VERITY®
knowledge base
article #17 in a series

HART intercivic

Verity Security Features

About this Document

Verity system security was designed following the most current best practices in voting and computer technology. In addition, Verity has been thoroughly tested by a voting system test laboratory (VSTL) accredited by the U.S. Election Assistance Commission (EAC), to ensure proper security and software functionality. The Verity system provides security in depth, with multiple, overlapping levels of physical and digital security features combined with comprehensive auditing capabilities. This document explains several of the most important security features of the Verity system, including:

- Device Physical Access Controls
- Kiosk Mode
- Device Secure Boot Process
- Whitelisting
- Tamper Evidence
- User Authentication
- Audit Logging
- Vote Security

Device Physical Access Controls

Non-standard physical connections are used for external ports on Verity devices, including the USB ports used for Verity Touch Writer printers, and the Verity Controller & Touch DRE booth connection cables. The use of non-standard port connections prevents unauthorized users from inserting any standard or commercial of-the-shelf cables or devices. In addition, the physical ports use non-standard wiring, which prevents any non-Verity device from being recognized.

As an added security measure, integral sliding port covers are included that may be secured with tamper-evident seals by the jurisdiction when the ports are not in use. Tamper-evident seals may also be fastened to the Verity device handles, and on locations that store ballots or vote data (for example, the vDrive compartments on Verity Scan or Controller and the external doors on the Verity Ballot Box). In addition, keyed locks are used to prevent unauthorized access to the vDrive compartment, ballot box, and device cases.

Kiosk Mode

All Verity workstations and voting devices operate in what is known as kiosk mode. In kiosk mode, users can only work in the Verity voting applications, thus preventing access to the desktop or operating system of the computer or device. This prevents introducing unauthorized applications to the computer, prevents malicious changes to the operating system itself, and enhances overall system security. Because of this enhanced security, all tasks that involve transfer of data to or from an external source (importing data, exporting data, saving archives, etc.) must be completed using external USB data storage devices.

Device Secure Boot Process

Software startup for each Verity voting device may take several minutes, due to security and data integrity checks performed by the Verity software. This process is included in the design of the Verity voting system to verify the authenticity of the software before allowing it to operate on the device, and is known as a secure boot process. The secure boot process includes write-protection technologies to prevent the installation of viruses and malware, and employs integrity checks on all software applications before they are allowed to run. These integrity checks validate that the software is in fact the trusted, authorized program (and not a malicious program with the same name).

Whitelisting

Whitelisting is the practice of limiting the applications that are permitted to run on a system. If a particular application attempts to execute on a system that uses whitelisting, the system checks the application against a list of permitted applications (the 'whitelist'). If the application is not on the list, the system prevents it from running. Verity workstations and devices use a whitelisting process to block all unauthorized applications from running on the system.

Whitelisting is the opposite of **blacklisting**, which is the method used by many antivirus programs. In blacklisting, certain applications that appear on a list (the 'blacklist') are blocked, while any that do not appear on the blacklist are allowed to run. The blacklist must be constantly updated as new threats emerge, and often cannot provide protection until after the system may already be infected. The disadvantage of blacklisting is that it is 'reactive' (responding only to viruses, applications, and malware that are already known to be a threat), while whitelisting is proactive (responding to *any* new threat that may occur, and eliminating the need to constantly update the list of malicious applications that must be blocked). Whitelisting allows the Verity system to protect itself both against the threats that exist today, as well as those that may exist in the future, without the need for the computer to be updated via the internet or any other means.

Tamper Evidence

All Verity software on Verity workstations and voting devices is tamper evident; any attempts to alter the function of the software would be evident when tested. Testing may be performed at any time, using built-in functionality that allows the user to export the **Hash Values** of the installed software on both Verity workstations and voting devices. A Hash Value is the digital 'fingerprint' of a software application; Hash Values can be externally compared to the trusted software build on file with the Election Assistance Commission (EAC), to ensure that the installed software is identical to the software certified by the EAC. For more information on **Hash Testing**, see the Verity Knowledge Base article *Hash Testing for Verity Software and Devices*.

In addition to the tamper-evidence of the software itself, Verity digitally signs certain data (e.g. election definition files, vDrives, etc.) to provide tamper evidence while maintaining transparency.

User Authentication

Verity applications are designed to ensure that they are accessible only by authorized users. Authorized users, in turn, are required to identify themselves using a login name and password prior to gaining system access.

Authorization

Role-based permissions determine the operations that each user can perform. Only users with the proper privileges can view or change data. Administrators assign a **user role** to each user, ensuring that each user has access only to the abilities and information authorized by the administrator.

Passwords and Authentication

In addition to an assigned user role, each Verity user also has a unique login name and password. Verity password management rules are modern and flexible. When each user logs in, Verity ensures that the user name and password are valid before the user can access the software. An administrator can configure user accounts for Verity in each jurisdiction. Hart recommends that all jurisdictions follow standard security best practices in regards to password complexity and the storage of user credentials.

Verity Key

Verity Key is a small security device that election staff program for each election. An authorized user must write a Verity Key for *each* new election, making the Key specific to that election. User passwords for Verity Key may be election-specific and user-specific.

Verity Key is part of the Verity Voting **two-factor authentication** process. Two-factor authentication requires that each user have something (a programmed Verity Key, inserted into the workstation or device) and know something (a relevant passcode associated with the Key). Verity must authenticate both the user passcode and the Verity Key together. Each Verity Voting application requires the Key before allowing certain operations to occur. Critical operations within the Verity Voting system require the user to insert the Verity Key and enter the passcode. Only when the Verity system authenticates the Verity Key and password will it allow the operation to continue.

Audit Logging

Verity records comprehensive logs for all activity performed in the Verity Voting system, as it occurs. Each Verity component (application or device) maintains its own log. Logs are a critical part of maintaining security by providing an audit trail. Logs are created uniformly across applications and voting devices.

Each Verity component writes two logs:

- **Audit log**: Contains election-specific logging events, such as any changes to an election and any exceptions or errors encountered in the application.
- **System log**: Contains events pertaining to system actions such as logins, password changes, etc.

Reading Audit and System Logs

Verity Audit and System logs use plain language, and are designed to be clear and easy-to-read. Audit logs allow the auditor to clearly see a list of events, the time the events occurred, and the user logged in when the event occurred. Log data includes the following information:

- The Verity application name and full version number (in header)
- The election ID (in header)
- Information for each event:
  - The date and time when the event occurred
  - The voting device serial number or workstation ID
  - The user logged in at time of event
  - The event name (in plain text)
  - The event details (in plain text)

Users may export application Audit Logs and System at any time, for the desired date/time range, from the appropriate workstation. Users may filter and export Device Audit Logs from Verity Count. Users can export logs as comma-separated values (CSV) to allow for external data searching and additional filtering.

Vote Security

The ballot choices of each voter are stored in the Verity System as Cast Vote Records (CVRs). To protect voter privacy, CVRs are not stored in any discernable order. In addition, CVRs do not contain voter information connecting a ballot (or CVR) to a specific voter. The use of digital signatures makes CVRs tamper-evident. CVRs are stored in multiple locations for security and auditability, risk mitigation, and disaster recovery. Users can filter and export CVR data for external auditing purposes using the Verity Count Auditing Dashboard. CVR data may be filtered by any one or a combination of several criteria, including location (polling place, precinct, or district), voting equipment type, voting type, and ballot content (contest or choice).