Hart Verity Voting 2.5

The Hart Verity Voting 2.5 election system was examined at the Secretary of State's Election division office starting on Monday, 1/4/21 through Friday, 1/8/21. Much of the examination was done remotely due to the ongoing Covid-19 pandemic. I spent a day on site to examine and test the equipment.

The 2.5 release was certified by the Federal Elections Assistance Commission (EAC) in September 2020. Release 2.5 is a modification to the 2.4 release which was certified in Texas in 2020. Jurisdictions interested in this system are advised to review the findings outlined in my report for the 2.4 release.

The major changes to this release are the upgrade of the MS-Windows operating system (OS), the upgrade of the database software, and the introduction of a new voting device, the Touch Writer Duo Standalone, and a new carrier container to facilitate curbside voting.

The following table lists the Verity 2.5 components used for the examination.

Table 1 - Releases for Proprietary Software Components

Software	Version	Location
Verity Data (data management)	2.5.0	central
Verity Build (election definition)	2.5.0	central
Verity Central (central bulk high-speed scanner)	2.5.1	central
Verity Count (tabulator/accumulator/reporting)	2.5.0	central
Verity Scan (precinct scanner)	2.5.1	polling location and/or central
Verity Touch Writer (BMD)	2.5.1	polling location
Verity Touch Writer Duo (BMD)	2.5.1	polling location
Verity Touch Writer Duo Standalone (BMD)	2.5.1	polling location
Verity Touch (DRE)	2.5.1	polling location
Verity Controller (used to activate and record votes of daisy chained devices)	2.5.1	polling location
Verity Print (ballot on demand)	2.5.1	polling location
Verity Relay (Data transmission software)	2.5.0	polling location

For a detailed listing of all the hardware components and applications (including COTS) used in the 2.5 release please refer to the EAC's certification test report.

Findings

- The responses provided on Form-101 are acceptable.

- The Technical Data Package (TDP) documentation provided appears to be adequate.

- The system limitations specified in the EAC's Scope of Certification document are acceptable.

  The system supports either 3000 or 2000 precincts depending on whether it has a 64GB vs 32GB configuration. This is adequate for Harris and Dallas counties.

  The single sheet ballot limit on a vDrive for Verity Scan has been increased to 25,000 to support a long early voting period.

- The pre-marked and the manually voted test ballots were recorded and tallied correctly.

- Accessibility testing worked well except on a Duo machine. The audio ballot was not working until the device was rebooted. The audio ballots should be tested on each device prior to opening the polls. This would normally be done in the warehouse.

- The significant COTS software changes to the system are:

  1. EMS workstations: Windows Embedded Standard 7 OS is being replaced with Windows 10 Enterprise 2019 LTSC. The database engine SQL Server 2012 has been replaced with SQL Server 2017.

  2. Precinct devices: SQL Server 2012 is replaced with SQLite 3.29.

- Verity Relay is not sold or used in Texas. It cannot accidentally be used because it requires different firmware and a modem in the Verity Scan devices.

- The Verity Print (BMD) is outside of the certification scope. It is used to print a regular paper ballot for any ballot style on demand at a voting location.

- Straight-party voting would have to be configured in Verity Build during the election setup if the law changes. If it was accidentally configured, it would be obvious during the ballot print preview.

- Two-factor authentication: 1) a Verity key, and 2) a password is needed for all critical operations, such as tabulating votes.

  The system's security was also enhanced by including the path and names of the files in the digital signatures of the files. This will provide evidence if a file was moved (change of path), or if a file or folder was renamed within a vDrive.

- The system software was successfully built and the hash values were verified to match the values of the executables sent from the EAC. A jurisdiction should have one person do the hash creation and export, and another person to do the comparison, so that they are not relying on a single person to validate the software.

  Software validation is done by running a program within the Verity system to produce hash values of only executable files. The process to produce the hashes is fairly straightforward for both the EMS servers and the precinct machines. The program creates a sha256 hash in base-64 representation for each of the exe's and dll's and is written to a manifest file. According to the documentation, the jurisdiction should request the *Verity Production_Validated_Manifest.zip* archive file for their software release from the EAC. That file contains hashes produced by the VSTL using the trusted build of the release at the end of the federal testing campaign. A 3rd party program (hashCompare.exe was used during the examination) is used to compare the manifest file generated by the VSTL to the manifest file generated by the jurisdiction. It compares the manifest files in total, not each executable's hash. If the hash for one of the executables is different, the comparison will fail indicating that the software is not the certified software.

  Because the file of hashes is generated by both the VSTL and a jurisdiction using Verity software, it is a violation of the EAC's VVSG requirement which states: *"The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer."*

  The hashes should be generated with a tool outside of the Verity system even though the Verity system is using a COTS library to produce the hash. The VSTL, which has the technical expertise, should develop a tool to generate the hashes without any Verity software. I think if the manifest file was created by the VSTL without using the Verity software, it would serve the purpose of the requirement to validate that the software on the jurisdiction's machines is the same as what was certified by the EAC.

  The non-compliant software validation needs to be corrected. However, I do not believe this should prevent certification of this release. All vendors need to improve their validation process. Software validation should be easy to run so that it is used not just after the system is installed, but before and after each election.

- PVR records list all races, but only the voter's selections. If no selection is made, it is indicated on the PVR. All PVR's are scanned using OCR.

  Both PVR and regular ballots are verified to be for the correct election before scanning by the central and precinct scanners. The election's ID is stored in the bar code for regular paper ballots, in a QR code for the PVR ballots.

  Scanners can read both PVR and regular ballots. A Verity Central scanner needs to be told the type of ballots to be processed for each batch of ballots. However, it can be configured with the default type so that the scanner doesn't have to switch the read mode. The Verity Scan precinct scanner determines the ballot type automatically.

- If a precinct machine has a catastrophic failure (i.e. system alert from hardware failure), an election worker can create a recovery vDrive and export temporary logs to a USB stick. When an alert happens, the system locks everything down and an error is presented on the screen. If a precinct machine has a vDrive, it will contain the logs. If there is no vDrive installed in the machine (e.g. Duo's connected to a Verity controller), the logs are written to "temporary logs". The recovery vDrive option captures the logs which can enhance disaster recovery and to assist in diagnostics and troubleshooting.

- The new voting device added to the election system is the Verity Touch Writer Duo Standalone.The standalone's voting UI (user interface) is the same as the older Duo except aVerity Controller is not used. Therefore, it may be a cheaper solution for small counties.

  A regular Duo cannot be used for a standalone Duo. There is a difference in the firmware.

  Both types of Duo's can be connected to the new Duo Go carrier for curbside voting. The Duo Go is a container that has a printer (see photo below). A poll worker sets up the Go carrier with a Duo tablet and inserts a blank PVR ballot stock sheet in the printer before bringing it to the curbside. After voter votes, the printer prints the PVR. Since the PVR is taken to a Verity Scan to be read, a privacy envelope or other means is necessary to protect the voter's privacy.

  The Duo Go can be used with either the Duo standalone or the regular Duo.
  A poll worker needs to initialize each voting session. For the regular Duo, the ballot style is loaded from the Verity Controller. The Duo standalone gets the ballot style from its vDrive.

  Because a Duo needs to be reinserted into its base station for each voter to initialize a new voting session, the Duo Go is better for low volume curbside voting. The Verity Touch (DRE) can also be used for curbside. The Verity Touch (DRE) might be a better option if curbside voting is used frequently.

  Duo Go carrier's usb port is used to send data to the printer, and if equipped, accept input from disability devices.

- Verity Central is used to resolve voter intent for undervotes and overvotes. Write-ins can be adjudicated in Verity Central or Verity Count, but it seemed to be easier in Verity Count.

- If a voter needs a provisional ballot, the poll-worker at the check-in desk will click a box to designate it as such. The provisional ballots are flagged as such in the QR code for the PVR's or the bar code on the regular paper ballots.

  Provisional paper ballots, both regular full-face and PVR's cannot be scanned in the precinct. If the voter accidentally tries to insert their ballot into a Verity Scan machine an error is displayed (see photo below).

- Votes can be added manually in Verity Count. This should be done only when 2 people are present. Any report indicating where ballots were cast should indicate the manual entry. This is not the case currently and so manual entry could be missed. The manual entry operation is logged in the election log, but this is not sufficient since the log is typically long and a manual entry line could easily be missed.

  For the DRE voting on the Verity Touch, the electronic CVR record is flagged as a provisional ballot and must be dispositioned in the Verity Count program in order to be processed. The public counter on the Verity Touch is not incremented. Jurisdictions need to be aware of this if they are comparing the number of signatures on the voting location's signature roster to the number of ballots cast at that location.

- If a new Verity Controller is needed, a new vDrive is needed because vDrives are married to the device that it is first inserted into. vDrives are generic until they are inserted into a device. They can be used on any device that requires a vDrive.

- Ballots from an old election are not accepted by Verity Scan or Verity Central scanners. All ballots are read, but those from the wrong election were not scanned. The report for the batch includes the rejected ballot(s) position(s) in the stack.

- Logs are not searchable from within the Verity System. They must be exported to search. It is important to look for errors throughout the election processing, so it should be easy to search the log without the need to export.

  Manual entry of votes does not create a CVR (cast vote record). The votes are added directly to the database. Manual entry needs to be prominently reported so that it is not missed by anyone reviewing the results by device type. Current reports do not show this.

- The Verity workstations are booted into kiosk mode by default. It is necessary to toggle a setting in Verity and reboot in order to access the Windows operating system.

  The Workstations use mirrored drives to make sure that the election data is safe from corruption due to hardware failure.

- On the day I was onsite I accessed the MS-Windows operating system on a Verity Count workstation. The access to OS was logged in the Verity system log file (see photo below). You cannot determine everything that might have been done because regular Windows commands are not logged. However, I believe the digital signing of data files would prevent undetected manipulation.

  For example, I was able to modify the Verity system log using MS Notepad and then save it. Verity indicated that system log was corrupted when workstation was booted back into Verity (see photo below). I also attempted to run a SQL editor program that I had on a thumb drive. I was prevented from running the program.

- The SQL server database is protected by a random generated password. It is only known by Hart.

Conclusion

The Verity Election System, Release 2.5 is a solid update to the 2.4 release. There are no issues that should preclude a jurisdiction from upgrading, or using the 2.5 release for the initial installation of the Verity system. I recommend that it be certified.
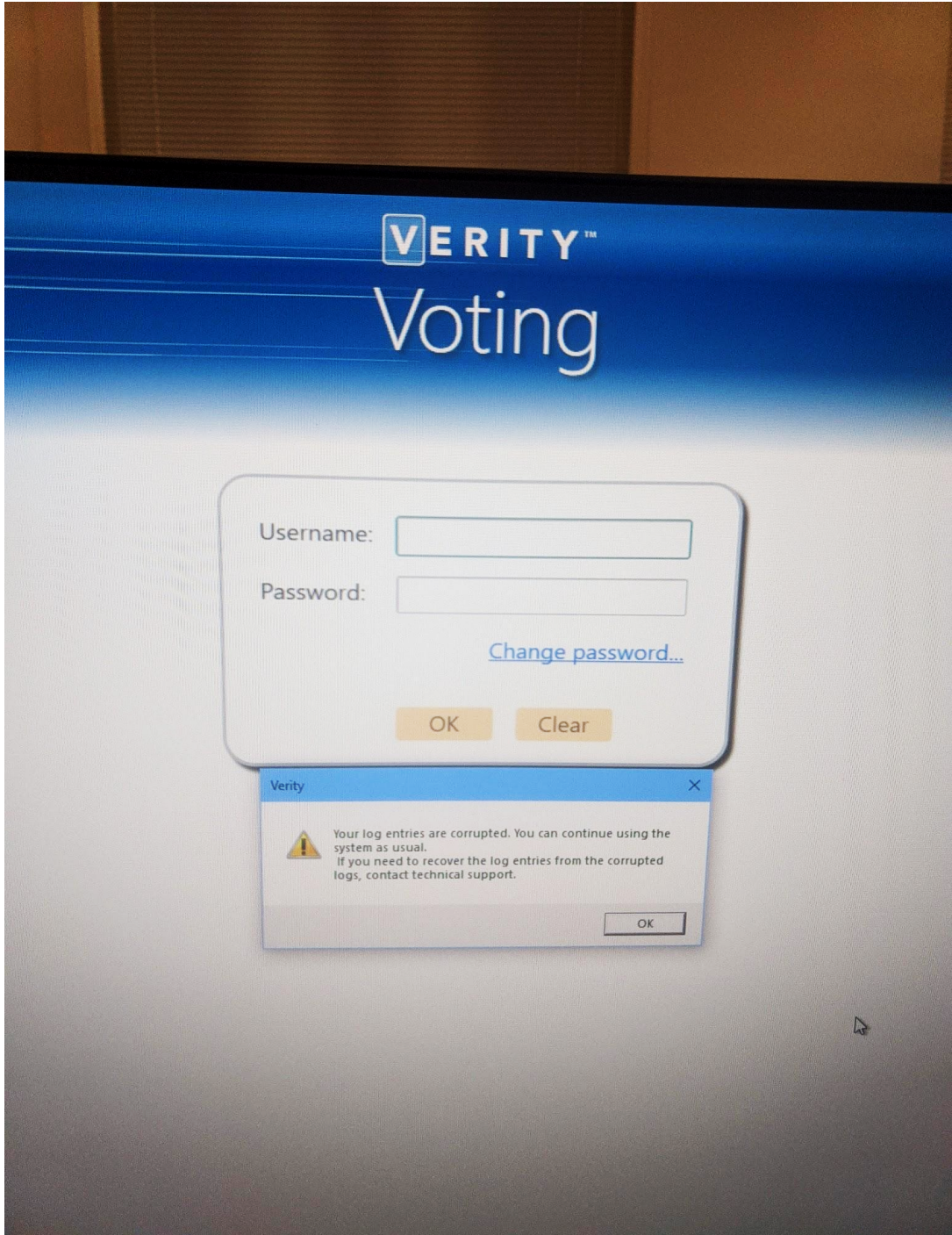
Tom Watson
Examiner

Photos
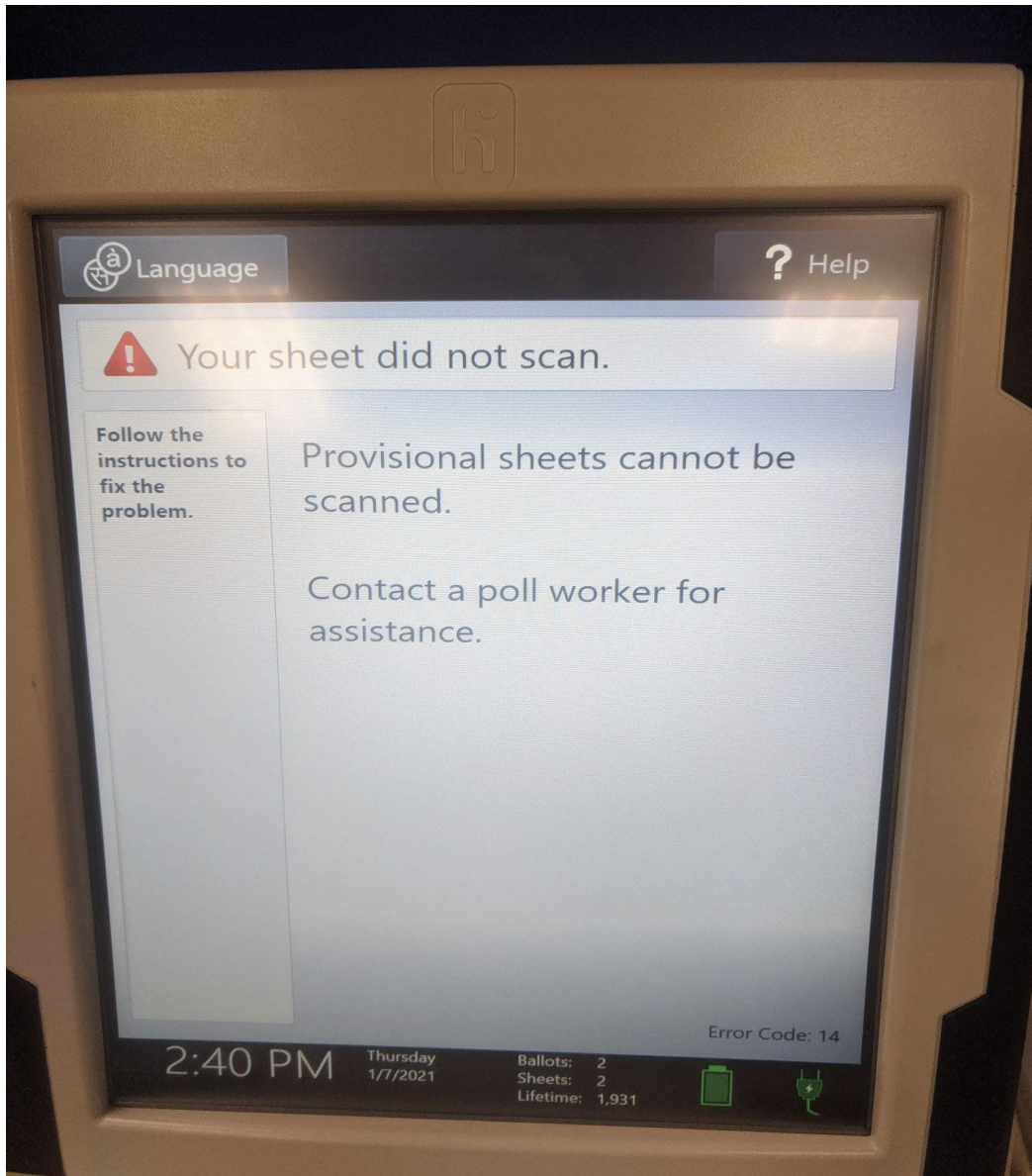
Error message displayed when trying to scan provisional ballot into Verity Scan machine

Duo Go carrier for curbside voting.

Error message indicating that the log file was corrupted.

		The system is shutting down
0	Starting up	The system is starting up
0	Current Certificate Set	Name: J; details: 9A 48 37 BF 70 7C B1 6F A4 BD 99 F3 39 FC B7 2F C5 7D 74 5B
0	Error occurred	The previous Log file is Corrupted
0	Error occurred	Renamed corrupted log file system.D1400000112.log to system.D1400000112_2021-01-07-11-55-58-520967.CorruptedLog
0	View loaded	View name: 'Your log entries are corrupted. You can continue using the system as usual. If you need to recover the log entries from the corrupted logs, contact technical support.' message box
0	Button pressed	Button name: OK
0	User Authorization	User 'user' log in is successful
0	Application opened	

Corrupted log file entry in the log.