Voting System Examination of Election Systems & Software EVS 6.1.1.0

Brian Mechler, Technical Examiner
Exam Dates: August 21, 2020
Report Date: September 20, 2020

1 Background

An examination of the Election Systems & Software (ES&S) EVS 6.1.1.0 voting system was conducted at the Texas Secretary of State Elections Division offices on August 21, 2020. EVS 6.1.1.0 is a comprehensive voting system which can consist of a subset of the following components [1][2][3]:

- Electionware - a suite of end-to-end election management software applications
- ExpressVote Previewer – a ballot preview utility
- PaperBallot – a ballot layout editor
- Event Log Service – a service which monitors and logs users' interactions with the Election Management System (EMS)
- Removable Media Service - a utility that runs in the background of the Windows operating system used for media validation purposes
- ExpressTouch - a direct recording electronic (DRE) voting device which supports electronic vote capture (for use in Texas only as a curbside voting device)
- ExpressVote XL - a ballot marking device (BMD) that provides a large-format touch screen interface and integrated thermal printer
- ExpressVote (HW 1.0 & 2.1) - a BMD that provides a touch screen interface and printer
- DS200 - a digital scanner and tabulator for use in the polling place
- DS450 - a central scanner and tabulator
- DS850 - a central scanner and tabulator with increased speed compared to the DS450
- ExpressLink - a standalone application that interfaces with voter registration systems (e.g. electronic pollbooks) and the ExpressVote Activation Card Printer
- ExpressVote Activation Card Printer - a small thermal printer used to print the ballot activation code on a vote summary card
- Toolbox – a software suite run on non-EMS workstations

Configuration options are presented in detail in [3]. The Election Assistance Commission (EAC) certification includes tables that describe in detail the voting system software components, voting system platforms, hardware components, and system limits [2].

Due to the COVID-19 pandemic, some of the examiners, including myself, participated in the exam remotely using a video teleconferencing system. This exam was conducted in tandem with an exam of EVS 6.0.3.0 which will be covered in a separate report. A one day exam was sufficient due to the fact that 6.0.3.0 and 6.1.1.0 are software-only updates relative to their previously certified baselines.

The Secretary of State obtained the software and firmware images used in the EAC certification directly from the EAC Voting System Test Laboratory (VSTL). ES&S personnel used those same files to perform installation under the supervision of the examiners. In [4]-[11], ES&S provides instructions for the identification and verification of the components included in EVS 6.1.1.0.

The examination also consisted of vendor presentations, a mock election, and a free-form session where examiners could ask follow-up questions.

There were no accessibility tests performed during this exam. There have been no updates to the voter facing hardware or firmware since the previously certified EVS 6.1.0.0. At the time this report was submitted, the certification documentation for EVS 6.1.0.0 was not yet hosted on the Texas Secretary of State website. Documentation of this nature can typically be found at:

https://www.sos.texas.gov/elections/laws/ess_system.shtml

2 Election Management System

The election management system (EMS) is a set of servers, workstations, and software which provides an end-to-end solution for jurisdictions to define, manage, configure, export, and tabulate elections. The following subsections will describe the hardware workstations and servers, media, software, and observations from the exam.

2.1 Hardware

EMS workstations can be standalone or act as a client connected to a server. Client and standalone workstations are all Dell products. The following models have been certified by the EAC for use with EVS 6.1.1.0:

- Latitude 5580
- OptiPlex 5040, 5050, and 7020

The client/standalone workstations run 64-bit Windows 10 Enterprise LTSC SP1 as the operating system (OS). The server certified by the EAC for use with EVS 6.1.1.0 can be a Dell PowerEdge T430 or T630. The server hardware runs 64-bit Windows Server 2016 as its OS.

When election hardware is networked together is must be done in a closed network environment. In [12], ES&S defines a closed network environment as consisting of “a stand-alone server used for a specific purpose, such as an Election Management System (EMS) like Electionware, with restricted

access to specific workstations and no connection to any other network. Only EMS components are allowed on this network, and any voting system component at a precinct voting site is forbidden from being connected."

Best practices for physically securing EMS workstation and server hardware are found in [13].

The only change to EMS hardware is "the option for increased physical RAM on the EMS in the client, server and/or standalone configurations (optional)." EVS also "increased the amount of virtual RAM available to Electionware (optional)." [14]

2.2 Media

There were no changes to the format or use of media between EVS 6.1.0.0 and 6.1.1.0.

2.3 Software

Electionware is the suite of ES&S software modules used for administering elections. There were only minimal changes to Electionware between EVS 6.1.0.0 and 6.1.1.0 [14].

- "Added critical Windows security updates available at the time of certification testing."
- "Included the recommended Arial fonts"
- "Provided a method for modifying the Microsoft Windows password policy to not expire on the EMS (optional)."
- "Added an updated JAR file to prevent relocated JAI classes from loading. This prevents the Internal Error displayed when attempting to view ExpressVote XL write-in images."
- "Adjusted misalignment of write-in snippets for ExpressVote XL and ExpressVote vote summary cards so they reflect the correct ballot image."
- "Provided an additional internal Postgres system logging message to enhance the security and performance of the database."
- "Provided an additional user logging message to enhance the transparency and security of the database. This additional logging is included within the Reporting module to assist users during ballot adjudication."
- "Removed all empty entries in the CVR export report."

2.4 Observations

There were no issues related to the EMS during the mock election and subsequent tabulation and reporting.

The change note that mentions the misalignment of a write-in snippet refers to an issue with the adjudication UI. The voter's write-in choice is correctly printed on the ballot. ES&S told examiners that supplemental documentation with a work-around was provided to jurisdictions using affected versions of EVS. I recommend jurisdictions reach out to ES&S to ensure they have received these documents.

In 6.1.1.0, the option is provided to set EMS passwords that don’t expire. Jurisdictions should never take advantage of this option. The “Election Security Best Practices Guide” published by the Texas Secretary of State recommends forced updates of passwords every 90 days as a priority best practice [15].

3 Voting Devices

ES&S is requesting certification of four different voting devices (one DRE and three BMDs). All devices employ touchscreens and can be configured with accessibility peripherals. The hardware and firmware of the ExpressTouch, ExpressVote XL, and ExpressVote (HW 1.0 and 2.1) remains unchanged since EVS 6.1.0.0. Best practices for physically securing these devices can be found in [13].

3.1 Observations

Examiners observed the installation of firmware, Election Qualification Codes (EQCs), and election definitions on the ExpressVote HW 2.1. No other voting devices were used in the mock election. Refer to EVS 6.1.0.0 exam reports for further detail on the user experience of ES&S voting devices. Because there were no updates to these devices in this version of EVS, concerns raised by examiners during the EVS 6.1.0.0 exam still remain.

During the mock election, no issues were observed with the casting of ballots, tabulation of votes, or reporting of results.

4 Scanners

ES&S is requesting certification of three different scanning devices in EVS 6.1.1.0; the DS200 which is designed as a precinct scanner, and the DS450 and DS850 which are both central scanners. All scanners are capable of scanning both hand-marked paper ballots and machine-marked vote summary cards. The hardware and firmware of the DS200, DS450, and DS850 remains unchanged since EVS 6.1.0.0. Best practices for physically securing these devices can be found in [13].

4.1 Observations

Only the DS200 and DS850 were used to scan and tabulate ballots during the mock election. No issues were observed with scan quality, accuracy, or reliability. The devices did not appear prone to jams or other slow downs.

Refer to EVS 6.1.0.0 exam reports for additional detail on ES&S scanning devices. Because there were no updates to these devices in this version of EVS, any concerns raised by examiners during the EVS 6.1.0.0 exam still remain.

5 ExpressLink and ExpressVote Activation Card Printer

These components are not within the scope of this certification exam nor are they a part of the EAC certification. Nevertheless, they are listed as part of the Form 100 [1], and this section will briefly describe their purpose.

The ExpressLink is a standalone software application that interfaces with electronic pollbooks and the ExpressVote Activation Card Printer. The ExpressVote Activation Card Printer prints a bar code at the top of a vote summary card that encodes the ballot style that the voter should receive. The voter can then use the pre-printed vote summary card to activate their own voting session and receive the correct touchscreen ballot on ExpressVote and ExpressVote XL BMDs.

The ExpressVote Activation Card Printer also provides a mechanism for marking a ballot as provisional and preventing it from being prematurely scanned and accepted as a regular ballot by the precinct scanner.

5.1 Observations

Neither the ExpressLink nor the ExpressVote Activation Card printer were demonstrated during the exam.

Based on the functionality described in the ES&S technical data package, large polling places may benefit from these devices since they will likely reduce the workload on already busy poll workers and reduce voter waiting times.

6 Toolbox

This component is not within the scope of this certification exam nor is it a part of the EAC certification. Toolbox is designed to run on the Windows 7 operating system, and must be run on a host separate from the EMS closed network environment.

The Toolbox has three main components [16]:

- Test Deck – used to create test decks for use in logic and accuracy (L&A) testing
- Text to Speech – used to create audio playback files for use with ADA-compliant devices
- Media Restore – used to securely clear data from ES&S Delkin USB media and reformat media to the FAT32 file system
- Data Conversion - used to convert exported election data to formats compatible with Electionware

6.1 Observations

The Test Deck, Text to Speech, and Data Conversion modules were not demonstrated during the exam. Media Restore was used to create election media for the mock election. No issues with its use were observed.

7 Hash Verification Issues

EVS 6.1.1.0 (as well as other EVS versions) has multiple issues with its prescribed hash verification procedures.

Hash verification is the process that is used to ensure that the software and/or firmware of a voting system matches exactly with what was certified by the EAC. A hash is the output of a cryptographic function run on a file or program executable. If a file or program is changed in any way, it will produce a different hash result.

Hash verification is a critical component of acceptance testing to ensure the proper delivery of voting systems. In Election Advisory No. 2019-23, jurisdictions are directed to perform a complete system validation which includes the verification of hashes [17]. Though not yet mandated by the State of Texas, I believe that jurisdictions should perform hash verification on all voting system equipment before and after each election.

7.1 ES&S Personnel Performing Hash Verification

It was disclosed during the concurrent EVS 6.0.3.0 exam that ES&S personnel have performed the hash verification process instead of their customers. Jurisdictions should always perform this process themselves. To have the vendor perform a required component of acceptance testing creates, at best, a conflict of interest. The Secretary of State Elections Division has taken an action to work with ES&S and their Texas customers to better define their roles and responsibilities with respect to acceptance testing and hash verification.

7.2 Bug in Hash Verification Script

The hash verification process involves the creation of two USB thumb drives; one containing the system export data of the system to be verified and the other containing the verification scripts and trusted hash file. A host separate from the EMS is booted using a live Ubuntu DVD. The live Ubuntu DVD allows the user to run the Linux OS from the DVD without altering the non-volatile memory of the host computer. The export and scripting media are then mounted and a set of scripts are run to configure the user's environment, compute hashes of the system export data, and compare those hashes with the trusted hash file.

While working through this process, I initially overlooked the instruction to add the trusted hash file to the scripting media. Despite the missing trusted hash file, the verification script erroneously reported that the exported hashes matched the trusted hashes.

```
$ ./DS200-VerifyHash.sh DS200-TxSos6110ExamAug2020
diff: HashTrusted-DS200.txt: No such file or directory

DS200 firmware matches Trusted Hash File.
Hash File, DS200-TxSos6110ExamAug2020_Hash.txt, copied to output
```

Though this example shows the output of the DS200 verification script, the bug is also present in the verification scripts for the DS450, DS850, ExpressTouch, ExpressVote (HW 1.0 and 2.1), and ExpressVote XL devices.

ES&S's documentation states [5]:

> *If the DS200 firmware matches the Trusted Hash File, the following message will be displayed.*
>
> ```
> DS200 firmware matches Trusted Hash File.
> Hash File, DS200-Identification_Hash.txt, copied to output.
> ```
>
> *Where, DS200-Identification is the name used to identify the DS200 for which the verification reports were generated.*
>
> *If the DS200 firmware does not match the Trusted Hash File, the following message will be displayed.*
>
> *For details, see Appendix F Results when DS200 Firmware Does Not Match.*
>
> ```
> DS200 firmware DOES NOT MATCH Trusted Hash File!
> Difference report, DS200-Identification_Report.txt, copied to output.
> Hash File, DS200-Identification_Hash.txt, copied to output.
> ```

It could be very easy for personnel performing hash verification to assume a good result when, in actuality, no hash comparisons were made. Within their scripts, ES&S should have performed explicit checks on the existence of the two files being compared; failing loudly if either does not exist.

A common open-source application, diff, is used to compare the hash files. In order to determine if they match, ES&S only examines the text that diff writes to the standard output stream. In doing so they miss the error messages written to the standard error stream. In general, it is bad coding practice to condition a critical decision on the written output of a 3rd party application. The reason is that the developer would have to know every possible output (intended or otherwise) in order to craft a reliable conditional.

A more robust way to check the result of the diff call would have been to query its exit status. The diff manual clearly defines the meaning of its exit status as [18], "0 if inputs are the same, 1 if different, 2 if trouble."

It is my opinion that this bug (in addition to the overall process) indicates that ES&S has not developed their hash verification process with sufficient care, quality assurance, and concern for usability.

When jurisdictions run their hash verification, they should carefully examine the media they create for correctness and carefully monitor the output of the verification scripts to make sure no error messages are printed along with text claiming a successful result.

Texas' Election Security Best Practices Guide [15] states that as a priority best practice jurisdictions should "ensure that every election function from ballot programming to Election Night Reporting uses a two-person verification method in which one person performs the task and a second person witnesses and verifies the accuracy and integrity of the result." It is not clear to me whether this guidance includes the hash verification process or acceptance testing activities, but it should.

7.3 Lack of Traceability in Procedure for EMS Hash Verification

The hash verification document for the EMS host(s) describes a procedure where the user creates a set of "golden" hashes immediately after installation [4]. Subsequent checks are only verified against this "golden" set. This procedure, as written, only verifies that the EMS has not been altered since the first installation; it is not traceable to the hashes generated by the EAC. ES&S should document a procedure that jurisdictions can use to verify EMS hashes against those created by the EAC.

8 Conclusions

The ES&S hash verification process has been a growing issue of concern over the past few certification exams. In this exam, their customer relations with regard to this process have also become a concern. At this point, these issues have been communicated in detail to ES&S. I ***will not*** recommend certification of future ES&S releases unless they make substantial improvements to the ease-of-use, reliability, and traceability of their hash verification process.

As a mitigation for EVS 6.1.1.0 and past versions of EVS, I strongly recommend jurisdictions perform hash verification for themselves using a two-person verification method as described in Texas' Election Security Best Practices Guide.

With appropriate procedures in place, EVS 6.1.1.0 is a comprehensive voting system that is secure, accurate, and easy for the voter to use. ES&S's responses to the Voting System Certification Form 101 are truthful and adequate [19]. The system tabulated and reported results accurately during the mock election portion of the exam.

I recommend certification of EVS 6.1.1.0.

9 References

[1] Application for Texas Certification of Voting System – Form 100, Election Systems & Software, ES&S EVS 6.1.1.0

[2] United States Election Assistance Commission Certificate of Conformance, ES&S EVS 6.1.1.0, EAC Certification Number: ESSEVS6110, Jul-27 2020
URL: https://www.eac.gov/voting-equipment/evs-6110

[3] System Overview, ES&S Voting System 6.1.1.0, Document Revision 1.2, Document ID ESSSYS_6'1'1'0_D_SYSOVR

[4] Verification Procedure: Election Management System, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EMS

[5] Verification Procedure: DS200 Precinct Scanner and Tabulator, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_DS200

[6] Verification Procedure: DS450 High-Throughput Scanner and Tabulator, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_DS450

[7] Verification Procedure: DS850 High-Speed Scanner and Tabulator, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_DS850

[8] Verification Procedure: ExpressTouch, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_ETOUCH

[9] Verification Procedure: ExpressVote Hardware 1.0, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EVOTE_HW1'0

[10] Verification Procedure: ExpressVote Hardware 2.1, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EVOTE_HW2'1

[11] Verification Procedure: ExpressVote XL, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EVOTEXL

[12] Electionware Vol. I: Administrator Guide, Software Version 6.0.1.0, Revision 1.0, March 2020

[13] Best Practices for Physically Securing ES&S Equipment, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_SPC_SECBESTPRACT

[14] System Change Notes, ES&S Voting System 6.1.1.0, Document Revision 1.2, Document ID ESSSYS_6'1'1'0_D_CHANGENOTES

[15] Election Security Best Practices Guide, Texas Secretary of State Elections Division, April 2020, URL: https://www.sos.texas.gov/elections/forms/election-security-best-practices.pdf

[16] Electionware Toolbox User Guide, Software Version 4.0.0.0, Document ID EW_Toolbox_4’0’0’0_SOP

[17] K. Ingram, Director of Elections, Electronic Voting System Procedures Advisory, Election Advisory No. 2019-23, Oct-23 2019, URL: https://www.sos.texas.gov/elections/laws/advisory2019-23.shtml

[18] http://manpages.ubuntu.com/manpages/xenial/man1/diff.1.html

[19] Voting System Certification – Form 101, EVS 6.1.1.0