Software Improvements

ABN: 85 008 655 418

Wednesday, 14 May 2008
Our Ref: C03193/STL03264

Committee Secretary
Joint Standing Committee on Electoral Matters
Department of House of Representatives
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Secretary

Re: Inquiry into the conduct of the 2007 election and matters related thereto

As with all Government agencies, the Australian Electoral Commission (AEC) faces rising community expectations in the age of the Internet and Digital communications.

The electorate expects to do things electronically, particularly the young. Their mobile phones are a critical personal accessory and they expect to interact with governments through the Internet. The wider population wants to see improved systems, reduced costs and productivity gains while at the same time expecting privacy and integrity of our existing excellent systems maintained and enhanced.

The AEC has been at the forefront of using digital methods and with the 2007 trialling of electronic voting systems (e-voting) has gained invaluable experience in understanding how these systems operate and the issues involved.

The approaches presented in this submission represent the next step in the evolution of voting systems and will keep Australia at the forefront of voting systems while containing costs and in the longer term potentially reducing costs. In summary, the following can be achieved:

i) Allow persons with most forms of disability to vote unaided and secretly.
ii) Bring electronic remote, secret, voting to any terminal connected to the Internet.
iii) Give voters more choice in how they cast their votes.
iv) Increase the level of voter registration
v) Move towards the 2020 objective of registration of most young people and new citizens as soon as they are eligible to vote.
vi) Increase the integrity and currency of the electoral roll.
vii) Increase the speed that votes are counted.
viii) Keep Australia in the forefront of voting systems and provide a platform for future innovation.

This submission outlines the history of electronic and remote voting in Australia and points the direction for the AEC to take the next steps in the development of remote e-voting and electronic enrolment.

At the 2007 Federal Election the Australian Electoral Commission (AEC) undertook two trials of e-voting:

- at polling places, kiosk e-voting for blind and vision impaired electors using an eVACS® solution, and
- remote e-voting for Australian Defence Force (ADF) personnel on 'active duty' overseas at the time of the election.

There are two aspects of these e-voting trials on which I would like to provide comment:

i) maximising value for the cost of providing kiosk e-voting; and
ii) controlling access for remote e-voting.

In addition, comment is made on a reliable approach regarding electronic enrolment using the same technology applicable to remote e-voting.

Maximising value for the cost of providing kiosk e-voting

The legislation enabling the kiosk e-voting trial, limited the trial to allowing only electors who are blind or have vision impairment to vote electronically. This limitation is in marked contrast to the first trial of electronic voting undertaken in Australia in the Australian Capital Territory (ACT) in 2001, where the emphasis was on providing electronic voting to assist a range of electors to have a 'secret' vote. In addition to people with vision impairment, the ACT trial assisted people from non-English speaking backgrounds (instructions in multiple languages) and people with poor reading skills (audio). A key feature of the eVACS solution is that the system used by the vision impaired is the same as that used by everyone else. Hence in the ACT anyone can elect to vote electronically at a polling place where e-voting is provided.

Another aspect of the on-going use of e-voting for ACT elections, is the criteria used for selecting the locations at which e-voting is provided. In the ACT these are locations accessible to people with vision impairment, as well as normal polling places where large numbers of votes are recorded. The intent is to maximise the number of people who vote electronically, which has two benefits:

i) the average cost per voter to provide the e-voting solution is reduced, and
ii) the cost to input non-electronic vote data to enable electronic counting is also reduced.

The AEC always referred to the 2007 trial as a trial of electronically assisted voting. Ballot representations were printed for the House of Representatives and the Senate for counting using the normal processes: manual counting for the House of Representatives and re-entering the data to be counted electronically for the Senate. Once the ballot representations had been printed for a voter, all vote data for that voter was removed from the kiosk e-voting machine. As a consequence none of the in-built counting features of eVACS were utilised. The re-entering of Senate votes in particular could be seen as unnecessary cost, as well as providing a potential opportunity to introduce error given the ballot representations were printed on A4 sheets and bore no resemblance to the actual Senate ballots, apart from the order of groups and candidate names.

Removing the limitation to "assist blind and vision impaired people to vote" and enabling electronic vote data to be stored would enable the AEC to provide a more cost-effective kiosk e-voting solution.

Controlling access for remote e-voting

There are a number of groups of voters whom the AEC has identified as not having access to regular polling places and who could significantly benefit from access to remote e-voting:

- ADF personnel, as per the 2007 trial
- electors in Antartica
- electors in other remote localities
- electors with a disability
- electors travelling or working overseas,
- people in remote localities of Australia

(See http://www.aec.gov.au/Voting/report.htm and http://www.aec.gov.au/pdf/voting/E-voting_report.pdf)

Voting typically involves three processes:

1) voter registration (enrolment)
2) voter identification (a check against the electoral roll)
3) voter authentication to ensure one vote per voter (provision of one set of ballot papers)

These processes are equally applicable with e-voting.

Apart from the AEC trial, in Australia kiosk-type voting is in on-going use in the Australian Capital Territory (since 2001), and has been used for a trial in 2006 in Victoria. For e-voting as used in either the Australian Capital Territory or Victoria, the normal enrolment and identification processes are followed, with a unique access token provided to each voter to ensure only one vote per voter. In the ACT, access tokens (in the form of a barcode) are randomly assigned to voters to ensure no linkage between the voter and their vote, and to determine the ballots to be displayed.

For the AEC kiosk trial in 2007, again normal enrolment and identification processes applied with access to e-voting managed via a barcode used by a polling official to start a voting session, select the correct State and Division, and then end the voting session. All polling officials had identical barcodes so ensuring only one vote per voter was managed by election procedures, including the requirement for eVACS to print ballot representations that were placed in declaration envelopes.

The AEC remote e-voting trial required a separate enrolment (in addition to normal enrolment) and used a cumbersome process for controlling access, in which Personal Identification Numbers (PINs) were generated and linked directly to ADF personnel registered to vote electronically, and then sent by ‘registered post’ (requiring the recipient to sign for receipt) to each.

None of these access approaches is particularly cost-effective when considering electronic voting for large numbers of remote voters, as well as ensuring no linkage between a voter and their vote.

The electronic identification process managed by Edentiti (described in detail in the Attachment) provides an extremely efficient and highly cost-effective identification mechanism which when combined with random allocation of access tokens at the time of voting via eVACS, enables the provision of cost-effective secure e-voting to remotely located Australian voters in all of the six (6) groups identified by the AEC.

In brief, Edentiti provides an identity verification system by which an individual is able to establish their 'edentiti' which they can use to verify electronically who they say they are. As part of the initial verification process a voiceprint is recorded. The availability of a voiceprint with an 'edentiti' enables an intending voter to prove electronically who they are at the time they want to vote.

Electronic enrolment

The AEC currently enables people to download an Electoral Enrolment form from their website, as one of the ways to obtain an enrolment form. Various ways to prove identity are acceptable with declaration(s) either by the person seeking to enroll or others depending on the circumstances. The form is then posted to the AEC for processing. The whole process takes some days or weeks to complete.

The Edentiti identity verification system can be easily integrated into the existing AEC registration system as an extra verification technique to complement existing enrolment processes. The enrolment process with Edentiti can be completed within minutes at any hour of the day.

In section 5 of the Attachment a trial of electronic enrolment is proposed by incorporating the Edentiti verification system as part of the existing processes in place at secondary education institutions to assist students to identify themselves for the purpose of obtaining a driver's (learner) license or opening bank accounts. A successful trial would set the scene for the adoption of the Edentiti approach to prompt and enable young people eligible to enrol to register for AEC enrolment while at school or college. This would satisfy the 2020 summit recommendation on a more automated process for young people to enroll to vote but done in a privacy friendly way (http://www.australia2020.gov.au/report/index.cfm).

Final remarks

The Attachment to this letter is classified as Commercial-in-Confidence and was prepared for the AEC, and is therefore not available for publication by the Committee.

However, Mr Kevin Cox, Chief Technical Officer, Edentiti Pty Ltd and myself are available to meet with the Committee to discuss any of the content of this letter and Attachment.

Yours sincerely

Carol J Boughton

Carol Boughton
Managing Director

Proposal for the

AEC

Australian Electoral Commission

on

Electronic Enrolment and Remote Electronic Voting

April 2008

edentiti

eVACS®

This page is intentionally left blank.

Contents

Executive Summary 4
1 Introduction 5
2 Remote electronic voting 5
2.1 Background 5
2.2 Remote e-voting 6
2.2.1 Voter registration for remote e-voting 6
2.2.2 Voter identification for remote e-voting 7
2.2.3 Voter authentication for remote e-voting 8
2.2.4 Other features of remote e-voting 9
2.2.5 The remote e-voting process 9
3 Potential concerns 10
3.1 Privacy 10
3.1.1 Privacy with eVACS 10
3.1.2 Privacy with Edentiti 10
3.1.3 Individuals establishing relationships with other agencies 11
3.2 Accuracy of voice authentication 11
3.2.1 Coercion of the voter 11
3.3 Security 11
3.3.1 Edentiti 11
3.3.2 eVACS 12
3.4 Scalability 12
3.4.1 The last minute rush to vote 13
3.5 Reliability 13
3.5.1 Denial of service 13
4 Electronic enrolment 14
4.1 Background 14
4.2 Outline of the System operation 14
5 Trials 16
5.1 Electronic enrolment trial 16
5.1.1 Student verification process 16
5.2 Remote e-voting trial 17
6 Other potential benefits 17
6.1 Change of Address 17
6.2 EE-trial benefits 17
6.3 2020 summit recommendation 18
6.4 Visually impaired, other languages, other disabled access 18
6.5 Death notification 18
7 Pricing and savings 18
7.1 Estimated savings 19
8 Final comments 19

Executive Summary

Edentiti Pty Ltd (Edentiti) and Software Improvements Pty Ltd (Software Improvements) have joined together to provide an integrated highly reliable cost-effective secure, privacy friendly, electronic verification for electoral roll on-line registration and remote electronic voting (the System).

The Edentiti-eVACS remote electronic voting (e-voting) solution is based on the identification system from Edentiti and the eVACS® voting system from Software Improvements. Both these systems are existing operational products. A version of eVACs was used by the AEC at the 2007 Federal election to assist blind and vision impaired voters. Edentiti is used by Australian ASX listed companies to provide identification services to satisfy the new Australian AML/CTF "know your customer" legislation.

From a user perspective, the System is voluntary and would operate in parallel with existing AEC systems and would require minimal changes to the existing systems. It meets all the requirements of the Australian Privacy Act 1988.

The System replicates the existing paper based system and may not require any legislative changes as the electronic operations versus more manual operations are likely to be covered by the Electronic Transactions 1999 legislation.

Operating costs are based on the number of people who identify themselves and vote using the System. There are no development or rental costs for the AEC to adopt the System, although there may be some cost associated with tailoring eVACS to AEC requirements. If adopted the System will help the AEC contain costs, introduce new facilities to make it easier for many to vote – particularly the site impaired and those with handicaps, and increase enrolments of the young. The latter providing a privacy secure method for addressing the 2020 Summit idea to have universal automatic enrolment.

A low cost phased incremental strategy to introduce the system is recommended starting with selected Canberra Secondary Colleges for enrolment and a small student or industrial election for voting. The enrolment trial could be in operation within a month of a decision being made to proceed.

1 Introduction

Non-polling place electronic voting, particularly for remote voters, provides both advantages and disadvantages as reported in the document on the AEC website at (http://www.eca.gov.au/reports/electronic_voting.pdf). The major disadvantage identified in this joint Australian Electoral Commission (AEC)/Victorian Electoral Commission (VEC) March 2001 report is security, with two aspects in particular:

2 to ensure the system is not exposed to attack that would interfere with the elector's votes, and

3 to provide a level of confidence as to the identification of the elector at the time of voting.

The May 2007 distributed denial of service attacks on Estonian websites, primarily targeting the Estonian Government, banking, media and police sites, demonstrates not just the potential but also the reality of potential impacts of 'cyber attacks'.

The basis of this proposal to the AEC is to demonstrate how with the Edentiti-eVACS remote e-voting solution key security and elector confidence can be addressed.

In addition, the Edentiti means of verification of the identity of an elector provides an inexpensive means for the AEC to provide electronic electoral roll registration and change of enrolment details for all electors and can be made available immediately the proposed trial is complete.

This proposal for the use of the Edentiti-eVACS solution by the AEC follows a meeting on 26 March 2008 with Tim Pickering, First Assistant Commissioner, Electoral Operations and Rod Whitaker, Manager, Genesis Program, and provides more information on:

- the Edentiti-eVACS remote e-voting solution;
- potential concerns and how they are mitigated (privacy, access to other agency information, security of data, accuracy of voice authentication, the 'last minute rush to vote', scalability, reliability);
- electronic enrolment with Edentiti;
- possible trial(s) to test impacts and savings; and
- pricing.

2 Remote electronic voting

2.1 Background

At the 2007 Federal Election the Australian Electoral Commission (AEC) undertook two trials of e-voting:

- kiosk e-voting, at polling places, for blind and vision impaired electors using an eVACS solution, and
- remote e-voting for Australian Defence Force (ADF) personnel on 'active duty' overseas at the time of the election.

Elsewhere in Australia, kiosk-type voting is in on-going use in the Australian Capital Territory (since 2001), and has been used for a trial in Victoria. For e-voting as used in either the

Australian Capital Territory or Victoria, voters were provided with a unique access token to ensure only one vote per voter. In the ACT, access tokens are randomly assigned to voters to ensure no linkage between the voter and their vote, and to determine the ballots to be displayed. For the AEC kiosk trial, access to e-voting was managed by polling officials together with the requirement for electronic votes to be converted to paper ballot equivalents, which were then handled using declaration envelopes in the same way as postal (declaration) ballots.

The AEC remote e-voting trial used a cumbersome process for controlling access, in which Personal Identification Numbers (PINs) were generated and linked directly to ADF personnel registered to vote electronically, and then sent by 'registered post' (requiring the recipient to sign for receipt) to each.

None of these access approaches is particularly cost-effective when considering electronic voting for large numbers of remote voters potentially spread across thousands of locations, as well as ensuring no linkage between a voter and their vote.

The electronic identification process managed by Edentiti (described in detail in section 4.2) provides an extremely efficient and highly cost-effective identification mechanism which when combined with random allocation of access tokens at the time of voting via eVACS, enables the AEC to provide cost-effective secure electronic voting to remotely located Australian voters.

2.2 Remote e-voting

The three key aspects to remote e-voting are: i) voter registration, ii) voter identification and iii) authorised access to vote.

2.2.1 Voter registration for remote e-voting

There are three potential avenues by which an elector could pre-register to vote electronically:

- an additional feature is included with the current on-line entry form to verify enrolment details,
- choosing to register to vote electronically on initial enrolment via Edentiti, and
- a special e-voting enrolment process using Edentiti.

2.2.1.1 AEC on-line enrolment verification

The existing AEC on-line enrolment verification could be modified to include a link to the Edentiti verification system.

The AEC currently provides an on-line enrolment verification facility (https://oevf.aec.gov.au/) accessed via the AEC website. By entering their Surname, Given Names, Street Name, Suburb or Town, and State, an elector is able to verify their enrolment details as recorded by the AEC.

If enrolment is not confirmed for the details entered on-line, the following message is displayed, together with advice on what to do next.

✖ FAILED TO CONFIRM YOUR ENROLMENT

If enrolment is confirmed, the following information is displayed on screen:

✓ **ENROLMENT CONFIRMED**
Your enrolled address is <address as entered>
Your Federal Division is <name of Division>
Your State Electoral District is <name of District>
Your Local Government Area is <name of Local Government Area
Your Local Government Area Ward is <name of Ward in LGA>

With these procedures already in place, registering to vote electronically becomes a simple extension to these existing processes.

Assume an individual is already enrolled to vote. By using the exact same on-line entry form currently available on the AEC website, an elector could enter their own details and, when enrolment is confirmed, select an option to register to vote electronically. The elector would also select their language of choice and be able to specify other criteria such as large fonts.

On selecting this option, the elector is given access to the Edentiti environment (most likely via an "IFRAME" in the middle of the screen so the elector appears to still be on the AEC website) enabling the elector to establish their electronic identification, including registration of a voice print, voice phrase and telephone contact (land line, mobile or VOIP via a PC), as per section 4.2.

2.2.1.2 Initial enrolment

The second avenue to register to vote electronically is perhaps the simplest and cheapest. When a person chooses to enrol electronically, as part of their Edentiti verification they are asked if they do not want to register to vote electronically.

2.2.1.3 Independent process to register to vote electronically

The third avenue involves creation of a separate e-voting registration process linked to the AEC website, which could be for just a single election event or a permanent preference to vote electronically (or at least until the elector opts to change their preference).

2.2.2 Voter identification for remote e-voting

Creating an electronic identification with Edentiti enables remote e-voting in a way which establishes the identity of the elector at the time they want to vote, and does not pre-link the elector to a PIN or access token. While the Edentiti verification system can use a range of biometrics for unique identification purposes, at this time the most widely available, less intrusive and easily available to the elector is their voice print. In the future, the biometric can be extended to other schemes such as a pre-registered phrase for those who cannot hear or speak.

The process for identification to enable voting electronically is as follows:

- elector accesses AEC website and selects 'Vote electronically', in the same way an elector is currently able to select 'Check your enrolment details' or 'Electorate search';

- on selecting 'Vote electronically' a screen is displayed asking for elector details (for example, name and date of birth), similar to 'Check your enrolment details', with an OK button;
- on selecting OK, and being confirmed as a registered electronic voter, an 'IFRAME' (linked to Edentiti) is displayed with the message:

  You will be contacted shortly on your registered phone. Please recite your pre-recorded voice phrase when requested.

  OR

  If you do not have access to your registered phone, please call this number XXXX XXXX and recite your pre-recorded voice phrase when requested.
- a match with the registered voice print and voice phrase triggers the following actions:
  - the voter is marked as verified to vote electronically
  - the voter is randomly allocated an authentication token, based on their enrolment address, which determine the ballots to be displayed,
  - the particular authentication token is marked as 'assigned' in the authentication token database with no link to the voter, and
  - the authentication token is passed to the eVACS voting server, and
  - the Welcome screen for e-voting is displayed.

2.2.3 Voter authentication for remote e-voting

On receipt of the authentication token as per section 2.2.2, the voter is taken to the eVACS-Internet 'Welcome' screen for e-voting, with the full functionality of eVACS available.

For example, on the eVACS Welcome screen the voter could select (from a set of languages chosen by the AEC) which language they would like to use for the voting process, if the voter has not already registered a language choice with Edentiti.

After their language selection the first ballot (House of Representatives) with content based on the authentication token is displayed, with all instructions in the language of choice, as well as in English if needed. All other ballots are then displayed in sequence with associated confirmation screens.

On confirming their choice/s for the last ballot to be displayed, the following actions are triggered:

- the (encrypted) choices for all ballots are stored in the secure eVACS votes database
- the link between the vote session and the authentication token is removed
- the authentication token is marked as 'used' in the authentication database
- the Acknowledgement screen is displayed advising the voter that they have completed their vote.

2.2.4 Other features of remote e-voting

The scenario described in sections 2.2.1.1 to 2.2.1.3 reflects the situation where a voter chooses to simply follow the ‘standard’ remote e-voting process. However, there are other scenarios that must also be incorporated into the process.

As with the AEC website function enabling verification of voter enrolment details, there needs to be a process for dealing with a voter who has not pre-registered to vote electronically before attempting the voter identification process. From an Edentiti perspective, it is feasible to provide an option for the voter to “register to vote electronically” from the Voter Identification screen, given the intending voter is able to ‘verify’ their identity by their relationships and leaving a voice print. However, this approach conflicts with the normal process of ensuring enrolment by a specified date and creates difficulties for the AEC in having to estimate without any basis the number of authentication tokens required per electorate to be generated internally by eVACS in order to maintain the ‘closed system’ security feature of eVACS.

Other scenarios depending on AEC requirements include:

- voter abandons vote before confirming all ballots;
- voter believes ballots are for the wrong electorate; and
- voter to be issued with receipt on voting (this could be held in the individual’s identification vault on Edentiti).

2.2.5 The remote e-voting process

Assuming a voter is registered to vote electronically, the remote e-voting process is as depicted in Diagram 1.

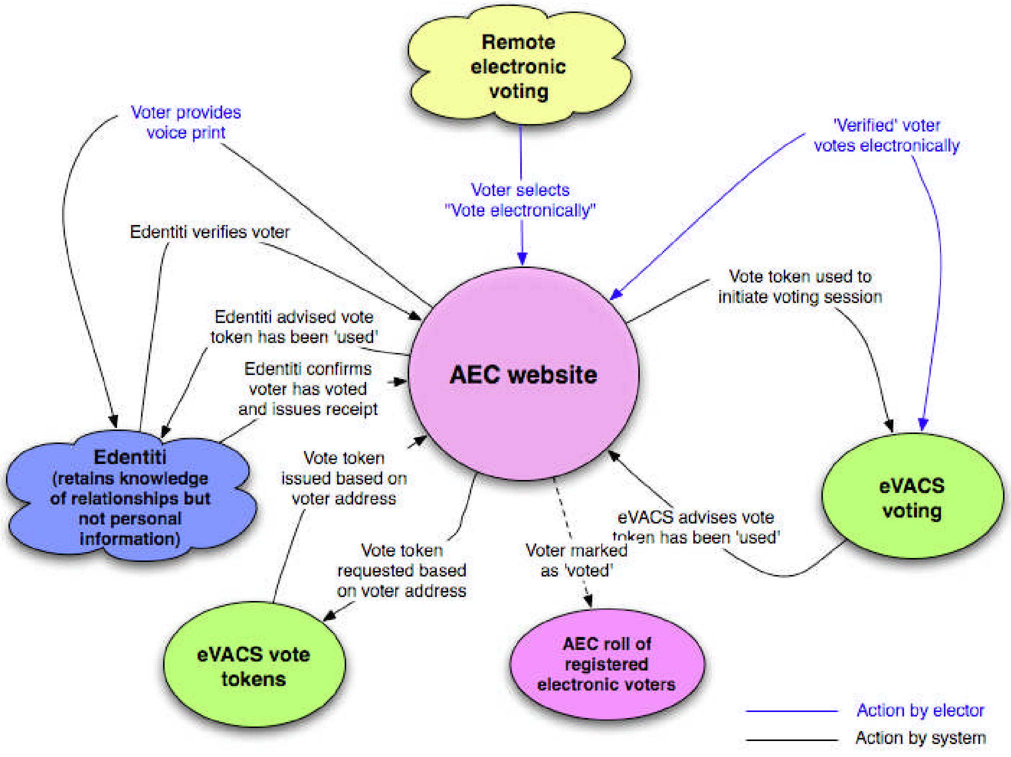
Remote electronic voting
Voter provides voice print
Voter selects "Vote electronically"
'Verified' voter votes electronically
Edentiti verifies voter
Vote token used to initiate voting session
Edentiti advised vote token has been 'used'
Edentiti confirms voter has voted and issues receipt
AEC website
Edentiti (retains knowledge of relationships but not personal information)
Vote token issued based on voter address
eVACS voting
eVACS advises vote token has been 'used'
Voter marked as 'voted'
Vote token requested based on voter address
eVACS vote tokens
AEC roll of registered electronic voters
Action by elector
Action by system

Diagram 1 – Remote e-voting with Edentiti and eVACS

3 Potential concerns

3.1 Privacy

Privacy is at the heart of the Edentiti – eVACS solution.

There are three key areas relating to privacy:

i) the linking of vote details to a voter,

ii) the retention of private information within Edentiti, and

iii) accessing private information held by another organization.

3.1.1 Privacy with eVACS

The AEC is already familiar with the privacy aspects of eVACS from the kiosk e-voting trial in 2007. With eVACS, no private information is used to access electronic voting, nor is any personal information stored in the eVACS votes database. The implementation as proposed in Diagram 1 clearly has no linkage between the vote details and the voter.

3.1.2 Privacy with Edentiti

Edentiti does not store private data or identifiers, only public information such as name, address, email address and contact phone numbers. Relationships with other organisations are stored but only as an indicator, on whether the person has established that they have a verified relationship with an organisation.

A document "Online Identity Verification Privacy & Legislative Compliance Overview" is available on request from Edentiti. Most identification systems work by organisations having access to information about a person and checking what the person says against stored data. Edentiti uses a different paradigm. Edentiti provides a tool for an individual to prove assertions that they make about themselves. Instead of the organisation trying to check information about a person Edentiti allows the individual to check their assertions and report the result of the check to the requesting organisation. This is privacy friendly as the requesting organisation does not need to know the details that a person uses to verify themselves.

For example, to check if a person has a tax file record the person needs to use their tax file number. It is not permitted for an organisation to collect a tax file number and to use it for identification purposes. It is permitted - and in fact required - for an individual to use their tax file number when identifying themselves to the tax office.

Edentiti acts a service provider to the individual, enabling the individual to verify their assertion that they have a tax file record with the tax office. Edentiti does not keep the tax file number and it is only ever used and seen by the individual. Inside the Edentiti system the tax file number is discarded as soon as it has been used to confirm that a relationship exists between the person and the ATO.

This principle means that the privacy of an individual is protected as their personal data is not stored - only the result of an operation.

Edentiti helps individuals prove they are who they say they are by enabling them to demonstrate they have multiple electronic relationships and to control access to their own information.

External examination of these claims is fully supported and encouraged.

3.1.3 Individuals establishing relationships with other agencies

A number of government agencies have a person's private information accessible to that person on-line. The example provided in section 3.1.1.2 of a verification of a relationship via Edentiti illustrates a person being able to demonstrate a relationship with the tax office by inputting their tax file number on a public website. While this is a legitimate reason to use the public facility it would be better for the government agency to provide this service in a direct way. There are no privacy issues, in fact the reverse. The ability for an individual to ask any organisation for a yes no answer on whether they hold information about them is part of the Privacy Act 1988.

Once the relationship with a particular organisation has been established, the verification process as part of remote e-voting does not involve contacting that organization again. Of the three enrolment processes referred to in section 2.2.1, only in the case of a special enrolment process for e-voting (section 2.2.1.3) is there potential for a large number of people seeking to prove they had a relationship with a particular organisation. As this is done at the time of registration the impact on the organization is minimal and in terms of traffic is much less than search engine random harvesting of information.

3.2 Accuracy of voice authentication

Voice authentication has identification accuracy in terms of error rates equivalent to fingerprints. In addition to the voice print, Edentiti uses information contained in the telephone number, the source of the call, the IP address of the browser, and the voice print text. This is the equivalent of a three-factor authentication and gives a high degree of certainty that it is the registered person who is voting.

3.2.1 Coercion of the voter

Accurate voice authentication does not prevent coercion any more than postal voting prevents coercion, but the Edentiti system does offer other tools for people to protect themselves from coercion and misrepresentation.

3.3 Security

In the context of electronic voting, there are many potential risks to security, related to software security, hardware security and system security when the hardware and software are combined. The Edentiti-eVACS solution for e-voting addresses these risks in a number of ways.

Both eVACS and Edentiti have been designed and implemented with security in mind. This means that specific security features are in-built rather than add-ons provided to address security aspects identified by external parties.

3.3.1 Edentiti

Edentiti systems are hosted by the Bulletproof organisation operating out of Australia's largest hosting environment in Sydney. There are many Internet connections into the system.

A minimal number of ports are open on the servers. All access for registration or voting comes via the AEC website and these links are secure and encrypted. Denial of service attacks on the Bulletproof systems would not affect the links to the AEC systems so the only risk of a denial of service would be an attack on the AEC website.

The Edentiti system is the only software running on the servers. The hardware configuration consists of a three level clustered system with many computers serving the network, many computers serving the processing, and many computers servicing the database.

Data is replicated on the Bulletproof storage with hot recovery in the event of disk failure. Cold backups are available from remote storages.

As remote e-voting is done over a period of days some minutes of interruption – although unlikely – can be tolerated.

All Edentiti systems are audited and access is strictly controlled.

More information on the physical and technical security of the Edentiti system is available on request.

3.3.2 eVACS

Specifically for eVACS the security features are:

- limited functionality of the operating system; contains only those operating system functions absolutely necessary to support the restricted and menu driven eVACS functions
- installation on the hardware automatically reformats the disks
- no executable software downloaded to voter's PC
- encrypted votes stored on a physically secure server in two separate databases (raid1 format)
- only completed votes stored
- downloading of votes only possible after voting stops and with access control
- audit log of all activities

eVACS procedures operate against any attempt to introduce malicious code:

- eVACS is a closed system
- code is made available for independent audit and verification
- audited code is the actual and only code used for an election
- access controlled

3.4 Scalability

Both the eVACS and Edentiti software systems have no limitation on the number of users. Any limitation on the Edentiti-eVACS solution derives from a limitation in accessibility to the AEC website and/or the hardware used.

The Edentiti implementation uses modern information systems technologies, so that when extra capacity is needed extra virtual computers are added to the server farm. This can be accomplished instantly so that in periods of high demand the server farm allocates more resources from its large server farm to the Edentiti application.

The hardware put in place for eVACS use is mainly dependent on the maximum number of users seeking access at any one point in time via the AEC website. As part of the security aspects once the AEC website has been accessed, the voter is taken to a separate server for electronic voting. The requirements of this server would be determined in association with the AEC.

3.4.1 The last minute rush to vote

An important consideration in the scalability of the Edentiti-eVACS solution is to allow for last minute voters, in the way elector at a polling place are able to vote after the official closing time providing they are standing in the queue to be marked off the electoral roll at 6:00 pm. Similarly, anyone who has commenced a vote verification process at closing time should be able to complete his or her vote.

As already stated, the combination of the capability of increasing the number of computers for verification via Edentiti and the selection of the appropriate sized eVACS servers, ensures that the Edentiti-eVACS solution for remote e-voting is able to handle any 'last minute rush to vote'.

3.5 Reliability

Reliability is designed into software and processes. For hardware though, failure is managed through risk management practices, since there are no guarantees that a particular piece of, even brand new, hardware will not fail.

The core eVACS software demonstrated its reliability during the 2007 Federal Election trial of kiosk e-voting for the blind and vision impaired. eVACS already uses two separate databases to mitigate against failure and for remote e-voting a complete replica of the eVACS server is recommended.

If the voter's own hardware fails, then a browser-based voting system, such as eVACS, allows the voter to use alternative hardware.

Similarly, the Edentiti electronic verification process uses many alternative phone numbers and communication paths, as a risk management as well as operational strategy.

The actual Edentiti System is hosted by Bulletproof in Sydney using a virtual server farm to provide a reliable service 24/7 with rare scheduled downtime to update the system. Obviously an update during the election period would not be scheduled.

3.5.1 Denial of service

As referenced in section 1 the potential for a 'cyber attack' to engender denial of service must be taken seriously, post the Estonian experience in 2007.

There are potentially two avenues in which denial of service could be implemented:

i) access to the AEC website, and

ii) detection of the traffic passing from the AEC website to the private URL for Edentiti hosted with Bulletproof.

In relation to the latter, Bulletproof has sophisticated practices in place to monitor and deflect and attempt to engender a denial of service. These practices are well established and are regularly brought into play to maintain Bulletproof operations.

As to the AEC, a range of techniques for both deterrence and management are available for the AEC to implement, if they have not been implemented already as part of internal AEC website practices.

While a denial of service attack may be less significant in relation to enrolment or registration to vote electronically, the inability to vote process must be minimized.

4 Electronic enrolment

4.1 Background

As mentioned in section 2, the Edentiti identity verification system (the System) can be easily integrated into the existing AEC registration system as an extra verification technique to complement existing processes. It requires no change to existing systems except to accept electronic registration.

4.2 Outline of the System operation

The System mimics the current paper based forms and can be thought of as an optional alternative to the existing AEC processes for registration.

Current enrolment process	Edentiti electronic enrolment process
Person downloads enrolment application form from the AEC website	Person fills in electronic enrolment form on the AEC website
Person completes enrolment form, providing proof of identity • driver's licence • other documents to be sighted by authorised person • details of two people confirming identity	AEC provides details to Edentiti
Person completes declaration and signs • including declaration and signature of authorised person or persons known to the applicant	Applicant provides information to be used to verify existing relationships.
Completed application is submitted to AEC	Individual verifies relationship via Edentiti
AEC checks application	Edentiti advises AEC identity has been verified
AEC posts applicant of enrolment details	AEC advises applicant of enrolment details electronically

The process of completing an enrolment with identity verification using Edentiti can be completed within minutes where information can be provided to verify another electronic relationships. More time is taken if verification requires contacting two persons to confirm identity, but this can be completed within hours depending on the response time of the persons contacted. In comparison, completing the current manual process takes a matter of days or even weeks.

A more detailed description of the Edentiti process follows.

A person registers by filling out an electronic form on the AEC website. They verify their identity through Edentiti who keeps a record of their name, address and how their identity was verified. The person identifies themselves by asserting they have relationships with other organisations or people (see Diagram 2).

These relationships are proven by the assertions being checked with one or more third parties. This is achieved in different ways with the most common being to confirm that the person's details exist on another database. Another method is to ask other verified people to confirm an identity. Any private details used to confirm an identity are only seen by the person being identified. They are discarded immediately they are used and only the result of the assertion is retained. Edentiti or the AEC can engage external audits to verify this claim.

As part of the verification process, a person can optionally record and store one or more biometrics such as a voice print. The biometric is stored with Edentiti and used by the person to later confirm their identity. Importantly, the biometric acts to protect the individual from identity theft and enables them to prove that a transaction made in their name as a result of identity theft was made by someone else.

If a voice print is stored then the voice print can be used through a 'telephone' (land line, mobile or PC based) as a feature of electronic identification to enable authentication/signature for other on-line processes. The validity of Edentiti signatures has been examined by - Deacons and their report titled "Electronic Signatures" and is available on the Edentiti website.

Anyone may of course identify himself or herself to Edentiti at http://www.edentiti.com and establish their 'edentiti' at any time. Should a person already have an 'edentiti' then the existing established verification is drawn on for electronic enrolment with the AEC.

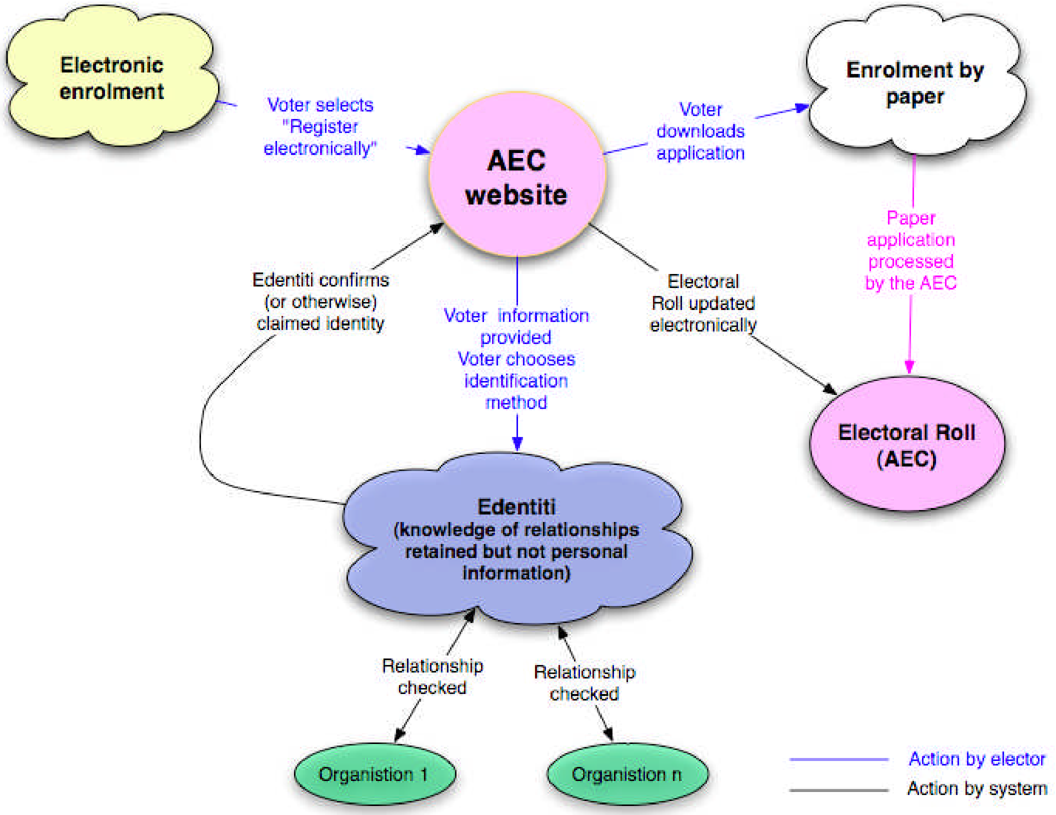
Electronic enrolment
Voter selects "Register electronically"
AEC website
Voter downloads application
Enrolment by paper
Paper application processed by the AEC
Edentiti confirms (or otherwise) claimed identity
Voter information provided Voter chooses identification method
Electoral Roll updated electronically
Electoral Roll (AEC)
Edentiti (knowledge of relationships retained but not personal information)
Relationship checked
Relationship checked
Organistion 1
Organistion n
Action by elector
Action by system

Diagram 2 – Enrolling to vote - electronic or paper application

5 Trials

Normally before embarking on a change in practices a trial is undertaken to assess the impact of implementing the change, and establishing the costs and benefits. The following two sections, 5.1 and 5.2, provide ideas for AEC consideration in first undertaking a trial of the electronic enrolment process (section 5.1) before implementing a trial of remote e-voting (section 5.2). These suggestions represent a low cost phased incremental strategy to introduce the system. The enrolment trial could be in operation within a month of a decision being made to proceed.

5.1 Electronic enrolment trial

A trial of electronic enrolment (EE) using the Edentiti verification system has the objective of proving the Edentiti system works in a relatively controlled environment where both the AEC and Edentiti have easy access to participants. Such an environment is attainable with a trial involving one or more Canberra Secondary Colleges.

The EE-trial itself would be designed and implemented with the assistance and active participation of the Secondary Colleges as they can integrate with other services that they may already provide such as helping students identify themselves for the purpose of obtaining a driver's (learner) licence or opening bank accounts.

The AEC would have a private URL link that would be issued to the trial schools. This could be on the Edentiti website or on the AEC website.

The student would be presented with a registration form to enter personal details:

Name, Address, Date of Birth,

The AEC allocates an elector number to this student but marks it as unverified. The AEC then 'sends' the student to Edentiti along with the elector number (which is never seen by the student).

For new electors Edentiti looks at the name and date of birth. If it appears that the person may be in the System, Edentiti asks them if they are already in the System and, if so, asks them to say their voice print. If it matches and the person has been verified elsewhere to the AEC requirements, then Edentiti 'returns' the student to the AEC with the information on how the person was verified. If the person does not have enough verification then they are asked to provide more before the request is returned to the AEC.

5.1.1 Student verification process

The first step is for the student to agree to a set of conditions. Then Edentiti prompts the student to:

- call a free number and record their voice print;
- select their school (from a list of approved ones) and an authorised person (from a list of approved people in the school);
- enter the email address or mobile phone number, name and address of an adult who knows them; and

- supply a mobile phone number and/or an email address for future contact.

The latter provides a means of Edentiti contacting the student after the verification process has been completed.

5.1.1.1 Checking with the nominated people

The nominated two people, school person and known adult, both receive an email or an sms asking them to logon to Edentiti to verify the identity of a student of a given name.

The school person would have previously been registered through Edentiti and been through an identification induction course, and so would be able to logon with their email and their voiceprint. Once logged on they would see a list of students with date of birth and address who had requested verification. They would check with the school records the date of birth and the address and click a box to verify then submit.

The known adult would go through a normal identification process on the Edentiti website including recording their voiceprint to prove who they are; they would assert they were on the electoral roll and that would be checked, and they would supply two other forms of identification to establish known relationships. Once verified, the System would prompt them to verify the identity of the student.

With the student verification complete, the AEC would be advised the student is a verified person and depending on their age eligible to vote.

5.2 Remote e-voting trial

Having demonstrated the viability of the Edentiti verification process for electronic enrolment with the EE-trial, a trial implementation of the Edentiti- eVACS remote e-voting solution is the next step. In this case, a small (in comparison to a Federal election) fee for service election, possibly an industrial election or student election, could provide a controlled environment, in similar concept to that for the EE-trial, for a trial of remote e-voting following the process outlined in section 2.

6 Other potential benefits

6.1 Change of Address

Any person wishing to change their address would click on an AEC website link saying "change of address". If they have previously been identified through Edentiti then they would be asked to verify who they were through their voice print. If they were not identified through Edentiti they would be asked to identify themselves and would go through the same identification process as new AEC enrolment registration.

As mentioned previously the AEC can form relationships with other organisations, both public and private to assist each other and users when users change addresses. We envisage a time when a person changes their address and contact details with one organisation and are prompted to ask if they would like to change their details elsewhere. This would improve the currency of the AEC data and would increase the number of registrations.

6.2 EE-trial benefits

The EE-trial with Canberra Secondary Colleges would prove useful in the wider introduction of the Edentiti System with other organisations such as the post office, telcos and moving companies who record change of addresses for people. Other cases where there is a change of information about a person are when they rent properties or get married. With the active cooperation of these other organisations the AEC records can be automatically checked to see if they need updating and if so the person can be prompted to change their AEC record as well.

The same principle could apply for updating other government agencies details when an AEC address or contact details change.

6.3 2020 summit recommendation

One of the 'top ideas' from the Australian Governance section of the 2020 Summit (see Initial Report at http://www.australia2020.gov.au/report/index.cfm) is "Universal automatic enrolment and re-enrolment of eligible voters".

A longer term by-product of the Edentiti system, if it were introduced in most Australian schools, is that most young people in Australia who were eligible to vote would be prompted to register for AEC enrolment. This process could be extended to other government agencies where a person could be checked for enrolment and if not enrolled to vote they could be asked if they wished to enroll. This would satisfy the 2020 summit recommendation on a more automated process for young people to enroll to vote yet done in a privacy friendly way.

6.4 Visually impaired, other languages, other disabled access

At the time of enrolment or registration to vote, a person can specify special requirements within Edentiti. Although this will not be available in the trial, it is a relatively simple extension to the system and will mean that each special requirement that is enabled is available to all electors no matter where they are located.

6.5 Death notification

Registered executors of estates will be able to access a deceased person's edentiti and be able to notify the AEC to remove the person from the roll.

7 Pricing and savings

The underlying pricing principle is to charge a unit cost per transaction, be it identity verification for initial enrolment, registration to vote electronically or identity verification for voting. Basing costs on transaction costs - particularly if the AEC replaces many high cost transactions with lower cost transactions - makes it simpler and easier for the AEC to budget trials and large-scale deployment. On going development and maintenance of the system is covered through the transaction costs; hence there are no annual maintenance fees.

The transaction costs for enrolling and for change of addresses and other details of enrollment can be given as these systems are in operation for other clients with less than 200,000 verification of registrations. The long-term price to the AEC for enrollment will be $1 per enrolment or change of details. For the trials with smaller numbers the cost will be $5.

The transaction costs for the voting system cannot be given until the specifications and methods are agreed. Costs that will need to covered include:

- cost of providing voice verification (or other biometric identification);
- cost of providing hardware and services for eVACS systems or cost of using other service providers. These costs could be relatively high as there are peak load considerations; and

- cost of providing online Help Services as either backup to the AEC or as a completely outsourced solution.

There are additional costs to be taken into account:

- Audit/Certification of the software,
- Secure Socket Layer certificate/s,
- Special services for voter access (see 6.4 above).

7.1 Estimated savings

In the absence of detailed current costs it is not possible to provide a comprehensive calculation of the cost savings that might be achieved. However an estimate of the magnitude of the likely savings is possible.

Figures available from the AEC website show that the average cost of the 2004 election was about $9 per vote. The cost of ‘paper’ remote votes is likely to be greater than this average, say, in the order of $10 per vote. ‘Electronic’ remote voting for the foreseeable future will only be an option and so the infrastructure for ‘paper’ remote voting will still have to be in place. In other words, if the transaction cost of a remote vote was say $5 then savings would not be $10 minus $5 because the average cost of remote paper votes would increase. However, it can be anticipated that the savings are likely to be of the order of half the difference between the average cost of a remote paper vote and the transaction cost of an electronic vote.

The main benefit from the proposed Edentiti-eVACS remote e-voting system is to provide a better service, decrease the number of people who vote informally, improve accessibility to voting for those with special needs, and to reduce the cost and time to voters to both enroll and to vote. Remote e-voting will help future proof the AEC against increases in costs and help keep the cost per vote in future elections relatively stable.

The AEC provides voting systems for other organisations. The AEC will be able to compete efficiently in the market place for other clients using the Edentiti-eVACS system as they will not be restricted by legislation and by the fact that voting is compulsory. That is, they can conduct elections that can be 100% electronic and remote and this will reduce the operational costs.

8 Final comments

Using an electronic identification process is a choice for the individual and so too with electronic voting.

The Edentiti-eVACS solutions forming the basis of this proposal are considered complementary to other enrolment registration and voting options provided by the AEC, thereby maintaining choice for the individual.

At the end of the day, it is the would-be elector then voter who makes the choice.

The Edentiti-eVACS solution is based on proven technology. The AEC is already familiar with the core eVACS system and Edentiti is providing identification services to satisfy the new Australian AML/CTF "know your customer" legislation.

The level of confidence in the identification of the voter is unmatched when using the voice print and relationship-based Edentiti process. Hence, with the Edentiti-eVACS integrated systems the AEC would have available a remote electronic voting service which addresses the identified major disadvantages.