NIST Voting Technology Series
NIST VTS 200-2 ipd

Implementation Guidance for the VVSG 2.0

Multi-Factor Authentication

Initial Public Draft

Ryan Galluzzo
Gema Howell
Andrew Regenscheid
Carter Casey
Chelsea Deane

This publication is available free of charge from:
https://doi.org/10.6028/NIST.VTS.200-2.ipd

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Voting Technology Series
NIST VTS 200-2 ipd

Implementation Guidance for the VVSG 2.0

Multi-Factor Authentication

Initial Public Draft

Ryan Galluzzo
Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Carter Casey
Chelsea Deane
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.VTS.200-2.ipd

January 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Technical Series Policies

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added in final publication]

How to Cite this NIST Technical Series Publication
Galluzzo R, Howell G, Regenscheid A, Casey C, Deane C. (2023) Implementation Guidance for the VVSG 2.0: Multi-Factor Authentication. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Voting Technology Series (VTS) NIST VTS 200-2 ipd. https://doi.org/10.6028/NIST.VTS.200-2.ipd

NIST Author ORCID iDs
Ryan Galluzzo: 0000-0003-0304-4239
Gema Howell: 0000-0002-0428-5045
Andrew Regenscheid: 0000-0002-3930-527X

Public Comment Period
December 5, 2023 – ~~February 5, 2024~~ March 1, 2024

Submit Comments
election-security@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0) modernizes standards for the use of multi-factor authentication in voting systems. This document aims to provide guidance to those who will need to implement the VVSG by reviewing the multi-factor authentication requirements in the VVSG 2.0, putting these requirements in the context of work to be done by vendors and election officials, and discussing the impact that the new standards may have on U.S. elections moving forward.

Keywords

implementation guide; multi-factor authentication; voting; voting system; voluntary voting system guidelines; VVSG.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: election-security@nist.gov.

Table of Contents

Introduction

The Help America Vote Act of 2002 (HAVA) established the Election Assistance Commission (EAC) and tasked it with developing requirements for the functionality, accessibility, and security of voting systems. HAVA also established the Technical Guidelines and Development Committee (TGDC), which is chaired by NIST, to assist EAC in the development of voluntary standards and guidelines related to voting equipment and technologies. In the years since HAVA's enactment, NIST, in partnership with the TGDC, has assisted EAC by providing technical expertise during the creation of voting system requirements and has developed the Voluntary Voting System Guidelines (VVSG).

The most recent iteration of the VVSG and the first major revision, version 2.0, was approved on February 10, 2021. A major goal of the revision was modernization—adapting to new technologies and best practices in voting and elections. There can be challenges accommodating these features in legacy hardware and states may discuss this with their voting technology vendors and consider the impact when developing technology refresh plans. Recognizing that some changes to the guidelines may significantly alter how voting system vendors and election officials operate, NIST has developed this supplemental implementation guide to support their transition to the requirements of the VVSG 2.0.

Purpose and Scope

This implementation guide, and others in this series, provide context for complex requirements, make recommendations for meeting them, and detail any major impacts expected in the coming years. MFA in its many forms can be applied to support a broad range of online and in-person use cases directly impacting the voting experience. From voter registration to absentee voting processes, to election official access to physical voting systems. *While there is substantive value to exploring the full range of MFA applications, this paper focuses exclusively on access to Voting Systems by election officials. It does not cover access by voters to voting systems.*

Specifically, this guide outlines the requirements needed to implement multi-factor authentication (MFA) on voting systems. It starts with background information on what MFA is, the purpose of implementing MFA, and the necessity to implement offline MFA. Section 2 describes the goals of the VVSG requirements for using MFA to mitigate unauthorized access to election systems. Section 3 provides information on common MFA best practices that are used across multiple vendors. Finally, Section 4 outlines what is required of election officials in order to effectively implement MFA.

Scope

The first line of defense for most computer systems is authentication. Authentication is the process by which a user verifies their identity by demonstrating control of an "authenticator" – a mechanism that proves their identity. Authenticators are categorized into three different "factors":

- something you know (e.g., passwords or personal identification numbers–PINs),
- something you have (e.g., hardware tokens or applications), and
- something you are (e.g., biometrics).

Traditionally, authentication is commonly accomplished with a password. Unfortunately, passwords are vulnerable to compromise—malicious actors can use stolen passwords, obtained through phishing (misleading communications), through brute-force (repeatedly trying combinations) attack, or accidental exposure (written on a piece of paper or otherwise left in public view) to gain access to an election system. The best way to mitigate these threats is to implement an authentication scheme that relies on more than one factor for authentication. This is known as Multi-factor Authentication (MFA).

A common example of MFA is when a user first authenticates with a password, then inputs a code from a physical security token or an authenticator app on a mobile phone. The addition of multiple factors into the authentication process blunts the risk of stolen credentials by introducing redundancy. Even if a password is stolen, a second factor can prevent a system from being breached.

Goals of the VVSG MFA Requirements

Previous versions of the VVSG did not contain requirements for multi-factor authentication. At the time that the first version of the VVSG was written, MFA was not as widely used as it is today. Since 2005, MFA has become a standard viewed as necessary for securing systems against phishing and other cyber-attacks. With the heightened risk of external factors (for example, criminal syndicates, politically motivated or hacktivist groups, domestic violent extremists, or adversarial nation state actors) seeking to influence or interfere in the U.S. election process, there is also an elevated concern that targeted threats could be exacted before, during, or after election day. To protect voting systems from modern threats, MFA requirements were included in VVSG 2.0.

Protecting Critical Operations and Administrator Accounts

Two primary areas of voting systems require the heaviest protections: critical operations and administrator accounts. Critical operations are vital to ensuring voting systems are functional during elections (e.g., storing ballot images and tabulating ballots) and include the ability to update the voting system to protect against vulnerabilities (e.g., updating software or altering authentication methods). Administrator accounts have privileged access to implement these critical operations, which is why it is important that these accounts use MFA.

Based on these considerations, NIST recommended two requirements: 11.3.1-B, Multi-factor authentication for critical operations, and 11.3.1-C, Multi-factor authentication for administrators. These, as their names and the discussion above would suggest, require multi-factor authentication for accessing critical operations and administrator accounts. Critical operations are defined in the VVSG 2.0, 11.3.1-B, as:

1. runtime software updates to the certified voting system,
2. aggregation and tabulation,
3. enabling network functions,
4. changing device states, including opening and closing the polls,
5. deleting or modifying the CVRs and ballot images, and
6. modifying authentication mechanisms.

Usable Security

The VVSG is written to help ensure security while not interfering with the work of conducting elections. While MFA is important to securing critical functions and accounts, it adds additional authentication steps, which could impact the election process (e.g., cause delays). Usability testing, included under Requirement 8.4-A, *Usability tests with election workers*, is important to ensure security features like MFA have minimal impact on elections.

Vendor Implementation

Vendors will be responsible for including MFA functionality in their voting systems. Because MFA was not previously required, adding the security feature may require additional planning and preparation. Elections have unique procedures and requirements that vendors will have to take into consideration. These include but are not limited to the following:

- cost-effective solutions due to election offices' tight budgets,
- varying election office system infrastructures, and
- ad-hoc account assignment due to the temporary workforce environment.

Usability Testing

As mentioned earlier, 8.4-A, *Usability tests with election workers*, requires voting system manufacturers to conduct usability testing of the voting system's setup, operation, and shutdown. Usability testing must include election workers, who are the primary users of voting systems. This analysis should include a usability study of the vendor's MFA implementation. The analysis is important because MFA can cause delays and confusion if usability is not considered in the selection of the MFA implementation. Additionally, when recruiting subjects to conduct usability testing, vendors must do in a manner that reflects the demographics and capabilities that would be expected at their polling sites. While this is particularly important for systems that may use biometric technologies as part of their authentication scheme – due to potential deviations in performance based on demographics – it is just as critical to account for availability and familiarity with technology such as smart phones, security keys, and authenticator apps.

Voting Systems Multi-Factor Authentication and Constraints

The VVSG 2.0 states that voting systems must not be configured to establish a connection to an external network or connect to a device external to the voting system (see Requirement 14.2-E, *External network restrictions)*. This means that voting systems must be designed to maintain an air gap from outside systems, which includes any centralized, jurisdiction-wide authentication system and mobile devices. This also means that out-of-band authentication is not permitted because the voting system is unable to communicate with an individual through any networked channel (e.g., email or mobile application).

The VVSG 2.0 also restricts the use of wireless communications. Requirement 14.2-C, *Wireless communication restrictions,* states that voting systems must not be capable of establishing wireless connections. This means that authenticators that use secure wireless connections (e.g., devices that use near-field communication or NFC) cannot be used in a VVSG 2.0 MFA implementation.

These realities constrain the options available for multi-factor authentication.

Authentication Deployment Patterns

Given the constraints imposed by the VVSG requirements, there are two common deployment models that vendors may consider for their voting systems. The first deployment model uses centralized authenticator management over a local area network. I second deployment model is based on local authentication with the user authenticating directly to a specific device. Each model presents its own challenges, constrains and considerations that may impact the types of authenticators and authentication architectures vendors choose to provide.

Centralized Authentication (Local Area Network)

In this deployment model, users and their authenticators are enrolled and managed via a centralized authentication or access server connected to all voting system endpoints. For example, the user would register their PIN and a biometric at an enrollment terminal. When they attempt to access an individual voting device, that device captures their PIN and a biometric sample, which are transmitted and compared to stored information, and an access decision made at the central authentication server before being transmitted back to the local device. Centralized management can be valuable in the event of an authenticator loss or compromise, allowing administrators to revoke lost authenticators and reset them for the authorized users. Conversely, centralized systems inherently require a more complicated architecture and the ability to securely connect to all endpoints in the system. This increased complexity can result in increased costs for successful implementations.

When a voting system architecture includes a local area network, this model provides several benefits. Specifically, centralized management can facilitate the enrollment of users through single event, manage access policies consistently, and provide the ability to rapidly revoke or remove access across all connected devices in a synchronized manner.

Local Authentication (On Device Authentication)

In this model, the enrollment and management of identities and authenticators is handled locally on the specific device to which the user is accessing. For example, the user enrolls a password and a biometric on specific device. When the user returns, they input their passwords and biometric, which are locally compared to stored values, and an access decision made based on those results.

This model is heavily dependent on the features and capabilities of the specific voting devices being used, e.g., integrated biometric sensors, and user management capabilities. This model can provide a manageable, cost-effective approach to implementing multi-factor authentication, particularly for voting system architectures and deployments that have a relatively small number of devices. However, it may be challenging to configure and maintain as the number of devices and users grow. Similarly, this model presents challenges in the event of a compromise of credentials, as a user’s accounts and authenticators would need to be invalidated on each device where those credentials have been enrolled. This could increase the time to remediate a compromise and leave systems vulnerable for an extended period while the user’s access is removed on each impacted device.

Authenticator Options

Due to the constraints mentioned in the previous section, practical options for multi-factor authentication on voting system devices are more limited than those for online or digital applications that allow for the use of network or internet access. Particularly challenging for voting systems is the ability to communicate with the authenticator to enable the exchange of authenticator data. For example, online systems can easily make use of near-field communication (NFC) or text messages to mobile phones to exchange authentication information. However, the restrictions on voting system connectivity limit the types of authenticators to a few primary options: authenticators that allow for user input of information, the connection of authenticators via physical ports (e.g., USB or integrated smart card reader), or the capture of biometric information via integrated sensors (e.g., fingerprint scanners or cameras).

Below are the recommended authenticators that may be integrated into future voting systems.

Memorized Secrets

Description: A memorized secret is commonly referred to as a *password*, or, if numeric, a PIN. These are secret values intended to be memorized by the user and are either selected by the user or randomly generated for each user. Administrators would enter their password on the voting system device, which would be verified either by the device itself or a central server on a local area network before granting administrative access. The requirements in Section 11.3.2 of the VVSG 2.0 address the use of passwords in voting systems, including a requirement to meet SP 800-63B's minimum password length of 8 characters. Find more information in 800-63B under Section 5.1.1 *Memorized Secrets.*

Capabilities and Advantages: Passwords, and other memorized secrets, are broadly supported in software components commonly used within voting systems. As a "something you know" authentication factor, memorized secrets are commonly paired with possession-based authenticators in multi-factor authentication.

Potential Challenges: Passwords are vulnerable to theft and misuse. They can be shared with unauthorized individuals or written down and stored in unsecured locations. If users are allowed to select their own passwords, they may choose passwords that could be easily guessed. Passwords can also be forgotten, requiring a recovery process to reset the password.

Examples: Passwords, PINs, and Passphrases.

One-Time Password (OTP) Devices

Description: OTP Devices generate a series of random characters, used for authentication, that change either based on time or every time a code is used. The device generates these unique codes leveraging a symmetric key and a nonce shared with the authentication server. When the user manually inputs the code generated by the device, it is compared to the one generated on the server to confirm the user is in possession of a valid authenticator (a process known as "verification"). There are two types of OTP Devices: Single Factor OTP devices and Multi-Factor OTP devices. Single Factor OTP devices generate the code and make it available to the user without requiring them to enter another factor to access it (for example a hardware device that displays the code on a screen). Multi-factor OTP Devices require the user to present another factor before displaying the code (for example authenticator applications on a smartphone that require the user to enter a PIN or biometric before revealing the code). Additional information can be found in 800-63 B in Sections 5.1.4 and 5.1.5.

Capabilities and Advantages: Due to their ephemeral nature, OTPs limit the risk of exposure created by more persistent authenticators such as memorized secrets and look-up secrets. As a result, they are less vulnerable to brute force and guessing attacks. They are also widely available and, in the case of authenticator applications, freely available to end-users on their personal or enterprise devices. However, the latter is premised upon the decision to allow the use of mobile devices – particularly personally owned devices – as part of an authentication scheme.

Potential Challenges: The primary challenge of using OTP devices is the enrollment of the authenticator and sharing of the necessary key and nonce information to conduct verification of the authenticator code. This can typically be achieved by one of two ways, depending on the capabilities of the authenticator device. One method involves leveraging a properly formatted barcode, such as a quick response (QR) code, generated by one of the two elements to exchange key information. Such barcodes can be read using cameras on voting system devices or mobile device. A second method involves manually inputting keys from the devices – this can be done in bulk if run centrally or individually if registering locally. The manual input process can present user challenges due to the length of the keys. QR code exchange typically only supports OTP devices that take the form of authenticator apps, which may not be available or authorized for users.

An additional potential challenge for an offline system is that the system must be capable of validating OTPs over an extended period of time. Time-based OTPs (TOTPs) that refresh every 1 or 2 minutes rely on properly synchronized time between voting system devices and OTP authenticators. Maintaining clock synchronization could be difficult in offline environments. However, there are approaches that help to mitigate such problems, as well as OTPs that aren’t timing dependent; they instead change each time the authenticator is used.

Examples: Authenticator Applications, Code Generation Devices.

Cryptographic Authenticators

Description: Cryptographic hardware devices form a direct connection with a system to cryptographically prove the user’s possession of an established secret – specifically a cryptographic key. These can take the form of hardware authenticators – where the symmetric or asymmetric keys used for authentication are stored on a physical device (for example a smart card) or software authenticators where the keys used for authentication are stored on a smart phone or other computing device. Furthermore, cryptographic authenticators can be either single factor – where no additional factor is needed to unlock stored keys – or multi-fa–tor - where an additional factor is required to unlock secured keys (for example with a PIN or biometric).

The connection between a cryptographic authenticator and a computer system can generally be formed in several ways. For example, the authenticator and computer system may exchange information via a physical connection (e.g., USB port or a smart card reader), by manual or optical exchange mechanisms (e.g., QR code), or using wireless connectivity (e.g., NFC or Bluetooth). However, due to restrictions on connectivity and usability considerations, the primary method recommended for voting systems is through the physical connection of an authenticator to the system. Additional information can be found in 800-63B under Sections 5.1.6 – 5.1.9.

Capabilities and Advantages: Cryptographic authenticators provide high assurance in the identity of the end-user as they are unique to that user or device, are computationally challenging to guess due to their use of cryptography, and resistant to phishing when bound to a communication channel or domain. For these reasons they are used for the highest risk use-cases in government and industry.

Additionally, models based on a Public Key Infrastructure (PKI) can ease the burden of enrollment regardless of deployment pattern by allowing for the distribution of certificates and public key information to voting systems in advance of election of activities. For example, all users that require MFA could be issued smart cards whose certificates have been issued from a centralized Certificate Authority that the jurisdiction’s voting system devices have been configured to trust during pre-election activities. This would allow for an issuance process that does not require enrollment at individual voting devices. All could be configured, offline, with the complete certificate and key information associated with the jurisdiction’s users.

These characteristics make PKI-based cryptographic authenticators particularly well-suited for large-scale deployment and use on non-network voting systems. There is a relatively mature ecosystem of commercial-off-the-shelf components and devices, such as smart cards and associated smart card readers, that can be integrated with voting systems to support this multi-factor authentication method.

Potential Challenges: The challenges with cryptographic authenticators are primarily associated with cost and the complexity associated with maintaining appropriate cryptographic capabilities (e.g., certificate authorities, key management). Additionally, physically accessing the system to connect the authenticators is complicated in voting scenarios since the need to secure physical ports – such as standard USB ports – often requires breaking and replacing a physical tamper-evident seal during elections, making regular, operational use of these ports challenging. While smart card readers that are integrated into voting systems could resolve this issue by remaining available when USB ports are sealed, not all voting systems have such integrated components. Finally, cryptographic authenticators may be more expensive than many other authenticator types, although different technologies and products will have varying procurement and maintenance costs.

Examples: Smart Cards, Hardware Keys (e.g., FIDO security keys), FIDO Authentication Apps, and Platform Authenticators (e.g., Passkeys).

Biometrics

Description: Biometrics is the measurement of physiological characteristics including – but not limited to – fingerprint, iris patterns, or facial features that can be used to recognize an individual and authenticate their access to a system. On devices that use biometrics to authenticate users, a local sensor, such as a camera or fingerprint scanner, is used to capture a biometric sample. A biometric comparison algorithm then compares the presented biometric sample against previously enrolled reference characteristics for a given user– a process referred to as one-to-one verification.

The performance of a biometric verification system is typically described in terms of its false match rate (FMR) and false non-match rate (FNMR). FMR is the rate at which the system incorrectly determines that an imposter’s biometric sample matches an enrolled sample. FNMR is the rate at which it fails to determine that a genuine sample matches an enrolled sample.

In commercial devices, biometrics are commonly used to authenticate single-user devices, such as mobile devices. In addition, some multi-factor cryptographic authenticators include integrated biometric sensors to unlock the use of a cryptographic key for authentication purposes.

Capabilities and Advantages: Biometric authentication systems can provide convenient user experiences. They typically do not require the user to carry a physical token that could be lost, nor are users expected to memorize a secret that could be forgotten. Modern biometric authentication technologies can capture and compare biometric samples quickly. Some commercial-off-the-shelf devices contain integrated biometric sensors. In other cases, biometric authentication technologies can be supported with peripherals connected to a device.

Potential Challenges: Biometric authentication systems are nearly always designed for and support only local authentication to a single device. In most cases, biometric data cannot be imported from or exported to other devices. As such, the use of biometric authentication technologies in voting systems would most likely require each voting system administrator to enroll their biometrics manually on each device they may need access to during an election. This could be logistically impractical, particularly in large jurisdictions. Procedures for allowing additional administrators to be enrolled on specific voting devices once deployed at a polling place could mitigate some of those challenges.

NIST research indicates that there are variations in performance between biometric comparison algorithms and across different demographic groups. Various factors can contribute to these deviations in performance, including the algorithm used, the data used to train the algorithm, the camera used to capture the biometric images, the quality of the images, and the environment in which the system is used.

Examples: Face recognition and fingerprint recognition.

Look-up Secrets

Description: A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the user and the system or device they are attempting to access. During the authentication process, the user must look up the appropriate secret from that set based on a prompt from the device. For example, the device could ask the user to provide a code that appears in a specific row and column in a table printed on a card. Each code is single use, which means a list will run out after a certain number of logins. Look-up secrets are simple, but not typically designed for frequent use. Look-up secrets are most used for account recovery in online scenarios. Since they are susceptible to guessing/brute force, loss, or theft, and – due to their replacement after each use – poor user experience, they are not an ideal authenticator particularly when paired with a password. It is therefore recommended that they be an authenticator of last resort – used only if no other form of MFA is viable. Find more information in 800-63B under Section 5.1.2 *Look-Up Secrets*.

Capabilities and Advantages: Look-up secrets do not require voting systems to contain special hardware; they are typically entered by users using physical or on-screen keyboards.

Potential Challenges: Scaling look-up secrets for use across multiple voting system devices could be challenging. If the voting system architecture does not include a central, locally networked server to perform user authentication, administrators may need to use different look up secrets for each voting system device to prevent repetition of individual secret values on look up cards.

Examples: Grid Cards, Recovery Codes, and One Time PADs.

Authenticator Combinations

Multi-factor authentication requires the combination of more than one factor to achieve the desired security properties. There are two common methods by which this can be achieved: either 1) deploying two separate single factor authenticators, or 2) deploying multi-factor devices (e.g., a multi-factor crypto device) that combine two factors into a single authenticator. With the former, it is important to remember that when selecting individual authenticators, the selection of two authenticators of the same factor (e.g., two “something you know” authenticators) does not constitute multi-factor authentication. The table below highlights the different types of authenticators discussed above and groups them into factor types. When implementing, vendors and election officials should select authenticators from two different factor types based on their users, technologies, budget, and operational constraints.

Something you know	Something you have	Something you are
- Memorized Secrets (Password, PIN)	- OTP Device (OTP Hardware, OTP Application) - Cryptographic Authenticator (Security Token) - Look-up Secret (One-time Pad, Grid Card)	- Biometric (face, finger, iris)

Where vendors choose to implement multi-factor devices, it is important to ensure the ability to enforce policy on those devices to preserve MFA. There are two primary approaches to achieving this with most modern authenticators; either a local biometric or an "activation secret" – a password or PIN of at least six characters used only for authenticating to the local device.

For purpose-built authenticators such as smart cards or security tokens (e.g., FIDO keys), implementing two factors on a device can be achieved through the configuration of the devices when procured and activated. For example, mandating a PIN entry prior to allowing the stored key on a cryptographic authenticator to be unlocked for primary authentication. It is particularly important to note that many products offer multiple configurations, and it should not be assumed that an activation secret or biometric is the standard operating mode for the authenticators. Each authenticator should be configured and validated during the registration process to ensure it is operating in multi-factor mode and consistent with a defined policy.

This becomes somewhat more complicated when leveraging multi-purpose devices such as smartphones – particularly if the decision is made to allow for users to leverage personal devices. Often multi-factor authenticators rely on the organic capabilities of smart phones to provide the initial "unlock" factor. With devices that do not include capabilities such as mobile device management (MDM), there may be no means to assure that activation secret or biometric policies are being enforced at the device level for authentication purposes. It is therefore recommended that devices that are intended to be used as multi-factor authenticators be supported by the necessary means to enforce policy on the device – either through MDM or by issuing organizationally owned devices. This is less of a concern where a device is only expected to operate as a single factor in a multi-factor scheme – for example running an OTP application that will be coupled with a password or PIN that will be directly entered into a voting system device.

Election Official Responsibilities

The MFA should not substantially modify the responsibilities of election officials. However, attempts to implement technologies and solutions will require pointed modifications to activities that are already core to the election official's role in securing elections. Specific considerations include:

Procurement & Acquisition: Requirements for MFA need to be built into anticipated procurement and acquisition processes from the start. Understanding a specific jurisdiction's technical capabilities, existing systems, and user population is key to ensure that the MFA systems deployed to support voting systems are appropriate and successful in achieving their desired outcomes. Officials should evaluate their existing systems, planned improvements, and overall resources to develop acquisition strategies for implementing MFA consistent with the VVSG 2.0 requirements. Officials with existing systems should work with vendors to identify MFA capabilities and ensure they are integrated into vendor roadmaps as future capabilities. Where possible, vendor customer support services to address MFA challenges and issues should be clearly defined as requirements within procurement documentation and agreements.

Implementation: Successful MFA deployments are contingent upon a well-defined strategy and structured, tested processes for managing the lifecycle of authenticators. Perhaps most critical, Election Officials need to ensure that there are well defined processes and procedures for issuing, registering, activating, and de-activating authenticators to end-users. The exact mechanisms by which this is achieved will depend on the capabilities of voting systems and the authenticators chosen for a given implementation. At a minimum though, these processes must be defined, documented, and tested prior to scaled implementation to ensure the integrity of the authentication process and identify potential performance challenges.

Training: Security is dependent on understanding, and MFA is no exception. To support successful implementations, election officials will need to provide a comprehensive training program to teach users both the technology being deployed and its value in protecting election processes. Furthermore, training should be augmented by tools, job aides, and other artifacts to support user awareness and self-service to the extent feasible. Administrators and system owners should be well versed in the technology and troubleshooting well in advance of major election events. Tabletop exercises that include authentication failures should be planned and executed to promote readiness and improved processes. Vendors should be included in tabletop exercises and consulted as part of training programs when feasible.

References

Help America Vote Act of 2002 (HAVA), Pub. L. No. 107-252, 116 Stat. 1666- 1730. https://www.govinfo.gov/content/pkg/STATUTE-116/pdf/STATUTE-116- Pg1666.pdf#page=62

U.S. Election Assistance Commission (2021) Voluntary Voting System Guidelines. (EAC, Washington, D.C.). Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

Anti-Phishing Working Group (2023), Phishing Activity Trend Reports, Available at https://www.antiphishing.org/trendsreports

Grother P, Hanaoka K, Ngan M (2019) Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8280. https://doi.org/10.6028/NIST.IR.8280

Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63B

Appendix A: Referenced VVSG 2.0 Requirements

This appendix includes a quick reference to the VVSG 2.0 requirements that are mentioned in this document.

8.4-A – Usability tests with election workers

The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.

The tasks to be covered in the test must include:

1. Setup and opening for voting, which involves:
    a. operation during voting;
    b. use of assistive technology or language options that are part of the voting system;
    c. shutdown at the end of a voting day during a multi-day early voting period, if supported by the voting system;
    d. shutdown at the end of voting including running any reports;
    e. providing ballots in different languages;
    f. selecting the correct ballot type (for example, for vote centers); and
    g. setting up the voting system to use different display formats and interaction modes.
2. The test participants must include election workers representing a range of experience.
3. The manufacturer must submit a report of the results of their usability tests, as part of the TDP using ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].

Discussion

Voting system manufacturers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible voting system. This requirement covers the procedures and operations for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition or system repair. These "normal" procedures should not require any special expertise. The procedures may require a reasonable amount of training, similar to the training generally provided for temporary election workers.

Related requirements:	2.2-A – User-centered design process
	7.3-O – Instructions for election workers

11.3.1-B – Multi-factor authentication for critical operations

At a minimum, the voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:

1. runtime software updates to the certified voting system,
2. aggregation and tabulation,
3. enabling network functions,
4. changing device states, including opening and closing the polls,
5. deleting or modifying the cast vote records and ballot images, and
6. modifying authentication mechanisms.

Discussion

NIST SP 800-63-3, *Digital Identity Guidelines* [NIST17c] provides additional information useful in meeting this requirement. NIST SP 800-63-3 defines multi-factor authentication (MFA) as follows:

"An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are.

Multi-factor authenticators include, but are not limited to the following:

- Username & password
- Smartcard (for example, voter access card)
- iButton
- Biometric authentication (for example, fingerprint)

Multi-factor authenticators can be tested for usability to ensure an appropriate balance of security, usability, and functionality. A significant impact to usability may require revision of the multi-factor authenticator implementation.

Related requirements: 8.4-A – Usability testing with election workers

11.3.1-C – Multi-factor authentication for administrators

The voting system must authenticate the administrator with a multi-factor authentication mechanism.

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-e by requiring multi-factor authentication for the voting system administrator group or role.

Prior VVSG source: VVSG 1.1 - I.7.2.1.2-e

14.2-C – Wireless communication restrictions

Voting systems must not be capable of establishing wireless connections as provided in this section.

Discussion

Wireless connections can expand the attack surface of the voting system by opening it up to overthe-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired. Examples of how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, or
- removing wireless hardware within the voting system.

This requirement does not prohibit wireless hardware within the voting system so long as the hardware cannot be used e.g. no wireless drivers present.

This requirement applies solely to voting systems that are within the scope of the VVSG. It is not a prohibition on wireless technology within election systems overall. This requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack.

Related requirements:	8.1-E Standard audio connectors 15.4-C – Documentation

14.2-E – External network restrictions

A voting system must not be configured to:

1. establish a connection to an external network, or
2. connect to any device external to the voting system.

Discussion

The basic instructions provided by a vendor should clearly indicate that the intended use and installation of voting systems implements an air gap between the voting system and external networks or external devices. This requirement is intended to limit the voting systems attack surface and disallow connections of the voting system to technologies such as:

- e-pollbooks,
- public switched telephone networks (PSTNs), and
- cellular modems.

In particular, connections to the internet expand the attack surface even further than other wireless technologies because the data traverses over the internet, which reaches all over the world. This type of access allows a malicious actor to attack from various distances, meaning they do not have to be in close proximity of a polling place or near a specific jurisdiction. Exposure to the internet could allow nation-state attackers to gain remote access to the voting system. With remote access an attacker may be able to view all files within a voting system and make modifications to files within the voting system. These files may include election results and ballot records.

This type of exposure could also make voting systems vulnerable to ransomware. Ransomware is a type of malware that could deny access to election data or functionality, usually by encrypting the data with a key known only to the hacker who deployed the malware. Ultimately an attacker could render a voting system non-operational until a ransom is paid.

Related requirements:	15.4-B – Secure configuration documentation