# Elections ACT

# Upgrade of eVACS® for the 2024 ACT Legislative Assembly Election

## Multi Factor Authentication

**Document Status: Final**
**Version 1.1**
**March 2023**

# Copyright Notice



## Disclaimer

In compiling this document on Two Factor Authentication, 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 document om Two Factor Authentication, eVACS is the same as eVACS®

## eVACS® 2024 upgrade documentation tree

- Contract with 2024 Upgrade requirements
- Operational Concept Description
- System Specification - Part 1 including 2024 upgrade requirements
- Interface Specification - Setup election
- Installation Manual
- User Manual - Election server
- User Manual - Ballot Viewer
- User Manual - Polling Place server
- User Manual - Telephone Voting server
- **Multi Factor Authentication**

# 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 |
|---|---|---|---|---|---|
| 2022-10-13 | 0.1 | Initial Draft | CJB | CVB/JZ | |
| 2022-10-17 | 0.2 | Includes comments from SIPL | CJB | | |
| | 0.3 | Includes comments from EACT | CJB | CVB | |
| 2023-03-08 | 1.0 | Includes use of 'Authentication USB" | CJB | CVB | |
| 2023-03-16 | 1.1 | Addresses reviewer comments | CJB | | 2023-03-21 |

## Distribution

| Name and Appointment | Document Name | Date of Issue | Version |
|---|---|---|---|
| Jiv Sekhorn, eVACS® Upgrade Project Manager, EACT | Multi Factor Authentication | 2019-08-06 | 0.2 |
| Jiv Sekhorn, eVACS® Upgrade Project Manager, EACT | Multi Factor Authentication | 2023-03-23 | 1.1 |

.

# Contents

# 1. Introduction

## 1.1 Background

One of the requirements from Elections ACT for the upgrade of eVACS® for the 2024 ACT Legislative Assembly Election is to introduce multi-factor authentication across eVACS®, specifically for accessing the menus of the eVACS® election and voting servers. Further any such authentication arrangement must be able to integrate with eVACS® operating system and existing software and hardware, and should be used in combination with eVACS® master passwords (requirement 50 of [1]).

## 1.2 The eVACS® context

eVACS® is a 'closed system'. Thus, any authentication mechanism must not change this essential, and overarching, security property of eVACS®.

In addition to preserving the 'closedness' of eVACS®, it is also important to ensure that any authentication mechanism that is to be applied by humans is not complicated or tedious – especially in circumstances where immediate or urgent access is required – but at the same time enables confidence that any potential vulnerabilities are mitigated.

Of course, any additional security measures must increase security without compromising normal operation.

Finally, it is not a good idea to create or use unproven tools to help with (perhaps non-standard) encryption/decryption processes, possibly exposing eVACS® to the introduction of new vulnerabilities.

The multi factor authentication solution as implemented as part of the upgrade for eVACS® 2024:

a. continues use of the operating system (CENTOS) and encryption software (VeraCrypt) proven in eVACS® 2020,

b. does not change the operations within eVACS®, except for server restarts

c. the security associated with voting server restarts has been strengthened by introducing:

   i) a Public Key/Private Key pair for each voting server and known only to that server,

   ii) use of the Public Key via an encrypted USB-FD, referred to as the Authentication Key and Authentication USB-FD, and

   iii) a password on voting servers for access if the Authentication Key is inaccessible.

## 1.3 Document Purpose

Described herein is the multi factor authentication solution implemented for eVACS® 2024, the operation of the solution, including the creation of encrypted USB-FDs, and managing missing, damaged or unreadable authentication keys.

## 1.4 Reference Documents

Documents referenced in this Multi Factor Authentication document include:

1. Attachment B to the Deed of Variation to the Contract in relation to the Electronic Voting and Counting System (eVACS) Enhancements, Services and Support, dated 06 July 2022;

2. *VeraCrypt for Windows and CentOS7*, Upgrade of eVACS® for the 2020 ACT Legislative Assembly Election, version 0.4, July 2020

## 1.5 Glossary

| Abbreviation or Term | Meaning |
|---|---|
| ACT | Australian Capital Territory |
| Authentication Key | The public key of a public key/private key pair generated by a voting server which authenticates access to that server. |
| Authentication USB | A USB that has been encrypted via VeraCrypt using a 'keyfile' to which an Authentication Key has been downloaded from the voting server to which the Authentication USB is associated. |
| CJB | Carol Boughton |
| CVB | Clive Boughton |
| DEC | Deputy Electoral Commissioner |
| EACT | Elections ACT |
| e.g. | For example |
| Empty encrypted USB | A USB that has been encrypted via VeraCrypt using a 'keyfile' but has no authentication key loaded. |
| eVACS® / eVACS | electronic Voting and Counting System |
| eVACS® 2020 | The eVACS® system as implemented for the 2020 ACT Legislative Assembly Election |
| eVACS® 2024 | The eVACS® system as implemented in the upgrade for the 2024 ACT Legislative Assembly Election |
| JZ | Ji Zhang |
| keyfile | A file such as a photo (.png) that is used instead of a password for encrypting a USB with VeraCrypt |
| SIPL | Software Improvements Pty Ltd |
| USB-FD/USB | Universal Serial Bus (USB) Flash Drive |

# 2. Multi Factor Solution for Accessing eVACS® servers

## 2.1 Overview

Previously, starting up the Election Server after setup required the password entered on initial setup and the Election Server QR code, while starting a voting server after setup required only the voting server QR code.

eVACS® 2024 now requires for any voting server the use of an encrypted USB-FD containing an Authentication Key specific to that server.

Schedule 2.2(a)(xi)

For any subsequent start-up of a voting server, the USB-FD with the unique Authentication Key for that server - the 'authentication USB-FD', will be required. In addition, a Global (Admin Server) password has been introduced for voting servers to enable access should the Authentication Key be inaccessible.

## 2.2 Setting up for multi factor authentication

Schedule 2.2(a)(xi)

Schedule 2.2(a)(xi)

Schedule 2.2(a)(xi)

– END OF DOCUMENT –