103-31, 107 Stat. 77-89. Available at https://www.govinfo.gov/content/pkg/STATUTE107/pdf/STATUTE-107-Pg77.pdf

[7] Janover, W., & Westphal, T. (2020). *Signature Verification and Mail Ballots: Guaranteeing Access While Preserving Integrity—A Case Study of California's Every Vote Counts Act*. Election Law Journal: Rules, Politics, and Policy, 19(3), 321-343. Available at https://law.stanford.edu/publications/signature-verification-and-mail-ballots-guaranteeing-access-while-preserving-integrity/

[8] Vote At Home Institute (2022) *2022 Mailed Out Ballot Use Rates Of Total Registered Voters.* (VAHI, Washington, D.C.). Available at https://voteathome.org/portfolio/2022-mailed-out-ballot-use-rates-of-total-reg-voters/

[9] Elections Performance Index (2023) *Mail Ballots Rejected in 2020*. Available at https://elections.mit.edu/#/data/indicators?view=indicator-profile&indicator=ABR&year=2020

[10] Baumeister, L., Quesenbery, W., Laskowski, S. J. (2023). *Administering Accessible Vote by Mail Systems*. (NIST, Washington D.C.). Available at https://nvlpubs.nist.gov/nistpubs/vts/NIST.VTS.100-1.pdf

[11] Bernhard, M., Benaloh, J., Alex Halderman, J., Rivest, R. L., Ryan, P. Y., Stark, P. B., Wallach, D. S. (2017). *Public evidence from secret ballots. In Electronic Voting*. Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings 2 (pp. 84-109). Springer International Publishing.

[12] ElectionGuard (n.d.). *What is Election Guard?* (ElectionGuard). Available at https:www.electionguard.vote

[13] National Association of Secretaries of State (2023) *Election Administration Needs Data Integrators* (NASS, Washington, D.C.) https://www.nass.org/sites/default/files/2023-02/Enhanced-Voting-White-Paper-NASS-Winter23.pdf

Additional Reading

Government

Electronic Signatures in Global and National Commerce Act of 2000 (E-SIGN), Pub. L. No. 106-229, 114 Stat. 465. https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

Cybersecurity and Infrastructure Security Agency (2020) Signature Verification and Cure Process Available at https://www.cisa.gov/sites/default/files/publications/signature-verification_cure_process_final_508.pdf

IRS (2022) *IRS Statement — New features put in place for IRS Online Account registration; process strengthened to ensure privacy and security* https://www.irs.gov/newsroom/irs-statement-new-features-put-in-place-for-irs-online-account-registration-process-strengthened-to-ensure-privacy-and-security

Receipt of voter's ballot; cure period (2023) AZ SB 1518 Available at https://custom.statenet.com/public/resources.cgi?id=ID:bill:AZ2023000S1518&cuiq=cebcefa4-252a-5dcb-aeb1-7fc87d570de0&client_md=23899911200c24bf8d0cf966383cac49&mode=current_text

Non-governmental Organizations

Orey R, Fernekes C (2021) What's on the Horizon for Remote Voter Identity Verification? (Bipartisan Policy Center, Washington, D.C.). Available at https://bipartisanpolicy.org/explainer/remote-voter-id/

Orey R, Bacskai O (2020) *The Low Down on Ballot Curing* (Bipartisan Policy Center, Washington, D.C.). Available at https://bipartisanpolicy.org/blog/the-low-down-on-ballot-curing/

The Council of State Governments (2022) *Ballot Curing 101*. Available at https://www.csg.org/2022/09/20/ballot-curing-101/

Altamirano J, Wang T (2022) Ensuring All Votes Count: Reducing Rejected Ballots Trends in Mail Ballot Rejections in 2020. (Harvard Kennedy School ASH Center for Democratic Governance and Innovation, Cambridge, MA) Available at https://ash.harvard.edu/files/ash/files/ensuring_all_all_votes_count.pdf?m=1660330598

Disability Advocacy

Disability Scoop (2022) *Voters With Disabilities Face New Ballot Restrictions Ahead Of Midterms* https://www.disabilityscoop.com/2022/04/19/voters-with-disabilities-face-new-ballot-restrictions-ahead-of-midterms/29808/

Living with Disability (YYYY) *Signature Name Stamps*. Available at https://livingwithdisability.info/signature-name-stamps/

United Spinal Association (2020) *United Spinal Files Complaint Against Social Security Administration For Alleged 'Wet Ink' Signature Requirements* https://unitedspinal.org/social-security-administration-complaint/

News

https://www.cpr.org/2022/12/06/colorado-signature-ballot-voting-lawsuit/

Commercial

Docusign (2021) *eSignature Legality in The United States* Available at https://www.docusign.com/products/electronic-signature/legality/united-states/

Docusign (2022) *Making the Signing Experience Accessible to All* Available at https://www.docusign.com/blog/making-the-signing-experience-accessible-to-all

Digisign (2018) *3 Types of Digital Signature* Available at https://digisign.id/eng-3jenisdigi.html

GoConcepts *How Do You Electronically Capture A Signature From Someone Who Has Difficulty Writing?* Available at https://www.itfordd.com/blog/electronically-capture-signature/

Hirschfield A, Dunn S (2021) *6 questions you should ask on a digital identity project* (Public Digital, London UK) Available at https://public.digital/2021/09/09/6-questions-you-should-ask-on-a-digital-identity-project

Journey (2022) *The Many Faces of Authentication.* Available at https://journeyid.com/blog/the-many-faces-of-authentication/

Journey (2022) *Verified??* Available at https://journeyid.com/blog/verified/

Sectigo (2021) *What Are the Different Types of E-Signatures?* https://sectigo.com/resource-library/different-types-of-e-signatures

Signeasy (2022) *The Ultimate Guide to Electronic Signature Verification* Available at https://signeasy.com/blog/business/electronic-signature-verification/