WOTE 2006 Contribution

Standards for e-Voting:

The Results of the Work of the OASIS Election & Voter Services Technical Committee

Prepared by: John Borras and David Webber
Committee Members
Date: 14 June 2006

Abstract

Voting is one of the most critical features in our democratic process. In addition to providing for the orderly transfer of power, it also cements the citizen's trust and confidence in an organization or government when it operates efficiently. Society is becoming more and more web / collaboration oriented and citizens, used to the high degree of flexibility in the services provided by the private sector and in the Internet in particular, are now beginning to set demanding standards for the delivery of services by governments using modern electronic delivery methods.

The implementation of electronic voting would allow increased access to the voting process for millions of potential voters. Higher levels of voter participation will lend greater legitimacy to the electoral process and should help to reverse the trend towards voter apathy that is fast becoming a feature of many democracies. It is also recognised that more traditional voting methods will exist for some time to come, so a means is needed to make these more efficient and integrate them with the newer electronic methods.

In the election industry today, there are a number of different services vendors around the world, all integrating different levels of automation, operating on different platforms and employing different architectures. With the global focus on e-voting systems and initiatives, the need for a consistent, open, auditable, automated election system has never been greater.

This paper focuses on reviewing the aspects of the OASIS EML standard and shows how it can provide the facilitation for trusted electronic voting systems. Included is an assessment of the minimum functional mechanisms that ensure audit trail and crosschecking that allow verification of voting to be implemented.

Introduction

One aspect that has been cited as an enabling feature of trusted electronic voting systems is the use of open public standards in the operation and process models that can be used across voting systems implementations. The vision is to create a transparent and certifiable solution between implementation components that can be independently verified and audited regardless of who the developer is.

Whilst known technology mechanisms and processes clearly add to the confidence surrounding the operation of an e-Voting system there are clearly many more aspects that when put together can represent a trusted and rigorously verifiable system.

The Council of Europe (CoE) Ministers commissioned a two year study of adopted legal, operational and technical best practices that essentially encompass a voter bill of rights for e-enabled elections.

The OASIS Election Markup Language technical work (EML) pre-dates the Council of Ministers work, originating from the USA and UK, and has subsequently been developed to both encompass and respect the CoE's findings on voter rights and also to provide open public transparent voting methods through the use of XML-based markup techniques. EML v4.0 has been adopted as a formal OASIS member standard in February 2006 and had previously been endorsed by the COE for use in elections.

This paper focuses on reviewing the aspects of the OASIS EML standard and shows how it can provide the facilitation for trusted electronic voting systems. Included in this is an assessment of the minimum functional mechanisms that ensure audit trail and crosschecking that allow verification of voting to be implemented. This baseline benchmark therefore can be used to compare to existing implementations to identify shortfalls and gaps that can expose critical operational factors that can compromise the results in an e-Voting system. Interestingly a combined paper and e-Voting system may also offer more security than paper or pure digital voting systems alone. A key factor in this is enabling voter verified ballots that consist of a dual-step process that allows the voter to independently confirm that their vote is being recorded accurately.

The OASIS Election & Voter Services Technical Committee

OASIS provides for its members to constitute and operate technical committees to develop technical specifications and standards in an open, transparent way. The procedures for doing this and the rules for running a technical committee are available at their website www.oasis-open.org. Membership is open public and includes technology experts and industry vendors.

The OASIS E&VS Technical Committee was formed in March 2001 and since August 2001 has been chaired by a representative of the UK Government. The Committee Membership includes Governments, Corporations, Election Services providers, and Academia from North America and Europe. As with all OASIS work contributions to the standard has included funded and unfunded.

The Charter of the Committee is:

> "to develop a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations."

The Committee has recognised the need for information to be exchanged at several points in the election process because several parties and system suppliers could be involved. There is a

need to service dissimilar systems and equipment, and voting has to be an open, transparent process. To this end it has developed the Election Markup Language (EML) which is now a full OASIS Standard.

What is e-Voting?

For the purposes of their work, the Committee has adopted a very wide definition of e-Voting. It is taken to encompass either an election or a referendum that involves the use of electronic means in all or part of the processes. The process begins with voter and candidate registration, through the casting of votes and ending with the counting and declaration of results.
It also includes various scenarios ranging from voting supervised by election officials in a controlled environment to remote voting where the casting of the vote is done by a device, such as a computer input device or voice activated telephone, that are not necessarily in a prescribed and controlled election location.

What is EML?

EML has been developed as a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organisations. The objective has been to introduce a uniform and reliable way to allow systems involved in the election process to interoperate. The overall effort attempts to address the challenges of developing a standard that is:

- **Multinational**: Our aim is to have these standards adopted globally.
- **Flexible**: Effective across the different voting regimes (e.g. proportional representation or 'first past the post') and voting channels (e.g. Internet, SMS, postal or traditional paper ballot).
- **Multilingual**: Flexible enough to accommodate the various languages and dialects and vocabularies.
- **Multimedia**: able to support disabled and non-visual voting access methods
- **Adaptable**: Resilient enough to support elections in both the private and public sectors.
- **Secure**: Able to secure the relevant data and interfaces from any attempt at corruption, as appropriate to the different requirements of varying election rules.

EML currently includes process specifications, data definitions and XML Schemas for:

Pre-election processes:

- Candidate Nomination, Response to Nomination and Approved Candidate Lists
- Referendum options formulation
- Voter Registration information, including eligible voter lists
- Various communications between voters and election officials, such as polling information, election notices, etc.

Election Processes:

- Ballot information (contests, candidates, etc.)
- Voter Authentication
- Vote Casting and Vote Confirmation

Post Election Processes:

- Election counts and results
- Audit information pertinent to some of the other defined data and interfaces

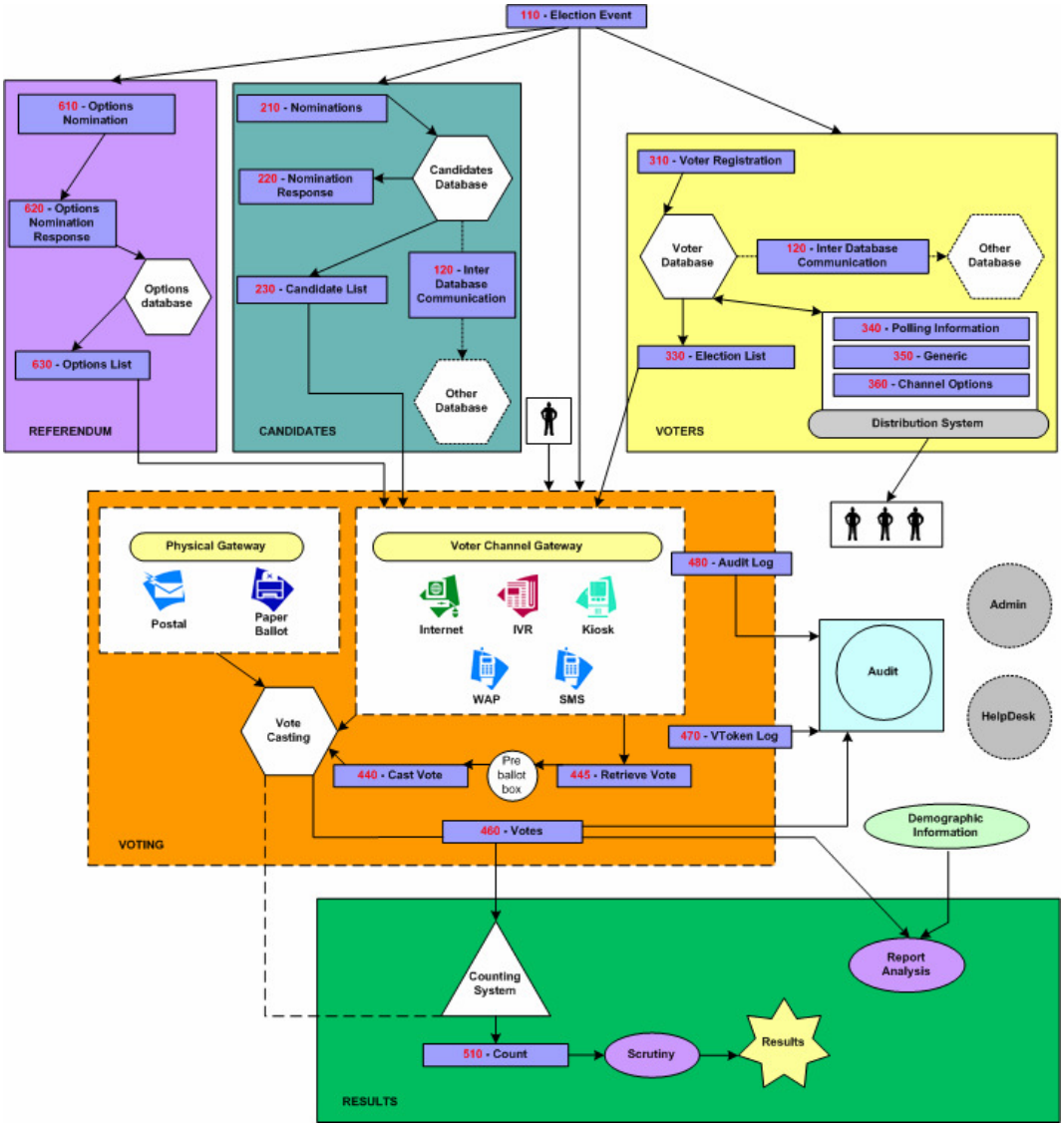
How to use EML

As an international specification, EML has had to meet a very wide range of voting requirements and is thus generic in nature. Therefore it needs to be tailored for specific scenarios and to meet specific business rules and practices. Some aspects are indicated in EML as required for all scenarios and so can be used unchanged. Some aspects (such as the ability to identify a voter easily from their vote) are required in some scenarios but prohibited in others, so EML defines them as optional. Where they are prohibited, their use must be changed from an optional to prohibited classification, and where they are mandatory, their use must be changed from an optional to required classification. Similarly many parts of EML are extensible using the standard facilities of XML. It is not intended that all parts of EML have to be used. Indeed the majority of the current e-voting activities and pilots are only focussing on specific aspects, e.g. voter registration, vote counting. To-date we have not certified a complete end to end implementation as such complete comprehensive uses of e-voting is still an emerging story.

Table 1 – EML V4.0 transactions by schema

Schema Name	Purpose
EML 110 – election event	Information about an election or set of elections. It is usually used to communicate information from the election organizers
EML 210 – candidate nomination	Used to nominate candidates or parties, consenting or withdrawing
EML 230 – candidate list	Contest and candidates details
EML 310 – voter registration	Used to register voters for an election
EML 330 – voter election list	Details of actual voters for an election
EML 340 – polling information	Notification to voter of an election, their eligibility and how to vote
EML 410 – ballot	Describes the actual ballot to be used for an election
EML 420 – voter authentication	Used for voter authentication during a voting process
EML 440 – cast vote	Actual record of vote cast
EML 460 – votes group	Group of votes being transferred for counting
EML 480 – audit log	Documents access to voting records and reason
EML 510 – count	Results of election contest(s) and counts
EML 520 – result	Communicating specific result details on candidates and elections

The schemas themselves then relate to the actual voting processes. The following diagram illustrates these processes and the data flows between them. The numbers in red are the XML schema numbers in EML.



Terminology

Terms used to describe the voting processes, such as ballot and candidate, carry different meanings in different countries and even within jurisdictions by those speaking the same national language. Within EML the basic concepts are defined as follows:

Ballot - A set of candidates or referendum options for a particular contest, within one or more elections for which votes are cast.

Candidate - An individual or party standing in a contest.

Cast Vote - A ballot containing the preferences of the voter.

Contest - A contest is that part of an election in which an individual can vote.

Election - An election comprises one or more related contests over a defined period of time.

Voter - A person who is eligible to vote.

Development of EML

The committee recognised very early on because of the great variety of voting rules and practices around the world, it could only develop an international standard if it based it on an agreed set of voting processes. It also had to address the confusion caused by different vocabularies as mentioned above. Resolving these very difficult problems and getting to a common base has

meant that it has taken over 5 years to develop the current version of EML, Version 4, using the open, public technical committee processes provided by OASIS (http://www.oasis-open.org). It started initially with input from just the UK and USA and the early versions reflected only the voting practices in those two countries. Other countries gradually joined in eg New Zealand and Australia, and their requirements were included.
The next major input came from the 43 member states of the Council of Europe, and the use of EML has been incorporated in its Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, which was adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies.
Along the way lessons learnt have been fed in from e-voting pilots carried out in a number of countries, e.g. UK.
The Committee is currently working on version 5 which will include further enhancements and meet some new requirements. When this work is completed later this year it is the Committee's intention to submit EML to become an ISO Standard.
EML will continue to evolve and mature as more experience of e-voting techniques is gained and current concerns, e.g. security of remote voting, are addressed.

Benefits of EML

For EML to be successful there has to be a win-win situation for both suppliers and end-users. The following are the practical benefits of adopting EML expected by all members of the Technical Committee. These are in addition to supporting trustworthy elections mentioned below.

For Election Officials:

- More choice of products and suppliers
- Less dependency on a single supplier
- Avoid proprietary lock-in
- Stability or reduction in costs
- Consistency in adoption of business rules

For Suppliers:

- Greater chance of doing business
- Standardised customer requirements
- Reduced development costs
- Accommodate future changes more easily
- Common core but allows local customisation / extension

Security

Security is a major concern within e-voting and whilst EML doesn't pretend to solve all the known problems, many of which are fundamental Internet security issues rather than specifically e-voting ones, it has addressed the following aspects and provided solutions for:

- Identity authentication
- Right to vote authentication
- Vote sealing and non-repudiation of vote accuracy
- Vote confidentiality
- Voting Audit

Trustworthy Elections

The identification of the need to improve election practices and procedures is something that has been evolving over a long period of time. The need for improved vote security and extended access is just as real in a traditional election scenario as it will be in future e-voting opportunities. There have been several notable elections where doubt lingers as to the verifiability of the results or the practices performed. The aim of all, that are interested, should be that the confidence in any election result should be unchallengeable and beyond doubt. Dependent and Trustworthy Elections form the foundation of democracy that is not open to compromise or manipulation.

Whilst the perception of election risk seems to be mainly concentrated on the introduction of new methods of voting, all the risks are just as likely to happen in any type of voting system whether it is the old and trusted system, or the most modern.
It is important to look at all stages of an election, from registration to the declaration of the result, and to develop practices and procedures to both demonstrate and guarantee fairness and dependable elections.
It is easy to assume that it is only since the introduction of 'automation' at any level, that verifiability and validation has become essential but obviously that is not the case. It is important to ensure that all types of voting systems, manual and automatic, have demonstrable security standards that can be validated and verified at every level.

Trustworthy elections require an entire trustworthy electoral system

Much of the academic research in election security has concentrated on the security of the vote and very little concerning the overall process. Whilst most of the publicity around the 2000 US Presidential Elections was centred on 'chads', it is recognised that problems centred around voter registration were also a huge contributor to the number of complaints and dissatisfaction with the result.
Whilst concerns have been concentrating on safeguarding the vote, it is essential that we all take seriously the importance of registration. As we saw in the US elections with no registration there is no vote. At the same if a person manages to get included on a register more than once, or on more than one register, it becomes that much simpler to vote for each entry with little risk of challenge.
It is considered that there are reasonably easy methods to avoid over registration, using personal identifiers etc, provided it is possible to check across all available registers – not so easy unless there is a national register available. However it is much more difficult to ensure that everyone who is entitled to vote is actually registered to do so.

Where is the risk?

To provide a Trustworthy Election we need to identify what are the risks and then look at the way in which those risks can be mitigated. At the same time we need to be aware that for voting to be accessible and convenient we are restricted to what risk mitigation we can extend to.
It would be so easy to make voting methods so safe that it would be difficult to use them so there is a need to achieve a sensible balance.
Currently there is a real sense of a need to seek ways to improve the security of the absent vote. Most of us will have heard many of the horror stories of vote harvesting; voter coercion; fraudulent use and no doubt many others. When looking at the problems and trying to find the solutions, we need to be consciously aware of the real benefits that the ability to vote by post, internet or telephone etc has given to so many people.
Do the risks outweigh the advantages or do the advantages excuse the risks? How do we safely reach a balance?
The challenge facing us all is widening the opportunity to vote whilst at the same time narrowing the opportunity of misuse. This challenge extends across all voting channels and requires an approach that can be universally accepted.
It is easy to assume that the traditional methods of voting, with a stubby pencil, present less of a risk of possible misuse than some of the newer accessible channels being promoted. This, of course, is not the case, though the risks may differ they are just as pertinent and valid.
Fears over e-enablement provision are varied, with some concentrating on risks of hardware failure and loss of service, to the risk of software being manipulated for political advantage. Risks of hardware failure, whilst real, are no more a problem that those associated with present arrangements ie polling place becoming unavailable at short notice, or a lost or destroyed ballot box.
Risks of software, or hardware, manipulation can be minimised by accreditation and the introduction of acceptable standards. In addition by the acceptance of interoperability of data and systems independent authentication is possible.

Responsibility of providing trustworthy elections

The responsibility of providing trustworthy elections must be shared by all involved including Election Managers, Governments and Suppliers; democracy relies on it. Developments like EML make that provision possible whether it is for a traditional or e-enabled election.

In accepting that responsibility everyone involved in election provision must work towards the development of systems and procedures that dispel the fears that currently exist and lead towards understanding and acceptance. If we can create globally acceptable standards we will genuinely provide Trustworthy Elections for all. For this reason the systems we need to develop must be explainable, affordable, usable and sustainable.

Paper and Electronic Voting Comparisons

While the debate continues as to the various benefits of traditional voting processes compared to newer ones involving electronic voting methods, the following table provides some aspects and analysis between them. Ultimately the optimal solution is one that combines the strengths of both, and we consider such a trusted voting methodology in the next section.

Table 1 - Comparing sole-use solutions of paper and e-voting

Paper Only		**e-Voting Only**	
Strengths	**Weaknesses**	**Strengths**	**Weaknesses**
Direct voter ballot verification. Persistent nature of content. Familiar and traditional trust. Strong audit trail. Physical access can be controlled. Anonymous mechanism. Mature open marketplace of vendors. Established operational practices. Resistant to technology attacks. Distributed process. No mechanical failures.	Ballot-box security. Clumsier counting. Voter intimidation. Ballot-box stuffing. Voter access. Disenfranchised voters. Large local variances. Speed of results. Slow to setup. Distances of citizens from polling stations.	Accuracy of counting. Speed of counting. Multi-lingual support. Enforced procedures. Disadvantaged access. Encryption safeguards. Centralized distribution of ballot details. Operation can be certified.	Mechanical failure. Sabotage. Voters cannot directly verify actions. Ephemeral nature of content / audit / storage. Trust and “Big Brother”. Electronic break-ins. ‘Castle’ lure for attacker. Remote access.
Opportunities	**Threats**	**Opportunities**	**Threats**
Provide foundation for trusted voting processes internationally.	New technology exposes new weaknesses. Abuse by officials.	Standards create open marketplace. Open elections with citizen involvement. Less voter intimidation.	Vendors align to political parties. Vote selling. Anonymity compromised. Manipulation by officials.

Using EML with trusted voting mechanisms

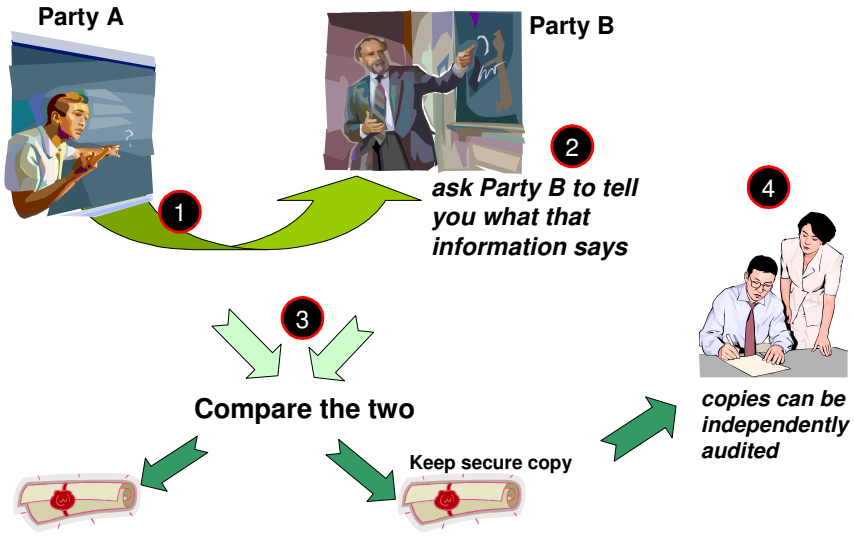
Recently work has been undertaken to examine mechanisms that can provide both voter verified ballots and 100% audit cross tabulation between multiple data sources in a trusted election process. EML can provide a pivotal role by providing an exactly matching vote recording mechanism that can then be crosschecked between the various data sources. Unlike proprietary vendor voting system records the function and purpose of each discreet part of EML voting records is defined and the purpose known. Interoperability testing further validates that functionality existent in the EML XML voting records exactly match the standard requirements and nothing else.

The challenge can be simply put as: how does the voter know and can independently verify that the computer has recorded their vote accurately and actually made it available to be counted?

This trusted voting method can be envisioned in two ways; first from the perspective of voter, and then from the audit recording and EML-based result counting software. In the envisioned trusted voting process two or more independent sources are always created for voting records that can then be crosschecked and verified.

Figure 1 below shows the voter perspective of establishing trust conceptually. The principles used here were first articulated by MIT as a two part trusted method - where one computer device is used to independently verify the operation of the original balloting device.

Figure 1 – Conceptual Trusted Logic

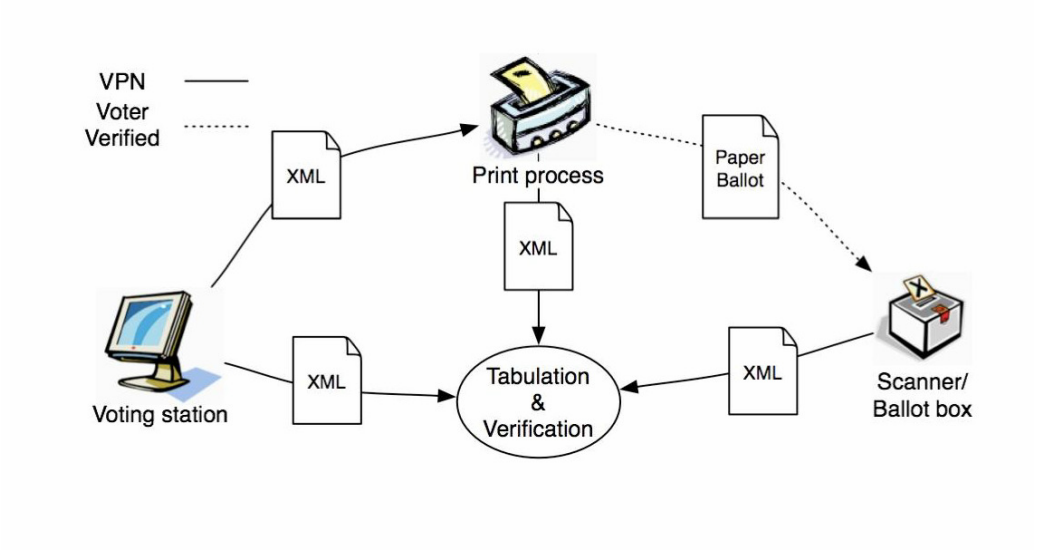


Then figure 2 shows the process from the computer perspective and the recording of XML records of the events and ballot vote transactions so that independently generated and then secured XML records can be used to crosscheck and audit the whole process automatically. This method and approach is designed to mitigate common attacks and threats to voting systems.

An example would be ensuring 3 separate vote records derived from the use of an e-Voting device storing an EML XML vote record; a printing device that then formats a paper ballot from

the EML XML vote record and a voter verified paper ballot is produced (typically including scanned barcodes). In such an approach EML XML records are produced independently by the printing and scanning devices themselves. All such voting records should exactly correlate and of course can be producing during the voting process by different manufacturers' devices, not just a single source solution. Figure 2 illustrates this overall approach.

Figure 2 – Practical Use Model for Voter Verified Paper Ballot example



Referring to figure 2 the VPN (Virtual Private Network) is the use of secure networking between the devices in the polling location that allows each independent device to participate in the voting process. Having the printing and scanning devices physically separated from the voting station and limiting the network services to only allowing the exchange of XML in EML formats removes the opportunity for the voting station to directly manipulate or control the external devices (compared to them being connected to peripheral ports on the voting station itself). The exchange of the XML records also provides the means to monitor and certify what content is actually transferred.

Overall the EML standards provide the tools and the means in XML to facilitate the underlying mechanisms in Figure 2. For example by combining the voter record content XML with the paper ballot layout content XML the print process can create the paper ballot that is then verified by the voter as matching their choices made at the voting station.

Most importantly these methods can be independently tested and demonstrated to be accurate by using a test suite of XML samples. Again also, vendors can independently supply components – such as an EML compatible printer.

Whereas today's voting systems use highly propriety and non-verifiable recording formats clearly higher levels of trust can be derived from using systems that conform to open public standards that allow the operational use of the recording formats used to be independently verified, stored and audited.

Also important is the ability to automate content checks of such vote records when using EML XML. Vote counting operations can be compromised if cast ballot records contain content other than just a simple record of the vote selections made. Clearly additional cues and hints could be concealed in proprietary vendor voting records that could direct counting software. Whereas with the public open standards the content can be prescribed and then software written to independently check that content conforms to those rules.

Also counting software itself can be built that independently computes the results and that too can be then verified using a suite of independently prepared test records.

EML in Practice

Notwithstanding vendor proprietary implementations the use of open standards based e-voting is still in its infancy as customer attention to the needs is minimal and consequently there are only a few case studies that can be referenced to show how EML supports the e-voting process. Nevertheless EML itself has been developed over the years from early pilots and so does represent a core of lessons learned and fielded experience. The following are good examples of where EML is being used in live situations today:

UK's e-Voting Pilots

The UK Government has embarked on an election modernisation programme and as part of this has over the last few years conducted a number of e-voting pilots. These pilots have included the full range of remote e-voting channels in addition to traditional and postal voting methods. In support of these pilots a UK Localisation of EML was produced and has been used in some of the pilots.

UK's CORE project

Another aspect of the UK's election modernisation programme has been to e-enable the voter registration procedures. The Coordinated Online Register of Electors (CORE) project has produced a localised version of the EML voter registration XML schemas for use in future voter registration exercises and mandated their use on suppliers.

Belgium Local Elections

A localised version of EML is currently being developed to support the Flemish local elections in the autumn of 2006.

USA election proof of concepts

Several US ballot examples are currently being developed in open source implementations using EML v4.0 XML ballot results tabulation including scanned paper balloting and electronic form voting.

Further Adoption

The Technical Committee will continue to look for and support opportunities to implement EML building on the lead being taken by national governments, e.g. UK, Belgium, and the CoE Recommendation. Its plan to make EML an ISO standard will help raise the profile and should encourage more suppliers and end-users to adopt it.

Summary

The OASIS EML standard consists of tried and proven XML formats for storing both information pertaining to the operation of elections and also the election vote cast details, counts and election results. As such EML provides a comprehensive set of tools for implementing digital electronic voting.

The content of the EML records has also been designed to operate in a wide variety of election methods and ballot systems. This is particularly developed to incorporate the requirements adopted by the Council of Europe Ministers' report on electronically administered elections.

In addition EML can be incorporated into wider methods that seek to provide trusted voting systems. Such systems may combine both paper and e-Voting devices together to provide voter verifiable processes. The EML XML provides an excellent foundation for implementing auditable records from multiple sources within such a trusted operational model. Furthermore because EML provides a "lingua franca" between election systems and devices it can allow implementers to choose from a wider set of providers' equipment to build with.

Contacts and Additional Information

EML is a product of the OASIS Election & Voter Services Technical Committee. The processes, data and XML schemas defined by the Committee are detailed in a number of documents. These include:

- EML Process and Data Requirements
- EML Data Dictionary
- EML XML Schema Descriptions

These and other documents can be obtained through the OASIS website at www.oasis-open.org.

For more information on how to participate in EML activities, please contact the E&VS Technical Committee through http://www.oasis-open.org/committees/election