Clear Ballot

ClearVote 2.1

ClearAccess Security Specification

ClearAccess Security Specification

Clear Ballot Part Number: 100050-10017

Copyright © 2012–2020 Clear Ballot Group. All rights reserved.

This document contains proprietary and confidential information consisting of trade secrets of a technical and commercial nature. The recipient may not share, copy, or reproduce its contents without express written permission from Clear Ballot Group.

ClearAccess, ClearAudit, Clear Ballot, ClearCast, ClearCount, ClearData, ClearDesign, ClearVote, DesignServer, DesignStation, Image-to-Ballot Traceability, MatchPoint, ScanServer, ScanStation, Speed Accuracy Transparency, Visualization of Voter Intent, Visual Verification, and Vote Visualization are trademarks or registered trademarks of Clear Ballot Group.

ScandAll PRO is a trademark of Fujitsu Limited. All rights reserved. Other product and company names mentioned herein are the property of their respective owners.

Clear Ballot Group
2 Oliver Street, Suite 200
Boston, MA 02109
857-250-4961
clearballot.com

Document history

Date	Description	Version	Authors
01/06/2017	Initial submission to EAC.	1.0	Nel Finberg
02/03/2017	Minor typographical and reference-related edits.	1.0.1	Nel Finberg
05/15/2017	Revised responses to Volume I, 7.4.4, 7.4.5 and 7.4.6.	1.1	Nel Finberg
06/16/2017	Minor updates for vote-by-mail campaign.	1.1.1	Joni G. McNutt
07/20/2017	Updated Documentation in Software distribution section.	1.2	Nel Finberg
07/26/2017	Updated Documentation in Software distribution section.	1.3	Nel Finberg
09/29/2017	Software access controls section revised. Program unit ownership, Bootstrap/monitor/ device-controller software and Protection against malicious software sections revised to include hardening in software installation.	1.4	Nel Finberg
10/19/2017	Minor edits.	1.4.1	Nel Finberg
10/31/2017	Fixed typo in section 7.4.6f.	1.4.2	Nel Finberg
01/19/2018	Vote-by-Mail campaign 2.	1.4.3	Joni G. McNutt
04/13/2018	Sections renumbered to use new numbering scheme.	1.4.4	Mike Quigley
04/12/2019	Added encryption of ADF files. Minor edits.	1.4.5	Mike Quigley
06/21/2019	Minor edits	1.4.6	Joe Srednicki
11/04/2019	Minor edits and formatting fixes.	1.4.7	Joe Srednicki
12/20/2019	Changed Appendix A to Chapter 3.	1.4.8	Joe Srednicki
02/12/2020	Minor edits.	1.4.9	Joe Srednicki

Table of contents

Preface

This section defines the purpose of this document. It contains the following subsections:

- About this document
- Scope of this document
- Intended audience

About this document

This document provides the security specification for the ClearAccess accessible voting system. It complies with the documentation requirements of *VVSG Volume I, 7 Security Requirements* and *Volume II, 2.6 System Security Specification*.

✓ A ClearVote® system can comprise the ClearAccess®, ClearAudit®, ClearCast®, ClearCount® and ClearDesign® products. Jurisdictions are not required to purchase all products. You can ignore references to any ClearVote products that are not part of your voting system. Also ignore implementation options that are not relevant to your policies and procedures.

Scope of this document

This document contains the following sections:

- Chapter 1. Security requirements
- Chapter 2. System security specifications
- Chapter 3. ClearAccess security specifications

Intended audience

This document is intended for state and federal election officials and their voting system test laboratories as part of the technical data package (TDP) required to certify the ClearVote voting system for use. This document is also used by Clear Ballot personnel who support election officials and election staff.

Chapter 1. Security requirements

1.1 General access control policy

This section describes the ClearAccess general access control policy.

1.1.1 Software access controls

The hardening built into the ClearAccess installation process and manual hardening steps limit access to the installed software. See the *ClearAccess Installation Guide*.

Users must provide valid credential to log in to ClearAccess. See "ClearAccess security specifications" on page 20.

To verify that the installed software is certified, see the *ClearAccess System Identification Guide*.

1.1.2 Hardware access controls

The following documents describe recommended policies for controlling access to hardware:

- The *ClearVote Security Policy* describes access controls for voting equipment.
- The *ClearAccess Installation Guide* describes the hardening procedures built into the installation process and manual hardening steps.

1.1.3 Communications

The ClearAccess system is not connected to and does not communicate with any external network. The ClearAccess station and other devices, such as printers, communicate over a closed wired Ethernet.

For recommended policies on restricting communications, see the following:

- The *ClearVote Security Policy*
- The *ClearAccess Installation Guide*

1.1.4 Password management

For recommended policies, see "Password Management" in the *ClearVote Security Policy*.

1.1.5 Operating system

For recommended policies on protecting the operating system, see "Hardening the ClearAccess Station" in the *ClearAccess Installation Guide*.

1.1.6 Supervisory access privileges

For recommended policies on supervisory access privileges, see the *ClearVote Personnel Deployment and Training Plan*.

1.1.7 Segregation of duties

See "ClearAccess roles" in the *ClearAccess Supervisor Guide*.

ClearAccess provides five roles that represent a set of permissions assigned to categories of users.

1.1.8 Additional characteristics

The *ClearVote Security Policy* describes access control for all products.

Individual access privileges

See the following:

- "ClearAccess roles" in the *ClearAccess Supervisor Guide* describes the permissions assigned to each user
- The *ClearVote Personnel Deployment and Training Plan* describes roles from a procedural perspective

Authorization limits

An individual's authorization can be limited to a specific phase of the election depending on the assigned user role. For example, the Poll Worker role is not available in Pre-election mode.

Even when an assigned role allows access to certain software operations, the current phase of the election may restrict these operations. For example, some setup operations must take place before an election opens and are not allowed during an election.

For the scope of each user role, see "ClearAccess roles" in the *ClearAccess Supervisor Guide*.

Ballot casting

This section does not apply to ClearAccess. ClearAccess is not used to cast ballots or count votes.

1.1.9 Access control measures

ClearAccess implements the following access control measures.

Data and user authorization

See "ClearAccess security specifications" on page 20.

Program unit ownership

The ClearAccess software represents a single piece of executable code running on a Windows platform. The Windows configuration controls program-unit ownership and applicable boundaries. See the hardening procedures in the *ClearAccess Installation Guide*.

Port protection devices

The hardening process disables disables all networking services on the ClearAccess station. See "Hardening during installation" in the *ClearAccess Installation Guide.*

Clear Ballot also recommends applying seals to any external ports not intended to accommodate accessible input devices.

Security kernels

The Windows operating system used by ClearAccess has inherent security features, but the ClearAccess software does not use any specific security kernel.

1.1.9.1 Keys

This section describes the use of keys in ClearAccess.

Special protocols

ClearAccess does not use special protocols.

Message encryption

ClearAccess uses message encryption as described in "ClearAccess security specifications" on page 20.

Controlled access security

The *ClearVote Security Policy* describes access controls for voting equipment and methods for preventing unauthorized system.

1.2 Physical security measures

This topic describes physical security measures in ClearAccess.

1.2.1 Polling place security

Poll workers have responsibilities for maintaining polling place security. See "Security responsibilities" and "Security during voting" in the *ClearAccess Poll Worker Guide.*

For the system shut down procedure, see "Shutting Down the ClearAccess Station" in the *ClearAccess Poll Worker Guide*.

Also, see the security practices and policies designated by your jurisdiction.

1.2.2 Central count location security

This requirement does apply to ClearAccess because it is not used for central counting.

1.3 Software security

This topic covers ClearAccess software security.

1.3.1 Software and firmware installation

Firmware

No software is resident as firmware on the ClearAccess station.

Permanent software installation

The only software that is permanently installed on the ClearAccess station is the ClearAccess software.

The *ClearVote Security Policy* guide advises the jurisdiction to provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

Bootstrap/monitor/device-controller software

The Windows operating system contains the system bootstrap, monitor, and device-controller software. This software resides on the Clear Ballot voting device.

Only the ClearAccess software and its associated exception handlers can activate and control the Windows operating system. See the *ClearAccess Installation Guide* for a description of system hardening.

Election-specific programming

Election-specific programming is never installed or resident on the ClearAccess device as firmware.

Source code/compilers

No source code, compilers, or assemblers are resident or accessible on any of the hardware components of the system. Clear Ballot software is written in both JavaScript and Python, which are interpreted languages. Clear Ballot packages the interpreters with the ClearAccess software.

The interpreters and the ClearAccess software that uses them are packaged together by Clear Ballot. The interpreters get installed together with the ClearAccess software. See the *ClearAccess Installation Guide*.

1.3.2 Protection against malicious software

The ClearAccess accessible voting system is never installed on a public network. The hardening process ensures protection from unauthorized intrusion. See the *ClearAccess Installation Guide*.

Windows Defender provides protection against threats such as viruses, worms, Trojan horses, and logic bombs. Clear Ballot recommends updating Windows Defender before every election. See "Updating Windows Defender Antivirus" in the *ClearAccess Maintenance Guide*.

1.3.3 Software distribution and setup validation

ClearAccess complies with the following requirements:

- *VVSG Volume I, 7.4.4*, see "Software distribution" on the next page
- *VVSG Volume I, 7.4.6*, see "Software setup validation" on page 14

To verify the integrity of the voting system software, hash the contents of the software on the distribution media and check the results against the hash value(s) provided in the *ClearAccess System Identification Guide*.

Also use the *ClearAccess System Identification Guide* to check that only the certified software is present. This process ensures that voting system equipment is in a proper initial state before being used.

The ClearAccess system is for voting and printing ballots in a polling environment.

ClearAccess is a single software executable installed on a standalone computer. This computer is never to be connected to any network or the internet. The ClearAccess station is configured with the following devices:

- An external ballot printer
- A numeric keypad
- A sip-and-puff device
- Headphones that play an audio ballot

1.3.4 Software distribution

Section 7.4.4 of the VVSG Volume 1 references procedures that makes repeated reference to the NIST National Software Reference Library (NSRL). However, the NSRL is not implemented for the purposes referenced. Instead, the ClearAccess software is held in escrow in accordance with the appropriate procedures.

Software documentation

The only third-party C++ source code in the software is found in the following directory and its subdirectories:

```
source/src-pcos/scanner-control/pdiscan
```

All code in this directory and its subdirectories is third-party code.

Technical Data Package

The *ClearAccess Technical Data Package* includes the following documentation:

- *ClearAccess Acceptance Test Checklist*
- *ClearAccess Procedures*
- *ClearAccess Database Specification*
- *ClearAccess Functionality Description*
- *ClearAccess Hardware Specification*
- *ClearAccess Installation Guide*
- *ClearAccess Maintenance Guide*
- *ClearAccess Poll Worker Guide*
- *ClearAccess Security Specification*
- *ClearAccess Software Design and Specification*
- *ClearAccess Supervisor Guide*
- *ClearAccess System Identification Guide*
- *ClearAccess System Overview*
- *ClearAccess Voter Guide*

The following ClearVote documentation is also applies to the *ClearAccess Technical Data Package*:

- *ClearVote Approved Parts List*
- *ClearVote Ballot Stock and Printing Specification*
- *ClearVote Configuration Management Plan*
- *ClearVote Glossary*
- *ClearVote Personnel Deployment and Training Plan*

- *ClearVote Quality Assurance Program*
- *ClearVote Security Policy*
- *ClearVote System Overview*
- *ClearVote TDP Checklist*
- *ClearVote Test and Verification Specification*

The following documentation is intended for the end user:

- *ClearAccess Acceptance Test Checklist*
- *ClearAccess Installation Guide*
- *ClearAccess Maintenance Guide*
- *ClearAccess Poll Worker Guide*
- *ClearAccess Poll Worker Instructions*
- *ClearAccess Simplified Voter Instructions*
- *ClearAccess Supervisor Guide*
- *ClearAccess System Identification Guide*
- *ClearAccess Voter Guide*
- *ClearVote Approved Parts List*
- *ClearVote Ballot Stock and Printing Specification*
- *ClearVote Glossary*
- *ClearVote Personnel Deployment and Training Plan*
- *ClearVote Security Policy*
- *ClearVote System Overview*

Each document contains a unique part number that appears on the reverse side of the cover page.

Vendor

The name of the vendor is "Clear Ballot Group", also identified as "Clear Ballot" or "CBG".

Product name

The name of the product this Technical Data Package is applicable to is "ClearAccess". The entire suite of products to which the EAC submission is applicable to is "ClearVote".

Product version

The ClearAccess product version included with this certification application is 2.1.

Certification application number

The application number of this certification submission is CBG-CV-14.

Filenames

The ClearAccess Build Procedures document the following:

- Filenames and installation paths of the software components installed on the ClearAccess station
- Third-party software
- Any applicable installation programs

The only third-party C++ source code in the software is found in the following directory and its subdirectories:

source/src-pcos/scanner-control/pdiscan

All code in this directory and its subdirectories is third-party code.

Certified software verification

See "Trusted external interface" on the next page.

Voting system provisioning

Clear Ballot maintains a repository of jurisdictions that use the ClearAccess voting system. Field operations staff and certification personnel will maintain this list.

1.3.5 Software setup validation

Unauthorized software

See the *ClearAccess System Identification Guide*. Use the listings in this document to check that the voting equipment does not contain any unauthorized software.

Software verification process

See the *ClearAccess System Identification Guide*. Use this guide to verify the following:

- The correct software is loaded.
- No unauthorized software is present.
- The software installed on the ClearAccess device has not been modified.

The *ClearAccess System Identification Guide* contains reference information provided by the EAC or a designated repository.

Process without installed software

The process for verifying the ClearAccess software does not use the software installed on the ClearAccess station.

Documentation

See the *ClearAccess System Identification Guide*.

Voting software modification

See the *ClearAccess System Identification Guide*. Check the listings in this document to verify that the software has not been modified.

Software listing method

To list the software installed on the ClearAccess system, see the *ClearAccess System Identification Guide.*

COTS software/hardware

The software verification process can be performed using COTS software and hardware available from sources other than Clear Ballot Group.

FIPS 140-2 cryptographic module

All files are presented in the software verification process with hashes generated by a FIPS 140-2 level 1 or higher cryptographic module.

Clear Ballot products are written in the Python language using the standard Python libraries. The standard Python hashing libraries use OpenSSL on the Linux platforms, including Ubuntu and the Windows cryptographic libraries on the Windows platforms. Where native Python support does not exist, a thin wrapper has been created to access the underlying cryptographic libraries.

Clear Ballot products running on Ubuntu build the FIPS-certified version of OpenSSL during the build process. Clear Ballot products use the OpenSSL FIPS version that is included as part of the FIPS 140 certificate and are build to conform with the security policy defined in the certification process. See https://www.openssl.org/docs/fips.html for more information.

Clear Ballot products running on Windows use the cryptographic system provided by the Windows operating system.

When the Clear Ballot products start up, they check that the cryptographic module is operating in FIPS mode. If not, the product displays an error message and does not proceed.

Verification process

The EAC or designated VSTL must provide authorized reference information for the ClearAccess software on unalterable storage media.

Trusted external interface

The USB ports on the ClearAccess station provide a trusted external interface for verifying the ClearAccess software.

Protected external interface

A USB port can be protected by sealing it when not in use for software verification.

Physical indicator

The external interface (USB port) for exporting a list of installed software files and corresponding hashes is active when the corresponding signals appear on the About screen during the software verification process. The external interface is inactive for exporting the listing of software files and hashes when the About screen is inactive.

Disabled during voting

The About screen used to export a listing of software files and hashes for verification is inactive during voting.

Read-only access

The About page used to generate a listing of installed software files and corresponding hashes directly reads the voting system software. No third-party software is required for this process. The About page does not update the installed ClearAccess software.

Static and initial values

ClearDesign initializes all variables for a specific election. ClearDesign configures the geographical, reporting, ballot, and audio content for an election. After configuring the election in ClearDesign, election personnel export the election definition to an encrypted accessible definition file (ADFx). Election personnel then import the ADFx to the ClearAccess station.

The ClearDesign software offers reporting functionality that allows for a comprehensive review of the election. For more information on ClearDesign reporting, see the *ClearDesign User Guide*.

User who log in to the ClearAccess by using the Election Administrator or Poll Worker roles can verify the integrity of the following information:

- The codes for Election Administrator, Poll Worker or Voter roles
- ADFx content
- Election audit log

The Ballot Report can verify voting-session statistics for an election.

ClearAccess maintains the following non-election static and dynamic variables:

- Software version
- Date and time
- System Log
- System Administrator code
- Maintenance code

The integrity of the System Log is automatically verified when the System Administrator or Maintenance user logs in. The validity of the System Administrator and Maintenance codes are automatically verified after logging in successfully.

After loading an election, a user can verify the software version, date, and time by printing the Ballot Report.

1.4 Telecommunications and data transmission

This section does not apply to ClearAccess because it never communicates with an external network.

1.5 Use of public communications networks

This section does not apply to ClearAccess because it never transmits data over public telecommunications networks.

1.6 Wireless communications

This section does not apply to ClearAccess because it never uses wireless communication.

1.7 Independent verification systems

ClearAccess is not a vote-casting or vote-tabulating system; therefore, this section does not apply.

1.8 Voter verifiable paper audit trail requirements

ClearAccess is not a DRE system; therefore, this section does not apply.

Chapter 2. System security specifications

2.1 Security risks addressed by the system

"Security requirements" on page 7 addresses Volume I, Section 7 of the VVSG.

2.2 Means by which risks are addressed

See "ClearAccess security specifications" on page 20.

2.3 Process used to test/verify effectiveness of security capabilities

Clear Ballot has submitted documentation with this Technical Data Package indicating that ClearAccess meets this requirement.

2.4 Maintaining currency of security capabilities

See the *ClearVote Security Policy* and "Updating Windows Defender Antivirus" in the *ClearAccess Maintenance Guide*.

2.5 Access control policy

See the following:

- *ClearVote Security Policy*.
- "ClearAccess Roles" in the *ClearAccess Supervisor Guide*
- *ClearVote Personnel Deployment and Training Plan*

2.6 Access control measures

See the following:

- "Access control measures" on page 9.
- *ClearVote Security Policy*.

2.7 Equipment and data security

For information on the system capabilities that prevent disruption of the voting process and corruption of voting data, see the following:

- "ClearAccess security specifications" on page 20
- ClearVote Security Policy

2.8 Software installation

Only install valid certified software from Clear Ballot or an authorized agency on the voting equipment. Follow the procedures in the *ClearAccess Installation Guide*.

After installation, verify the software. See the *ClearAccess System Identification Guide*.

Allow only qualified and authorized personnel to install the software and harden the system.

2.9 Telecommunications and data transmission security

These requirements do not apply to ClearAccess because it never transmits data over telecommunication connections.

2.10 Other elements of an effective security program

2.10.1 Administrative and management controls

The *ClearVote Security Policy* describes administrative and management controls for the voting system and election management.

2.10.2 Internal security procedures

The *ClearVote Security Policy* describes internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode.

2.10.3 Operational procedures

See the *ClearVote Security Policy*.

2.10.4 Physical facilities

See the *ClearVote Security Policy* for information on securing physical facilities used voting systems.

2.10.5 Organizational responsibilities/personnel screening

For a description of organizational responsibilities and personnel screening policies, see the *ClearVote Personnel Deployment and Training Plan*.

Chapter 3. ClearAccess security specifications

This topic describes security for ClearAccess data and logs.

3.1 Access control overview

Users log in to ClearAccess by selecting a role and entering a code. A role assigns permissions to perform a set of functions. The state of the election determines when a user is allowed to perform the functions associated with an assigned role.

3.1.1 Roles for access control

Table 3-1 lists the roles for access control. A role assigns a set of permissions.

Table 3-1. ClearAccess roles

Role	Permissions
Maintenance	Can access system setup and logs only to help diagnose issues. Cannot access election data.
Administrator	Can access system setup, logs. Can load and unload elections. Cannot access election data.
Election Administrator	Can access election data, view the logs, perform pre-election testing, and prepare the system for voting.
Poll Worker	Can open and close polls, and view the logs.
Voter	Can only vote a ballot.

3.1.2 Authorization

When ClearAccess receives a request to access data, the software checks the role of the user to validate that access is allowed. ClearAccess performs this check for each data-access request. ClearAccess denies the request when permissions associated with the role of the user do not allow access the to type of data requested.

Valid user credentials, including codes, are required to upgrade the software.

3.1.3 Authentication

Each user who log in to the ClearAccess is required to enter a code.

The user-entered code is hashed using a standard algorithm and then validated against the hash stored in the system database. The authentication information (user code) is stored as a hash of the code to ensure confidentiality.

A user having the Administrator role can change the System Administrator and Maintenance codes. The other codes are set in ClearDesign and are specific to each election.

3.2 Keys

This section describes the use of keys in ClearAccess.

3.2.1 System data key

System data, such as the System Log, is protected and validated by using a *SystemKey*. The SystemKey is a randomized initial vector, encrypted with a PBDF2 hash of the associated role code and random initial vector, and stored in the system configuration file under the following labels:

- "Administrator" for the System Administrator role
- "Maintenance" for the Maintenance role
- "System" for the current election, encrypted with the ElectionKey rather than the role code

The SystemKey is also used for determining the HMAC of System Log entries.

When the code associated with a role changes, the SystemKey is re-encrypted using the new code. When an election is loaded, the SystemKey is decoded using the current role’s code and re-encoded using the ElectionKey and the election data.

Persistent Data:

- Administrator.key
- Maintenance.key

3.2.2 Election data keys

Election data (ADFx files and Election Log) is protected and validated using an *ElectionKey*. The ElectionKey is a randomized initial vector generated by ClearDesign when the ADFx file is created. The ElectionKey is encrypted using the PBDF2 hash of the associated role code and a random initial vector.

The Election Key is stored in the election configuration file under the following labels:

- "electionCode" for the Election Administrator role
- "pollworkerCode" for the Poll Worker role

- "votingCode" for the Voting session role

The ElectionKey is used in creating the HMAC for the ADFx data and the election log entries.

Persistent Data:

- ElectionAdminstrator.key – created by ClearDesign
- PollWorker.key – created by ClearDesign
- VotingSession.key – created by ClearDesign
- System.key – created when election opened

3.2.3 Key file format

The content of the .key file is:

InitialVector|EncryptedData

Where the items are:

- InitialVector (IV) – The initial vector, stored in Hex encoding, that is randomly created when key file is created
- EncryptedData – The encrypted data, stored in Hex encoding, of:
    - "KEY=" – a static string that is used to validate the file is decoded correctly
    - key – the generated key

3.3 Accessible data file (ADFx)

The ADFx is an encrypted zip file that contain one or more files. One file in the zip file is config.csv. This file contains the comma-separated fields listed in Table 3-2 and other fields.

For a description the ADFx, see the *ClearDesign Accessible Definition File Guide*.

Table 3-2. Fields in config.csv

Field	Description
ElectionAdminstrator.key	The election key encoded using the Election Administrator code
PollWorker.key	The election key encoded using the Poll worker code
VotingSession.key	The election key encoded using the Voting Session code
System.HMAC	The HMAC of all the files except the config.csv file

3.4 Log data

ClearAccess Audit log records use block chaining and HMAC technology to ensure integrity.

The first record in a log consists of a randomly generated Initial Vector and the generated HMAC of the last record in the log stored in Hex encoding. Subsequent records consist of the data followed by an HMAC stored in Hex encoding. The HMAC is created using the record data and either the previous record's HMAC as IV or the IV in the case of the first log record.

The HMAC of the System Log is calculated using the SystemKey. The HMAC of the Election Audit log is calculated using the ElectionKey.

3.5 Validation

The ADFx file is validated upon log in using an HMAC that uses the ElectionKey as the secret for the HMAC. The ADFx is validated when the election is first loaded as well as when the election is initially opened in a ClearAccess session. The hashed user code is used to decrypt the election key, then the ElectionKey is used to validate the files in the ADFx.

ADFx validation only takes place when the Election Administrator, Poll Worker, or Voter access the system, since only the ElectionKey encrypted by the hashes of these role codes are stored in the ADFx.

If all the files fail to validate then the assumption is the code was incorrect. If only some of the files fail to validate then the assumption is that the ADFx file has been corrupted or modified. In either case ClearAccess will not load the ADFx file.

Log files are validated upon log in using an HMAC using the appropriate key as the secret for the HMAC, the election key for the Election Audit log and the system key for the System Log. The hashed code is used to decrypt the key, then key is used to validate the log files.

The Election Log file is validated when an election user (Election Administrator, Poll Worker, Voter) opens the election. The System Log file is validated when any user logs in.