**An OASIS White Paper**

# The Case for using Election Markup Language (EML)

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. The consortium produces open standards for Web services, security, e-business, and standardization efforts in the public sector and for application-specific markets. OASIS was founded in 1993. More information can be found on the OASIS website at http://www.oasis-open.org.

The Election & Voter Services Technical Committee's objective 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.

# Table of Contents


Overview ..... 4
Introduction ..... 5
Advantages of using EML ..... 5
Trustworthy Elections ..... 7
Accrediting Electoral Services ..... 9
How to use EML ..... 11
Localisation ..... 11
Getting Started ..... 11
Summary ..... 12
Contacts and Additional Information ..... 12
Appendix A – Resume and History of EML ..... 13
What is e-Voting? ..... 13
What is EML? ..... 13
Security ..... 14
Development Timetable ..... 14
Appendix B – Comparisons ..... 15
Paper and Electronic Voting Comparisons ..... 15
EML and Proprietary Systems Comparisons ..... 16
Appendix C – Case Studies ..... 17
Appendix D – References ..... 21

# Overview

This paper sets out the case for using EML in e-enabled elections and shows the advantages and value that using EML can make to running some or all parts of such elections. It has been primarily written for an audience of election officials, candidates and other decision makers in the voting process. However it will also be of interest to voters to help their understanding of the evolving e-voting environment, and also suppliers of e-voting systems and services who may be required to implement EML in their offerings.

With the advent of e-enabled elections it was recognised that at various points in the end-to-end voting process there would be a need to exchange data in a structured way between hardware, software, and service providers and no standard existed for that purpose. EML was developed to fill that gap, the objective being to introduce a uniform and reliable way to allow systems supporting the election process to interoperate. The standard has been designed to be used in both public and private elections and can be used for all or any part of the e-enabled election process, such as voter registration, casting of the vote, e-counting and communication of the result. EML has been used in public elections in several countries since 2003.

The paramount objective of all involved in running elections is to ensure they are seen to be trustworthy. EML goes a long way towards supporting this objective by providing common interfaces at different points in the voting process that can be tested and audited to ensure accuracy, consistency and verifiability. It allows for a "mix and match" of equipment from different equipment suppliers, thus avoiding concerns often raised by the use of a single supplier and their proprietary software.

In addition to elections being seen to be trustworthy, it is essential to build confidence in the use of all electronic equipment. This can be done through accreditation of the equipment. The rigour of any accreditation is significantly improved if the testing is done against the use of interfaces based on open standards, and EML can and is being used to support local, regional and national accreditation schemes.

It is extremely unlikely that in the future elections will not have some e-enabled component(s). It's probably more a question of how many components and when they are introduced. But there are still many concerns to be allayed and a good deal of confidence that needs to be built before e-voting becomes the norm. However EML is the base on which to build future e-enabled elections that will be trustworthy, open and creditable.

# Introduction

Voting is one of the most critical features in the democratic process. In addition to providing for the orderly transfer of power, it also cements the citizen's trust and confidence in an organisation or government when it operates efficiently. Society is becoming more and more web 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 allows 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 recognized 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.

One aspect that has been cited as an enabling feature of trusted voting systems is the use of open public standards in the operation and process models that can be used across voting systems implementations. In the election industry today, there are a number of different service vendors around the world, all integrating different levels of automation, operating on different platforms and employing different architectures. With the increasing global focus on e-voting systems and initiatives, there is a need to remove the inherent concerns associated with proprietary systems by instead using open systems that are consistent, auditable and automated. The vision is to create a transparent and certifiable solution between implementation components that can be independently verified and audited regardless of the e-voting solution developer.

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.

This paper focuses on reviewing the aspects of the OASIS EML standard [ref 1] and shows how it is being used to make all parts of the end to end processes of voting, including electoral registrations and counting, work better and providing the facilitation for trusted electronic voting systems. Appendix A provides a resume and history of EML.

## Advantages of using EML

The question usually asked about why any particular standard should be used is "What advantages will it bring me?" In addition to supporting trusted election systems, the benefits of adopting EML are as follows:

**For Election Officials:**

More choice of products and suppliers

Less dependency on a single supplier

Avoids proprietary lock-in

Stability or reduction in costs

Consistency in adoption of business rules

Supports scalability, transparency and interoperability

Provides basis for accreditation – see later section

**For Voters:**

Supports trustworthiness of systems – see next section

Supports security of the vote

Provides confidence in e-voting systems

**For Suppliers:**

Greater chance of doing business

Standardised customer requirements

Reduced development costs

Accommodates future changes more easily

Common core but allows local customisation / extension

# 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 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, there are comparable risks 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 any 'automation' that verifiability and validation have 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', problems related to 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 the importance of registration is taken seriously.. As was seen in the US elections with no registration there is no vote. At the same time 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. This is easiest if there is either a national register or a common way to communicate between local registers, perhaps using a central copy of these registers. This, in turn, requires common standards for the transfer of registration data such as that provided by EML. 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 the risks are 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 and very expensive 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, and fraudulent vote use. When looking at the problems and trying to find the solutions, there is a need to be consciously aware of

the real benefits to citizens that the ability to vote by post, internet or telephone methods etc in addition to traditional polling stations 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 pencil and paper, 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 than those associated with present arrangements eg the polling place becoming unavailable at short notice due to weather or building problems, or a lost or destroyed ballot box.

Risks of software, or hardware, manipulation can be minimised by proper independent accreditation procedures and the introduction of acceptable open public standards. In addition by the acceptance of interoperability of the data and systems then 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 an e-enabled election. See Appendix B for a more detailed analysis of this point.

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.

# Accrediting Electoral Services

To meet the challenges of trustworthy elections conducted with the aid of electronic voting components and systems, fundamentally the electronic systems not only need to be trusted, but also need to be seen as trustworthy by the voting population. There is always the need for public verifiability of the whole voting process and this is particularly true when electronic voting components/systems are used to assist public voting within a democracy.

The electronic voting components whether they are stand alone paper e-counting systems, "Direct Recording Electronic" voting machines or fully integrated e-voting systems, require trust to be placed in those components and systems. This trust will not happen unless there is a measured way to assess, certify and accredit the electronic components used in the election process.

The establishment of an Accreditation, Assessment and Certification framework for electoral systems and services – sometimes referred to as an Electoral Assurance Framework - provides a mechanism to achieve this. It provides an independent way of ensuring that systems meet the electronic electoral service requirements and reduces the risk of deploying inappropriate systems, selecting unsuitable service providers and perhaps more critically, acting upon invalid results.

**Establishing a Electoral Assurance Framework:**

- Provides an essential foundation for the deployment of electronic systems/services within public elections.
- Provides enhanced confidence in electronic electoral systems/services.
- Saves money. Without an Assurance Framework, electoral systems/services would need to be assessed on an individual basis for each election. The aggregate cost of assurance across all the systems for all elections would be very high. If, however, an Electoral Assurance Framework is established, whereby election systems can be certified as having been assessed, then significant savings can be made. Whilst the initial cost of the certified systems may be higher, the savings made by no longer needing to repeatedly assess the systems in detail for individual elections would more than offset the higher cost of certified systems.
- Eases the procurement burden on governments, other organisations and administrators seeking to implement electronic electoral services through the development of clear requirements and prior evaluation of systems against these requirements.
- Eases the process of quality assurance during the short timescales available in the run up to an election.
- Provides stability and potentially growth in the electronic electoral market through the availability of clear requirements and accreditation needs of electronic electoral systems/services that could apply internationally.

Electoral services being assured need to support all types of public elections, including national government elections on an international stage. Electoral services need to be delivered on an international basis and assessed in accordance with internationally agreed standards and practices.

EML defines open interfaces between the various processes involved in elections and electoral management. Such open XML interfaces can provide convenient points at which the Electoral Assurance Framework can assess the various components of electoral systems. The assessment required can be

made appropriate to the impact of a security problem with a particular component of an electoral system/service and hence establish the level of trust that can be required/placed in that component.

The standardised interface points provided by EML also enable the ability to employ multiple trust paths within an electoral system. Thus, as an example, the standard auditing interface could enable the verification and audit systems to be totally independent from other parts of the electronic electoral system giving rise to trusted voting auditing processes which could be independently assessed under the Electoral Assurance Framework.

# 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 may need 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 [ref 4]. 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, eg voter registration, vote counting. There are very few complete end-to-end EML implementations to date as e-voting systems use is still maturing globally.

## Localisation

It is very unlikely that any voting regime would be able to use EML straight out of the box. There will almost certainly be a need to "localise" EML to reflect national, regional or local circumstances, laws and time honoured practices. See Appendix C for information about the UK's localisation of EML [ref 5]. This will entail restricting certain parts, and/or adding local elements.

## Getting Started

First using the generic business and technical models defined in EML [ref 3] identify which areas of e-enabled elections are within your remit and from that which schemas may be appropriate for your usage.

Having identified the relevant schemas review the EML Data Dictionary [ref 3] to determine which data elements are appropriate for your use, either as they are or with modification. Similarly identify other data elements that you require which will need to be added in as part of your localisation.

From the computing technology stance there are provided a set of EML schemas that apply to each step of the election process. The schemas define the information used at each step and hence control the processing. These schemas can then be extended as required and additional constraints added for your particular local voting regime. This is explained in detail in the EML Schema Descriptions document [ref 3]. We recommend the use of Schematron [ref 6] to handle and apply these localisations, but other technologies or techniques can be used (such as OASIS CAM templates).

There is now a great deal of experience of EML within the membership of the OASIS E&VS Technical Committee and they can provide initial advice for organisations that are new to e-enabled elections.

# Summary

The OASIS EML standard consists of tried and proven XML formats for handling 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 e-enabled elections.

The content of the EML records has also been designed to operate in a wide variety of election methods and ballot systems. This includes the requirements adopted by the Council of Europe Ministers' report [ref 2] on electronically administered elections, see Appendix C.

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 from which to build their election systems.

## Contacts and Additional Information

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

- EML Process and Data Requirements

- EML Data Dictionary

- EML Schema Descriptions

These and other documents including some recent case studies, see Appendix C, can be obtained through the OASIS website [ref 1].

For more information on how to participate in EML activities, please contact the E&VS Technical Committee.

# Appendix A – Resume and History of EML

## What is e-Voting?

In the context of EML, e-voting has a very wide definition. 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 processes begin with the declaration of an election or referendum, followed by 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 using a device, eg PC or telephone, not controlled by an election official.

## 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**: the 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.
- **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 specifications 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

## Security

Security is a major concern within e-voting and whilst EML didn't set out with the intention of solving 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

## Development Timetable

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. 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 Council of Europe [ref 2] and the latest version reflects the input from its 43 member states. Along the way lessons learnt have been fed in from e-voting pilots carried out in a number of countries, eg UK.

So it is not unreasonable to claim that EML now meets universal needs but at the same time allows implementers the flexibility to localise it to meet any specific detailed business rules or practices.

EML will continue to evolve and mature as more experience of e-enabled elections is gained and current concerns, eg security of remote voting, are addressed.

Currently work is underway to develop EML v5.0 following which it will be submitted to ISO for their endorsement.

# Appendix B – Comparisons

## 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, thus reducing the risk of large scale vote rigging.

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

## EML and Proprietary Systems Comparisons

The more important debate is not about paper versus electronic methods but whether e-voting applications should be run using proprietary software or open standards like EML. The following table provides some aspects and analysis between them.

| EML | | Proprietary Systems | |
|---|---|---|---|
| **Strengths** | **Weaknesses** | **Strengths** | **Weaknesses** |
| Based on common processes but allows local customisation / extension<br>Persistent nature of content.<br>Consistency in adoption of business rules<br>Provides strong audit trail.<br>Allows more choice of products and suppliers<br>Avoids proprietary lock-in<br>Supports scalability, transparency and interoperability<br>Provides basis for open accreditation processes.<br>Reduced development costs for suppliers<br>Accommodates future changes more easily<br>Open source solutions available. | Limited practical implementations.<br>Not yet fully matured.<br>Expertise required for initial set-up.<br>Can cause process loading problems. | More mature implementations available.<br>Out of the box solutions can make initial set-up quicker. | Proprietary lock-in.<br>Higher development costs.<br>Expertise required for initial set-up.<br>Not transparent.<br>Makes interoperability difficult.<br>Lack of open audit trails.<br>Does not support change easily.<br>May require processes to be tailored to meet software.<br>Does not provide for open accreditation processes.<br>No open source solutions provided. |
| **Opportunities** | **Threats** | **Opportunities** | **Threats** |
| Provide foundation for trusted voting processes.<br>Standards create open marketplace. | New technology may expose weaknesses. | | Vendors align to political parties.<br>Anonymity may be compromised. |

# Appendix C – Case Studies

### 1. Council of Europe Recommendation

Probably the most significant piece of work in recent times concerning e-voting has been that carried out by the Council of Europe. Following a study by all member states, a recommendation on the future of e-voting was endorsed by the Committee of Ministers on 30 September 2004. The recommendation set out standards for the legal, operational and technical aspects of running e-enabled elections and as part of that EML was endorsed as the technical standard to be used for data interoperability. Full details are available at www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/.

### 2. UK – e-voting pilots

Over the past few years the United Kingdom has conducted a number of e-voting pilots, testing a range of channels from remote Internet voting, digital TV and mobile phones. A full report on the last set of pilots is available at www.electoralcommission.org.uk/elections/may2003.cfm. More recently the focus of attention has been on postal voting but now a new series of e-voting pilots has been announced for the May 2007 Local Authority elections , see www.dca.gov.uk/elections/suppdocs.htm. For the initial pilots a UK Localisation of EML was produced, see http://www.govtalk.gov.uk/schemasstandards/schemalibrary_schema.asp?schemaid=201 and this will be enhanced for any future pilots.

### 3. UK – CORE project

The United Kingdom is running a project to e-enable its electoral registration procedures. The co-ordinated online record of electors (CORE) will in due course provide for national access of all voter registration data and will use EML to support the capture and exchange of data. Further details of project CORE are available at www.dca.gov.uk/consult/core/cp2905.htm .

### 4. Belgium

EML was used in the local elections in Flanders on 8th October 2006. A report on the elections is available at: www.oasis-open.org/apps/org/workgroup/election/download.php/20745/LV2006_Local%20Elections%20Flanders%202006-v0%2031_V01%5B1%5D.00.pdf. The results of the elections are available at: http://vlaanderenkiest.be

### 5. Open Voting

An open source version of EML v4.using the new OpenScan source code and samples based on elections for New York State are available at http://emlvoting.org. The software is designed to run under Apache and Tomcat and WAR file is provided including build and source.

### 6. e-POLL

The European Commission has been running a pilot project over the last couple of years to test out remote voting. Project e-POLL (Electronic polling system for remote voting operations) has completed its initial phase and plans are now being finalised for the next phase which will include the use of EML. Further details of the project are available at www.e-poll-project.net/ .

### 7. Using EML with trusted voting mechanisms – USA developments

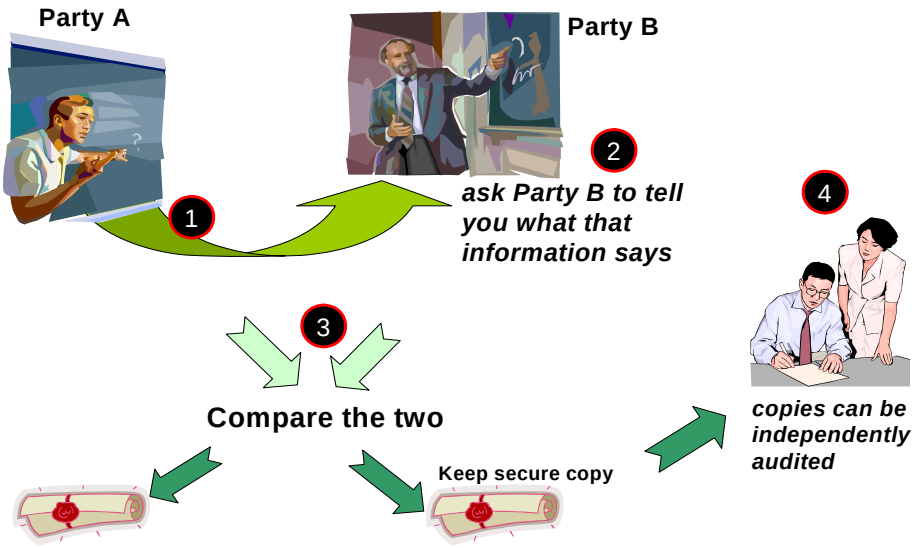
Recently work has been undertaken in the USA to examine mechanisms that can provide both voter verified ballots and 100% audit cross tabulation between multiple data sources in a trusted election process. EML can provide a pivotal role by providing an exactly matching vote recording mechanism that can 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 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 the Massachusetts Institute of Technology as a two part trusted method - where one computer device is used to independently verify the operation of the original balloting device.

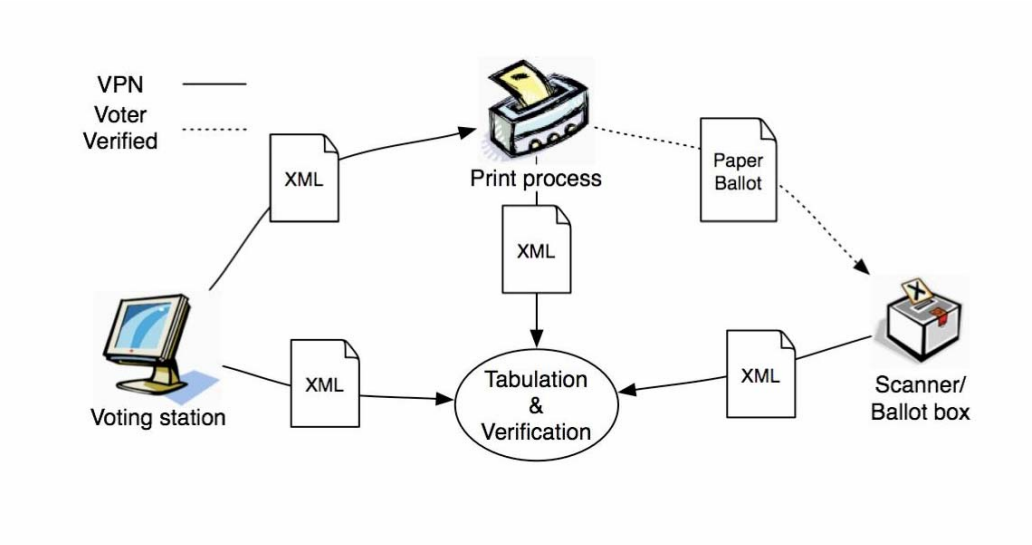
**Figure 1 – Conceptual Trusted Logic**



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 (possibly 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.

# Appendix D – References


1. Election Mark-up Language *OASIS*
   see OASIS Election and Voter Services TC
2. The Council of Europe e-Voting Recommendation
   see www.coe.int/
3. The EML Standard version 4 documentation
   see www.oasis-open.org/apps/org/workgroup/election/download.php/18158/EML v4.0 - OASIS Standard.zip
4. XML Schema 1.0 *W3C*
   see www.w3.org/XML/Schema
5. The UK Localisation of EML
   see GovTalk – EML UK Customisation v2.1
6. The Schematron Assertion Language 1.5 (ISO/IEC 19757-3:2006)
   see www.ascc.net/xml/schematron/