Elections ACT

Upgrade of eVACS® for the 2020 ACT Legislative Assembly Election

Operational Concept Description

Document Status: Final
Version 1.1
December 2019

Copyright Notice

Disclaimer

In compiling this Operational Concept Description document, Software Improvements Pty Ltd has relied upon the accuracy and completeness of information provided by Elections ACT.

eVACS®

eVACS® is a registered Trade Mark of Software Improvements Pty Ltd.

Where used in this Operational Concept Description, eVACS has the same meaning as eVACS®

eVACS® Upgraded Documentation Tree

- Contract with Upgrade requirements
- Project Management Plan
- **Operational Concept Description**
- System Specification - Part 1 eVACS requirements including upgrade requirements
- System Specification - Part 2 Scenario Analyses
- System Design and Software Specification
- Interface Specification - Setup election
- Interface Specification - Voting
- Interface Specification - IVR (Telephone voting)
- Installation Manual
- User Manual - Election server
- User Manual - Voting server

Document Control Information

The controlled version of this document is in electronic form.

All hardcopy versions are uncontrolled.

Modifications

Date of this Revision	Version	Comment	Author	Reviewer	Release
2019-08-04	0.1	Initial Draft	CVB	CJB	
2019-08-12	0.2	Expanded Draft	CJB	RB	
2019-09-09	0.3	IVR content revised and extended	CJB	JS	
2019-11-15	0.4	Revised following comments from EACT	CJB		
2019-12-26	1.0	Amended to reflect changes in voting sequence and touch screen operations, and includes description of new report for LAPPERDS	CJB		2019-12-30

Distribution

Name and Appointment	Document Name	Date of Issue	Version
Rohan Spence, DEC, EACT Jiv Sekon, Project Manager, EACT	Operational Concept Document	2019-09-09	0.3
Rohan Spence, DEC, EACT Jiv Sekon, Project Manager, EACT	Operational Concept Document	2020-02-14	1.0

Contents

1. Introduction

1.1 Overview

Elections ACT (EACT) is responsible for conducting elections and referendums for the ACT Legislative Assembly, and maintaining the ACT electoral roll. EACT is a Statutory Authority and is responsible for providing ACT citizens with an independent electoral service that meets their needs and enhances their understanding of, and participation in, the electoral process.

Electronic voting at selected polling places in the ACT was first introduced at the 2001 Legislative Assembly election, using the electronic voting and counting system known as eVACS®. Minor upgrades and enhancements were implemented for later Legislative Assembly elections, but following a review after the 2016 Legislative Assembly election eVACS® is now to be enhanced to provide an updated system with increased functionality and features. In particular, eVACS® is to be moved to a more contemporary platform, with improvements in security, and inclusion of a secure telephone voting module.

1.2 Document Purpose

This Operational Concept Description (OCD) describes at a high level the desired enhanced version of eVACS®, that during the development phase will be referred to as 'eVACS® Upgrade'. The structure of the document is as follows. First, the background and structure of the existing version of eVACS® is described. Second, a summary of the desired enhancements is given. Third, the two preceding sections are consolidated to give a self-contained – but still high-level – description of the desired enhanced eVACS® Upgrade system.

The purpose of this document is to provide the Software Improvements Pty Ltd (SIPL) Project Team with a specification of the requirements of the eVACS® Upgrade. The OCD will form the basis from which system requirements will be developed. The resulting System/Subsystem Specification will then form the basis for developing a detailed Software Requirements Specification and Interface Requirements Specification (IRS) documents.

1.3 Document Management

The OCD will be reviewed and amended, if required, at the first major milestone of the project. The eVACS® Upgrade Project Manager is responsible for this review in conjunction with the EACT Project Manager, and for ensuring all project personnel are advised of any variations. Any significant changes to this OCD should be reviewed and approved by the EACT Project Manager or nominated delegate.

1.4 Reference Documents

Documents referenced in this OCD include:

1. Business Requirements Specification ICT Business System upgrade - eVACS®, version 1.0;

2. Contract – Electronic Voting and Counting System (eVACS®) Enhancements, Services and Support: ACTGS reference 636238 Final Version 23 July 2019, including the Statement of Requirements at Schedule 2 being a modified version of the Business Requirements Specification;

3. Unified Modeling Language (UML) Specification - Version 2.5, May 2015. Object Management Group (OMG) website - https://www.omg.org/spec/UML/2.5; Sections 11.6 (Components) and 10.4 (Interfaces) are typically used to describe high level views of systems.

4. Executable UML: A Foundation for Model-Driven Architecture by S. Mellor & M. Balcer, 2002 (Addison Wesley). Chapters 3 and 15 provide description of Domain Charts and Domain Verification as part of the Executable UML methodology for constructing and executing models, which are constructed using a large subset of UML 2.5. Domain Charts are a precursor to Component Diagrams (now standardised in UML 2.5)

5. BridgePoint (BP) 6.1 Style Guide to xtUML Modeling, 2011 (from BP Help System). BP is an open source toolset that supports Executable UML and is maintained under the banner of xtUML.org on the world-wide web (WWW).

6. BridgePoint 6.1 The xtUML Modeling Guide, 2011 (from BP Help System).

7. Guide to the preparation of operational concept documents ANSI/AIAA G-043A-2018

8. Safe and Secure Software – updated for SPARK 2014, John Barnes, 2015, AdaCore

9. ISO/IEC 8652 Information Technology – Programming Languages – Ada, 3rd edition December 2012

2. Current eVACS®

2.1 Background

For the October 2001 ACT Legislative Assembly election EACT introduced a non-Internet electronic voting within four pre-poll centres around Canberra for two weeks prior to Election Day and at a number of polling places on Election Day. A computer program on a separate 'counting' server allowed the upload of data from electronic votes or manual data entry of paper ballots in order to count all votes according to the Hare-Clark rules of the ACT.

SIPL provided the software (known as eVACS®) for voting and counting for the 2001 and 2004 ACT Legislative Assembly elections and the Casual Vacancies that occurred between those two elections. For the 2008 Legislative Assembly election, EACT introduced scanning of paper ballots, and eVACS® was modified to enable the upload of electronic vote data from the scanning process. Scanning of paper ballots has continued to be used in all subsequent elections up to 2016.

2.2 Operational policies and constraints

The ACT has a relatively complex electoral system. The system used is the Hare-Clark single transferable vote system of proportional representation. Currently the Legislative Assembly comprises 25 members, with 5 members being elected to represent each of 5 electorates. The ACT voting population is approximately 300,000 electors. The ACT has fixed term elections, originally every three years, but from 2004 at four-year intervals. The next Legislative Assembly election is in October 2020. (More details about the ACT voting system are available on the EACT website https://www.elections.act.gov.au.)

To vote, electors are asked to number candidates in the order of their preferences, using sequential numbering starting with '1' being their most preferred. Candidates are listed on the ballot paper in columns, with registered political parties and non-registered party groups given their own column. Independent candidates are listed together in one or more columns.

The order of the candidates' names in each column is changed from one ballot paper to another using a system called Robson Rotation. This aspect of the voting system gives candidates equal chances to be at the top of their particular column across all variations (60 for 5 member electorates) of the ballot paper. Voters must vote for candidates; they do not have the option of voting for parties.

A ballot is considered formal if there is a first preference indicated. The voting instructions recommend voters give at least as many preferences as there are seats in the electorate, and then as many further preferences as desired.

2.3 Description of current eVACS®

The following is a broad view each of the five modules forming the electronic voting and counting system as operated in the ACT:

- Election setup
- Electronic voting
- Data entry of paper ballots

- Counting ,and
- Reporting

2.3.1 Election setup

The following information is input by officials into the setup server:

- Election name and date
- Names of electorates
- Details of pre-poll and polling places, including batch numbers for paper ballots
- Names of parties fielding candidates for the election
- Names of candidates, arranged by electorate and by party
- Names of candidates who are ungrouped – who do not belong to any of the parties, arranged by electorates
- The form of the ballot papers

The setup server generates the voting server software, including operating system, that is loaded on to hardware to create the voting server at each polling place, referred to as the polling place server.

2.3.2 Electronic voting

The voting client presents voters with the ability to select instructions in their language of choice selected from English and a number of additional languages which may change between elections depending on the use of those languages within the community. For example, in 2016 the languages which could be selected were:

- Arabic
- Chinese – Simplified (Mandarin)
- Croatian
- Greek
- Italian
- Korean
- Lao
- Persian / Farsi
- Portuguese
- Serbian
- Spanish
- Vietnamese

Voters with disabilities are also able to use the system, for example, instructions through earphones are provided to voters with vision-impairment. To date, audio instructions have only been available in English.

Those voters who decide to vote electronically are issued with a barcode by a polling official who also marks their name on the electoral roll. The barcode is used to verify to the voting interface that the voter has a right to vote in a particular electorate. At the voting booth, instructions on how to vote are displayed. Several levels of help are available.

The voter begins the voting process by having their barcode read a first time. If the barcode is accepted, a full view of the ballot paper for their specific electorate is displayed.

Using a telephone-style keypad, the voter selects their candidates in preference order. When each candidate is selected, the next sequential preference number is displayed (or announced via audio). A voter is able to choose not to vote for any candidates - thus making an informal vote. Options to cancel a preference or begin again are provided. There is also an option to 'hide' their vote if a voter needs to seek help from an official. When the voter selects the 'Finish' (#) key, the voter is required to have their barcode read a second time to confirm their selection of candidates. The system provides security that will allow the voter to cast only one vote per barcode.

After the vote has been confirmed, voting data is stored initially in two locations.

After polling closes first preference distributions are calculated before all the voting data is transferred to the vote counting system via removable WORM disks. Data is protected by an MD5 checksum and two randomly generated 128-bit keys. The daily cumulative voting data is also transferred with the same securities in place.

2.3.3 Paper ballots

For those electors who vote using a paper ballot the voting procedures remains unchanged. Voters are asked to mark sequential preferences on their ballot paper up to the number of seats to be filled for their electorate, or for as many more candidates as they desire. A single '1' marked on a ballot paper is considered a formal vote. The ballot paper is then folded and deposited in a cardboard ballot box.

2.3.3.1 Data entry of paper ballots

At the close of the poll, at each polling place the lodged paper ballots are unfolded and counted to first preferences and bundled into batches according to the candidate for whom the voter's first preference is indicated. These bundles form the basis of the batches to be entered into the vote database. Following first preference results being reported, the ballot papers are transferred to a central location where they are manually entered into the vote database. The paper ballots are keyed in the batches as compiled at the polling places. Each ballot paper is keyed by two operators as a way of verifying operators' input; a supervisor resolves any differences.

2.3.3.2 Scanning of paper ballots

Since 2008, paper ballots for scanning are unfolded, first preferences counted and then bundled into batches. As per the data entry procedures, following first preference results being reported, the ballot papers are transferred to a central location where they are scanned. Once any unreadable papers have been examined, the electronic vote data is exported and imported into the eVACS® counting system.

2.3.4 Counting and reporting

The vote counting program enables an automatic Hare-Clark scrutiny for the election. The program calculates preference distribution results using data obtained through electronic voting and electronic vote data obtained from paper ballots to provide progressive reporting from election night onwards. The results are presented as scrutiny and distribution sheets.

2.4 Design and security

A range of security features were built into the design of eVACS® in 2001, and these are inherent in the 2016 version. They are:

- a non-Internet solution, being a secure ethernet-based LAN at each polling place
- both voting and data entry terminals being equivalent to dumb terminals with no data stored on them
  - voting access is barcode controlled
  - data entry access is password protected
- a server at each polling place with physical protection, authorised access controls, duplicate hard drives, and only menu driven functionality
- any existing software or operating system on any of the hardware is removed as part of the installation process for eVACS® software modules
- any vote data transferred from polling places is protected with an MD5 checksum and two randomly generated 128-bit keys
- all printouts, such as scrutiny sheets, are printed directly with PostScript and cannot be altered
- counting and data (voting and data entry) servers with only authorised access and menu driven functionality
- only authorised software can be used for an election, and the software for polling servers is generated by the election set-up server, and
- the operating system is a cut down version of Linux, only supporting the functions required by eVACS®.

eVACS®, as used in 2016, is written in the 'C' language and, as mentioned above, the operating system is a cut down version of Linux. During the years since 2001 the operating system has been upgraded, although currently is not the latest version.

3. Justification and need for changes

There are two main concerns driving the need for changes in eVACS®:

- Modernisation of the underlying technologies and hardware, including security, and
- Improved usability and accessibility for voters

3.1 Justification for changes

Following independent review of eVACS® after the 2016 Legislative Assembly election, together with concerns raised by Members of the Legislative Assembly, the following are being addressed via the proposed upgrade:

- modernisation of the underlying technologies and hardware
  - currency of operating system
  - more appropriate language with better security and functionality features
  - absence of modern-day management and security protocols (such as database encryption)
  - system not meeting compatibility requirements of modern hardware
- improved usability and accessibility
  - out-of-date screen displays
  - replacement of keypads for navigation (touch screens for non-B&VI electors)
  - an alternative secret voting process for electors who have difficulty in attending polling places (telephone voting module)

A number of other improvements to the processes of installing and operating eVACS® have also been identified for inclusion in the upgrade.

3.2 Description of changes

The changes required can be summarised as follows:

Access passwords – to be accepted a password to meet ACT Government and ASD password security standards.

Audio – .WAV files to be used.

Audio files to be nested for easy identification of individual files by EACT staff

Autonomy – no details of an election to be hard coded into the software. Configuration of the system is to be possible with specific inputs as part of tailoring the system for a particular election. Such tailoring is to continue to be carried out by EACT staff without the need for intervention of SIPL staff.

Ballot layout – the layout of electronic ballots is currently fixed. As part of the setup process, the format of a ballot paper to be customisable for an election, including configuration of:

i) font size for candidate names
ii) font type, size and placement of text.

Ballot rotations - eVACS® allows for Robson Rotations based on 5 and 7 member electorates, although currently all electorates have only 5 members. Flexibility in having different numbers of members should not be deleted from the system; this includes allowing for input of number of members and the associated rotation sequences.

Barcodes– 1D barcodes used by voters to be replaced with 2D barcodes (QR codes).

Official, or master QR code, to be introduced for use by officials to access new menu for selection of appropriate reset options on voting clients with touch screens.

QR codes able to be prepared as postscript file for provision to contracted printer, as well as ready-for-printing inhouse.

Convert SHA-2 encrypted hash code output to QR code at polling place server to be read as input to election sever when uploading vote data.

Counting – provide for the calculation of vote values rounded down to 6 decimal places.

Counting to be based on Ada 2012 and stored procedures.

Data entry of paper ballots - the data entry module of eVACS® to continue to be operational; however, as EACT considers the likelihood of use to be very remote, the ‘C’ data entry module is not to be rewritten but simply integrated into the modernised eVACS®.

Error codes – error codes to have a direct reference to the exact nature of the error. The nature of error and resolution actions to be detailed in system documentation.

Hardware – dependencies on particular hardware configuration items to be minimised, for example, the existing eVACS® places requirements on the choice of printers.

Incorporation of touch screens for voting, noting that the use of a setup with a telephone-style keypad and audio instructions will continue to be available at each polling place for B&VI electors.

Unused ports on hardware at polling places to be decommissioned via the operating system.

Polling place and telephone voting servers to be capable of supporting printing of reports, hence the connection of a printer.

The absence of disk readers in modern hardware, challenges the continued use of WORM disks for installation of software on hardware and the transfer of data. Hence, disks to be replaced with secure USB memory sticks that support encryption of contents.

Multiple languages – the interfaces used by voters to be based on Unicode text and available in multiple languages, where the number and specific languages to be used can vary between elections.

Unicode text also to be used for all interfaces used by officials and the reports generated by the system.

Multiple polling place servers – currently the polling place servers, one per electorate, are created by loading a voting server installation created by the election setup server. This manual process is to be replaced with an automatic load process using an isolated LAN connected to the election setup server. As part of the installation process, automatic testing to ensure correct operation of the server is to be implemented.

Identification of the polling place of a particular voting server is to be undertaken after delivery to the polling place.

Multiple voting clients – each polling place has multiple identical voting clients connected via a LAN to the polling place server. The manual process of installing the voting client software onto hardware to be replaced with an automatic load and test process from the polling place server.

Network encryption – eVACS® currently uses http for communications across the LAN at each polling places. Update to https (currently based on TLS1.2) to ensure all these communications are encrypted.

Printing – In addition to scrutiny sheets, new reports to be printed include:

i) first preference count for each polling place and telephone voting after close of polling on Election day
ii) reports of errors, votes not concluded, languages used, and use of B&VI system printed individually and collectively
iii) SHA2 hash in QR code form in association with daily export of votes at polling places
iv) Scrutiny sheet preference tracking report

Privacy – ensure no potential link between voter and their vote by eliminating any timestamp associated with a vote, shuffling votes within votes database on polling place server and encrypting votes with SHA-2 algorithm. (see also Vote data encryption)

Reports – the format of scrutiny sheets and other generated reports is currently fixed. The reporting software to be flexible enough to support a variety of different types of reports, noting that a number of additional reports are required:

i) frequency of types of error code experienced during polling
ii) number of electronic votes commenced but not concluded
iii) number of occurrences of selection of each language other than English
iv) number of occurrences system accessed by B&VI electors
v) ‘result of count’ (first preference count) undertaken after close of polling on Election day to be printable
vi) report for import into LAPPERDS (see Appendix B for file format)
vii) Scrutiny sheet preference tracking report

Scanning of paper ballots – scanning of paper ballots to continue outside of eVACS®. The electronic vote data obtained from scanning to continue to be imported into eVACS®.

Setup procedure – the existing eVACS® setup server comes with certain database tables already created; these tables to be created from data entered during the autonomous election setup procedures.

The change to daylight saving occurs during the pre-poll period for ACT Legislative Assembly elections. Date of change to be incorporated into required setup election data so that servers can automatically change the date during operations.

To support testing of the system, provide for the resetting of the date and time without needing to adjust the settings in the BIOS.

Software – All existing functionality to be migrated from ‘C’ to Ada 2012, with SPARK used to ‘prove’ the integrity of the software.

Provide for a version of the source code easily publishable on the Elections ACT website, as well providing to an independent code auditing company.

Provision of a transparent and controlled mechanism for recovering data from a failed hard drive.

Telephone voting server – incorporation of a telephone voting module requires inclusion of a telephone voting server. Although similar in purpose to a polling place server, because additional functionality is required, a separate telephone voting server installation and creation via the setup election server is necessary.

Vote data encryption – vote data to be encrypted in the polling place server database using SHA-2 algorithm and when exported.

Vote reconstruction – as part of confirming a vote, the current voting client sends to the voting server not only the list of preferences but also the list of keystrokes used to construct the vote. The voting server then 'reconstructs' the vote using the keystrokes and compares it with the list of preferences. Only if there is a match is the vote confirmed. (A failure to match should never occur.) This checking to be continued for the B&VI booth at the polling centres.

With the introduction of touchscreens for voting, where used the list of keystrokes to be replaced with a list of screen touches for comparison with the preferences list.

Vote transfer – vote data to be encrypted for transfer from polling place server to election server, with mandated entry of 'hash code' before upload to election server possible.

Voting – display a particular coloured screen for an agreed period of time to visually indicate that an elector has successfully finalised the casting of their vote.

Preference box and candidate name to be a single touch element on touch screens.

4. Concept for upgraded eVACS®

Encompassed in this section is a description of all the elements to comprise the upgraded eVACS®.

4.1 Background, objectives and scope

The scope of the upgraded eVACS® is essentially the same as eVACS® but with an additional module to support telephone voting. The latter, to provide specifically an alternative to enable electors with a disability and blind and vision impaired electors who have difficulty attending a polling place to vote in secret.

As indicated in section 3, a key objective of the eVACS® upgrade is modernising the system and its development. To that effect the system is to be:

i) modelled and the model used to autogenerate code, thereby reducing the potential for coding errors and the testing time during development of components
ii) migrated to Ada 2012 using SPARK, which is used for the development of high integrity systems where predictable and highly reliable operation is essential

Improved security is another key objective, but without diminishing the existing in-built security features, by:

- Ensuring only audited software is used for an election, and the software for different modules is generated by and installed via the election setup server
- Only menu driven functionality is available, with some access controlled via official (master) QR codes
- Maintaining a LAN at each polling place but moving from http (without encryption) to https (with encryption) for all communications between voting clients and the polling place server
    - https also to be used for communications between the telephone voting server and the IVR system
- Moving from one dimensional (1D) barcodes to 2D barcodes (QR codes) for accessing the voting clients at polling places
- Ensuring vote data is encrypted in the database and when being transferred from polling places
- Moving from MD5 and 128-bit security to SHA-2 algorithms
- Mandating the entry of security on the election server when vote data is being uploaded
- Implementing ACT government approved length passwords whenever passwords are used
- Using two-factor authentication for telephone voters
- Physically limit the availability of ports on voting server hardware

A third key feature is improving accessibility via:

- adoption of touch screens, and
- introduction of telephone voting.

4.2 Operational policies and constraints

For use in any Legislative Assembly election the upgraded eVACS® must comply with the relevant legislation and other regulations. Such legislation governs:

- The format of ballots: order and arrangement of columns and rows
- Rotation of candidates on a ballot
- What constitutes a formal ballot
- What types of informal ballots can be accepted
- Counting procedures
- Reporting

The following high-level constraints – non-functional requirements – include many carried over from the current eVACS®.

4.2.1 Constraints on electronic voting

- The system shall allow input of preferences using a standard telephone style keypad.
- The system shall ensure that two copies of the electronic voting data are recorded in separate locations within the polling place immediately a vote is cast and confirmed by the voter.
- The system shall provide for the transfer of electronic voting information (not via the Internet or any publicly accessible network) from voting at pre-poll centres at the end of each pre-polling day and polling places at the end of polling on polling day to the vote counting system.
- The system shall not be connected to any outside network in any of the pre-poll centres, electronic-voting equipped polling places, and the central scrutiny centre so that unauthorised access to the system is prevented.
- While the telephone voting server must be connected to the IVR servers supporting telephone connection, the telephone voting server must be located in a secure environment and setup such that the only communications are via https to the IVR servers.
- The electronic voting interface shall incorporate recorded spoken instructions in English broadcast over disposable headphones for sight impaired people and for people with reading difficulties.

4.2.2 Constraints on electronic vote counting

- Configuration information to provide for a complete backup of data relayed to or captured by the system shall be provided.
- The system shall be capable of amendment to cater for enhancement and legislation changes.
- The system shall allow programming code to be independently audited and be available to scrutineers for verification and to ensure “what goes in is what comes out”.
- The system shall be secure and once the code is verified and audits are complete code should be certified and locked so no further changes can be made.

4.3 Description of the upgraded system

4.3.1 The operational environment and its characteristics

The operational environment is substantially unchanged from the previous releases of eVACS.

The upgraded eVACS® requires the following hardware components:

- PCs for servers capable of running Linux, includes election setup server, polling place servers and telephone voting server, and servers running Windows for the telephone IVR servers
- Printers (for printing 2D barcodes for testing and reports)
- All-in-one PCs with touch screen for voting clients at polling places
- PC for B&VI voting booth at each polling places, if all-in-one PC is not suitable
- Telephone-style keypads (for all B&VI voting booths at polling places)
- 2D barcode readers (for voter authentication and for official access to menus on the voting clients, polling place servers, telephone voting server and the Election server)
- Headphones (for use by vision-impaired voters)

4.3.2 Major system components

Upgraded eVACS® includes the following software components:

- Election setup server (one instance)
- Electronic voting client (many instances per polling place)
- Electronic voting server (one instance per polling place)
- Electronic telephone voting server (one instance)
- Paper ballot entry client (many instances)
- Counting and reporting server (one instance; including paper ballot entry server)

The components interact as follows:

- All information concerning the election is entered into the election setup server, which is used to generate installations for voting servers (polling place and telephone), and combined paper ballot entry/counting and reporting servers.
- All instances of the voting client are identical. All instances of the voting (polling) place server are identical.
- Each group of electronic voting clients installed in a polling place communicates with the electronic voting server installed at that polling place.
- All instances of the paper ballot entry client are identical. Each paper ballot entry client communicates with a paper ballot entry server.
- The telephone voting server interacts with the IVR component of the telephone voting system.

4.3.3 Interfaces to external systems or procedures

Paper ballots

A combination of electronic voting and paper ballots is permissible. Each paper ballot should have the number of the rotation printed on it; this number is entered during paper ballot entry so that the same ballot paper can be displayed for use by the DEO.

In eVACS®, paper ballots are batched into lots of 50 for data entry. Each batch is assigned a unique identifier composed of the electorate, polling place, and batch number for that polling place.

At the end of polling, officials empty the ballot boxes, group the paper ballots by first preferences and within each group into batches and attach a batch code for that polling place.

Paper ballots are also put into batches with unique identifiers for scanning. Electronic votes from scanning are uploaded to the counting module of eVACS® with identifiers based on the batch identifiers.

Telephone voting system

The telephone voting system comprising two operations:

i) registering to vote by telephone, and
ii) voting via telephone.

The registration process is a manual process in which electors call an EACT service and provide information to establish their identity and that they are on the electoral roll, a private Personal Identification Number (PIN) to be used later when voting, and an email address which is used to send a unique voting token to the elector. The PIN / voting token pair are used by the elector to authenticate themselves as a registered telephone voter. The PIN / voting token pairs are stored in the telephone voting server to support the authentication process.

4.3.4 Capabilities/functions of upgraded eVACS®

4.3.4.1 Integrity of the software and the ballot data

- Software components are loaded into the various client and server hardware components. The integrity of such software components shall be maintained: once configured by officials for a particular election, it shall not be possible to make modifications to, or otherwise tamper with the software.
- The system shall not allow ballots to be added, modified or deleted, other than by authenticated voters using the electronic voting client or telephone voting and DEOs using the paper ballot entry interface.
- The electronic voting system shall have a form of checking to verify that the voter intention as expressed by their interaction with the client software is consistent with the vote recorded.

4.3.4.2 Election setup

EACT officials provide the following election information to eVACS®:

1. name and date of the election
2. names of the electorates
3. details of pre-poll and polling places, including batch numbers for paper ballots
4. details of barcodes (e.g. polling place and electorate codes)
5. details of voting tokens for telephone voting (e.g. electorate codes)
6. information about rotation of candidates on the ballot
7. date daylight saving commences in the ACT
8. the form of the ballot papers
9. audio for vision-impaired voters
10. names of the parties
11. names of the candidates, identified by party (if any) or independent and electorate

Setup procedures take place in two phases:

Phase 1 Election information items 1, 2, 3, 4, 5, 6 and 7 are uploaded to eVACS®. Electorate and polling-place-specific barcodes, including Master Admin barcodes, are generated and exported for sending to a contractor for printing in 2D format. Voting tokens are generated and stored ready for incorporation into the telephone voting server installation software, and exported to enable assignment to registered telephone voters.

Phase 2 Election information items 8, 9, 10 and 11 are uploaded to eVACS®. The installation of voting servers can then be undertaken, including the installation for the telephone voting server.

4.3.4.3 Electronic voting

The following functional requirements are carried over from those placed on the existing eVACS®:

- The system shall ensure that each elector may vote at most once for the electorate in which they are enrolled.
- The system shall ensure that the ballot paper appears to the voter without bias to a particular candidate or party.
- The ballot paper should be easily readable.
- The system shall protect the anonymity of each elector.
- The system shall ensure that the system is capable of providing at the end of each day of the pre-polling period and polling day, electronic back-up copies (master and slave) of cumulative voting data held on the polling place server at each electronic pre-polling and polling centre.
- The system shall allow for voting data to be transferred to the vote counting system without being accidentally or deliberately lost, altered, copied or stolen.
- The data transfer should occur in a timely manner that ensures that the vote counting system is able to complete preference distribution of all votes cast electronically as soon as practicable on polling night.
- The system shall be secure and once the code is verified and audits are complete code should be certified and locked so no further changes can be made.

There are 4 key screens displayed on the voting client during the electronic voting process:

i) Welcome screen linked to selecting language and having barcode read
ii) Main (voting screen) where voters select their candidate choices in order of preference
iii) Confirmation screen - where voters review their choices and either Confirm (with a second reading of their barcode) or return to change their choices
iv) Thank you for voting (Acknowledgement or Acceptance) screen – advising that the voter's vote has been accepted

Other screens are used to display error messages, for informal voting, or if the voter wants to hide their vote while they seek assistance from an official.

Instead of navigating with a keypad to move between and around screens and to select candidates, with a touch screen voters will be able to touch a candidate's name/preference box and use screen buttons, such as 'Clear Choices', 'Undo Last Choice, for changing candidate selections, and 'Next', 'Go Back' to move between screens. The names of buttons are to be agreed with the EACT.

The setup for B&VI voters remains unchanged.

4.3.4.4 Data entry or scanning of paper ballots

For those electors who vote using a paper ballot the voting procedure and the collection of ballot papers remains unchanged. Similarly, the processes for obtaining electronic vote data from either data entry or scanning of paper ballots are unchanged.

4.3.4.5 Counting and reporting

The vote counting program produces the required scrutiny sheets for the election. The program calculates preference distribution results using the data stored in the 'committed' votes database, which contains electronic votes (from polling places and telephone voting server) and votes from scanning and/or manual entry of preferences from paper ballots. Progressive reporting, from election night onwards, is possible during the process of scanning or entering paper ballots.

The counting system can export its own vote data and import vote data generated by any electronic voting server. Each ballot stored in the votes database is tagged in such a way as to prevent it from being counted twice.

The counting system can also be operated when a casual vacancy arises and a countback is required.

The following functional requirements are carried over from those placed on the existing eVACS®:

- The system shall provide an audit trail for election results.
- The system shall be capable of being tested by election officials under load conditions to the satisfaction of election participants prior to acceptance of the system.

4.3.5 Performance characteristics

The following characteristics are carried over from those placed on the existing eVACS®:

- After the electronic voting client is used to cast a vote, the voting client shall be ready for the next elector within a specified time.
- After the paper ballot entry client is used to enter a paper ballot, the ballot entry client shall be ready to enter a new ballot within a specified time.

4.3.6 Quality attributes

The system shall allow programming code to be independently audited and be available to scrutineers for verification and to ensure "what goes in is what comes out".

Auditing of software is not a simple task and while eVACS® has passed all audits to date not every aspect of the software has been thoroughly examined. From Barnes (2015) "Ada introduces restrictions and checks, with the goal of providing freedom from errors. On the other hand 'C' gives the programmer more freedom, making it easier to make errors", which provides an argument to support migrating eVACS® from 'C' to Ada.

In addition, the Ada programming language has been a standard since 1983 (originally an ANSI standard), with the latest version of the Ada language issued as an ISO standard in December 2012 (known as Ada 2012).

After Barnes (2015) the recognised features of Ada that when used lead to quality programming include:

- Clear and unambiguous syntax
- Strong typing
- Limits the use of pointers
- Architecture that groups related entities together
- Object-oriented programming that encapsulates types
- Object construction controls

- Memory management
- Correct startup
- Safe and secure communication
- Concurrency within the language
- Certified with SPARK

Barnes (2015) describes Ada as “an excellent language for writing reliable software. Ada allows programmers to catch errors early in the development process. Even more errors can be detected by using SPARK without having to rely on testing – a difficult and error-prone process in itself, yet an indispensable part of the software process.

For the highest level of security-critical applications it is not enough for a program to be correct. It also has to be shown to be correct. This is usually called certification and is performed according to the methods of a relevant certification agency. SPARK is of great value in developing programs to be certified as safe or secure as appropriate. “

4.3.7 Provisions for security and recovery

The following characteristics are carried over from those placed on the existing eVACS®.

- The system shall ensure that two backup copies of the electronic voting data are recorded in separate locations within the polling place immediately after a vote is cast and confirmed by the voter.
- The system shall ensure that the system is capable of providing at the end of each day of the pre-polling period, electronic back-up copies of voting data from each pre-polling centre.
- The system shall provide for the transfer of electronic voting information (not via the Internet or any publicly accessible network) from voting at pre-poll centres and polling places at the end of polling on polling day to the computer vote counting system.
- The system should be capable of operating securely in order to ensure data is not accidentally or deliberately lost, altered, copied or stolen.
- The system shall support backup of the election setup and data entry servers.

As John Barnes (2015) stated “The world is becoming more and more concerned about both safety and security. Accordingly, it is important that software for systems in which safety or security are a major requirement should be safe and secure.” In 2019 security in government systems is of major importance, with governments in Australia requiring penetration testing and IRAPS to demonstrate the security of existing and new systems.

As a consequence, the security features within eVACS® are to further strengthened as in section 4.1.

4.4 User/affected personnel

The following categories of user are involved in the operation of eVACS®:

- Election officials
- Hardware and technical support
- Polling place officials
- Voters
- Data entry operators, if data entry of paper ballots is required

Although scanning operators are involved in scanning paper ballots, they have no involvement with eVACS®.

4.5 Support and maintenance

Support for EACT is negotiated on an as required basis.

With a four-year Legislative Assembly election cycle, eVACS® is only used every 4 years for an election, although recounts for Casual Vacancies may occur in the intervening period. EACT has included in the upgrade contract maintenance of the system in the year preceding the next election to ensure the latest versions of software are incorporated in preparation for the election.

5. Operational scenarios

Sample interactions with various components of the upgraded eVACS® are provided at a high level for electronic voting, including touch screen voting, keypad with audio voting and telephone voting, and data entry of paper ballots. The examples are not intended to capture all possible interactions within each component, but rather as an aid to understanding the broad scope of the system.

Detailed event-action lists are included in the Software System Specification.

5.1 Electronic voting

The following scenarios illustrates successful electronic voting by a voter. Treatment of error conditions (e.g. unsuccess read of barcode) or informal voting is omitted. There are three scenarios:

- Touch screen voting
- Keypad with audio voting
- Telephone voting

5.1.1 Touch screen voting

1. Voter has name marked off on electoral roll, receives e-voting card from polling official, and proceeds to electronic polling booth.
2. Voter sees Welcome message with option to select language and then instruction in selected language to scan e-voting card to start voting.
3. Voter places e-voting card under barcode reader. If valid e-voting card, the Main Voting screen is displayed, with the entire ballot paper viewable on screen.
4. Voter presses screen for desired first preference candidate. Preference box against Candidate name is highlighted and the number 1 appears in the box.
5. Voter then presses another candidate name for second preference and so on, with the number 2, etc appearing in the box next to the candidates in order chosen.
6. Voter presses NEXT button. The vote confirmation screen is displayed, which lists the names and parties (if any) of the previously selected candidates in increasing order of preference.
7. Voter has option to GO BACK to Main Voting screen or to scan e-voting card to cast vote.
8. Voter places e-voting card under barcode reader. If the two barcode reads match, the vote is accepted and the vote acceptance screen is displayed.
9. After a timeout, the Welcome screen reappears.

5.1.2 Keypad with audio voting

1. Voter has name marked off on electoral roll, receives e-voting card (and headphones if required) from polling official, and proceeds to electronic polling booth.
2. Voter puts on headphones (and if necessary seeks assistance to plug in headphones) and hears welcome message and instructions to press any key to find out what it does played in a loop, with message to scan e-voting card to commence voting.
3. Voter places e-voting card under barcode reader and If valid barcode the group heading where the cursor is randomly located is announced.
4. Voter navigates between groups by selecting the 4 (previous) or 6 (next) key, and up/down to candidates within a group by selecting the 2 (up) or 8(down) key.

5. When voter reaches first choice of candidate, audio announces the name of candidate and group, and when voter presses the SELECT (5) key, the name of candidate, group and the preference number, in this case ‘one’, are announced.
6. Voter navigates up/down between candidates and previous/next between groups and for each press of the Select key until they have selected all their preferences, numbered in increasing sequential order.
7. When all choices have been selected, the Voter presses the FINISH (#) key. The names of candidates and their groups and preference numbers are then announced in order commencing with their first preference.
8. If selection list is correct, the Voter places their e-voting card under the reader again. If the two barcode reads match, the vote is accepted.
9. Voter receives a message to say their vote has been accepted and thanking them for voting.
10. After a timeout, the welcome message is heard.

5.1.3 Telephone voting

1. Voter has previously registered for telephone voting, provided a private Personal Identification Number (PIN) and received an email with a unique voting token.
2. Voter calls the telephone voting number and selects 3 to vote (selecting 1 is registering to vote, selecting 2 to hear voting instructions).
3. Voter hears message welcoming them to the ACT Legislative Assembly election, and they are asked to enter their PIN followed by their voting token.
4. If PIN and voting token pair match with a pair in the database, audio is played with instructions on how to vote by using the telephone keypad and when they are ready to vote to press 3 (a currently unused key in the B&VI system).
5. Voter presses 3 and audio is played announcing the electorate of the ballot paper and at which group the system is currently located.
6. Voter navigates between groups by selecting the 4 (previous) or 6 (next) key, and up/down to candidates within a group by selecting the 2 (up) or 8 (down) key.
7. When voter reaches first choice of candidate, audio announces the name of candidate and group, and when voter presses the SELECT (5) key, the name of candidate, group and the preference number, in this case ‘one’, are announced.
8. Voter navigates up/down between candidates and previous/next between groups and for each press of the Select (5) key until they have selected all their preferences, numbered in increasing sequential order.
9. When all choices have been selected, the Voter presses the FINISH (#) key. The names of candidates and their groups and preference number are then announced in order commencing with their first preference.
10. If selection list is correct, the Voter enters their PIN again. If the PIN is a match with that entered at the start of the voting session, the vote is accepted.
11. Voter receives a message to say their vote has been accepted and thanking them for voting.
12. The system then terminates the telephone connection.

5.2 Paper ballot entry

The following scenario illustrates successful entry of a batch of ballot papers. The treatment of error conditions (e.g. entering an invalid batch number) is omitted.

1. DEO enters the batch number of the ballots. The batch number is accepted.
2. DEO enters rotation number of the first ballot paper in the batch. The rotation number is accepted, and the electronic version of the ballot paper is displayed.
3. DEO enters the preferences selected on the first ballot paper.
4. DEO presses the END PAPER key. The ballot confirmation screen is displayed.
5. DEO presses the ENTER key. The ballot is accepted.

6. DEO enters remaining ballot papers of the batch in the same way.
7. DEO presses the END BATCH key. The batch confirmation screen is displayed.
8. DEO presses the ENTER key. The batch is accepted.

Annex A: Format of file for upload to LAPPERDS

The file format for the csv file output, to be uploaded to LAPPERDS, is defined by the EACT as follows.

- Format: CSV (comma separated values)
- Header row required (but column names not important)
- Name: FirstPreferences*.csv (the * part is optional and can be anything)
- Columns:

Position	Column heading	Mandatory?	Value/relation
1	PollingPlaceID	mandatory	qryELAPPSPollingPlaces-withpasswords.csv column 1
2	ElectorateID	mandatory	qryELAPPSElectorates.csv column 1
3	CandidateFirstName	mandatory	qryELAPPSCandidates.csv column 1
4	CandidateLastName	mandatory	qryELAPPSCandidates.csv column 2
5	PaperCount	optional	Paper first preference
6	ElectronicCount	optional	Electronic first preference

Clarifications

- It is a single file, but it can be uploaded multiple times.
- Two of the columns (Paper Count and Electronic Count) are optional, and if omitted will be considered zero. However, as with all CSV uploads, when a column value is omitted, the column must still be denoted with a comma.
- The required format for informal votes is to use the word “Informal” in place of both ‘CandidateFirstName’ and ‘CandidateLastName’ fields.
- The CSV file is just plain text.

Example content for a test file:

```
PollingPlaceID,ElectorateID,CandidateFirstName,CandidateLastName,PaperCount,ElectronicCount
103,2,Chris,Bourke,167,73
80,2,Yvette,Berry,320,
66,4,Informal,Informal,71,
```

Annex B: Glossary

Abbreviation or Term	Meaning
ACT	Australian Capital Territory
ACTEC	ACT Electoral Commission (also EACT)
ACTGS	ACT Government Solicitor
Ada	Ada is a structured, statically typed, imperative, and object-oriented high-level computer programming language
ANSI	American National Standards Institute
AIAA	American Institute of Aeronautics and Astronautics
ASD	Australian Signals Directorate
B&VI	Blind and Vision Impaired
CJB	Carol Boughton
CVB	Clive Boughton
DEC	Deputy Electoral Commissioner
DEO	Data Entry Operator
EACT	Elections ACT
eVACS® / eVACS	electronic Voting and Counting System
IRS	Interface Requirements Specification
MD5	Message Digest algorithm 5
ICT	Information and Communications Technology
IT	Information Technology
LAN	Local Area Network
OCD	Operational Concept Description
Polling place	Includes pre-poll centre and locations where voting occurs on Election day and at which electronic voting is to be provided
Pre-poll centre	A location in the ACT where voting is permissible prior to election day and at which electronic voting is to be provided
QR code	A form of 2-dimensional barcode (2D barcode)
RB	Russell Baird
SHA-2	Secure Hash Algorithm 2, a set of cryptographic hash functions
SIPL	Software Improvements Pty Ltd
SPARK	A formally defined computer language based on the Ada language, intended for the development of high integrity software used in systems where predictable and highly reliable operation is essential. Is especially used in safety critical systems.
WORM	Write Once Read Many

– END OF DOCUMENT –