Voting System Examination of Election Systems & Software EVS 6.2.0.0

Brian Mechler, Technical Examiner
Exam Dates: June 22-23, 2022
Report Date: December 22, 2022

1   Background

An examination of the Election Systems & Software (ES&S) EVS 6.2.0.0 voting system was conducted at the Texas Secretary of State Elections Division offices on June 22-23, 2022. EVS 6.2.0.0 is a comprehensive voting system which can consist of a subset of the following components [1-3]:

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

Toolbox – a software suite run on non-EMS workstations

Regional Results – a standalone application used to transmit preliminary unofficial results from regional sending sites to jurisdiction headquarters over the jurisdiction's dedicated network

ExpressTouch - a direct recording electronic (DRE) voting device which supports electronic vote capture (for use in Texas only as a curbside voting device)

ExpressVote (HW 1.0 & 2.1) - a ballot marking device (BMD) that provides a touch screen interface and printer

DS200 (HW 1.2 & 1.3) - a digital scanner and tabulator for use in the polling place

DS450 - a central scanner and tabulator

DS850 - a central scanner and tabulator

DS950 - a central scanner and tabulator

ExpressLink - a standalone application that interfaces with voter registration (e.g. electronic pollbook) systems and the ExpressVote Activation Card Printer

ExpressVote Activation Card Printer - a small thermal printer used to print the ballot activation code on the vote summary card

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

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]-[17], ES&S provides instructions for the identification and verification of the components included in EVS 6.2.0.0.

The examination also consisted of a vendor presentation, accessibility tests, a mock election, and a free-form session where examiners could ask follow-up questions and perform ad-hoc testing of the voting system. I did not witness the accessibility tests; those results will be presented in other examiners' reports.

Typically Examiners' reports are submitted to the Secretary of State within 30 from the end of the examination; however reporting deadlines were extended so that ES&S could respond to examiner questions and submit Engineering Change Order (ECO) 1143 to the EAC [32].

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 EMS hardware (workstations and servers), media, software, and observations from the exam.

2.1 Hardware

EMS workstations can operate standalone or act as clients connected to a server. Client and standalone workstations are all Dell products. They run Windows 10 Enterprise LTSC as their operating system (OS). The following workstations have been certified by the EAC for use with EVS 6.2.0.0:

>Latitude 5580

>OptiPlex 5040, 5050, and 7020

The server certified by the EAC for use with EVS 6.2.0.0 can be a Dell PowerEdge T430 or T630. The servers run Windows Server 2016 as the OS.

When EMS hardware is networked together is must be done in a closed network environment. In [18], ES&S defines a closed network environment as consisting of "a stand-alone server used for the specific purpose of using the Election Management System (EMS), 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 the EMS workstation and server hosts are found in [19].

The main change to EMS hardware since EVS 6.1.1.0 is the ability to use USB YubiKeys for optional dual factor authentication [20].

2.2 Media

USB sticks are still the primary form of media that the EMS uses to export election qualification codes (EQC) and election definitions. Custom Delkin USB sticks are required for most functions. Changes to media between EVS 6.1.1.0 and 6.2.0.0 include [20]:

- Support for USB 3.0 flash drives with 4GB, 8GB, 16GB, and 32GB capacity

- Support "for use of blank USB flash drives formatted by Windows 10 that contain the hidden System Volume Information folder

2.3 Software

Electionware is the suite of ES&S software modules used for administering elections. Updates to Electionware software between EVS 6.1.1.0 and 6.2.0.0 include [20]:

- Updated splash screen to remove copyright information

- "System option to print a unique audit ID in text and human readable form on each vote summary card or ballot. Tabulators capture the audit ID for Risk Limiting Audits"

- "Expanded an option to hide on-screen selection target boxes to the ExpressTouch and ExpressVote platforms"

- "Implemented a multi-card vote session for the ExpressVote as a Marker"

- "Add the ability to customize the "No Selection" text field used when a voter chooses to undervote a contest"

- Redesigned verification procedures to check installed EMS against hashes provided by EAC/VSTL

- "Added [verification] procedures for Data Communication server and COTS equipment"

- "Implemented the printing of a cross-out graphic in any possible barcode position not filled by a standard selection barcode"

- "Card Print Properties are now configured in the Touch Screen Ballot module"

- "Implemented the ability to support an activation card with a stub inserted into the ExpressVote and scanned without the stub on the tabulators with a single coding event"

- "Updated the Postgres Authentication from MD5 to SCRAM-SHA-256"

- "Updated the Java Advanced Imaging API to ensure compatibility with future Java releases"

- "Updated PostgreSQL to v11.9 to take advantage of security and performance updates"

- "Updated ActiveMQ Classic v5 to v5.16.0 to take advantage of security and performance updates"

- "Added enhancement to prevent users from placing content in panels reserved for Judges' Initial and Review boxes"

- "Updated software packaging tools to sync between proprietary software products" in Event Log Service

- Option to condense vote summary card layout

2.4 Observations

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

The EMS verification procedures have been simplified, and comparing hashes to a trusted set generated by the VSTL is a great improvement over the prior method where jurisdictions created their own trusted hashes immediately after installing the EMS. Verification is now traceable back to the EAC and VSTL (more details about verification procedures are in Section 8).

Hiding on-screen target boxes solves a potential user experience (UX) issue on the voting devices where voters may be drawn toward touching the edge of a selection region rather than the center.

The "Card Stub Support" feature was not demonstrated during the exam and I don't feel comfortable recommending use of this feature without Texas examiners getting a chance to observe it and understand its use-case.

Designing an election using a multi-card voting session should be avoided if possible since it would require significant modifications to poll worker training and voter expectations. A condensed layout of the vote summary card could be used to avoid multi-card voting sessions. The figure below shows how this feature groups selections by category to save space.

Figure 1: Condensed Summary Card Layout

3 Voting Devices

Voters interact with EVS 6.2.0.0 voting devices via touchscreens and accessibility peripherals. Devices in scope of this exam include the ExpressVote (HW 1.0 and 2.1) and the ExpressTouch. The ExpressVote XL was not included for certification in Texas with EVS 6.2.0.0. Best practices for physically securing these devices can be found in [19].

Changes to voting devices between EVS 6.1.1.0 and 6.2.0.0 include [20]:

- Upgrade and synchronization of the firmware across all hardware products.

- "Updated splash screens on hardware and software products to remove copyright information"

- Simplification and improvement of hash validation procedures

- ExpressVote Dual Express Cart configuration for holding two ExpressVote units, one for standing voters and the other that is ADA-compliant to accommodate a seated voter

- ExpressVote Ben Franklin Voting Booth configuration which can be re-positioned for seated and standing voters

- The ExpressTouch has an updated power supply and battery firmware to replace end-of-life parts

3.1 Observations

Examiners observed the installation of firmware, Election Qualification Codes (EQCs), and election definitions on the ExpressTouch, ExpressVote HW 1.0, and ExpressVote HW 2.1.

During the mock election and ad-hoc testing, no issues were observed with the casting of ballots, tabulation of votes, or reporting of results. The voter UI is intuitive and has remained consistent with past versions certified in Texas. Refer to previous exam reports for further detail on the use of ES&S voting devices [21]-[25].

During ad-hoc testing, a paper jam resulting from atypical voter behavior caused one of the ExpressVote units to stop accepting new vote summary cards. ES&S should attempt to recreate and understand the root cause of this issue.

4 Scanners

The scope of EVS 6.2.0.0 includes a precinct scanner, DS200, and three options for central scanners: DS450, DS850, and DS950. All scanners are capable of scanning both paper ballots and the vote summary cards produced by the BMDs. The DS950 is the intended replacement for the DS850. ES&S will no longer be manufacturing the DS850, but during the exam they committed to support it in future EVS releases. Best practices for physically securing these devices can be found in [19].

Changes to voting devices between EVS 6.1.1.0 and 6.2.0.0 include [20]:

- Introduction of the DS950 central count scanner and tabulator

- Upgrade and synchronization of the firmware across all hardware products

- "Updated splash screens on hardware and software products to remove copyright information"

4.1 Observations

The scanners were used to scan and tabulate ballots during the mock election and ad-hoc testing. No issues were observed with scan quality, accuracy, or reliability. The devices did not appear prone to jams or other slow downs. Refer to previous exam reports for further detail on the use of ES&S scanning devices [21]-[25].

5 ExpressLink and ExpressVote Activation Card Printer

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 subsequently uses the pre-printed vote summary card to activate their own voting session on the ExpressVote BMD.

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

5.1 Observations

Use of the ExpressLink and ExpressVote ActivationCard printer was not observed during this exam. Based on the functionality described in the ES&S technical data package (TDP), large polling places which serve voters from more than one precinct may benefit from these devices since they will reduce the workload on poll workers and increase voter throughput.

6 Toolbox

Toolbox includes a set of software utilities that can be used alongside the Electionware EMS. It includes modules to create test decks, convert text to speech, prepare USB media, and convert election data formats.

6.1 Observations

Most of the Toolbox modules were not demonstrated. The Media Restore module was used to prepare USB media used during the exam. No issues were observed.

Toolbox should never be installed on the same host as the Electionware EMS. The TDP does not address how the host running Toolbox should be secured. Since USB media will be introduced into this outside system, I recommend precincts physically secure the host computer running Toolbox according to the same best practices outlined by ES&S for Electionware workstations. Furthermore, the hosts running Toolbox should be run in a standalone fashion not connected to any networks.

7   Regional Results

Regional Results is a system and standalone application for transmitting preliminary unofficial results over the jurisdiction's dedicated wide-area network (WAN) from a regional sending site to jurisdiction headquarters on election night. A regional sending site is any location that has connectivity to the jurisdiction's dedicated WAN, e.g. fire station, police station, county offices, etc. Only results data are transmitted (i.e. no ballot images or cast vote records), and the messages are signed, encrypted, and sent over a VPN without connectivity to the internet via SFTP. Results data cannot be transmitted until after polls are closed. Figure 2 depicts the Regional Results network model [26].
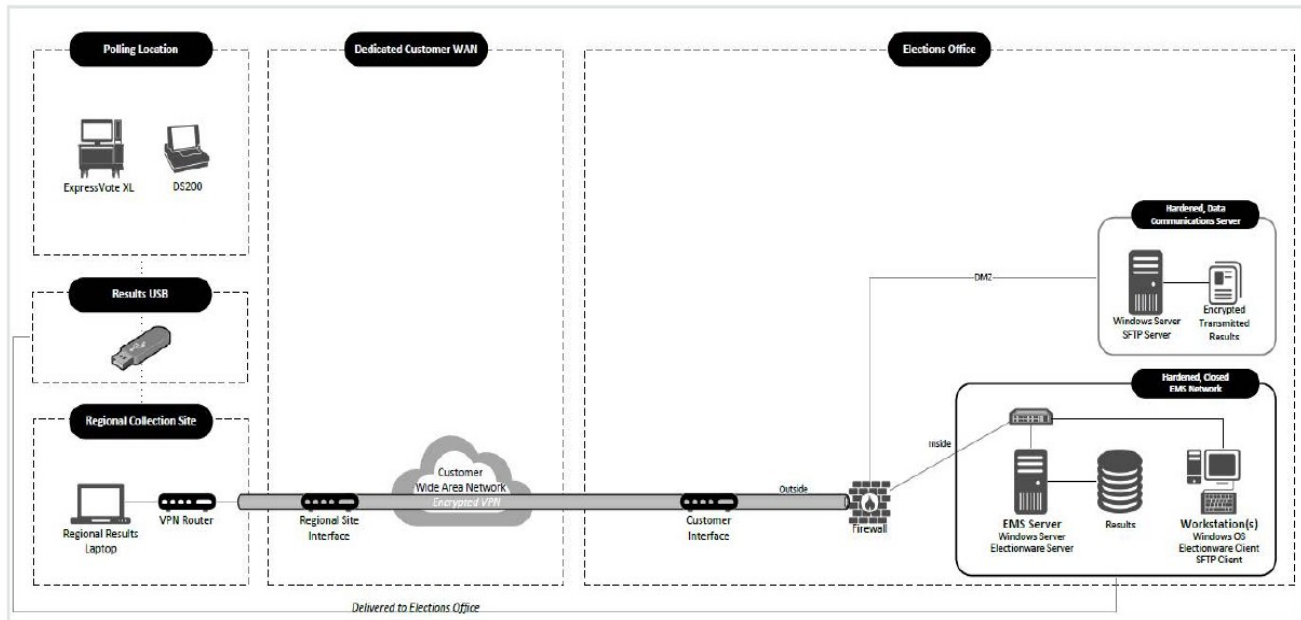

Figure 2: Dedicated Regional Results Network Configuration [26]

In the figure above, the hosts in the "Hardened Closed EMS Network" are running Electionware, but these hosts are not the EMS that is described in Section 2. These hosts are only used for the receipt of preliminary unofficial results and should never be connected to the closed network environment described in Section 2.1.

7.1 Observations

Examiners witnessed the installation and verification of Regional Results hosts as well as the transmission and receipt of unofficial results data. No issues were observed with this process.

The purpose of a system like Regional Results is not without merit. In Texas, we have some very large counties, both in terms of geography and population. In these large counties Regional Results could mitigate the challenge of providing timely reporting of unofficial results on election night.

Examiners and the vendor discussed procedures that could be followed to securely use this feature. These included marking any media that touched the Regional Results system as "dirty" to segregate it from media and systems used in the tabulation of official results. In the case of the ExpressTouch DRE, backup media can be created such that official media remain untainted by Regional Results. Creating an additional backup from the DS200 precinct scanner for this purpose is a more onerous process, but the ballots themselves are considered the official record should the DS200 on-board memory become corrupted for any reason.

To address concerns about confusion between the official EMS and the Regional Results EMS at the central site, the vendor suggested that users of the Regional Results EMS only be granted the rights of "reporting" users, that way they cannot access other features of that EMS host such as election definition and ballot creation. The vendor also indicated that they could restrict the licensing on the Regional Results EMS hosts to prevent non-reporting activities.

Unfortunately neither of the above mitigation practices are documented in the TDP made available to the examiners. In the available documentation, best practices for the use of Regional Results are scant. Thus, the burden falls almost entirely on the Texas Secretary of State or the local jurisdictions to define and document best practices for the use of Regional Results. The Secretary of State should use their authority to define a set of policies and procedures for the use of Regional Results that jurisdictions must follow. Furthermore, I recommend that the Secretary of State only approve vendor contracts that include Regional Results in the narrowest of circumstances where physical delivery of unofficial results on election night is a substantial challenge for the jurisdiction.

8   Hash Verification

Hash verification is a critical component of acceptance testing and logic and accuracy (L&A) testing of voting systems. It 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.

In [27] multiple issues with ES&S's prescribed hash verification procedures were identified and described. These issues included an install method which resulted in one file failing the verification check, a bug in their verification scripts which gave misleading output under certain circumstances, lack of traceability in the EMS host verification process, and a general impression that the verification procedures and their importance to election security were not taken seriously by ES&S.

ES&S has addressed most of these issues in EVS 6.2.0.0. The verification procedures are less cumbersome for users to follow. The quality of the verification scripts has improved. When files are missing in the comparison, users are properly alerted. The verification of EMS hosts is now performed against VTSL provided hashes. These improvements are a very important, welcome step in the right direction.

A couple of new issues with hash verification were uncovered during the exam. The procedure for EMS hosts differs from the voting devices and scanners in that the verification scripts are run on the host itself rather than exporting system files to be verified on a separate verification host. Ideally the system performing verification should be independent of the system under examination. In future releases, ES&S needs to update this procedure so that the EMS host can be independently verified or at

the very least provide the State of Texas with a reasonable explanation for why this would be infeasible.

The other issue is that the prescribed OS for the verification host, Ubuntu 16.04.1 LTS, is out-of-date. I don't have insight into ES&S's development cycle, but it is very likely that at least one if not two more modern versions of Ubuntu were available at the time of development (Ubuntu 18.04.1 LTS released 7/26/2018 and Ubuntu 20.04.1 released 8/6/2020) [28]. By the time VSTL testing of EVS 6.2.0.0 had commenced, the standard support window of Ubuntu 16.04.1 had almost closed. It is disappointing that neither ES&S nor the VSTL took note [29].

In response to this issue, ES&S rightly pointed out that the Extended Security Maintenance window for Ubuntu 16.04.1 LTS extends until April 2026. This is a moot point, the support and maintenance windows are only relevant if one is receiving regular system updates. In [4], ES&S states "The verification PC shall operate without a network connection. A network connection may cause changes to the hashing utility (openssl) that disables the FIPS-140 configuration." ES&S is correct to put this stake in the ground. The problem is that they opted for an old version of Ubuntu when newer versions were available. It is unlikely that their scripts are not portable to more modern versions of Ubuntu. The OpenSSL Cryptographic Modules in Ubuntu 18.04 and 20.04 comply with the FIPS-140-2 standard [30-31]. ES&S stays current with Microsoft Windows releases for their EMS, they should do the same with Ubuntu releases for their verification host. I recommend ES&S submit an engineering change order (ECO) to the EAC to update the verification host OS to a modern version of Ubuntu.

9   Conclusions

Overall the EVS 6.2.0.0 system performed well during the exam. The system tabulated and reported results accurately during the mock election portion of the exam. Voter facing features are easy to use. When configured properly and handled with good procedures EVS 6.2.0.0 is a system that is both secure and accurate.

However, the exam was not without issue. There were features introduced in EVS 6.2.0.0 that were either not well documented, not demonstrated during the exam, or both. Great improvements were made to the hash verification procedures, but at least one minor and one major issue remains.

I recommend EVS 6.2.0.0 be certified for use in Texas only under the following conditions:

- Use of the Card Stub feature is prohibited until the feature is sufficiently documented and demonstrated to examiners

- The EAC approves an ECO to update the verification host operating system

- Sale of Regional Results is restricted to counties that suffer significant impediments to timely reporting of unofficial results

- The Texas Secretary of State defines a set of policies and procedures which counties must follow to ensure the secure use of Regional Results

10 References

[1]   Application for Texas Certification of Voting System – Form 100, Election Systems & Software, ES&S EVS 6.2.0.0, Jun-22 2022

[2]   United States Election Assistance Commission Certificate of Conformance, ES&S EVS 6.2.0.0, EAC Certification Number: ESSEVS6030, Dec-23 2021
URL: https://www.eac.gov/voting-equipment/evs-6030

[3]   System Overview, ES&S Voting System 6.2.0.0, Document Revision 1.5

[4]   Verification Procedure: Overview. Document Revision 1.3, Document ID: ESSSYS_6'2'0'0_D_VERPROC_OVERVIEW

[5]   Verification Procedure: Regional Results, Document Revision 1.0, Document ID: ESSSYS_1'4'0'0_D_VERPROC_REGIONALRESULTS

[6]   Verification Procedure: Regional Results – Administrator's Guide, Document Revision 1.0, Document ID: ESSSYS_1'4'0'0_D_VERPROC_REGIONALRESULTS_ADMIN

[7]   Verification Procedure: DS200, Document Revision 1.0, Document ID: ESSSYS_2'40'0'0_D_VERPROC_DS200

[8]   Verification Procedure: DS450, Document Revision 1.0, Document ID: ESSSYS_4'1'0'0_D_VERPROC_DS450

[9]   Verification Procedure: DS850, Document Revision 1.0, Document ID: ESSSYS_4'1'0'0_D_VERPROC_DS850

[10]   Verification Procedure: DS950, Document Revision 1.0, Document ID: ESSSYS_4'1'0'0_D_VERPROC_DS950

[11]   Verification Procedure: ExpressTouch, Document Revision 1.0, Document ID: ESSSYS_4'2'0'0_D_VERPROC_ETOUCH

[12]   Verification Procedure: ExpressVote Hardware 1.0, Document Revision 1.0, Document ID: ESSSYS_4'2'0'0_D_VERPROC_EVOTE_HW1'0

[13]   Verification Procedure: ExpressVote Hardware 2.1, Document Revision 1.0, Document ID: ESSSYS_4'2'0'0_D_VERPROC_EVOTE_HW2'1

[14]   Verification Procedure: Data Communication Servertor Document Revision 1.2, Document ID: ESSSYS_6'2'0'0_D_VERPROC_DATACOMM

[15]   Verification Procedure: Data Communication Server Administrator's Guide, Document Revision 1.2, Document ID: ESSSYS_6'2'0'0_D_VERPROC_DATACOMM_ADMIN

[16]   Verification Procedure: Election Management System, Document Revision 1.3, Document ID: ESSSYS_6'2'0'0_D_VERPROC_EMS

[17]   Verification Procedure: Election Management System – Administrator's Guide, Document Revision 1.3, Document ID: ESSSYS_6'2'0'0_D_VERPROC_EMS_ADMIN

[18]   Electionware Vol. I: Administrator Guide, Software Version 6.2.0.0, Revision 1.1, September 2021

[19]   Best Practices for Physically Securing ES&S Equipment, ES&S Voting System 6.2.0.0, Document Revision 1.2

[20]   System Change Notes, ES&S Voting System 6.2.0.0, Document Revision 1.2

[21]   September 5-6, 2018 - Examiner Reports of Election Systems & Software Version E.V.S 6.0.0.0, URL: https://www.sos.state.tx.us/elections/laws/september2018-evs-6000.shtml

[22]   January 22, 2019 - Examiner Reports of Election Systems & Software Version E.V.S 6.0.2.0, URL: https://www.sos.state.tx.us/elections/laws/january-2019-evs-6020.shtml

[23]   June 26-27, 2019 - Examiner Reports of Election Systems & Software Version E.V.S 6.0.4.0, URL: https://www.sos.state.tx.us/elections/laws/june-2019-evs-6040.shtml

[24]   January 15-16, 2020 - Examiner Reports of Election Systems & Software Version E.V.S 6.1.0.0, URL: https://www.sos.state.tx.us/elections/laws/jan-2020-evs-6100.shtml

[25]   August 21, 2020 - Examiner Reports of Election Systems & Software Version E.V.S 6.1.1.0, URL: https://www.sos.state.tx.us/elections/laws/aug-2020-evs-6100.shtml

[26]   Regional Results Transfer User Guide, Software Version 1.4.0.0, February 2021

[27]   B. Mechler, Voting System Examination of Election Systems & Software EVS 6.1.1.0, Sept 2020, URL: https://www.sos.state.tx.us/elections/forms/sysexam/brian-mechler-ESS-exam-report-EVS6110-aug.pdf

[28]   Releases, Ubuntu Wiki, edited 2022-08-04 22:02:57, URL: https://wiki.ubuntu.com/Releases

[29]   Pro V&V Test Report for EAC VVSG 1.0 Certification Testing, Election Systems & Software (ES&S) Voting System (EVS) 6.2.0.0, EAC Project Number: ESSEVS6200, Version 3, Dec-17 2021, URL: https://www.eac.gov/sites/default/files/voting_system/files/ESS%20EVS6200%20Test%20Report.pdf

[30]   Ubuntu 18.04 OpenSSL Cryptographic Module, NIST Computer Security Resource Center Cryptographic Module Validation Program (CMVP), Certificate #3980, URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3980

[31]   Ubuntu 20.04 OpenSSL Cryptographic Module, NIST Computer Security Resource Center Cryptographic Module Validation Program (CMVP), Certificate #3966, URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3966

[32]   https://www.eac.gov/voting-equipment/engineering-change-orders/ess-1143