Software Requirements Specification for VEC vVote System

Matthew Casey, Chris Culnane,
James Heather and Steve Schneider

July 5, 2013

University of Surrey

Department of Computing

Computing Sciences Report

CS-13-02

SOFTWARE REQUIREMENTS SPECIFICATION

for

VEC vVote System

Version 1.3

Friday 5th July, 2013

Prepared by Matthew Casey

Contents

Revision History

Version	Name	Status	Date
0.1	Matthew Casey	Initial draft.	19th February 2013
0.2	Matthew Casey	Updated with comments from Chris Culnane, Steve Schneider and James Heather.	28th February 2013
0.3	Steve Schneider	Updated to remove Mixnet manager, and address further comments.	14th March 2013
1.0	Matthew Casey	Major revision to remove Ballot Allocation, Ballot Generation, Ballot Manager and PoD Peers for new PoD distributed ballot generation. Note that requirement numbers have changed.	10th May 2013
1.1	Matthew Casey	Updated with comments from Chris Culnane, Steve Schneider and James Heather.	16th May 2013
1.2	Matthew Casey	Updated with comments from advisory group.	6th June 2013
1.3	Matthew Casey	Updated to match contract specification.	5th July 2013

1 Introduction

1.1 Purpose

The purpose of the Software Requirements Specification (SRS) is to define the features and constraints of the Licensed Software (the System) to be developed for the vVote election system (the vVote System) by the University of Surrey for the Victorian Electoral Commission (VEC). The vVote System [BCH+12a, BCH+12b] is an end-to-end voter-verifiable election system based on Prêt à Voter [RBH+09]. This SRS defines only the back-end components needed to support the vVote System. It is assumed that all user interface components, with the exception of those administrative user interfaces needed to run key election processes and the public repository of election information, are provided separately to this back-end software and are therefore out-of-scope of the development.

The intended audience of this specification are the project sponsors, technical leads and developers. In particular, it is assumed that the reader has a detailed knowledge of voting systems and is familiar with the principles of verifiable voting, encryption protocols, threshold cryptography, digital signatures and digital certification. Specific terminology is provided in section 1.3 to overcome any ambiguity in definitions that are used.

1.2 Scope

This SRS defines the back-end and administrative user interface Licensed Software required to run an election using electronic voting for the VEC. This includes the software required to generate ballots, print ballots on demand for a voter, audit an unused ballot, register a vote, cancel a vote and storage and publication of all ballot, vote, audit and ancillary information such that the whole ballot is verifiable. Supporting structures needed to ensure that the System has high availability and sufficient performance during the voting period are also specified. One user interface is required, to provide public access to the published voting information, which in particular allows a voter to verify that their vote has been registered and included in the count.

This SRS does not specify the requirements for any of the hardware and software platforms in the System, although within this document assumptions are made as to the capabilities, including software, networking, availability, storage and performance, that each provides with benchmark performance requirements specified against a reference architecture. All hardware and software platforms are assumed to be provided for an election by the VEC with their own client software which will use the interfaces specified in this SRS to interact with the software being developed. The back-end software defined

in this SRS will be delivered as source code which the VEC must compile with appropriate Third-Party Software and Open-Source Software to build the System.

Several software components are also outside of the scope of this SRS since they are being developed separately. These include the Mixnet, Mixnet Manager, and user interface software required for the Audit Station, Cancel Station, Print on Demand and Electronic Ballot Marker. This user interface software will depend upon library components for communications and signature checking defined within this SRS and deployed on the user interface devices. All components interfacing with the System are expected to conform to the interface requirements defined in this SRS and it is the obligation of the VEC and their other contractors to comply with this in order that the System functions as required.

1.3 Definitions, Acronyms and Abbreviations

Above the Line (ATL): Allows a voter to choose a party with counting rules which require ballots to be counted as if they were in a Below the Line (BTL) ballot, filled in according to that party's pre-published full preference ranking of all candidates.

Audit Station: The equipment used to perform a print audit an unused ballot. Although conceptually separate to the Print on Demand Printer and treated separately within this document, the Audit Station may be run on the Print on Demand Printer.

Ballot: The ballot used by a voter to cast their vote. A ballot consists of an ordered series of candidates against which the voter may vote. Each ballot may consist of several races with separate lists of candidates.

Below the Line (BTL): Allows a voter to rank the candidates within the race irrespective of their party or the party's preferences.

Cancel Station: The equipment used to cancel a vote which has been cast by a voter. Only the voter can request that a vote is cancelled.

Certificate Authority: An authority for digital certificates. Certificates are needed for all equipment which encrypts or decrypts information or provides digital signatures.

Distributed Key Generation: The process where a distributed set of peers generate a share of a private key which can be used in threshold cryptography.

Electronic Ballot Marker (EBM): A tablet computer which scans a ballot candidate ordering and allows allows the voter to cast their vote.

End-to-end Voter-verifiable Election System: An election system in which all aspects can be publicly verifiable. Each voter can verify that their vote is cast as they intended and included in the count. This type of system does not require trust in any individual person or machine.

Generation Audit: Within the system, this term refers specifically to the auditing of a random selection of generic ballots after they have been generated on the Print on Demand printers. Once audited, a generic ballot is discarded and it cannot be used to cast a vote.

Generic Ballot: A ballot which has been generated by a Print on Demand Printer which has a sufficient number of candidate slots for any race and district within the election.

Key Generation: The generation of private/public key pairs used to encrypt information.

Legislative Assembly (LA): A race for the lower house where candidates are ranked by a voter when they cast their vote. There is one LA race for each of the districts of Victoria.

Legislative Council (LC): A race for the upper house which runs at regional level with different candidates in each region. Votes may be counted using either the ATL or BTL methods.

Mixnet: A system which can shuffle ballots and votes such that no individual or machine can discover which voter received which ballot and which voter cast which vote. The Mixnet is not specified in this SRS and is being developed independently of the System.

Mixnet Peer: An independent server within the Mixnet used to provide robustness, security and integrity. Each Mixnet Peer should be run independently.

Mixed Votes: Registered votes which have been mixed by the Mixnet so that it is provable that no individual vote can be identified with a voter. Once mixed the votes are decrypted.

Prêt à Voter: An end-to-end voter verifiable election system. The vVote System is a modification of the Prêt à Voter system to work for VEC elections with this SRS defining the back-end Licensed Software being developed by the University of Surrey for vVote.

Print Audit: Within the System, this term refers specifically to the auditing of an unused ballot after it has been printed. A voter may request that any unused ballot is audited to confirm that the ballot has been generated correctly. Once audited, a printed ballot is discarded and it cannot be used to cast a vote.

Print on Demand (PoD) Printer: Allows the printing of a ballot paper on demand showing the candidate ordering for a voter so that their vote can be cast. Throughout this document when we refer to the "Printer" we are in fact referring to the device that is connected to the printer.

Print on Demand Serial Number: A unique number which identifies a generic ballot. The serial number consists of a unique Print on Demand Printer identifier and a ballot identifier local to the printer.

Public Web Bulletin Board: A WBB which is a broadcast channel with memory which holds all published information regarding the election such that the election is end-to-end verifiable.

Private Web Bulletin Board: A WBB which is accessible only internally on a private and secured network connecting voting centres and central VEC facilities. The Private WBB holds all of the information regarding the election. Information includes ballots, valid and cancelled votes, audit logs, digital certificates, public keys and proofs. Information is published from the Private WBB to the Public WBB. To maintain the integrity of the System, no information may be retrieved from the Private WBB except receipts to indicate that information has been received, since all information is published via the Public WBB.

Private Web Bulletin Board Peer: An independent server within the Private WBB used to provide robustness, security and integrity. Each Private WBB Peer should be run independently.

Race: Within a single VEC election, voters may have to cast votes for the LA race and/or the LC race. Each race has a separate set of candidates and rules for counting the votes.

Reduced Ballot: A generic ballot which has been reduced to the required number of candidates for a particular district immediately prior to being printed by a PoD Printer for a voter.

Threshold Cryptography: Requires that a number of peers who have a share of the private key must cooperate to decrypt an encrypted message. Only a defined threshold of parties is needed to perform the decryption.

Threshold Signature: A digital signature which is either a cryptographically thresholded signature or a threshold number of individual signatures.

Victorian Electoral Commission (VEC): The organisation responsible for conducting Victorian State Elections.

Vote: A ballot which has been used by a voter to cast their vote.

Vote Receipt: A receipt given to a voter by the EBM guaranteeing that their vote has been registered. The receipt consists of a printer serial number, preference numbers and a threshold signature which can be used to verify the vote.

Web Bulletin Board (WBB): A general term for a repository of information which is accessed via standard web-based protocols. In this specification, a WBB is considered to be an append only repository, with the information already held on the WBB protected as read-only. See also 'Public Web Bulletin Board' and 'Private Web Bulletin Board'.

1.4 References

[BCH+12a] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, and Zhe Xia. A supervised verifiable voting protocol for the Victorian Electoral Commission. In *Electronic Voting*, pages 81–94, 2012.

[BCH+12b] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, and Zhe Xia. Using Prêt à Voter in Victoria State elections. In *Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*, 2012.

[CRS05] David Chaum, Peter Y. A. Ryan, and Steve Schneider. A practical voter-verifiable election scheme. In *ESORICS*, pages 118–139, 2005.

[Fre13] Free Software Foundation, Inc. Various licenses and comments about them - GNU project - free software foundation. http://www.gnu.org/licenses/license-list.html, 2013. [Accessed 16th May 2013].

[IEE98] IEEE Computer Society. IEEE recommended practice for software requirements specifications. http://standards.ieee.org/findstds/standard/830-1993.html, 1998. [Accessed 19th February 2013].

[IEE09] IEEE Computer Society. IEEE standard for information technology – systems design – software design descriptions. http://standards.ieee.org/findstds/standard/1016-2009.html, 2009. [Accessed 19th March 2013].

[Int08] International Telecommunication Union. International standard ISO/IEC 9594-8, ITU-T recommendation X.509: Information technology - open systems interconnection - the directory: Public-key and attribute certificate frameworks. http://www.itu.int/rec/T-REC-X.509-200811-I/en, 2008. [Accessed 27th February 2013].

[ISO09] ISO/IEC/IEEE. ISO/IEC/IEEE 16326:2009(E) systems and software engineering –life cycle processes – project management. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41977, 2009. [Accessed 18th April 2013].

[RBH+09] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à Voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

[RS06] Peter Y. A. Ryan and Steve Schneider. Prêt à Voter with re-encryption mixes. In Dieter Gollmann, Jan Meier, and Andrei Sabelfeld, editors, *ESORICS*, volume 4189 of *Lecture Notes in Computer Science*, pages 313–326. Springer, 2006.

[VAB+00] Alan Vermeulen, Scott W. Ambler, Greg Bumgardner, Eldon Metz, Trevor Misfeldt, Jim Shur, and Patrick Thompson. *The Elements of Java Style*. Cambridge University Press, Cambridge, UK., 2000.

[Vic12] Victorian Electoral Commission. Annual report: 1 July 2011 to 30 June 2012. https://www.vec.vic.gov.au/files/flashreport2012/VEC_ANN_REPORT12.html, 2012. [Accessed 19th February 2013].

[Vic13a] Victorian Electoral Commission. Electronic voting. https://www.vec.vic.gov.au/Vote/vote-eav.html, 2013. [Accessed 19th February 2013].

[Vic13b] Victorian Electoral Commission. How do I vote? https://www.vec.vic.gov.au/Vote/vote-howto.html, 2013. [Accessed 19th February 2013].

[Vic13c] Victorian Electoral Commission. How does voting work? https://www.vec.vic.gov.au/vote/vote-about.html, 2013. [Accessed 19th February 2013].

[Vic13d] Victorian Electoral Commission. Preferential voting. https://www.vec.vic.gov.au/Vote/vote-about-prefvote.html, 2013. [Accessed 19th February 2013].

[Vic13e] Victorian Electoral Commission. Where to vote. https://www.vec.vic.gov.au/Vote/vote-where.html, 2013. [Accessed 19th February 2013].

[XSH+07] Zhe Xia, Steve Schneider, James Heather, Peter Y.A. Ryan, David Lundin, Roger Peel, and Phil Howard. Prêt à Voter: All-in-one. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2007)*, 2007.

1.5 Overview

This document first presents the context in which the vVote System will be used together with a description of the software to aid understanding of the requirements. This context includes detail on the expected architecture of the vVote System which is not strictly specified in an SRS, but is required in order to ensure the correct separation of components for end-to-end verifiability. These details have been developed from an initial understanding of the Prêt à Voter system. Following this context, formal functional and non-functional requirements of the System are then fully specified, which rely upon this architectural understanding.

This document follows the IEEE "Recommended Practice for Software Requirements Specifications" using the template organisation for features [IEE98].

1.6 Project Contributors

The following people have participated in discussions or contributed to the specification of the vVote System: Richard Buckland, Craig Burton, Chris Culnane, James Heather,

Rui Joaquim, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriram Srinivasan, Vanessa Teague, Roland Wen, Douglas Wikström and Zhe Xia. Earlier stages of the system are described in [BCH+12a, BCH+12b].

2 Overall Description

2.1 Context

The guiding principle for the vVote System is that the election system should be publicly verifiable: individual voters should be able to check that their votes have been recorded as they intended and included unaltered in the count, and anyone should be able to check that all vVote votes are properly mixed and decrypted for input into the final tally. Every step of the process should be verifiable, and should not require trust in any individual person or machine. This principle is achieved within the Prêt à Voter voting system [CRS05, RS06, XSH+07, RBH+09], so that the requirements for the vVote System are based upon the operation of Prêt à Voter, modified for a VEC election.

In a VEC election voting can be divided between two races. Votes for the Legislative Assembly (LA) race are cast in all of the 88 districts of Victoria, with the same candidates (typically 8) being voted for in each region. Votes for the Legislative Council (LC) race run independently in each region, each with different candidates (typically from 20 to 40). In both races, voting consists of ranking the list of candidates (either all of the candidates when *full preferential voting* is required, or just the top number of candidates when *optional preferential voting* is required [Vic13c]). Ballots offer the option of voting Above the Line (ATL) *or* Below the Line (BTL). Here, a line is drawn across the ballot such that above the line, voters can cast their votes against a single party only, and the vote will be counted using the party's pre-defined preference, whereas if they vote below the line, voting is irrespective of the candidate's party and they must rank either all (full preferential) or the top number of candidates (optional preferential) [Vic13d].

Voting is compulsory in all Victorian State elections with approximately 3.6 million registered voters [Vic12]. Voting opens 2 weeks before the election day with local, out of state and overseas voting centres and postal voting [Vic13e], with candidates allowed to register in the preceding month up to the day before the election period starts. Electronic voting in VEC elections was first trialled in 2006 for the blind, partially sighted or for those with low literacy skills [Vic13a].

2.2 Product Perspective

The vVote System will provide a way in which existing paper-based voting can be supplemented with an end-to-end verifiable electronic voting system. Voters will be able to vote electronically using an EBM or by using a paper ballot. The vVote System will provide the high levels of availability and security required for compulsory secret ballots which have voting centres operating locally within Victoria, out of state and overseas

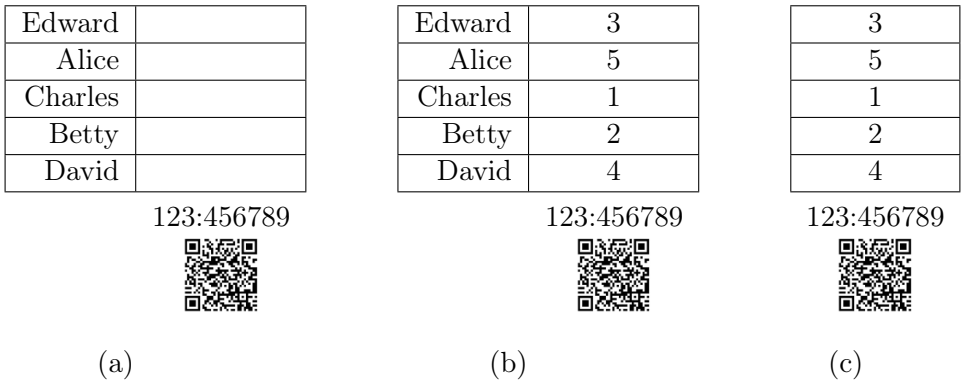

Figure 2.1: Prêt à Voter ballot: (a) blank ballot; (b) completed ballot (vote); and (c) record of choices without the candidates listed. Note that the QR code contains an encrypted form of the candidate ordering which is recorded (still in encrypted form) with the voter's rankings. The printer serial number for the ballot is included on the ballot.

during the 2 weeks of early voting. In this initial implementation, it is not intended that vVote will be used on the designated polling day, and all votes registered in the system will be transferred to the existing VEC vote tallying system for the final count, when they will be combined with the paper-based votes.

The key principle behind vVote is the ability to issue a printed record in the polling station that allows the voters to verify that this record reflects their intended vote, without revealing how they voted. This is achieved using the randomised candidate ordering technique introduced in Prêt à Voter [CRS05, RS06, XSH+07, RBH+09]. In the original Prêt à Voter scheme, the voter is issued with a physical ballot that has the candidate names on one side in a randomised order, and the vote boxes (to be filled by the voter) on the other side, as illustrated in Figure 2.1. Additionally, underneath the vote boxes is the permutation of the candidate order, encrypted under a thresholded public key to which no individual person or machine holds the decryption key. Down the middle of the page, between the candidate names and the vote boxes, is a perforation line. The voter marks their choices in the vote boxes and tears down the perforation line. The side with the candidate names is then shredded, and the voter submits the vote boxes to the system, and keeps a copy of the completed boxes, signed by the system. The system is not able thereby to learn how the voter voted, because the ordering of candidate names is shredded before the vote boxes are scanned; the vote boxes on their own do not reveal the vote. The records of the choices are made available online, allowing voters to verify that their votes are included, unaltered, in the count.

In the vVote System, this paper-based approach to protecting the randomised candidate ordering on a voter's ballot paper is replaced by an Electronic Ballot Marker (EBM). On arrival at a voting centre, the voter's identity is confirmed by a voting official. The official then requests a ballot for the voter. The next available generic ballot is selected

at a specific PoD printer and the full list of candidates is reduced to only those that are appropriate for the voter's district. Generic ballots are generated prior to the election. The printer's serial number and information on the unused candidates is then sent to the central system for authentication and to return a signature which validates that the ballot is authentic. The printer then prints the authenticated ballot for the voter so that the voter can see the candidate ordering to cast their vote.

To cast their vote, the voter scans the QR code displayed on their ballot to input the candidate ordering displayed on their ballot into the EBM. Once the voter has cast their vote, the EBM transmits the information with a digital signature to the central system which returns a signature on the ballot data to the voter. The EBM prints this signature and the voter's preferences and printer serial number. The voter checks the preference numbers against their printed candidate list and, optionally, checks the signature. This printout constitutes the receipt, and can be used to verify that their vote has been included unaltered in the count. Within the vVote System, each vote is stored encrypted under a threshold joint public key, such that no single machine can decrypt the votes. If the voter has made a mistake, they may cancel their vote.

To count all of the votes, the candidate identifiers in preference order are decrypted. In order to prevent the decrypted vote from being associated with a voter, the submitted choices are securely and verifiably mixed multiple times by a distributed system in which a peer in the system is operated by different individuals or organisations. This process of mixing on a Mixnet guarantees that, provided at least one peer has behaved honestly, there is no traceable link between an encrypted vote and its decrypted output. This process also provably guarantees that the set of encrypted votes corresponds (as a whole) to the set of decrypted votes.

During an election there are 3 distinct phases of operation: 1) pre-election, 2) vote casting, and 3) post-voting. To support voting during these phases, the vVote System will consist of components hosted in all voting centres as shown in Figure 2.2, and components hosted in multiple central locations as shown in Figure 2.3. Note that this document defines the requirements for the Licensed Software which is to be used within some, but not all, of these components. Only software to support the following components is included:

1. PoD Printer.
2. Private WBB Peer.
3. Public WBB.

All components for which software is not being developed by the University of Surrey interact with the vVote System via interfaces defined in this document. These are Audit Station, EBM, Cancel Station and Mixnet Peer. All interconnections between components are assumed to take place within a private Transmission Control Protocol (TCP) capable network infrastructure. The only external interface is via the Public WBB which is connected to the Internet to allow for public verification of the election. The Public WBB therefore sits outside of a firewall protecting the private network.

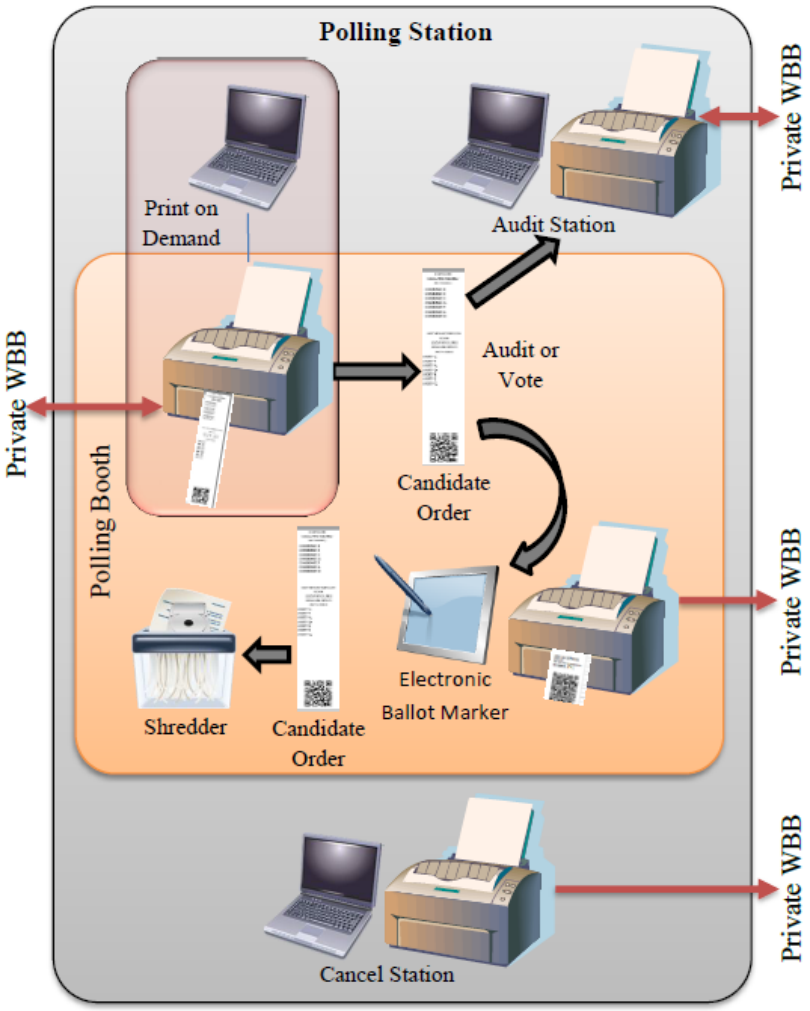

Figure 2.2: Components required in each voting centre. Definitions of each component can be found in section 1.3

Below is a summary of how these components interact during the 3 phases of the election:

Pre-election

Takes place prior to voting to include registration of all voters and candidates, and the preparation of voting centres, equipment and all processes necessary to carry out the election and declare a result.

During this phase, all equipment for the vVote System must be prepared and all public/private key pairs and digital certificates generated for all the required components. Generic ballots are then generated on each deployed PoD Printer.

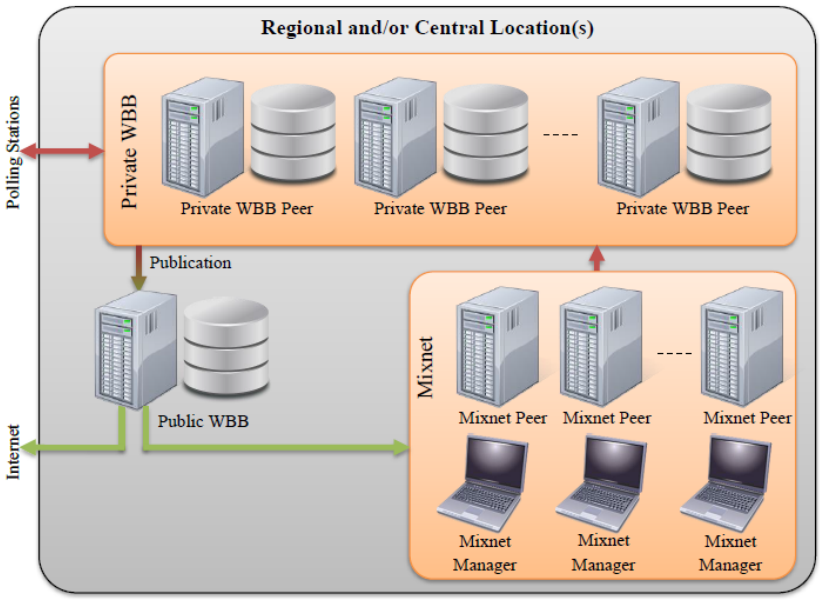

Figure 2.3: Components required in one or more central facilities to generate and distribute ballots, audit ballots, cancel votes, register votes and to perform the mixing and counting. Note that Mixnet and Public WBB Peers should be run by independent organisations in separate facilities to meet the demands of a fully end-to-end verifiable election and to provide for fail-over. Definitions of each component can be found in section 1.3

1. *Prior to an election, a register is maintained of all voters.*

   The vVote System needs to be scalable to generate sufficient ballots for all voters, together with spare ballots for auditing. Greater numbers of voters may require Mixnet Peers, Private WBB Peers and the Public WBB to have increased performance, storage and bandwidth capacity.

2. *Preparations are made during this period to staff and equip all designated voting centres, within Victoria and overseas.*

   The vVote System needs to be scalable to cope with the number of voting centres and associated equipment. All separate Audit Station, PoD printers and EBMs prior to the election will require individual private keys and digital certificates, provided by a Certificate Authority. PoD Printers will require randomness values to be able to generate ballots.

3. *Ballots are generated with all of the parties and candidates listed as required for the LA and LC elections.*

The vVote System needs to be able to generate the required number of ballots for each race with the correct candidates so that ballots can be printed when voting starts. Each PoD Printer generates generic ballots and is therefore supplied with appropriate randomness values for the required encryption operations. These randomness values are generated by the Mixnet Peers (principally peers which are independent to the Private WBB), which must therefore also have sufficient performance and peers to generate the randomness values required.

4. *Typically one month prior to an election, registration for candidates opens. Candidates may register up to a closing date which is typically 2 hours prior to the start of voting.*

   The vVote System needs to be scalable to cope with as many candidates as are registered for an election in each of the races being run. Once finalised, the list of candidates needs to be distributed to all PoD Printers so that they can form reduced ballots.

Vote Casting

Voting takes place in 2 phases: early voting in the 2 weeks preceding the designated election day in voting centres locally, out of state and overseas, voting then concludes on the election day [Vic13b]. Postal voting is permitted through both phases. The early voting phase requires the vVote System to operate with high availability during all of the overlapping opening hours of voting centres. The vVote System is intended to support early voting only, and as an alternative to paper-based voting. The distribution of ballots and registration of votes are time critical and must therefore operate in real-time with fail-over redundancy.

1. *During the voting period particular voting centres locally and overseas are open for pre-defined hours.*

   The vVote System needs to be operational to issue ballots, audit ballots, register votes and cancel votes across all defined local, out of state and overseas voting centre opening hours. The PoD printers, EBMs, Audit Stations and Cancel Stations all rely on real-time, secure communication with the Private WBB and Public WBB. Appropriate networking infrastructure needs to be in place with secure communications and digital signatures. The Private WBB needs to have a threshold number of operational peers for 24 hours per day during the 2 week period of voting.

2. *A voter casts their vote at a voting centre by first confirming their name and address with a voting official. The voting official will mark the voter's name on the electoral roll to record that they have voted and then issue the voter with the required ballot papers.*

A ballot is issued in real-time to a voter. Sufficiently fast networking and Private WBB Peers are needed to ensure that a threshold of responses is received by a PoD Printer within a defined time period so that a ballot can be printed.

3. *The voter then records their vote in a private booth.*

   The PoD printer prints only the QR code containing the encrypted candidate ordering.

4. *The voter casts their vote.*

   The EBM scans the candidate ordering from the printed ballot. The voter then casts their vote using the EBM display. The vote is then sent to the Private WBB with a threshold number of peer responses required to provide the voter with a signature which guarantees that the vote has been registered. The signed information is a receipt which can be used to verify the vote.

Post-voting

Once voting has finished, the count is performed. Once voting has closed, each of the votes for a race is mixed so that no voter can be associated with a vote. The mixed votes then have their candidate ordering decrypted. The count is performed by the existing VEC tallying system. Therefore, the mixed and decrypted votes are transferred to the tallying system. All required information which is needed to verify that all of the votes registered have been input to the tallying system is then published.

1. *Votes are counted following the defined counting scheme for each race.*

   Votes in vVote are mixed using the Mixnet to ensure that no vote can be traced to a voter. The votes are then decrypted and input to the tallying system. The Mixnet Peers need to have sufficient performance to conduct these processes within the required time period.

2. *The results are scrutinised.*

   Anyone may verify the election processes using the information which is published. Voters may verify that their vote has been input to the tallying system by using their vote receipt. The Public WBB provides a mechanism where the voter can provide details of their receipt and get confirmation that their vote was included. This information is published daily to the Public WBB.

3. *The election officials may call a recount, typically if results are close. A candidate may request a recount with the request considered by the election officials.*

   Mixing is performed only once for the Mixnet for a given race and batch of votes.

4. *The election is declared.*

All appropriate information is published to allow full end-to-end verifiability. The Private WBB publishes the required information to the Public WBB.

2.2.1 System Interfaces

The back-end Licensed Software being developed provides the following system interfaces, which are used for set-up of the vVote System:

Election Details: Provided as files which list the candidates, parties and races in the election. This will consist of 3 separate comma-separate-values (CSV) files:

VEC-areas.csv: This file contains 2 values per row in the following format:

```
region,district
```

A region contains a number of districts; each district belongs to only one region. In consequence, each region appears in multiple rows, while each district appears only once.

VEC-lower.csv: This file defines the LA (lower house) race and consists of 4 values per row:

```
district,candidate name,index,party name
```

The data contained within this file should be used to produce a list of candidate names, parties and identifiers for a particular district. The list should be in the order of the index values. The party name can be blank if a candidate is not affiliated to a party.

VEC-upper.csv: This file contains the data regarding the regional races for the LC (upper house). It consists of 8 columns per row:

```
region,grouping,grouping alpha index,grouping index,↩
candidate name,party,town,index
```

The region is electoral region, the grouping refers to how the candidate is to be grouped and thus also defines an entry for the ATL portion of the ballot. This is important because some parties (coalitions in particular) submit joint ATL lists, and so the candidate party may not be the same as the grouping party. Each party listed in a region in the grouping column should have an entry in the ATL list. The grouping alpha index and grouping index refer to party ordering. The candidate name and party are important for the BTL section of the ballot.

System Configuration: All vVote System components must be identified uniquely such that peers can be grouped and all components communicated with. This configuration information will be recorded within a single CSV file for all central and voting centre components, together with separate files for each digital certificate:

vVote.csv: This file contains 5 values per row in the following format:

```
name,ip address,port number,component type,certificate file
```

This details the unique name and IP address of the component, the port number it may be contacted on for vVote messages, which may be empty when the component does not receive messages, and the type of the component, which is either:

```
AUDIT_STATION
CANCEL_STATION
EBM
MIXNET_MANAGER
MIXNET_PEER
POD
PRIVATE_WBB_PEER_EXTERIOR
PRIVATE_WBB_PEER_INTERIOR
PUBLIC_WBB
```

A Private WBB Peer has interior and exterior IP addresses and ports to separate messages originating from central components, such as other peers, and messages originating from voting centre components, respectively. The certificate file is the local relative path to the file which contains the digital certificate for the component (which contains its public key). All digital certificates will be supplied in files conforming with the X.509 standard [Int08].

Note that it is assumed that all processor, network and storage management is achieved by the various operating systems and infrastructure independently of the System.

2.2.2 User Interface

The Public WBB provides a user interface to enable any individual or organisation access to the election information needed for verifiability. This user interface will be formed by a simple WBB with an appropriate data structure to allow navigation of the content. The Public WBB will also provide a web interface which allows a voter to enter the details of their vote receipt to allow them to verify that their vote has been registered and included in the count.

2.2.3 Software Interfaces

Since this document specifies the required back-end Licensed Software for the vVote System, the majority of the interfaces are software-based. All software interfaces are accessed using the communication interfaces described in section 2.2.4. The software interfaces are:

Audit Station to Private WBB Peers: All Private WBB Peers receive the same request from an Audit Station to audit a ballot. The relevant ballot is returned to the Audit Station in plain text.

Cancel Station to Private WBB Peers: All Private WBB Peers receive the same cancel request from a Cancel Station to cancel a vote. A threshold receipt for the cancellation is returned to the Cancel Station.

EBM to Private WBB: All Private WBB Peers receive the same vote registration request from an EBM. A threshold receipt for the vote is returned to the EBM.

PoD Printer to Private WBB Peers: All Private WBB Peers receive the same request from a PoD printer to store ballot ciphers for the generic ballots which have been generated.

PoD Printer to Private WBB Peers: All Private WBB Peers receive the same request from a PoD printer to authenticate a ballot given a voter's unique district, printer serial number and candidate randomness. A threshold signature is returned to the PoD printer.

PoD Printer to Private WBB Peers: All Private WBB Peers receive the same request from a PoD printer to open the commitment to the randomness used in generating a ballot selected randomly by the Private WBB Peers during auditing of the ballot generation.

Private WBB Peer to PoD Printer: For each PoD Printer which has ballots being audited after ballot generation, the printer receives a request to reveal the opening of the commitment to the randomness used in generating the ballot. The ballot is not then used for voting.

Private WBB Peer to Private WBB Peer: All Private WBB Peers periodically send a request to all other peers to confirm the data that they have stored matches on all peers. A hash code of the data stored is sent and each peer compares the hash with their own data storage hash. Success or failure of the hash comparison is returned to the sending Private WBB Peer.

Private WBB Peer to Private WBB Peer: If the hash code for the data stored by a Private WBB Peer in a particular session does not match the hash code sent by any other Private WBB Peer, then all of the data for a session is transmitted to all peers so that the data for a session can be reconciled.

Mixnet Peer to PoD Printers: All PoD Printers receive their respective randomness values for ballot generation from the all Mixnet Peers.

Mixnet Peer to Private WBB Peers: All Private WBB Peers receive the same request to store the commitment to the randomness used to generate ballots from all Mixnet Peers. A threshold receipt is returned to the Mixnet.

Mixnet Peer to Private WBB Peers: All Private WBB Peers receive the same request to store mixed votes from all Mixnet Peers. A threshold receipt is returned to the Mixnet.

Private WBB Peer to Public WBB: All Private WBB Peers send a request to publish election information to the Public WBB. No response is provided.

2.2.4 Communication Interfaces

All communication between components in the System will be achieved by sending raw byte data over TCP connections. Secure Socket Layer (SSL) connections using the host's digital certificate are used for authentication of the communication channel but not encryption to allow for deep packet inspection of the content. IP addresses for this communication will be specified in the component's configuration information (section 2.2.1). Messages and data are communicated via connections using JavaScript Object Notation (JSON) with appropriately defined schemas for validation. The data content, format and schema for each of the software interfaces will be defined during the design phase of the project.

2.2.5 Operations

The vVote system operation will differ depending upon the current election phase. During the pre-election phase, the System will be configured on an ad-hoc basis with the appropriate components for testing and deployment. The System is not expected to be fully operational during this period until immediately prior to the vote casting phase when candidate registration is complete and ballots are to be generated.

The System will be fully operational throughout the vote casting phase. This full operation will be fault-tolerant to prevent any loss of information or significant delay to voters. Note that it is assumed that all processor, network and storage fault-tolerance, storage redundancy and backup is provided by the various operating systems and infrastructure independently of the System and is provided by the VEC.

The System will remain fully operational until the count is declared and the election closed. Once all election information has been published to the Public WBB, the System may be decommissioned. However, the Public WBB needs to remain operational for an undetermined length of time so that any individual or organisation can verify the election results.

It is anticipated that a typical election will need to cope with in the order of 4 million voters using both electronic and paper-based voting, voting in 88 regions for an LA

and a LC race. In the LA race there may be in the order of 15 candidates across all regions, while in each regionally independent LC ATL and LC BTL races, there will be in the order of 10 and 40 candidates respectively. It is anticipated that up to 10% of all generated ballots may be used for auditing, and therefore sufficient spare ballots are needed to still allow all registered voters to vote. Note that these limits are indicative only and the System should be able to cope with reasonable higher limits for an election with sufficient infrastructure.

2.3 Product Functions

The Licensed Software defined in this SRS consists of 3 features: 1) PoD Printer 2) Private WBB Peer and 3) Public WBB. Only the Public WBB provides user features (section 2.2.2), whereas all remaining components are accessed via software interfaces (section 2.2.3). The System is configured via the system interfaces (section 2.2.1).

2.3.1 PoD Printer

A PoD Printer generates and prints ballots for voters. The software to be developed for the PoD Printer will generate ballots using supplied randomness and support communication with the Private WBB Peers. No user interface software is included in this back-end development.

When generating ballots during the pre-election phase, the PoD Printer receives randomness values for use in the encryption process. An anticipated number of sufficient generic ballots are generated by the printer such that each generic ballot has more than enough candidate slots than required for each race. The resulting ballot ciphers are sent to the Private WBB for storage.

When allocating a ballot to a voter, the PoD Printer uses the voter's district to reduce the next available generic ballot to a ballot with the correct number of candidates. The printer's serial number, voter's district and unused randomness values for the reduced ballot are then sent to the Private WBB to authenticate the ballot. Once authenticated, the PoD Printer prints the ballot.

2.3.2 Private WBB Peer

A Private WBB Peer stores all ballot ciphers that have been generated for an election. These are sent from each PoD Printer, stored and then published to the Public WBB. Similarly, whenever votes are mixed by the Mixnet, all Private WBB Peers receive the mixed votes, they are stored and then published to the Public WBB. All other public configuration information regarding the election is also published to the Public WBB, including race, party, region and candidate lists, digital certificates and proofs.

A Private WBB Peer handles all requests to authenticate a ballot, audit a ballot, the casting of a vote and the cancellation of a vote. All Private WBB Peers receive the same requests and perform the same processing.

The only information returned by a Private WBB Peer in response to any request is an acknowledgement signed using the Private WBB Peer's share of the threshold signature key, together with any necessary proofs. Information recorded by the Private WBB Peer is only output when it is published to the Public WBB. In this way, all election information is public and all vVote System components use the publicly available information.

A Private WBB Peer records the authentication of a ballot from a PoD Printer, rejecting the ballot if the data used to generate the reduced ballot is incorrect. In order to authenticate a ballot, a threshold number of Private WBB Peer requests must be received by the PoD Printer. The casting of a vote is recorded from any EBM, as is the auditing of a ballot and the cancellation of a vote.

Publication of information occurs periodically at a pre-set time for all Private WBB Peers so that the integrity of the published data is confirmed with a threshold number of peer signatures. Prior to publication, a hash code of the data stored by the Private WBB is sent to all other Private WBB peers. The hash code for each peer is compared to the receiving peer's own hash code. If the hash code matches, the publication proceeds. If any of the hash codes do not match then each peer sends a complete copy of the current session's data to every other peer. On receiving a copy of the data, each entry is combined with the peer's local data. If the entry was missing from its local storage, and the entry has a threshold number of peer signatures, then the entry is added/updated in the local storage. Once this reconciliation process is complete, the hash codes are compared again and the data published if a threshold of the hash codes match.

2.3.3 Public WBB

The Public WBB provides a public repository for all information published from the Private WBB Peers. The Public WBB also provides a web application to allow any voter to enter their vote receipt details and to confirm that their vote has been registered and input to the count.

The Public WBB broadcasts sufficient data to allow every voter to verify that their vote was included unaltered and anyone to verify that all the included votes were correctly mixed and decrypted. The validity of its broadcast is guaranteed by publishing a signed hash of its daily content in a medium that constitutes reliable broadcast with memory (such as radio or print media). This ensures that all visitors to the Public WBB read the same information, and hence get valid evidence that their vote is included.

2.4 User Characteristics

It is anticipated that three types of user will use the Licensed Software defined in this SRS. VEC IT staff are expected to deploy and configure the System using the defined system interfaces (section 2.2.1). This will include the running of the election processes.

The second type of user of the System are software developers and integrators who are expected to understand and use correctly the software interfaces defined in this

specification (section 2.2.3) with the appropriate JSON schemas defined in the design documentation.

Finally, it is expected that any member of the public or representative of an organisation may access the Public WBB to scrutinise all of the election information such that the election is independently verifiable. This will include a web application presented using Hyper Text Markup Language (HTML) to allow a voter to verify that their vote has been registered and included in the count (section 2.2.2).

2.5 Constraints

The vVote System provides end-to-end voter-verifiability which copes with malicious attacks provided certain constraints are meet. Principally, all necessary steps should be taken to protect the vVote System from unguarded attacks by using physical, network, storage and user security protection. These safeguards should be penetration tested by the VEC to ensure viability. However, the protocols in use enable the detection of attacks on the voting process if these safeguards fail or are circumvented by insider attacks. To achieve the desired level of robustness and security, the Private WBB and Mixnet Peers need to be physically placed in separate locations and administered by separate organisations such that no single individual or organisation can control all of a component's peers.

An operational constraint on the vVote System is its ability to cope with the demands of the election throughout the pre-election, vote casting and post-voting phases. This assumes that appropriate hardware, administrative, fail-over and backup procedures are operational. These requirements are outside the scope of this SRS.

2.6 Assumptions and Dependencies

The System will be designed and implemented using appropriate best practice in software development to include design and code standards and published security protocols. Where appropriate, all developed software will follow the coding standard defined in [VAB+00], and documents will follow the IEEE standards [ISO09, IEE98, IEE09]. To maintain the open verifiability of the System, all software will be released to the public under an open source free software license [Fre13].

The operation of the Licensed Software is dependent upon the supply from VEC of appropriate hardware and operating systems. It is also assumed that sufficient digital certificates, private/public key pairs and threshold keys are provided for all components operating within the vVote System.

2.7 Apportioning of Requirements

Development of the System will be in phases matching to the required features. The first feature to be developed will be the Private WBB since this provides the core functionality of the vVote System. Next the Public WBB will be developed so that published

information can be provided to the remaining components. Once complete, the PoD Printer will be developed. Once the components have been developed and factory tested, an integration phase will commence where each component will be integrated with their respective user interfaces which are being developed separately.

3 Requirements

3.1 External Interface Requirements

IR1. The System shall be configured using the election information provided in the CSV files specified in section 2.2.1.

IR2. The components within the System shall be defined within the CSV and digital certificate files specified in section 2.2.1.

IR3. All components within the System shall communicate using TCP with SSL via the IP address, port number and digital certificate for each component.

IR4. Messages to components shall be sent using the data format and content defined using JSON with a JSON schema.

IR5. The Public WBB shall provide access to all of the published election information.

IR6. The Public WBB shall provide HTML access for vote verification.

3.2 System Features

SF1. The System shall provide end-to-end verifiability for an election.

SF2. The System shall support electronic voting during the early voting phase for VEC LC and LA races in all VEC regions for all registered voters, all registered candidates and in all local, out of state and overseas early voting centres.

SF3. The System shall support full preferential voting.

SF4. The System shall support optional preferential voting.

SF5. The System shall support ATL voting.

SF6. The System shall support BTL voting.

SF7. The System shall enforce the mutually exclusive use of ATL or BTL on a vote where ATL and BTL voting is used on a ballot.

SF8. During the voting period, the System shall permit casting of votes, auditing of ballots and cancellation of votes.

3.2.1 PoD Printer

PP1. A PoD Printer shall generate generic ballots.

PP2. Randomness used in generating generic ballots shall be input to the PoD Printer from the Mixnet.

PP3. The System shall generate sufficient ballots for all voters to be able to vote in all races within an election.

PP4. The System shall be able to include the correct candidates for a race on a ballot prior to printing.

PP5. At a minimum, an extra 10% of ballots shall be generated in anticipation of ballot auditing.

PP6. A generic ballot shall only be used for voting or auditing once.

PP7. Each generated ballot for a race shall have a random candidate ordering.

PP8. The candidate ordering for a ballot shall be encrypted such that only a threshold decryption key is required to decrypt it.

PP9. A PoD Printer shall receive requests to print a ballot for a voter.

PP10. A ballot is uniquely identified.

PP11. When processing a request to print a ballot, a PoD Printer shall reduce an available generic ballot to have the correct list of candidates.

PP12. A PoD Printer shall send a request to authenticate the reduced ballot to the Private WBB.

PP13. A PoD Printer shall only print a ballot that has been authenticated by the Private WBB.

PP14. A PoD Printer shall receive requests to audit a generic ballot from the Private WBB.

PP15. When auditing a generic ballot, a PoD Printer shall send the randomness used in generating the ballot to the Private WBB.

PP16. An audited generic ballot shall not be used for voting.

3.2.2 Private WBB Peer

PR1. A Private WBB Peer shall be a central repository for all election information, including ballots, votes, cancelled votes, audit records and proofs.

PR2. A Private WBB Peer publishes information to the Public WBB.

PR3. A Private WBB Peer shall receive requests to store ballot ciphers.

PR4. All ballot ciphers are stored in persistent storage.

PR5. A Private WBB Peer shall request the generation audit of generic ballots from PoD Printers.

PR6. The open commitments to the randomness for generic ballots being audited after ballot generation shall be stored in persistent storage.

PR7. A Private WBB Peer shall receive requests to record a vote.

PR8. The vote shall be stored in persistent storage.

PR9. A Private WBB Peer shall receive requests to cancel a vote.

PR10. The cancellation of a vote shall be stored in persistent storage.

PR11. A Private WBB Peer shall receive requests to audit a ballot.

PR12. Audit requests shall be rejected for ballots which have been used to vote.

PR13. A Private WBB Peer shall generate the reduced ballot when auditing.

PR14. When processing a request to audit a ballot, a Private WBB Peer shall check all randomness commitments of the reduced ballot.

PR15. The decrypted ballot required for auditing shall be sent to the requesting Audit Station.

PR16. A Private WBB Peer shall receive requests to store mixed votes.

PR17. All mixed votes are stored in persistent storage.

PR18. A Private WBB Peer shall periodically compare its own locally stored information with the other Private WBB Peers.

PR19. All information identified during the comparison as missing shall be added to the local store provided there are sufficient threshold signatures for the information.

PR20. Once a threshold of Private WBB Peers agree on their locally stored information, all the stored election information shall be published.

PR21. Published election information shall include all ballots, votes, cancellations, audits, proofs and election information.

PR22. Votes and ballots shall be stored and published so that no vote or ballot can be associated with a voter.

PR23. All responses from a Private WBB Peer shall be signed using a threshold signature.

PR24. A sufficient number of Private WBB Peers shall operate such that a threshold of peers is maintained to publish the information required to guarantee end-to-end verifiability of the election.

3.2.3 Public WBB

PU1. The Public WBB shall be a central repository for all published election information, including ballots, votes, cancelled votes, audit records and proofs.

PU2. All information received by the Public WBB from the Private WBB shall be published if there is a valid threshold signature for the information.

PU3. The Public WBB shall allow a voter to verify that their vote has been registered as they intended and included unaltered in the count.

PU4. A voter shall verify their vote by providing their vote receipt information.

PU5. The vote receipt consists of a printer serial number, preference numbers and a threshold signature.

PU6. The Public WBB shall allow anyone to verify that all registered votes are included in the decrypted votes used for the count.

3.3 Performance Requirements

PF1. The System shall be able to generate, store and process at least 1 million ballots for an election to include sufficient for auditing.

PF2. The System shall be able to operate with at least 100 early voting centres configured inside Victoria, 8 nationally, and 37 internationally, and with 25 sets of portable equipment.

PF3. The System shall be able to operate with at least 8 LC regions configured and 88 LA districts.

PF4. For a LA race the System shall be able to operate with a maximum of 15 candidates.

PF5. For LC ATL and LC BTL races the System shall be able to operate with a maximum of 20 and 45 candidates respectively.

PF6. The System shall be able to operate with at most 800 combined ballot printing, ballot auditing, vote registration and vote cancellation requests received across all components within a 10 second period.

PF7. The reference architecture for the System shall use a quad-core Intel i7 processor running at 3.4GHz with 10GB of RAM and a 1TB hard disk.

PF8. A Private WBB Peer shall be able to respond to 95% of requests to authenticate a ballot, register a vote, cancel a vote and audit a vote within 10 seconds of receiving the request when running on the reference architecture.

3.4 Design Constraints

CO1. The software shall released to the public under an open source free software license [Fre13].

3.5 Software System Attributes

AT1. The System shall support early voting in Victoria, out of state and overseas.

AT2. The System shall support voting whenever an early voting centre is open during the voting period.

AT3. The voting period shall at a minimum be for 2 weeks with the System able to print ballots, audit ballots, register votes and cancel votes throughout this period, 24 hours per day, starting when all configuration information has been distributed to all components of the System.

AT4. All security protocols used by the System shall be made publicly available to ensure end-to-end verifiability.

AT5. Each component in the System shall have its own digital certificate.

AT6. Private WBB Peers shall use a threshold signature.

AT7. The software shall be written using Java 7 to ensure portability to all major server platforms.

AT8. Java library software shall be provided to support communications and signature checking on user interfaces devices.