Verifiable Voting in Victoria: from Prêt à Voter to vVote

Steve Schneider
University of Surrey

5th International Conference on E-Voting and Identity

September 4th 2015
Overview and Context

The Prêt à Voter verifiable voting system

From theory to practice: developing the design of vVote

Use in the Victorian State Election
Overall project led by Craig Burton at the Victorian Election Commission (VEC)

Surrey Project team:  
  Steve Schneider, Chris Culnane, James Heather,  
  Matthew Casey, James Rumble

Academic contributions:  
  Peter Ryan, Vanessa Teague, Steve Schneider,  
  Chris Culnane, James Heather, Rui Joaquim, Roland Wen

Further input/discussions:  
  Richard Buckland, Douglas Wikström

DemTech review team:  
  Carsten Schürmann, David Basin, Lorena Ronquillo

Code provided by:  
  VEC (front end), Surrey (back-end) and CryptoWorkshop (known for Bouncy Castle)
Overview

November 2014 Victorian State election.
   Early voting for two weeks 17-28 November
   Polling day 29th November

Early voting included: Electronically Assisted Voting provided by the vVote system in 24 early learning voting centres in Victoria (including 6 accessibility super centres), aimed at disability and LOTE groups. Also offered to all voters at Victoria House in London, UK

The vVote system was based around the original design of Prêt à Voter, a verifiable voting system. A number of developments to the design were necessary to apply it in this context.
Achievements

- **vVote** - the end-to-end verifiable (e2ev) electronic voting system used in the Victorian State Election early voting Nov 17-28. The back-end infrastructure ran for two weeks without a hitch, no downtime, patching or reboots required.

- The first time an end to end verifiable voting system has been used at scale to collect votes from blind voters, providing secrecy. [Audiotegrity within Scantegrity was the world first]
  - Also serves partially sighted, motor impaired, and LOTE.

- The first time an e2ev voting system has been used to collect remote votes.
  - Votes from London arrived immediately [Paper votes took two weeks to reach Victoria]

- The first time an end-to-end verifiable voting system has run across a wide geographical area, at a number of polling sites (24 in Victoria, + London).

- A controlled and limited deployment to manage risk of completely new technology: 1121 votes collected. (system scales to 1M). No challenges!
For the first time, **secrecy of the ballot** is enshrined in law, and ballot forms are regularised.

Campaigned for by the Chartists. (Lack of support for secret ballot in UK.)

Establishment of the new State of Victoria (established 1850, separating from New South Wales) offered the opportunity.
District vote:

Number the candidates in order of preference
Region vote:

Above The Line: select exactly one choice;  or

Below The Line: number the candidates in order of preference
Why introduce technology?

Accessibility

Multiple Languages

Long-distance voting

Widening participation

Cost savings (…)

Reliability and speed of counting

Efficiency and convenience

WANT e-voting but recognise the security issues. Hence VEC were interested in verifiability
Side remark - on a regular basis in the UK:

**The Telegraph**

**Digital democracy: will 2015 be the last paper-based general election?**

Paper-based voting is arguably one of the most archaic aspects of our democratic system. Sophie Curtis investigates how far we are from a 21st-century solution

---

**House of Commons**

**John Bercow calls for online voting in 2020 general election**

Commission set up by House of Commons Speaker also says there should be live social media coverage of debates

---

**56%**

56% of the British public support the inclusion of an #onlinevoting option in the upcoming EU referendum.

WebRoots Democracy/YouGov
July 2015 | 1,543 GB adults

Join the campaign for #onlinevoting at webrootsdemocracy.org/get-involved.
In current paper elections:
  - How can you check your vote was counted?
  - How can you challenge the system if you don’t think it was?
  - What if your vote was lost?
  - What if your vote was spoiled during counting?

You have to trust the system. [Some observation is possible.]
In current paper elections:
  – How can you check your vote was counted?
  – How can you challenge the system if you don’t think it was?
  – What if your vote was lost?
  – What if your vote was spoiled during counting?
You have to trust the system. [Some observation is possible.]
For financial transactions, this approach of trusting the system would be unthinkable.

- No receipts.
- No bank statements.
- No way of challenging mistakes (or fraud).

- You would have to pay the cost of any fraud on your account.

If you don’t trust your bank (for honesty or competence) you can change banks.

No such option with voting systems.
Ideally we want:
  voters to be able to verify their own votes have been included,
  …and to be able to challenge the election if not.

So they need some form of vote receipt.

Similar to banking: expect to see statements and transaction receipts. Don’t need to worry about the software banks are running, because you can check the output - software independence.

**Verifiability** gives the opportunity to check and audit elections analogous to statements and transaction receipts generated in banking.
The Prêt à Voter approach to verifiable voting
Candiates in random order

Different ballot forms have different orders

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice</td>
<td></td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>3. Crystal</td>
<td></td>
</tr>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td></td>
</tr>
</tbody>
</table>
The Prêt à Voter approach: ballot forms

Candidates in random order

Different ballot forms have different orders
1. Place X against desired candidate.
2. Separate left hand side.
3. Destroy left hand side.
4. Cast (scan) vote.
5. Take receipt home.

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Bob</th>
<th>Crystal</th>
<th>Diane</th>
<th>Elaine</th>
</tr>
</thead>
<tbody>
<tr>
<td>#197</td>
<td>Fx2g7H</td>
<td>4SQ10K</td>
<td>Ho0mbV</td>
<td>G6ffx1</td>
<td>Jw2Za1</td>
</tr>
</tbody>
</table>

#197 Fx2g7H
### Voting

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice</td>
<td>#197 Fx2g7H</td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>3. Crystal</td>
<td></td>
</tr>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td></td>
</tr>
</tbody>
</table>
Place X against desired candidate.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td></td>
</tr>
<tr>
<td>3. Crystal</td>
<td>X</td>
</tr>
<tr>
<td>1. Alice</td>
<td></td>
</tr>
</tbody>
</table>

#197
Fx2g7H
Place X against desired candidate.
Separate left hand side.

| 4. Diane |  |
| 2. Bob   |  |
| 5. Elaine|  |
| 3. Crystal|  |
| 1. Alice |  |

#197  
Fx2g7H
Place X against desired candidate.
Separate left hand side.
Destroy left hand side.
Place X against desired candidate.
Separate left hand side.
Destroy left hand side.
Cast (scan) vote.
Place X against desired candidate.
Separate left hand side.
Destroy left hand side.
Cast (scan) vote.
Take receipt home.
Implicit assumptions and issues

Secure printing (for privacy)

Secure chain of custody of ballots (for privacy)

Usability (scalability) of permuted candidate list

What if scanning doesn’t complete?
A voter might have the following concern:
- suspect ballot forms
- ‘what if the encrypted order doesn’t match the printed order?’
This should never happen if the ballot forms are correctly constructed.
A voter might have the following concern:
- suspect ballot forms
- ‘what if the encrypted order doesn’t match the printed order?’
This should never happen if the ballot forms are correctly constructed.

<table>
<thead>
<tr>
<th>#197</th>
<th>Diane</th>
<th>Bob</th>
<th>Elaine</th>
<th>Alice</th>
<th>Crystal</th>
</tr>
</thead>
</table>

Decryption

#197
Fx2g7H…
A voter might have the following concern:
- suspect ballot forms
- ‘what if the encrypted order doesn’t match the printed order?’
This should never happen if the ballot forms are correctly constructed.

Decryption

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>#197</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A vote for Crystal would be counted for Alice
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice</td>
<td></td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>3. Crystal</td>
<td></td>
</tr>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td>#197</td>
</tr>
</tbody>
</table>
Auditing the ballot forms

To audit a ballot form – a voter can have it decrypted without voting, and check that the result matches the printed candidate order.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice</td>
<td>#197</td>
</tr>
<tr>
<td>3. Crystal</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td></td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
</tbody>
</table>
To audit a ballot form – a voter can have it decrypted without voting, and check that the result matches the printed candidate order.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice</td>
<td></td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>3. Crystal</td>
<td></td>
</tr>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td></td>
</tr>
</tbody>
</table>
To audit a ballot form – a voter can have it decrypted without voting, and check that the result matches the printed candidate order. We introduce the option to audit as part of the voting process: “cut and choose”

Voters can do this with as many forms as they like (in principle!) This gives them confidence that the ballot forms are correctly constructed.

Q: How hard is this for voters in practice?
Q: How many have to do it in practice?
Voter receipts prevent election officials or hackers from altering or removing votes
Detection of bugs
Voters confirm inclusion of their vote

Public bulletin board of votes cast.

Voter’s receipt
Voter receipts prevent election officials or hackers from altering or removing votes
Detection of bugs
Voters confirm inclusion of their vote
Implicit assumptions and issues

Veracity of receipt for dispute resolution

Existence of append-only bulletin board
Votes can now be mixed and decrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]

Public bulletin board of votes cast.

```
#132  X
#128  X
#249  X
#197  X
```

→ ma7cd5

→ r2d2sw

→ c3pols

Elaine

Elaine
Votes can now be mixed and encrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]

Public bulletin board of votes cast.

- #132: ma7cd5
- #128: r2d2sw
- #249: c3pols
- #197: G6ffxl

Elaine
Alice
Elaine
Votes can now be mixed and decrypted. [NB: also applicable to STV]
Votes can now be mixed and decrypted. [NB: also applicable to STV]

Public bulletin board of votes cast.

Mixnet

→ Crystal
→ Elaine
→ Alice
→ Elaine

X
#132

X
#128

X
#249

X
#197

→ ma7cd5
→ r2d2sw
→ c3pols
→ G6ffx1
When the votes are cast:

Publish the votes cast (newspaper, or web bulletin board)
   - these should match the receipts, and voters can check.
Decrypt to reveal the encrypted votes.
Publish the revealed votes.
Count the votes.
Voters → Ballot Casting → Encrypted Votes → Ballot Shuffling by mixnet → Encrypted Votes → Decrypt and Count → Results

- Verify by receipts (individual)
- Verify by checking proofs (universal)
- Verify by public information (universal)

End-to-end verifiability
Application to Victoria

from Prêt à Voter to vVote and SuVote
November 2011 - November 2014
2011: Decision taken by VEC for a new electronic voting system. Initial discussions between Craig Burton (VEC) and Vanessa Teague (University of Melbourne). Prêt à Voter considered most suitable academic proposal for STV.

Nov 2011: Vanessa Teague’s initial Electronic Ballot Marker scheme adapting Prêt à Voter. Discussed within `Trustworthy Voting Systems’ project (Surrey, Luxembourg, Birmingham).

June 2012: Demonstrator developed by Surrey for VEC go/nogo decision by the Victorian Electoral Matters Committee.
- decision to proceed on the basis of the core concept,
- more work needed on the design, interface and procedures.
- a leap of faith!
- VEC managed the risk by keeping the numbers small and only offering to specific groups.
Oct 2012: Design challenges arising: Web Bulletin Board, Print on Demand

Dec 2012: Requirements specification

Feb 2013: Decision to proceed with vVote

May 2013: Design challenges resolved

Dec 2013: Delivery of SuVote system to VEC

Dec 2013 - Aug 2014: Integration and Testing

Feb - Mar 2014: Demtech review of system

Nov 2014 State Election
Victorian Electoral Commission (VEC) vVote system

Designed by a team of academics in collaboration with VEC

Back end implemented by Surrey

Front end (interface with voters) written by VEC

Mixnet written by CryptoWorkshop (known for Bouncy Castle)

Votes completed and submitted electronically; receipt issued.
Developing the design

necessity is the mother of invention

vVote: a Verifiable Voting System
Culnane, Ryan, Schneider, Teague

ACM TISSEC, 18(1) 2015
Key new developments

Key evolutions from Prêt à Voter:

- Electronic Ballot Marker
- Print on Demand
- A Secure and Robust Bulletin Board
New development 1: Electronic Ballot Marker (EBM)

- Issue: The Victorian Ballot regional ballot form has too many candidates to allow a voter to vote by hand against a randomised order

- Issue: Voters expect to vote against candidates presented in a legal order

- Solution (Teague Nov 2011): Electronic Ballot Marker (EBM) captures the vote electronically and completes the ballot form for the voter

Voting tablet: User interface for you to construct your vote, then submit it.
• Use an (offline) Electronic Ballot Marker to assist the voter to complete the ballot.
  • It will capture the voter’s preferences in a user-friendly way, and will print the preferences.
  • Voter is given a PaV ballot form on registration
  • Scans the QR code on the ballot form to get the permutation/candidates
  • Presents the candidates on the screen in the given fixed order
  • Captures the voters preferences via touch screen
  • Prints the preferences onto the ballot form in the appropriate permutation (a cheque scanner/printer was used)
  • Voter confirms selection, separates the ballot into two halves, and scans the selection.
  • **Benefit:** Alerts voter if ballot not well formed
  • **Benefit:** Can have accessibility plug-ins (vision/mobility impaired) and offer different languages.
  • **NB:** does lose the attractive feature of Prêt à Voter that no device learns the vote. This seems unavoidable.
The initial approach: using a cheque printer to print the selection

Handles the different races:

The front side

The back side
• **Use an Electronic Ballot Marker to assist the voter to complete the ballot.**

• **It will capture the voter’s preferences in a user-friendly way, and will print the preferences.**

• **Voter starts with only a (permuted order) Candidate List (one half of the ballot)**

• **Scans the QR code on the ballot form to get the permutation/candidates**

• **Presents the candidates in the given fixed order**

• **Captures the voters preferences via touchscreen**

• **Prints the preferences onto a separate receipt in the appropriate permutation**

• **Voter aligns the Candidate List and Preferences Receipt and checks they match**
**Problem**: voting centres must allow voters to vote in any district. This means serving 88 different ballot forms at any voting centre. It also means that distributing pre-printed ballot forms, the original (implicit) approach, is not an option.

Print on demand required! However, secure ballot generation must be retained, as the PoD equipment knows the permutations on the ballots.

**Solution**: (first attempt): generate encrypted ballots centrally in a secure environment, and re-encrypt on demand to serve them to polling places. Printer at polling place then prints the candidate list. **However**: Computationally too expensive, bottleneck from ballot server.

**Solution**: (April 2013): use polling place print tablets to do the computational heavy lifting, in advance, with centrally generated randomness.

_Faster Print on Demand for Prêt à Voter_, Chris Culnane, James Heather, Rui Joaquim, Peter Y. A. Ryan, Steve Schneider, Vanessa Teague, EVT/WOTE 2014
For each printer (i.e. one or two per polling station), `randomness generation servers` generate randomness, commit publicly (on the bulletin board), and encrypt and send to the printer tablet.

A threshold of the randomness servers are trusted for privacy and competence.

Printer uses the randomness to generate the encrypted ballot (this is the computational heavy lifting). The printer does not introduce any of its own randomness. This can be (and is) audited. Printer holds the ballots until they are required.

For authenticated voters during the election, the printer prints the next ballot in the sequence, with human readable candidate names for the required races. This ballot is then used with the electronic ballot marker to cast a vote.
“We don’t know how to build a secure bulletin board”

David Wagner, EVT’13 Keynote
Problem: We need to implement a Web Bulletin Board which is secure and robust (no single point of failure), and allows real-time (fast) accept/reject of posts and issuing of receipts.

- Only posted items may appear on the board
- Any item for which a receipt has been issued must appear on the board
- Clashes must not appear on the bulletin board
  (e.g. 2 votes for the same ballot form, or an audit and vote for the same ballot)
- Decisions to accept/reject posts, avoiding clashes, must occur in real time
- Items cannot be undetectably removed from the bulletin board

Uses threshold signatures for the bulletin board peers to jointly sign. Works provided a threshold (5 out of 7) participate correctly.
Problem: We need to implement a Web Bulletin Board which is **secure and robust** (no single point of failure), and allows real-time (fast) accept/reject of posts and issuing of receipts.

*No suitable algorithm in the peer-reviewed literature to achieve all of these requirements.*

Much discussion around this within the project in late 2012.

Solution: A suite of distributed agreement algorithms between peer servers with individual local databases, using threshold signatures:

- joint issuing of signed receipts in real-time - fast.
- a daily joint ‘publication’ - Byzantine protocol agreement on WBB contents

Formal verification took a year (elapsed time) and identified some improvements.


Chris Culnane, Steve Schneider, CSF 2014
System Architecture
How it looks

The Voting Ceremony
On arrival, the voter is confirmed for eligibility by a VEC poll worker, and marked off the list.

A candidate list is printed off for the races the voter is eligible to vote in. Ideally the poll worker does not see the printed candidate list.

The ballot form is given to the voter, who takes it to a polling booth.

Alternatively, this is the point at which the voter can have the candidate list audited.
Polling station: Australia House, London
Scan the candidate list into the electronic ballot marker (EBM)
The vote is then constructed through the touchscreen.

Audio options, with swipe gestures or telephone keypad interface are also available.
## Choice of language

<table>
<thead>
<tr>
<th>English</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amharic</td>
<td>ኢማርኛ</td>
</tr>
<tr>
<td>Arabic</td>
<td>العربية</td>
</tr>
<tr>
<td>Bosnian</td>
<td>Bosanski</td>
</tr>
<tr>
<td>Cantonese</td>
<td>广东话</td>
</tr>
<tr>
<td>Croatian</td>
<td>Hrvatski</td>
</tr>
</tbody>
</table>

Next
Customise interface

Visual settings

- Large Font
- Medium Font
- Black on White
- White on Black

AUDIO ONLY VOTING
District voting instructions

How to Vote for Your District

To vote on your district ballot paper, touch the box next to each candidate name in the order of your choice. Touch OK to start or touch BACK to return to the visual settings screen and change your selection.
Constructing the district vote

Albert Park District

4 ALBANY, Stephen Charles
   THE NATIONALS

3 BIRRELL, Ann
   AUSTRALIAN GREENS

2 FOLEY, Martin
   AUSTRALIAN LABOR PARTY

1 ALBERTYN, Frances

5 ALBION, William Alexander
   PEOPLE POWER - NO SMART METERS
Region vote instructions

How to Vote on Your Region Ballot Paper

You can either vote for one group or for individual candidates. If you vote for individual candidates you must choose at least five.

Touch here to vote for a group

Touch here to vote for individual candidates
Above The Line selection
Voting

... or Below The Line selection

Southern Metropolitan Region

PRESS HERE TO VOTE FOR A GROUP INSTEAD OF INDIVIDUAL CANDIDATES

BROAD, Jane
D.L.P. - DEMOCRATIC LABOR PARTY
Burwood

DRUMMOND, Bill
D.L.P. - DEMOCRATIC LABOR PARTY
Burwood

GUY, Madelaine Eve
D.L.P. - DEMOCRATIC LABOR PARTY
Burwood

IRELAND, Todd
D.L.P. - DEMOCRATIC LABOR PARTY
Burwood

ROYALL, Paul
D.L.P. - DEMOCRATIC LABOR PARTY
Burwood

HUPPERT, Jennifer
AUSTRALIAN LABOR
Caulfield

SALINA, Pablo
AUSTRALIAN LABOR
Caulfield

EDWARDS, Zoe
AUSTRALIAN LABOR
Caulfield

LENDERS, John
AUSTRALIAN LABOR
Caulfield

SUSUDDJEIWKS
AUSTRALIAN LABOR
Caulfield
## Review votes

### District votes
1. **ALBANY, Stephen Charles**
   - THE NATIONALS
2. **BIRRELL, Ann**
   - AUSTRALIAN GREENS
3. **FOLEY, Martin**
   - AUSTRALIAN LABOR PARTY
4. **ALBERTYN, Frances**
5. **ALBION, William Alexander**

### Region votes
1. **LENDERS, John**
   - AUSTRALIAN LABOR PARTY
2. **EDWARDS, Zoe**
   - AUSTRALIAN LABOR PARTY
3. **SALINA, Pablo**
   - AUSTRALIAN LABOR PARTY
4. **HUPPERT, Jennifer**
   - AUSTRALIAN LABOR PARTY
**Send My Votes.** This is the point at which the vote is cast.

**Completing Your Vote**

To complete voting click on the SEND MY VOTES button below. **ALERT!** Once you send your votes you CANNOT change how you voted.
Your receipt is printing. You may check your receipt against your candidate list to confirm how you voted. You can take the receipt home but you must discard the candidate list in the security bin before leaving.
Checking the receipt

The voter has the candidate list

The preferences receipt is printed.
The voter checks that the preferences on the receipt align with the selected candidates on the candidate list.

Once the voter is satisfied the preferences match the candidate list, the candidate list must be securely destroyed.
The voter has the candidate list

The preferences receipt is printed
The voter has the candidate list

The preferences receipt is printed

The voter checks that the preferences on the receipt align with the selected candidates on the candidate list
The voter has the candidate list

The preferences receipt is printed

The voter checks that the preferences on the receipt align with the selected candidates on the candidate list

Once the voter is satisfied the preferences match the candidate list, the candidate list must be securely destroyed.
The voter retains the preferences receipt, and uses it to check the bulletin board after the end of the day.

[evote.vec.vic.gov.au/wbb/findReceipt.html]
Receipt lookup

Voting Receipt 2080101:36
Recorded on the 24/11/2014 at BENDIGO WEST EVC 1

This is the voting receipt for the entered serial number. This information does not provide the voter’s voting choices, which are kept secret by the VEC. These preferences are NOT in ballot order. What you see should match the printed preferences receipt.

PREFERENCES RECEIPT
THIS IS NOT A BALLOT
VEC Voting receipt
My vote remains private

Serial Number 2080101:36
Bendigo West
(Not in ballot paper order)

2 4
1 3
5
6

Northern Victoria
Public Commitment: Herald Sun

Hash code of the WBB daily commit of 27th November 2014

Prevents subsequent changing of the published bulletin board
Deployment experience
November 2014 Victorian State election.

EAV deployed during Early voting for two weeks 17-28 November [Not allowed to be deployed on Polling day (29th November)]

Electronically Assisted Voting provided in 24 early learning voting centres in Victoria (including 6 accessibility super centres), aimed at disability and LOTE groups.

Also offered to all voters at Victoria House in London, UK

1121 votes taken electronically across the 88 district races and 8 region races (compared with 961 in 2010).

[NB The system had been tested for up to 1M votes, and to receive 800 in a 10s period]
Bulletin Board systems were up 100% of the time with no errors. Average response time was 0.3s

Log files indicated no unexpected exceptions occurred during live voting

London was offline intermittently due to local networking problems. Affected voters voted on paper ballots

**London:** Average voting session time was about 3 minutes: ATL approx 2.5 minutes, BTL approx 4.5 minutes

**Victoria:** Average voting session time about 9.5 minutes: ATL approx 9 minutes, BTL approx 11 minutes

Informal electronic votes: District 2.5% Region 1.15%
Informal paper votes: District 5.22% Region 3.43%
Ran the questionnaire on 3 days in the second week. Took a while to get VEC approval (having originally been refused).

Usability questions

Also asked about attitudes to e-voting and security
User Surveys (London)

The system was easy to use
- missed/can’t answer
- strongly agree
- agree
- weakly agree
- neither agree nor disagree
- weakly disagree
- disagree

Someone who sees receipt can know my vote
- missed/can’t answer
- strongly agree
- agree
- weakly agree
- neither agree nor disagree
- weakly disagree
- disagree

I have trust in the voting system
- missed/can’t answer
- strongly agree
- agree
- weakly agree
- neither agree nor disagree
- weakly disagree
- disagree

Concerned about e-voting security
- missed/can’t answer
- strongly agree
- agree
- weakly agree
- neither agree nor disagree
- weakly disagree
- disagree
Voters were aware of security issues with e-voting but still did it!

One voter (out of 20 I observed) did not want to vote electronically

Voters seemed satisfied and found it straightforward

The majority appeared to check the receipt against the candidate list

Some threw away the receipt when they had finished

One voter wanted to know why the system kept deleting his ATL vote when he went BTL. Evidently on paper he always voted ATL and BTL

A couple of voters did not like having to complete the order from first preference. They wanted to also start numbering in reverse
<table>
<thead>
<tr>
<th>Section/page</th>
<th>Sub-page</th>
<th>Go Live Date</th>
<th>Views</th>
<th>Reading Time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistance for voters</td>
<td></td>
<td>1/11</td>
<td>11,120</td>
<td></td>
</tr>
<tr>
<td>Electronic voting</td>
<td>Electronic voting detail</td>
<td>12/11</td>
<td>20,426</td>
<td>0:04</td>
</tr>
<tr>
<td></td>
<td>Find receipt / fetch</td>
<td>18/11</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verification data files</td>
<td>18/12</td>
<td>139</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source code repository</td>
<td>12/11</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Files</td>
<td>1/11</td>
<td>1505</td>
<td></td>
</tr>
<tr>
<td>Candidate Registration</td>
<td>Candidate Name</td>
<td>6/11</td>
<td>379</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pronunciation (to 15/11)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: VEC Electronic Voting web page and receipt lookup service hits: November 2014 – January 2015
Training of VEC staff, and educational material for voters, was not as extensive as we would have liked. Substantially more needed in future. Some staff did not feel very confident supporting the system.

VEC chose not to explicitly offer audit of ballot forms to voters for 2014
- they considered the concept too complex to explain in real-time
- therefore the end to end verifiability chain missed one of the links although
  - it was enabled within the system (and one test audit was carried out)
  - Teague’s Election Watch article explained it, so informed voters could have requested it (though none did).

**Point for future resolution:** Including ballot audit more systematically
- education of voters (though most want to vote and go)
- official auditors in addition? [cf Scantegrity]
Compromises and considerations for this deployment

No shredders were allowed in polling stations. Instead candidate lists were posted into a secure box for later shredding by VEC. ‘VEC know how to handle paper’. Elections Branch are very nervous of shredders in polling stations

Electronic votes decrypted after the mix, printed off, then manually entered into the count with all the other votes. Hence not end-to-end cast to tally. Verifiable only to the printing of votes

There was pressure within VEC Elections Branch to drop some of the verifiability elements for convenience and ease of use

Single point of trust (and failure): VEC held all the key shares and managed all the servers. The system enabled distribution of keys and servers but VEC chose not to deploy it for 2014
Verifiable voting - voters can check inclusion of their vote as they cast it, and can challenge the election if not

Integrity of the election can therefore be verified

Proofs of correct processing of the votes

Secrecy: cryptography is used to protect ballot secrecy. Threshold cryptography distributes trust and ability to decrypt

Developed into a system used in a real live election: in Victoria in November 2014 no challenges by voters or political parties

No other electronic or internet voting system currently in use anywhere in the world offers this
The vVote project has now concluded

The code is available as open source under GPL3: bitbucket.org/vvote

The Victorian Parliamentary Electoral Matters Committee Enquiry into the 2014 State Election is proceeding

Coasca Ltd is a start-up company out of Surrey University to commercialise the SuVote back-end of the system which provides verifiable voting
“The Polling”, William Hogarth, ~1760