Security and eVACS®

Prepared for Elections ACT

By

29 May 2019

Date	Version	Authored	Reviewed
22/05/19	0.1	CJB	CVB
26/05/19	0.2	CJB	
28/05/19	1.0	CJB	RP
29/05/19	1.1	CJB	

CONTENTS

1. Introduction

When introduced in 2001, a major requirement for eVACS® was that it be no less secure than the existing manual paper-based system used in the Australian Capital Territory (ACT) for Legislative Assembly Elections. As this was the first use of electronic voting for government elections in Australia, security became a major feature of the design of the eVACS® system. Significantly Elections ACT specified that Internet voting was not an option; electronic voting was only to be available at polling places.

Elections ACT has many procedures in place to ensure that the ACT community can trust elections. The challenge was to, at least, replicate these processes within an electronic voting system using eVACS® software.

There have been many developments in the security field since 2001 and improvements in security to reflect those developments are a key requirement for the upgrade of eVACS®. Importantly, all of the security features designed and implemented in 2001 continue to be relevant and these are described in section 2 to provide the basis for indicating where and why new or enhanced security features are being implemented (section 3).

2. Current eVACS® Security

The electronic voting system implemented by Elections ACT comprises more than eVACS® software. The software operates on hardware, in various environments and involving different authorised users. As a consequence there are many avenues that could be potential threats to maintaining security of the end-to-end electronic election process.

Apart from 'Acts of God', threats can arise from the actions by suppliers of election software and equipment, ACT Election Officials (including casuals taken on for an election) or external parties. Mitigation strategies are addressed in the following sections describing different aspects of the current electronic voting system.

The primary areas of functionality provided by eVACS® are: Setup Election, Voting, Data Entry, and Counting and Reporting. In addition scanned votes, from a separate system, are incorporated into eVACS® for counting and reporting.

2.1. Software related security

A key security feature is that the eVACS® software is independently audited and locked down prior to use in an election to ensure that the software only does what it is intended to do and votes cannot be added, deleted or amended. The software delivered for auditing comprises 4 CDs: i) election setup, ii) voting client, iii) data entry client, and iv) the source code. When any of the first three of these CDs is inserted into a computer any software of any nature existing on that computer is removed before the relevant eVACS® software is loaded. Only election officials are able to undertake setting up for, and operation during, a particular election.

The operating system used is a cut down version of Linux, only containing the functionality necessary to support eVACS® operations. Providing limited functionality mitigates against attempts to modify the software whilst in operation.

The voting client and data entry client are both basically dumb terminals, only requiring sufficient software to enable communication with the relevant server, and do not contain any specific election information, and importantly no vote data.

Once the election information for a particular election is available and input to the Election Server, the Voting Server application together with its operating system are generated by the

Election Server and burnt to a WORM CD – the polling place server CD. Again, when loaded to create a polling place server the hardware is wiped clean of any other software.

Security features related to the Election Server are as in Figure 1, and for a Polling Place Server in Figure 2.

2.2. Ballot and vote protection

The accuracy of ballot contents is the responsibility of Elections ACT and, likewise, the uploading to eVACS® of relevant election information including ballot details, with the latter password controlled.

When a ballot paper contains an elector's preferences (now a vote) the elector is responsible for placing their ballot paper in the Ballot Box and an Official is responsible for ensuring the votes are not removed for counting before the close of polling. After first preference counts are confirmed at the polling place, the ballot papers are transported with appropriate security measures to the security controlled central scrutiny location for scanning. Other procedures relate to tracking numbers of ballot papers issued or unused.

Electronic votes have similar protections:

i) votes are stored in a physically secure ballot box (a database on the polling place server and on two separate disks)
ii) votes cannot be counted until after polling closes (option is not available as a menu item beforehand)
iii) the results of a first preference count are displayed on the polling place server monitor
iv) the number of barcodes (see section 2.5 on authorisation) issued are compared with the number of votes in the first preference count
v) at the end of each polling day (pre-poll and election day) votes are exported to WORM CDs (duplicated for comparison) and to ensure data is not tampered with during transfer an MD5 hash code is generated and transferred with the CDs
vi) CDs are transported with appropriate security measures to the security controlled central scrutiny location

In addition, information transmitted between the voting servers and clients uses HTTP. As well, the vote preferences held on the server are compared with the key strokes that generated those preferences to ensure the voter's actual preferences are what are stored in the database as the elector's vote.

2.3. Protection of hardware

The following hardware is used in the election system (as at 2016):

Election Server - is located in access-controlled premises, has password-controlled access, is used for election setup, data entry, counting and reporting, and generates the software to establish polling place servers.

Polling Place Server – one at each polling place where electronic voting is available –is located out of sight of electors, with physical protection and password-controlled access.

Voting Clients – are connected via a LAN to the Polling Place server and each comprises display monitor with WYSE terminal. Terminal is completely hidden in lower section of voting booth and monitor is placed face up on voting booth shelf (so that only elector voting can see screen content). Voting clients are accessed using a barcode randomly issued to the elector by a polling official at the polling place and based on the elector's electorate. No vote information is stored on the voting client so that no additional physical protection is provided on the WYSE terminal.

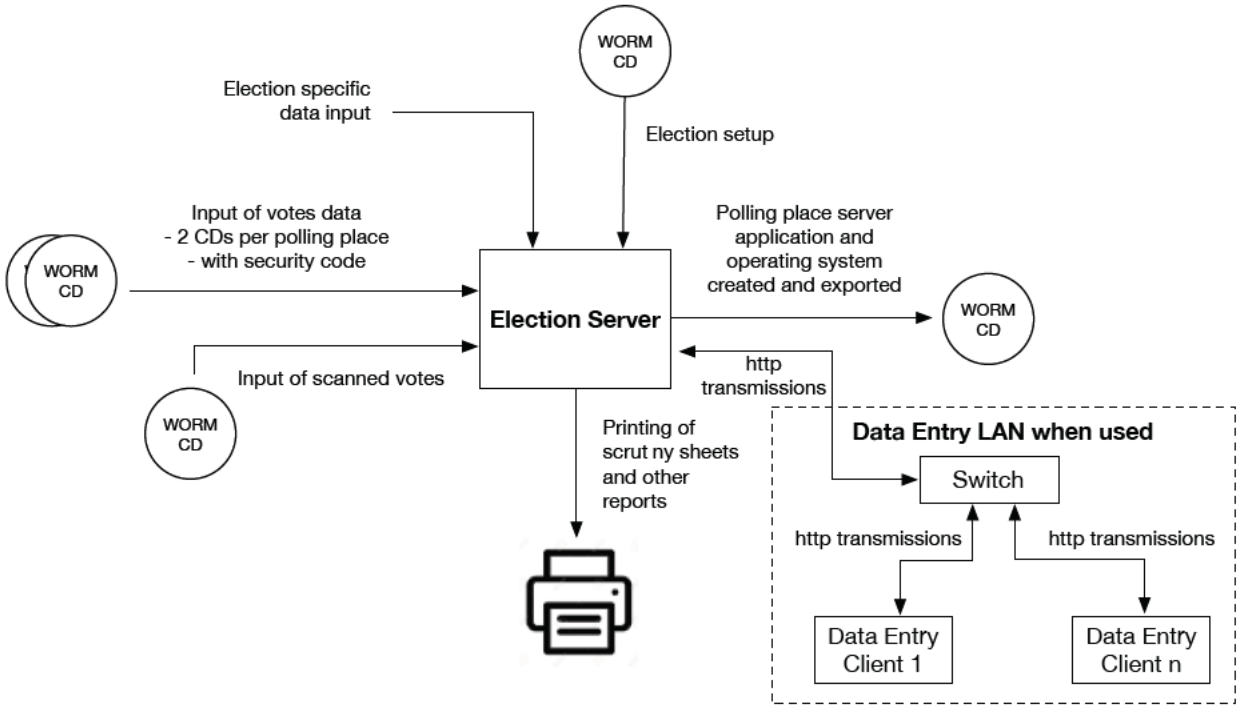

Figure 1 – Security features of Election Server functions

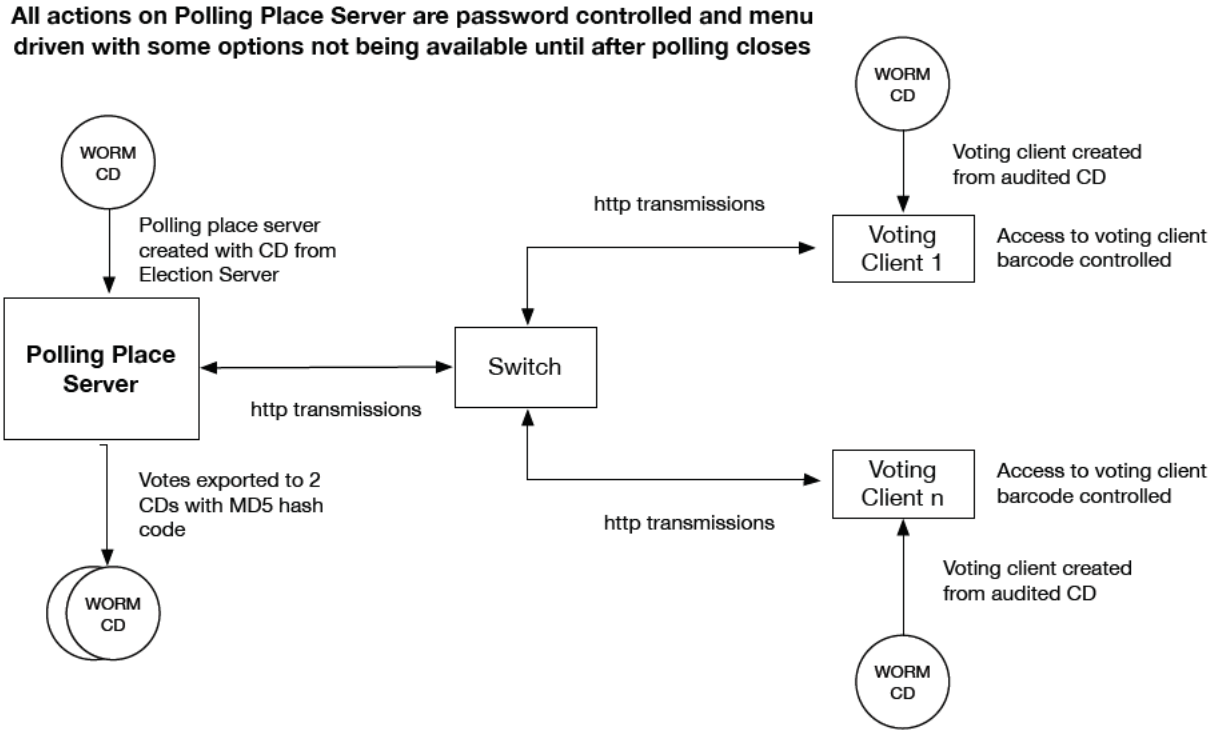

Figure 2 – Security features of Polling Place Server and associated LAN

Data Entry Clients – are located in a secure environment and are connected via a LAN to the Election Server.

Data Entry Server – is an application on the Election Server and does not have separate hardware. Activation is password-controlled.

2.4. Environment controls

The Election Server is setup in an access-controlled environment and is thereby physically protected.

At polling places, there are legislative controls that govern what can and cannot happen at the polling place when voting is occurring. However, there is still the potential for an individual to be unreasonable in their behaviour either during voting or when the polling centre is closed. Mitigation measures implemented include:

- having the polling place server hidden from public view and physically secure
- having the WYSE terminals used as voting clients hidden from public view
- not having any important information on the voting clients, so that if one is damaged in any way no information is lost
- securing unused and used barcodes in a similar manner to unused ballot papers and the ballot box for completed votes
- polling place out-of-hours protections

To mitigate against a natural disaster or failed out-of-hours protection, on a daily basis cumulative votes are exported to WORM-CDs at each electronic polling place and transported to central scrutiny, as per 2.2 v).

2.5. Authorisation controls

Access to any module of eVACS® is either password or barcode protected, and there is a log of each access.

Where access is via a password, the only possible actions are those available from the menu displayed. In addition, certain menu items are not available until after polling closes.

For an elector using a barcode to access the voting client, the only actions possible are to choose a language, select candidates in order of preference, modify selections, and confirm preferences.

3. Proposed upgrades to eVACS® Security

There are six security elements considered essential for the security of information and if one of these is omitted, information security is deficient and protection of information will be at risk. The six essential security elements are:

- Availability – ability to access information in a specified location and in correct format
- Utility – information has to be usable e.g. if the only copy of information is encrypted and the encryption key becomes unavailable the information is unusable
- Integrity – information is real, accurate and guarded from unauthorised user modification
- Authenticity/Authentication – proving identity and access rights
- Confidentiality – sensitive information can only be disclosed to authorised users
- Nonrepudiation – proof of authenticity and origin of data

In order to enhance the security of information within the electronic voting system, each of these elements has been assessed to determine if improvements can be made and these are then

reflected in the descriptions of how the security-related requirements in the BRS for upgrading eVACS® will be addressed.

Table 1 lists the security-related requirements in the BRS by requirement number and description, together with details of how those requirements are to be met.

Table 1 – Security-related requirements and the means to address

#	Requirement Description	Means of addressing requirement
2	Physically limiting the availability of ports on the hardware used within the polling place	Ports will be blocked via the Linux operating system, noting that blocking is specific to the port identifiers on particular hardware. As a consequence the operating version of eVACS® is expected to need upgrading any time the hardware is replaced. Elections ACT may also choose to physically seal ports not being used.
3	Shall be no less secure in its operations than the 2016 version of eVACS® An additional requirement identified under 'Implementation and Other Comments' for R3 is to: "deliver an electronic voting solution for electronic votes taken at polling places or via telephone voting that completely prohibits the possibility that: • an elector can be matched to their voting preferences - see R7 below; and • an elector's voting preferences can be deleted or altered in any way."	The overarching security design features implemented in eVACS® from 2001 continue to operate together with the following enhanced security features. i) replacement of barcodes with QR codes does not change the security of ensuring separation of elector from their vote at the polling place but increases the probability that the access code cannot be copied ii) changing from HTTP to HTTPS for communications between clients and servers automatically encrypts every transmission between client and server and introduces improved security of the votes, notwithstanding the security inherent in adopting an isolated LAN for voting at each polling place iii) encryption of votes in the votes database on each polling place and telephone voting server improves security of the votes, notwithstanding the physical security of the polling place servers that has been implemented since 2001, and the proposed placement of the telephone voting server in a secure environment iv) replacement of CD-ROMS with USB memory sticks can be handled by either hardware protected USB memory sticks (very expensive) or good quality USB memory sticks with encryption of data in one or multiple partitions. The program for encryption is included as part of the operating system on the polling place (and telephone voting if implemented) servers. The USB memory sticks need to be cleansed before use. v) separation from other modules of the telephone voting server with the software to setup the telephone voting server generated from the Election Server vi) independent auditing ensures that the eVACS®

		software does not add, delete or alter votes and the encryption of the votes provides further protection in database and when being transferred on USB memry sticks See also the design diagram at Figure 3.
5	Passwords throughout the system should only be able to be set if they meet ACT Government password security requirements.	ACT Government password requirements will be implemented similar to netVote*plus* with a minimum of 11 characters.
7	Ensure that an elector and their preferences cannot be matched through the use of timestamp data.	Two options were proposed by Elections ACT: i) shuffling the votes (see R8), and ii) removing the capture of timestamp data entirely. The second option will be implemented by ensuring there is no need for a time stamp to be stored with each vote. In the upgraded eVACS® all activities will be recorded with a time stamp and registered in a system log. Review of the log would show if there has been any suspicious activity. While this could be undertaken manually, programs could be implemented to look for particular (undesirable) circumstances and these identified in a separate log, which could be included with the daily transfer of vote data. Such logs are generated such that they cannot be altered in any way. Also, anyone attempting to view or print a log would be identified from their login. Hence, without time stamp information for each vote there is no possibility for an external party to link an elector with their vote, and extremely remote for an internal person due to the access controls imposed on polling place server functions.
8	Shuffle the votes when stored	Each vote will be encrypted before submitting to the votes database. The vote order within the votes database will be shuffled as part of the daily export process.
9	Fully encrypt the voting process	Encryption will be implemented as follows: - via TLS1.2 for all transmissions between the client and a server (transport layer encryption) - via SHA2 of each vote before submission to the votes database on a polling place, telephone or data entry server Only ASD approved cryptographic protocols, i.e. TLS1.2 and SHA2 are being used. The ISM specifically states that data already encrypted should not be encrypted again; hence there is no need to encrypt messages between the client and server, as well as encrypting the transmission. Also, that encrypted transmission is more important to ensure no man-in the-middle attack can access the information being

		transmitted.
10	Encrypt the cumulative record (data) of daily votes	As indicated at R9, data already encrypted should not be encrypted again. Therefore the encrypted votes in the database should not be encrypted again when exported as the daily cumulative record. Security to be employed with the USB memory sticks provides a further layer of protection for the encrypted votes. (see R35 as well)
11	Update the methodology used to ensure authenticity of exported data	MD5 encryption will be replaced with SHA2 encryption, the relevant encryption algorithm for 'data at rest' as per the ISM. The length of the SHA2 Hash is such that display/copy as with the MD5# is completely inappropriate. The proposal at R36 to print as a QR code will be implemented, noting that this incorporates implementation of a printer attached to each polling place and telephone voting server.
13	Mandate the entry of 'hash code' on the election server	The mandatory entry of the 'hash code' was an original design feature of eVACS® which is at odds with this requirement. If a change is required this will be implemented. This needs to apply to votes being uploaded from all polling place and telephone servers. The move to replace 'hash code' with QR code simply being read will improve process.
35	Replace CD-ROMs as the medium for upload and download of data	Change to use of USB memory sticks as identified above at R3, including requirement to cleanse before use and introduce public key (on USB memory stick) and private key (on Election Server) as well.
36	Replace alphanumeric 'hash code' with QR code produced by polling place server	An alphanumeric code will still be produced as an output from adopting SHA2 encryption (R11), as per the ISM, but the length of the SHA2 # is too long for display and then copying by the OIC at a polling place. The SHA2 encryption output will be converted to a QR code and printed via the Polling Place or Telephone Server for transfer with the end of day cumulative votes data, and report/s at close of polling day. QR code is to be read as input to Election Server to enable upload of votes from two USB memory sticks (R13)
50	Provide for a transparent and controlled mechanism for recovering data from a failed hard drive.	Two options are proposed for further detailed consideration and cost: 1. increase the number of RAID disks to four, and 2. controlled access as proposed by Elections ACT

Included at Figure 3 is a design diagram showing application of the new security features between the Election Server, the polling place servers and the voting clients. These include the

use of QR codes, secure USB memory sticks (USB sticks) and HTTPS for transmissions between a polling place server and its voting clients.

Also included in the Figure 3 are the proposed solutions for implementing Robotic Process Automation (RPA) for setup and installation of both polling place servers and voting clients (R15).

In order to reduce the workload associated with setup, an ethernet-based LAN connected to the Election server is proposed to create multiple polling place servers at the one time. This particular ethernet connection can only use HTTP for transmissions because during setup (after any existing software has been removed) the polling place server has no software to support HTTPS transmissions. Similarly, initially when the voting clients are being set up over the LAN at the polling place the transmissions can only use HTTP. As part of the voting client setup the functionality to use HTTPS transmissions during voting will be installed, as shown in Figure 3.

Not represented in Figure 3 is the setup for the proposed Telephone Voting Server. Although the Telephone Voting Server is basically the same as a polling place server, the differences mean that a separate menu item will be required for generating the Telephone Voting Server software. However, the intent is that the Telephone Voting Server be created in a similar manner to the polling place servers, that is, by direct Ethernet connection to the Election Server. The relationship between the Telephone Voting Server and the IVR servers as described in the Telephone Voting Proposal are the same as that between a polling place server and its clients, using HTTPS for transmissions.

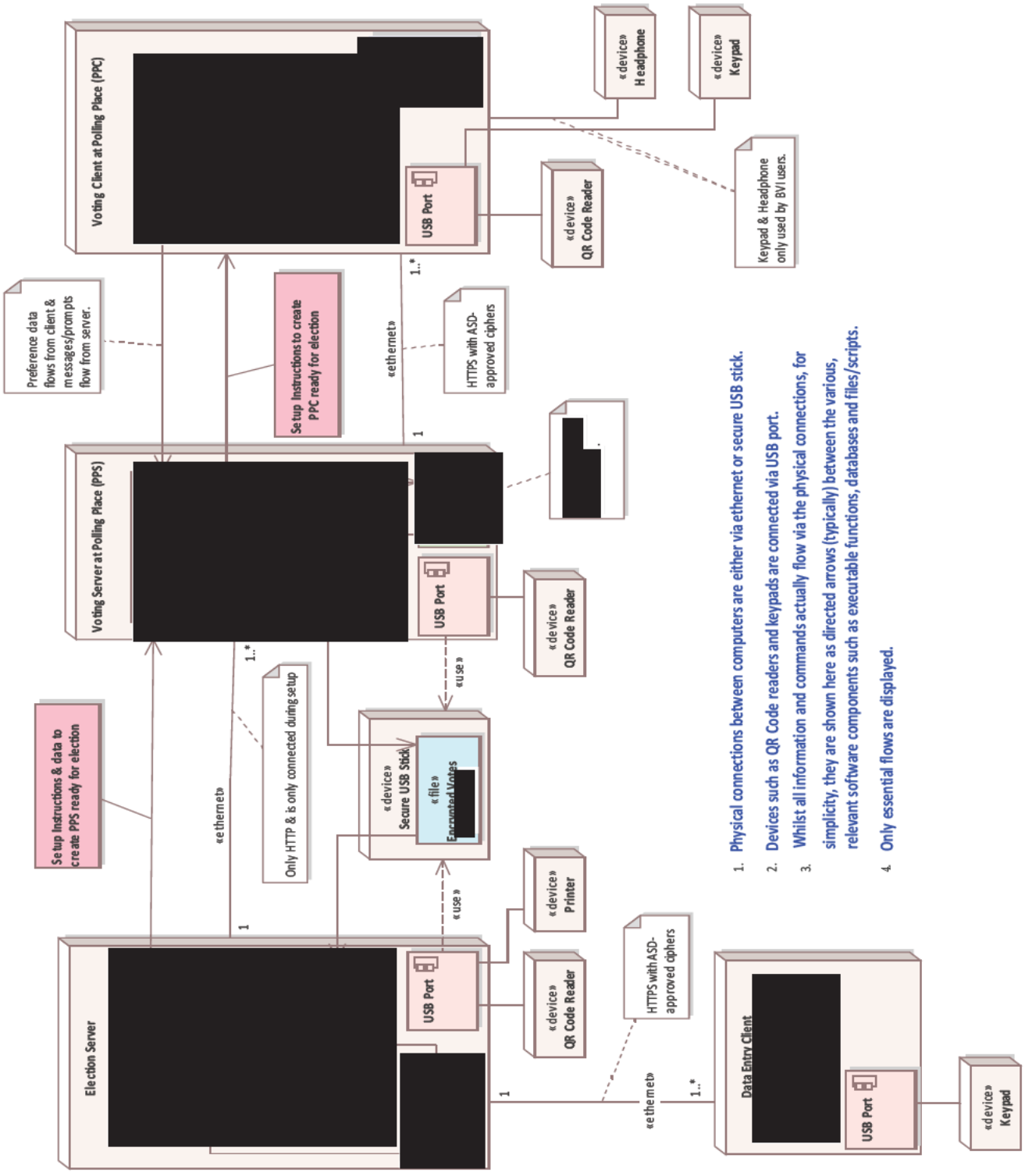

Figure 3 – Design of upgraded eVACS® showing changed and additional security features.

Abbreviations

ACT	Australian Capital Territory
ASD	Australian Signals Directorate
BRS	Business Requirements Specification
CD	Computer Disk
eVACS	electronic Voting and Counting System
HTTP or http	HyperText Transfer Protocol
HTTPS or https	HyperText Transfer Protocol Secure
ISM	Australian Government's Information Security Manual
LAN	Local Area Network
MD	Message-Digest algorithm
USB	Universal Serial Bus
WORM	Write Once Read Many