Hart Verity Voting 2.7

The Hart Verity Voting 2.7 election system was examined at the Secretary of State's Election division office on 3/1/23 and 3/2/23. An additional day (7/6/23) was spent at the Hart facility to examine and test the Verity Transmit sub-system.

The 2.7 release was certified by the Federal Elections Assistance Commission (EAC) in June 2022. Release 2.7 is a modification to the 2.5 release which was certified in Texas in 2021. There was a Verity 2.6 release, but it was not submitted to Texas for certification. This report will cover the significant changes since the 2.5 release. Jurisdictions interested in this system are advised to review the findings outlined in my report for the 2.5 release.

The major changes to this release are:

- The proposition text can now be wrapped on the paper ballots.
- Multiple users can simultaneously adjudicate the write-ins votes on ballots.
- A redesign of the Count dashboard for election night when processing the precinct vDrives.
- 7 new languages were added to the system.
- The ballot instructions fields have been increased, and there can be different instructions for paper and electronic ballots.

The following table lists the Verity 2.7 components used for the examination.

Table 1 - Releases for Proprietary Software Components

Software	Version	Location
Verity Data (data management)	2.7.1	central
Verity Build (election definition)	2.7.1	central
Verity Central (central bulk high-speed scanner)	2.7.1	central
Verity Count (tabulator/accumulator/reporting)	2.7.1	central
Verity Scan (precinct scanner)	2.7.1	polling location and/or central
Verity Touch Writer (BMD)	2.7.1	polling location
Verity Touch Writer Duo (BMD)	2.7.2	polling location
Verity Controller (used to activate and record votes of daisy chained devices)	2.7.2	polling location
Verity Touch Writer Duo Standalone (BMD)	2.7.1	polling location
Verity Print (ballot on demand)	2.7.1	polling location
Verity Transmit (Data transmission and receiving software) This release Includes ECO-1605	2.7.4	remote regional and central locations

For a detailed listing of all the hardware components and applications (including COTS) used in the 2.7 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 did encounter some navigational issues which can be reviewed in the legal examiners' reports issued by the Secretary of State.

  The audio ballots should be tested on each device prior to opening the polls.
- The system uses two-factor authentication for securing access: 1) a Verity key, and 2) a password is needed for all administration tasks (e.g election definition, tabulation, reporting).
- The system software was successfully built and the hash values were verified to match the values of the executables sent from the testing lab (VSTL). 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.

  Validation is necessary to make sure that the software on the jurisdiction's machines is the same as what was certified by the EAC.

  Software validation is done by running a program within the Verity system to produce hash values of only the 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 software at the completion of a federal testing campaign. A 3rd party program 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, which indicates 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 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.

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 could be used before and after each election. Not just after the system is installed.

- Election setup and ballot design and layout is done in Verity Data. Once the ballot definition, etc. is finalized, the election is locked. Until the election is locked it is not available in Vertify Build. Build is used to create media for devices. Elections are defined as either a Duo or Touch Writer election, not both.

- There have been situations in Texas where a candidate short name for Duo devices is not correct. Anytime the full name is created the short name is auto-generated. This short name should be reviewed and updated if needed anytime the long name is edited. Not just the first time. This could also happen if Hart is contracted to create the election definition.

- When a new election is created it is automatically given a new, unique election ID.

  If a new election is created from a previous election (to preserve precincts, etc.), it is easier to modify the races and delete the candidates outside of the Verity software (i.e. using a text editor), and then import the files back into Verity Data.

  A vDrive is married to a scanner once it is inserted in the scanner. You have to use the same Scan if the vDrive is pulled from the scanner. Normally, a vDrive is not removed from the Scan device until the polls are closed. A vDrive cannot be reused once the poll is closed.

- For early voting, the Scan devices are suspended - not closed. Polls cannot be closed until the defined date/time. Once a Scan is closed it cannot be reopened. Scan devices which are designated for early voting, cannot be used on election day unless the device is reconfigured with a new vDrive. Early voting Scans should not be closed because of the need to get precinct results tape, which cannot happen until the polls are closed.

The election definition must be configured to automatically print the result tape when the polls close. Otherwise the precinct tape cannot be printed as required by law.

- The votes (CVR's) are stored on the Scan devices not the Duo devices. The Duo Controller has the logs for each Duo that is connected to it, as well as its own log.

  The ballot images are also stored on the vDrives, but the election must be configured to do that. For paper ballots, Scan automatically stores snippet images of write-in votes so that they can be adjudicated. On the Touch Writer and Duo's, write-ins are inputted with a virtual keyboard so there are no hand-written write-ins.

- If a vDrive is nearing capacity, another Scan and new vDrive should be swapped in. The same scanner shouldn't be used because seals would have to be broken.

- The Scan devices have a CFast internal disk for data redundancy. A 2nd vDrive can be used in the Scan devices which will serve as a secondary copy of the election definition and the ballots cast on the device. Scan can be used without a 2nd vDrive, however if using Verity Transmit, it is required.

- The standalone Duo voting device does not tell you to take the printed ballot when a voter has finished making their selections. After printing the ballot, it says it is "ready to vote" again. This is the same message when the audio ballot is used. This is confusing. A screen or audio message should say something like, "Ballot printed, take ballot to scanner to cast vote".

- The messaging is not consistent between daisy chained Duo's and the standalone Duo. This may be because the daisy-chained Duo's are on release 2.7.2, and the standalone Duo is on release 2.7.1.

- As stated earlier, early-voting Scan devices can be put in a suspended mode. This allows the vDrive to be removed and then be imported to Count. Then it can be reinserted in the same polling place scanner and the poll unsuspended so voting can resume. This is how early voting ballots can be imported into Count before election day, and still have the scanner results tape printed on election day. If the election was closed on the scanner, the result tape would print automatically. It should not be printed before election day.

  A similar process could be used for reading mail-in ballots at a central site by a small (i.e. registered voters) county which doesn't need the capacity of the Verity Central scanner.

  At the Count workstation, early voting vDrives are uploaded to do the write-in adjudication before the results are tabulated. This allows a large county (over 100k population) to utilize the 4 days between the close of early voting and election day.

- There is a ballot sequential numbering option that provides a sequential number printed on the unvoted ballots. This potentially could violate voter privacy. The better option is

the unique ballot number option in Verity Build. This will generate a unique ballot number for each ballot. The number will be included in the ballot's barcode. The numbers are not serialized and are not associated with voters. The number will prevent scanning of duplicate paper ballots into the same sanner.

- **Verity Transmit Findings**

    - The examination and testing of Verity Transmit was done on 7/6/23 at the Hart facility in north Austin.

    - The purpose of Verity Transmit is to get unofficial results as soon as possible. It is a separate product, run on a dedicated Transmit device, to transmit unofficial CVR's from the Scans' backup vDrives, from remote regional centers to the central site. The Transmit sub-system is intended for large (i.e. registered voters), as well as counties with remote polling places. However, Transmit does add a significant amount of complexity to the processing on election night. Jurisdiction should consider this optional capability carefully before deciding to purchase it.

    - The Transmit software was built from source and the hashes of the for the transmit devices and central servers were good. The transmitting device looks similar to the other Verity polling place devices. The receiving station is an HP workstation.

    - The "official" results matched the "unofficial" transmitted results for the examination.

    - For Transmit, the election must be configured for 2 vDrives in a Scan device. When the poll closes, the Scan device writes to both vDrives. The 2nd drive is not a recovery drive, which is created only if the primary vDrive is lost or corrupted.

    - When a secondary vDrive is inserted into a Verity Scan device, the primary vDrive is duplicated to the secondary vDrive. The secondary is then used to send the CVR's using Transmit from a remote regional site back to the central site Transmit receiving station. The receiving station can then copy the data onto a new vDrive to be uploaded into a backup (unofficial) Count system.

    - The 2 Verity Count servers at the central site should be physically separated; sufficient to keep the unofficial vDrives, created on the receiving Transmit server separated from the official (primary) vDrives, which are driven to the central site from the polling locations. The primary vDrives are loaded into the official Count machine, the secondary vDrives are loaded into the unofficial Count machine.

    - When a remote transmission occurs, the data is stored in a file on the server. The file's digital signature is verified. The file is then automatically written to a vDrive if the system has been configured to do so. Or the write operation can also be initiated manually.

- Transmit send stations must be known (preconfigured) in the receiving station(s). The sending station is configured to try to connect to a specific (primary) receiver. A secondary receiver should be configured as a failover in the event that the primary receiver is unavailable.

- To begin transmitting, the Transmit sending operator will request a code from the receiving station. The receiving station operator will notice the request, generate a code, and then call the sending operator to verbally give the code. The sending operator inputs the code to start the transmission. All files are encrypted during the transmission.

- The documentation indicates that various network types could be used, but if possible ethernet should be used due to public perception of wireless technologies not being secure enough. However, cellular could be used in locations where the county ethernet is unavailable. The 3 big cellular network providers offer a non-public, more robust network that is typically used by first responders. A cellular router with ethernet could be used to connect to a “first responder” network. A VPN should be part of the configuration. The LAN connection from the router to the Transmit device should be ethernet, not WiFi.

- A duplicate vDrive could be created and transmitted from a 2nd sending Transmit station, but the Count program will reject uploading a vDrive if the CVRs have already been read. However, it will add new additional CVRs if they are found.

  Retransmission from the same Transmit sending station is rejected by that Transmit device because it knows it was already transmitted.

- There is not a message when the write operation on the receiving station is complete. This is probably because in automatic write mode, there could be multiple files being received and written from multiple remote transmissions. When removing a vDrive, the receiving operator needs to press the Pause button before pulling the vDrive to prevent possible corruption of the data.

- The 2.7.4 version of Transmit used for the examination incorporated a de minimis change (ECO-1605) made to the receiving Transmit software. The change was a fix to allow for the automatic write to a vDrive after the transmitted file is received and authenticated. Prior to the ECO fix, the operator would have to manually initiate the write operation. I concur that the ECO is de minimus, and further testing is not needed..

- There is no Verity Relay (the remote transmission option to the Scan devices) software in the Texas software build. The documentation includes Relay, but it cannot be configured with the Texas software build. When a jurisdiction orders a system, they use a separate SKU for the Texas product. This assures no modems, drivers, etc. are in the Scan devices.

Conclusion

The Verity Election System, Release 2.7 is a solid update to the 2.5 release. There are no issues that should preclude a jurisdiction from upgrading, or using the 2.7 release for their initial installation of the Verity system. I recommend that the system be certified.

Tom Watson
Examiner