

OASIS

ELECTION AND VOTER SERVICES TECHNICAL COMMITTEE

ELECTION MARK-UP LANGUAGE (EML): e-VOTING PROCESS AND DATA REQUIREMENTS

Version 2
5 September 2002



Document Control

Abstract

This document contains a high-level overview of the processes within an e-voting system and the data requirements of the flows between those processes. It also addresses security issues relating to the exchange of data, and also provide a glossary of terms to ensure a full understanding by readers of the document.

Current Version

Date	Version	Status	Editor/ Author
19 Apr 02	2.0 Draft	Draft Committee Specification version 2	Aoun Charbel John Ross Paul Spencer
4 June 02	2.0A Draft	Revised draft accommodating committee's comments	John Borrás John Ross Paul Spencer
12 July 02	2.0B Final	Draft Committee Specification for TC approval	Aoun Charbel John Ross Paul Spencer Eric Peterson
5 Sept 02	2.0	Committee Specification	

Change History

Date	Version	Status	Editor/ Author
13 May 02	1.0	Committee Specification	John Borrás John Ross Paul Spencer Charbel Aoun
18 Mar 02	1.1	Draft Committee Specification for public consultation	Aoun Charbel (Main) John Ross (Co- Editor) Paul Spencer (Co-Editor)
13 Mar 02	1.0e	Draft Committee Specification	Aoun Charbel John Ross Paul Spencer
01 Mar 02	1.0d	Draft Committee Specification	Aoun Charbel John Ross Paul Spencer
18 Feb 02	1.0c	Draft Committee Specification	Aoun Charbel John Ross Paul Spencer
14 Feb 02	D3.2	Draft Committee Specification	Aoun Charbel John Ross Paul Spencer



OASIS Copyright Notices

- (A) *"OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director."*
- (B) *"OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director."*
- (C) *"Copyright (C) OASIS Open (date). All Rights Reserved."*

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

- (D) *"OASIS has been notified of intellectual property rights claimed in regard to some or all of the contents of this specification. For more information consult the online list of claimed rights."*

Table of Contents

Executive Summary

1. Introduction

- 1.1 Business Drivers
- 1.2 Technical Drivers
- 1.3 The E&VS Committee
- 1.4 Challenge and Scope
- 1.5 Documentation Set
- 1.6 Conformance
- 1.7 Terminology

2. High-Level Election Process

- 2.1 The Human View
- 2.2 The Technology View
- 2.3 Outline
- 2.4 Process Description
- 2.5 Data Requirements

3. Security Considerations

- 3.1 Basic security requirements
- 3.2 Terms
- 3.3 Specific Security Requirements
- 3.4 Security Architecture
- 3.5 Internet voting security concerns

Appendix A Glossary/Terminology

Appendix B Internet Voting Security Concerns

Executive Summary

OASIS, the XML interoperability consortium, formed the Election and Voter Services Technical Committee in the spring of 2001 to develop standards for election and voter services information using XML. The committee's mission statement is, in part, to:

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

The objective is to introduce a uniform and reliable way to allow election systems to interact with each other. 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”.
- 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.

The primary deliverable of the committee the Election Markup Language (EML). This is a set of data and message definitions described as XML schemas. At present EML includes specifications for:

- Candidate Nomination, Response to Nomination and Approved Candidate Lists
- Voter Registration information, including eligible voter lists
- Various communications between voters and election officials, such polling information, election notices, etc.
- Logical Ballot information (races, contests, candidates, etc.)
- Voter Authentication
- Vote Casting and Vote Confirmation
- Election counts and results
- Audit information pertinent to some of the other defined data and interfaces

Overview of the EML Process and Data Requirements Document

To help establish context for the specifics contained in the XML schemas that make up EML, the committee also developed a generic election process model. This model identifies the components and processes common to many elections and election systems, and describes how EML can be used to standardize the information exchanged between those components.

Section 1 outlines the business and technical needs the committee is attempting to meet, the challenges and scope of the effort, and introduces some of the key framing concepts and terminology used in the remainder of the document.

Section 2 describes two complementary high-level process models of an election exercise, based on the human and technical views of the processes involved. It is intended to identify all the generic steps involved in the process and highlight all the areas where data is to be exchanged. The discussions in this section present details of how the messages and data formats detailed in the EML specifications themselves can be used to achieve the goals of open interoperability between system components. Section 2 also includes descriptions of the various EML interfaces, independent of the specific syntax requirements of a complete XML schema definition.

Section 3 presents a discussion of some of the common security requirements faced in different election scenarios, a possible security model, and the mechanisms that are available in the EML specifications to help address those requirements. The scope of election security, integrity and audit included in these interface descriptions and the related discussions are intended to cover security issues pertinent only to the standardised interfaces and not to the internal security requirements within the various components of election systems.

The security requirement for the election system design, implementation or evaluation must be placed with the context of the vulnerabilities and threats analysis of a particular election scenario. As such the references to security within EML are not to be taken as comprehensive requirements for all election systems in all election scenarios, nor as recommendations of sufficiency or approach when addressing all the security aspects of election system design, implementation or evaluation.

Appendices: The document concludes with a glossary of voting terminology, particularly useful as it indicates some of the issues that arise when attempting to normalize the requirements and even nomenclature of elections internationally.

1. INTRODUCTION

1.1 Business Drivers

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. In the past, changes in the election process have proceeded deliberately and judiciously, often entailing lengthy debates over even the most minute detail. These changes have been approached with caution because discrepancies with the election system threaten the very principles that make our society democratic.

Times are changing. 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.

Internet voting is seen as a logical extensions of Internet applications in commerce and government and in the wake of the United States 2000 general elections is among those solutions being seriously considered to replace older less reliable election systems.

The implementation of Internet 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. However, it has to be recognized that the use of technology will not by itself correct this trend. Greater engagement of voters throughout the whole democratic process is also required.

1.2 Technical Drivers

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, auditable, automated election system has never been greater.

The introduction of open standards for election solutions is intended to enable election officials around the world to build upon existing infrastructure investments to evolve their systems as new technologies emerge. This will simplify the election process in a way that was never possible before. Open election standards will aim to instill confidence in the democratic process among

citizens and government leaders alike, particularly within emerging democracies where the responsible implementation of the new technology is critical.

1.3 The E&VS Committee

OASIS, the XML interoperability consortium, formed the Election and Voter Services Technical Committee to standardize election and voter services information using XML. The committee is focused on delivering a **reliable, accurate and trusted** XML specification (Election Markup Language (EML)) for the structured interchange of data among hardware, software and service vendors who provide election systems and services.

EML, the first XML specification of its kind, and when implemented can provide a uniform, secure and verifiable way to allow e-voting systems to interact as new global election processes evolve and are adopted.

The Committee's mission statement is:

“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 services performed for such elections include but are not limited to voter role/membership maintenance (new voter registration, membership and dues collection, change of address tracking, etc.), citizen/membership credentialing, redistricting, requests for absentee/expatriate ballots, election calendaring, logistics management (polling place management), election notification, ballot delivery and tabulation, election results reporting and demographics.”

The primary function of an electronic voting system is to capture voter preferences reliably and report them accurately. Capture is a function that occurs between “a voter” (individual person) and “an e-voting system” (machine). It is critical that any election system be able to prove that a voter's choice is captured correctly and anonymously, and that the vote is not subject to tampering.

Dr. Michael Ian Shamos, a PhD Researcher who worked on 50 different voting systems since 1980 and reviewed the election statutes in half the US states, summarized a list of fundamental requirements, or “six commandments,” for electronic voting systems:

- 1- Keep each voter's choice an inviolable secret.
- 2- Allow each eligible voter to vote only once, and only for those offices for which he/she is authorized to cast a vote.
- 3- Do not permit tampering with voting system, nor the exchange of gold for votes.
- 4- Report all votes accurately
- 5- The voting system shall remain operable throughout each election.
- 6- Keep an audit trail to detect any breach of [2] and [4] but without violating [1].

In addition to these business and technical requirements, the committee was faced with the additional challenges of specifying a requirement that was:

- ❑ Multinational: our aim is to have these standards adopted globally
- ❑ Effective across the different voting regimes. e.g. proportional representation or “first past the post”.
- ❑ Multilingual – our standards will need to be flexible enough to accommodate the various languages and dialects and vocabularies.
- ❑ Adaptable – our aim is to provide a specification that is resilient enough to support elections in both the private and public sectors.
- ❑ Secure – The standards must provide security that protects election data and detects any attempt to corrupt it.

The Committee followed these guidelines and operated under the general premise that any data exchange standards must be evaluated with constant reference to the public trust.

1.4 Challenge and Scope

The goal of the committee is to develop an Election Markup Language (EML). This is a set of data and message definitions described as a set of XML schemas and covering a wide range of transactions that occur during an election. To achieve this, the committee decided that it required a common terminology and definition of election processes that could be understood internationally. The committee therefore started by defining the generic election process models described here.

These processes are illustrative, covering the vast majority of election types and forming a basis for defining the Election Markup Language itself. EML has been designed such that elections that do not follow this process model should still be able to use EML as a basis for the exchange of election-related messages.

EML is focussed on defining open, secure, standardized and interoperable interfaces between components of election systems. Thus providing transparent and secure interfaces between various parts of an election system. The scope of election security, integrity and audit included in these interface descriptions and the related discussions are intended to cover security issues pertinent only to the standardised interfaces and not to the internal or external security requirements of the various components of election systems.

The security requirement for the election system design, implementation or evaluation must be placed with the context of the vulnerabilities and threats analysis of a particular election scenario. As such the references to security within EML are not to be taken as comprehensive requirements for all election systems in all election scenarios, nor as recommendations of sufficiency or

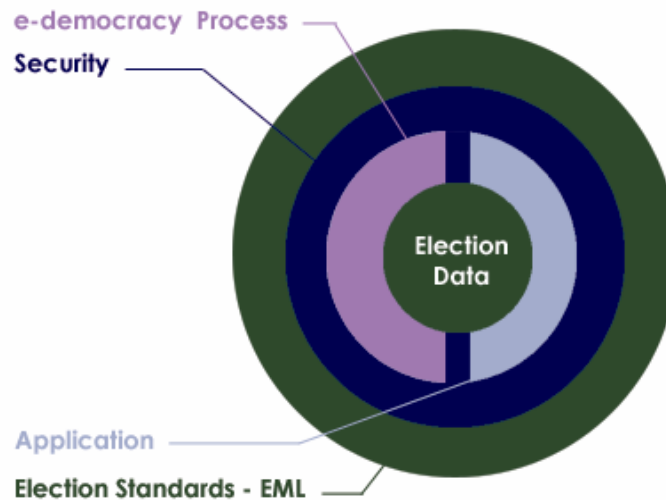
approach when addressing all the security aspects of election system design, implementation or evaluation. In fact, the data security mechanisms described in this document are all optional, enabling compliance with EML without regard for system security at all.

A complementary document may be defined which refines the security issues defined in this document

EML is meant to assist and enable the election process and does not require any changes to traditional methods of conducting elections. The extensibility of EML makes it possible to adjust to various e-democracy processes without affecting the process, as it simply enables the exchange of data between the various election processes in a standardized way.

The solution outlined in this document is non-proprietary and will work as a template for any e-voting system. The objective is to introduce a uniform and reliable way to allow election systems to interact with each other. The proposed standard is intended to reinforce public confidence in the election process and to facilitate the job of democracy builders by introducing guidelines for the selection or evaluation of future election systems.

Figure 1A: Relationship overview



1.5 Documentation Set

To meet our objectives, the committee has defined a process model that reflects the generic processes for running elections in a number of different international jurisdictions. The processes are illustrative, covering the vast amount of election types and scenarios.

The next step was then to isolate all the individual data items that are required to make each of these processes function. From this point, our approach has been to use EML as a simple and standard way of exchanging this data across different electronic platforms. Elections that do not follow the process model can still use EML as a basis for the exchange of election-related messages at interface points that are more appropriate to their specific election processes.

Finally, the committee will be conducting pilot studies using the prototype EML standard to test it's effectiveness across a number of different international jurisdictions. The committee document set will include:

- **Voting Process and Data Requirements** (This Document): A general and global study of the electoral process. Introduces the transition from a complete human process by defining the data structure to be exchanged and where needed. An EML schema is introduced and clearly marked.
- **EML Specifications:** This consists of a library of XML schemas used in EML and a document describing them. The XML schemas define the formal structures of the election data that needs to be exchanged.
- **Scenarios:** A selected set of scenarios with variations in election type / country. The objective of the scenarios is to show how documents 1 and 2 can be used in practice. Each scenario comprises a UML description and a set of sample XML messages.

1.6 Conformance

To conform to this specification, a system must implement all parts of this specification that are relevant to the interfaces for which conformance is claimed. The required schema set will normally be part of the purchasing criteria and should indicate schema version numbers. For example, in the future, the specification for an election list system might specify that a conforming system must accept and generate XML messages conforming to the following schemas:

Schema	Accept	Generate
EML110	v1.0	
EML310	v2.0, v2.1	
EML320	v1.0, v2.0	v2.0
EML330		v1.1
EML340		v1.0
EML350		v1.0
EML360		v1.3

A conforming system will then conform to the relevant parts of this specification and the accompanying schemas.

1.7 Terminology

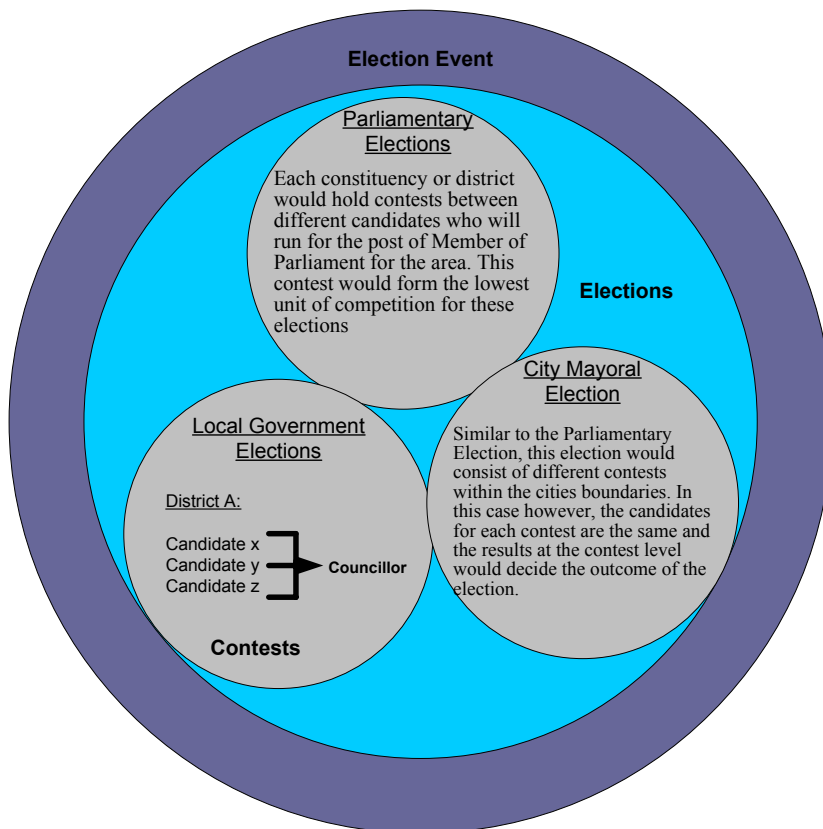
At the outset of our work, it was clear that the committee would need to rationalize the different terms that are commonly used to describe the election process.

Terms used to describe the election process, such as ballot and candidate, carry different meanings in different countries – even those speaking the same language. In order to develop a universal standard, it is essential to create universal definitions for the different elements of the election process. See appendix A for the terms used by the committee in this document.

Our approach was to regard elections as involving **Contests** between **Candidates or Options** which aggregate to give results in different **Elections**.

In practice however, electoral authorities would often run a number of different elections during a defined time period. This phenomenon is captured in our terminology as an **Election Event**. The model below uses a British context to describe our approach in general terms.

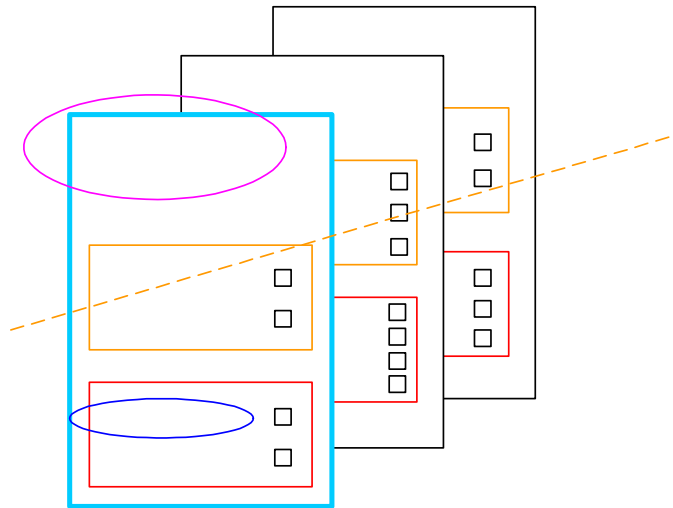
Figure 1B: The Election Hierarchy



In the detailed example below, there is an **election event** called the “Union Annual Election”. This comprises two **elections**, one for the National Executive Committee (NEC) and one for the International Liason Committee (ILC). Three positions are being selected for each committee, as a result, each **election** is made up of three **contests**. In region 1 (R1), the **contest** for each **election** has two **options** (or **candidates**).

Figure 1c below shows the three **ballots** (one for each region). The **ballot** is personal to the voter and presents the **options** available to that voter. It also allows choices to be made. During the election exercise, each voter in region 1 receives only the region 1 ballot. This ballot will contain the **candidates** for the (R1) contest for each of the two **elections**.

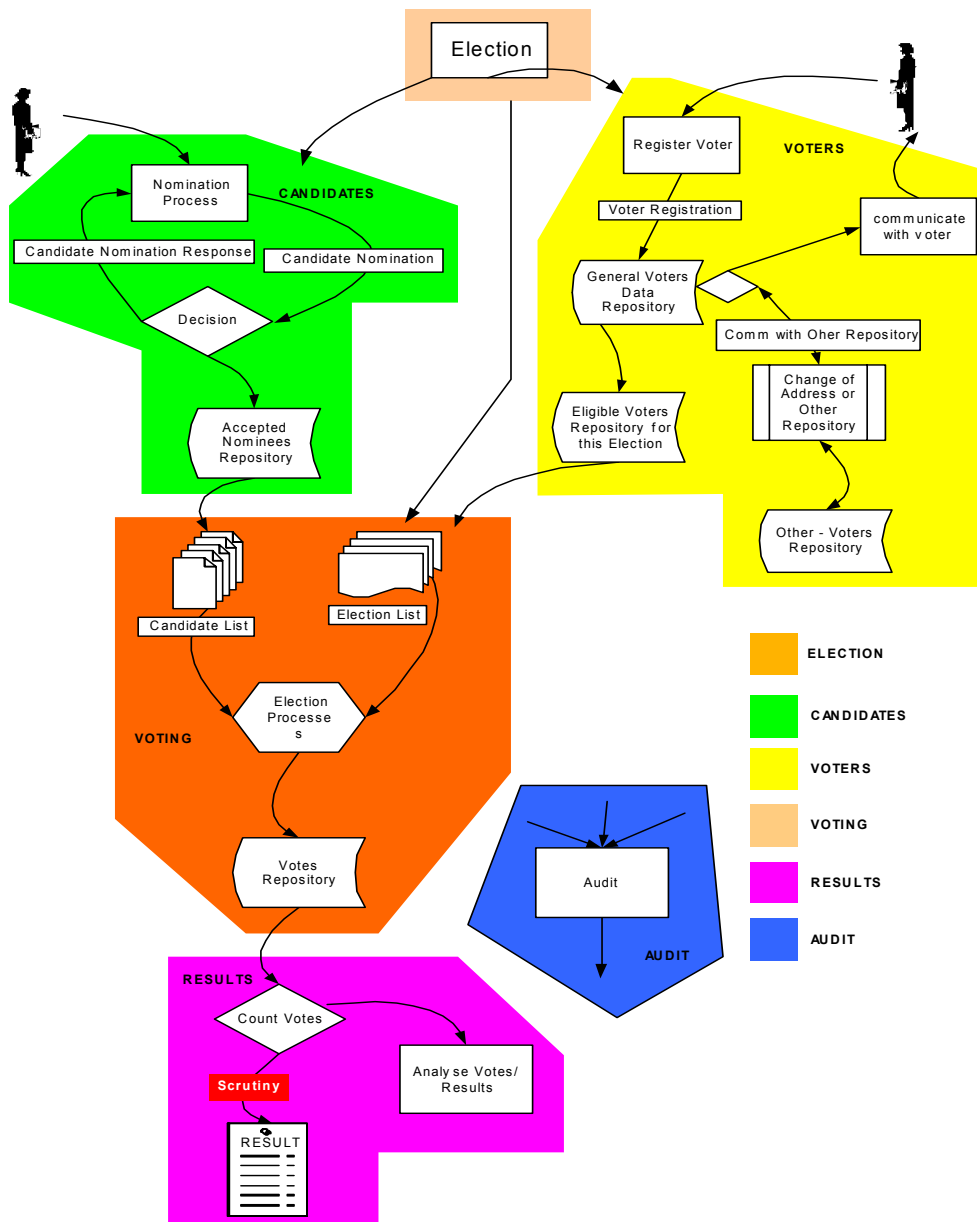
Figure1C: Union annual election



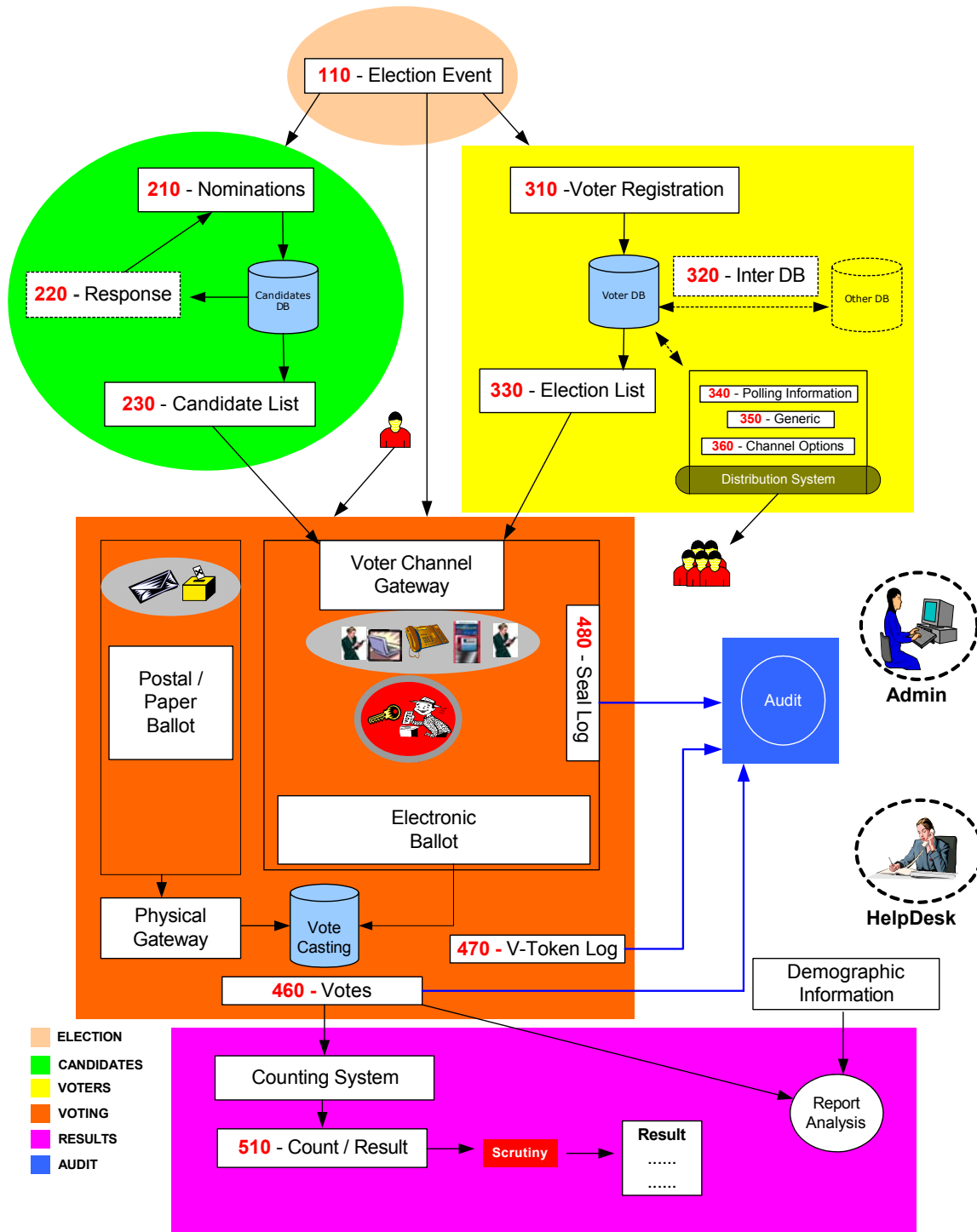
2. HIGH-LEVEL ELECTION PROCESS

Chapter 2 describes two complementary high level process models of an election exercise, based on the human and technical views of the processes involved. It is intended to identify all the generic steps involved in the process and highlight all the areas where data is to be exchanged.

2.1 Figure 2A: High Level Model – The Human View



2.2 Figure 2B: High-Level Model – The Technical View



2.3 Outline

This *high-level process model* is derived from real world election experience and is designed to accommodate all the feedback and input from the members of this committee.

For clarity, the whole process can be divided into 3 major areas, pre election, election, post election; each area involves one or more election processes. This document allocates a range of numbers for each process. One or more XML schema will be specified to support each process, this ensures consistency with all the figures and the schemas required:

- Pre election
 - Election (100)
 - Candidates (200)
 - Voters (300)

- Election
 - Voting (400)

- Post election
 - Results (500)
 - Audit
 - Analysis

Some functions belongs to the whole process and not to a specific part:

- Administration Interface
- Help Desk

- **Pre election**
 - Election (110)
 - Candidates (200)
 - Nomination (210)
 - Response to nomination (220)
 - Candidate List (230)
 - Voters (300)
 - Voter registration (310)
 - Inter database communication (320)
 - Election List (330)
 - Voter Communication
 - Polling Information (340)
 - Generic (350)
 - Voter Notification (360)

- **Election**
 - Voting (400)

- Ballot (410)
- Authentication (420)
- Authentication Reply (430)
- Vote and Casting (440)
- Vote Confirmation (450)
- Votes (460)
- V-Token log (460)
- Seal log (480)

➤ Post election

- Counting (500)
 - Count Result (510)
- Analysis

➤ Audit election

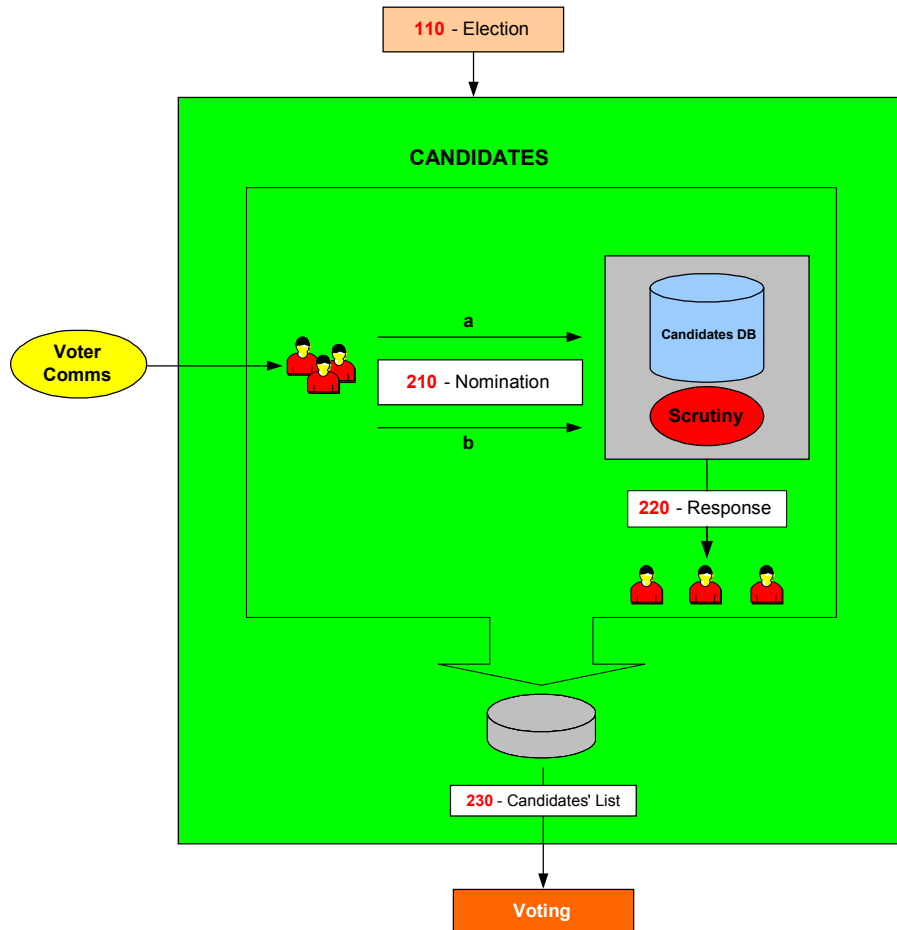
- Audit Analysis
- Audit Reporting

➤ Global functions

- Administration Interface
- Help Desk

2.4 Process Descriptions

Figure 2C: The Candidate Nomination Process



This is the process of approving nominees as eligible candidates for certain positions in an election. Schemas **210**, **220** are specifically applicable to candidates' nominations and do not apply for issues like surveys, referendums.

Irrespective of local regulations covering the nomination process, or the form in which a candidate's nomination is to be presented, i.e. (written/verbal), the committee anticipates that the process will conform to the following format:

- Voter Communications [**350-Generic**] declaring the opening of nominations will be used to reach the voters population eligible to vote for a position x in an election y.

- Interested parties will respond in the proper way satisfying the rules of nomination for this election with the objective of becoming running candidates. The response message conforms to schema **210**.
- A nomination can be achieved in one of two ways:
 - A Nominee will reply by attaching to his nomination a list of x number of endorsers with their signature.
 - Each endorser will send a letter specifying Mr. X as his or her nominee for the position in question.

The election officer(s) of this specific election will scrutinize those replies by making sure the requirements are fully met. Requirements for nomination vary from one election type to another, for example some elections require the nominee to:

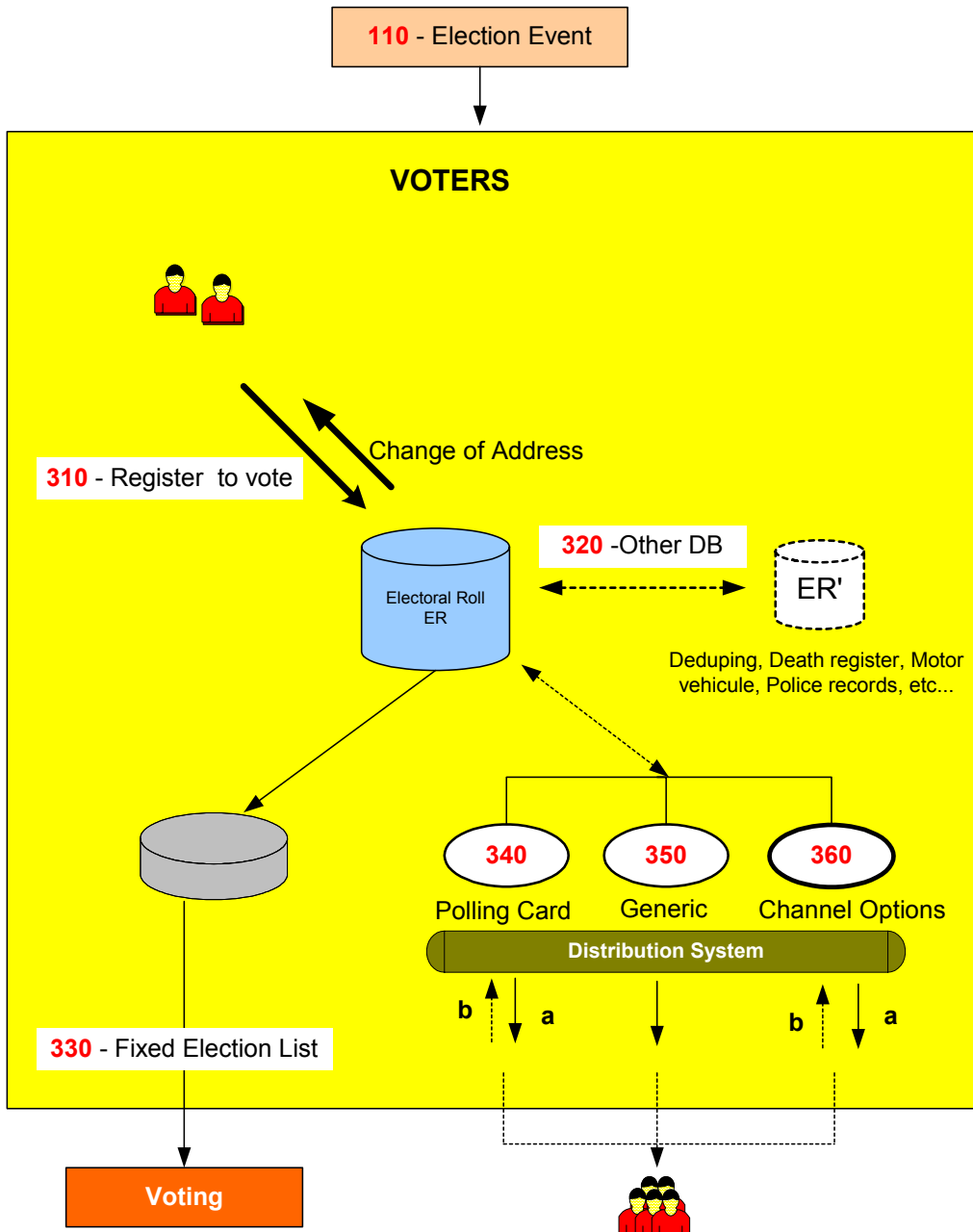
- Pay fees,
- Have x number of endorsers,
- Be of a certain age,
- Be a citizen more than x number of years,
- Etc.

Schema **210** provides mechanisms to identify and convey scrutiny data but since the laws of nomination vary extensively between election scenarios, no specific scrutiny data is enumerated.

Nominees will be notified of the result of the scrutiny using a message conforming to schema **220**.

The outcome of this process is a list of accepted candidates that will be communicated using a message conforming to schema **230**. It will be used to construct the contests and occurrence on the final ballot(s).

Figure 2D: Voter Registration.



The centre of this process is the Electoral Roll Database or the voters database. The input into this Database is the outcome of communications between “a voter” and “an Election Authority”. The subject of this correspondence can vary from adding a voter to modifying a voter; deletion of a voter is considered as part of modification.

This schema of data exchange is recommended irrelevant of the method a voter uses to supply his information. For example, a voter could register online or simply by completing a voter's form and posting the signed form. In the latter case, this schema is to be followed when converting the paper form into the electoral DB.

Another potential communication or exchange of data is with other databases such as those used by another election authority, government body, etc. Database exchanges will be required in some election scenarios; examples include geographical and organizational boundary changes.

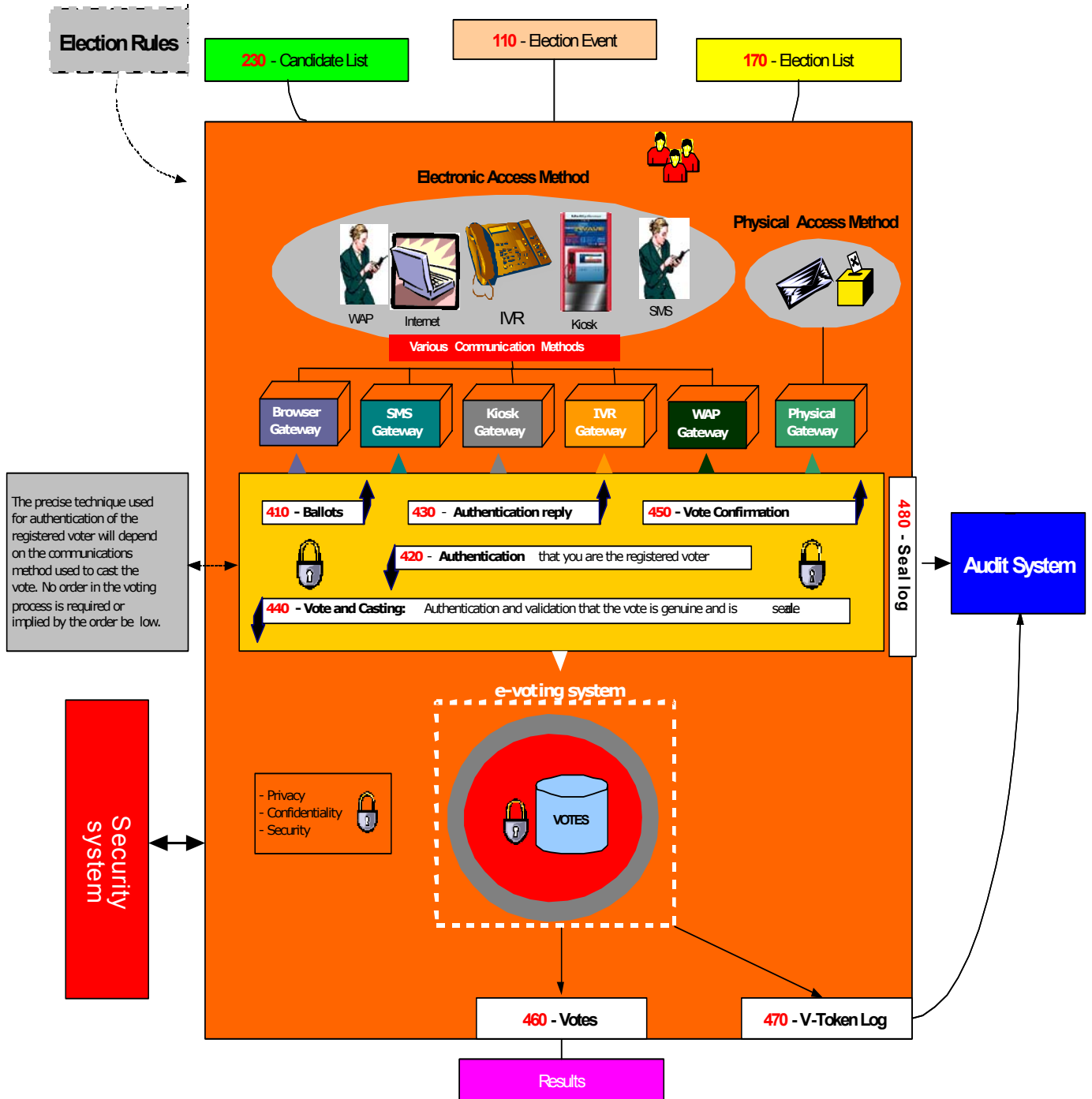
At a certain date, a subset of the voters DB is fixed from which the election list is generated [**Fixed Election List 330**]. The election list will include a list of all eligible voters/contest/elections for an election event.

It is here that we introduce the concept of voter communications. Under this category we divided them into three possible types of communications:

- Channel options.
- Polling Information.
- Generic.

The communication method between the Election Authority and the voters is outside the scope of this document, so is the application itself. This document does specify the data needed to be exchanged.

Figure 2E: The Voting Process



We assumed various systems would be involved in providing the voting process and regard each system as an independent entity.

As this figure shows, the voter will be voting using a choice of physical channels such as postal, polling place or paper ballot (the “physical access methods”), or the voter can vote using “electronic access methods” where he/she will utilize a number of possible e-voting channels.

Each channel may have a gateway acting as the translator between the voter terminal and the voting system. Typically, these gateways are in proprietary environments, the following schemas are to be used when interfacing to such gateways: **410, 420, 430, 440** and **450**. These schemas should function irrespective of the application or the supplier’s favored choice of technology.

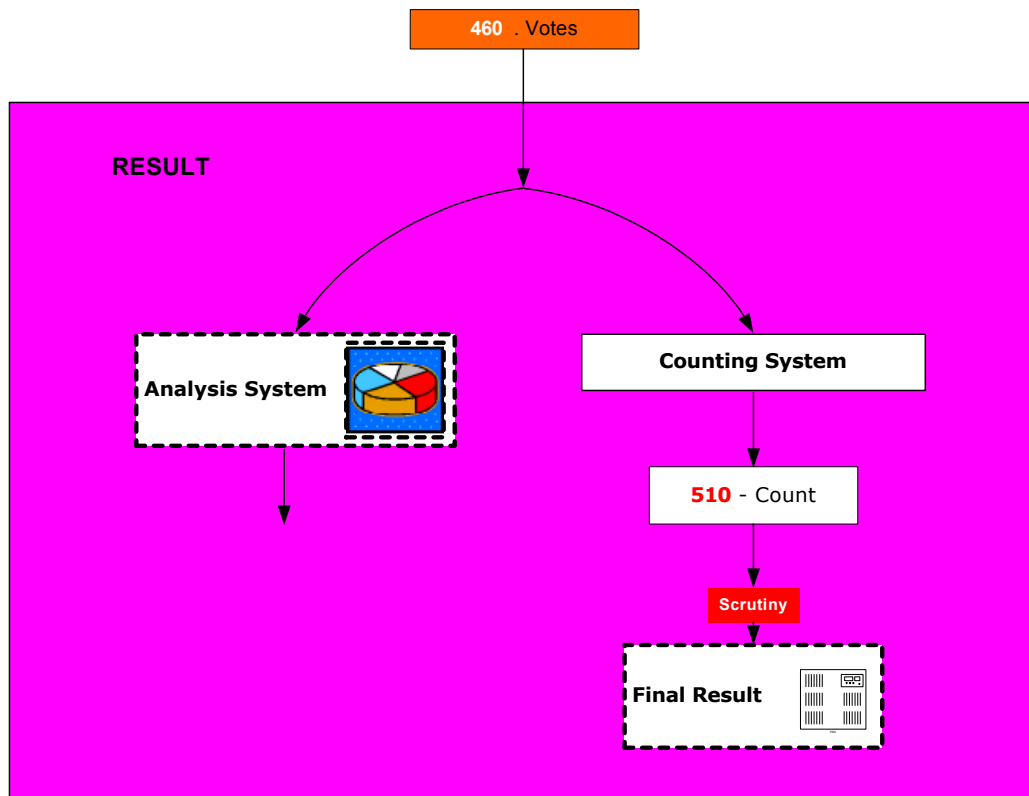
Where a voter’s right to vote in any particular contest needs to be determined, this is defined by the parameters of his V-Token. See section 3 for more information on security and the V-Token.

In some scenarios the right to vote may need to be qualified. This may occur if the voter’s right to vote is challenged or if the voter is given the temporary right to vote. In this case the vote needs to be cast by a voter with a qualified V-token. The reason for the qualification shall always be present in a qualified V-token and the qualification may need to be investigated before the vote is counted as legitimate.

The V-Token and qualified V-token are part of Schemas **420, 440, 450, 460** and **470**. To create balloting information, input data is needed about the election, the options/candidates available and the eligible voters; see schemas **230, 110** and **170** for exchanging such information between e-systems. However, a mapping process may be required in the e-voting system to map the various raw input data into output data for one ballot for one voter. This document uses the term election rules to define how this mapping is to be done in a particular election. When a precise election rule is needed is it identified by the election rule ID.

The current document assumes election rules themselves are implementation specific, thus by specifying the election rule ID the e-voting system can do the necessary mapping between voter, candidate, election and bylaws of the election to produce the ballot. Other issues that can be identified as affecting the election rules are geographical or organizational boundaries.

Figure 2F: Vote Reporting



Two of the post election items are the result and the audit report. Audit is discussed in the next section.

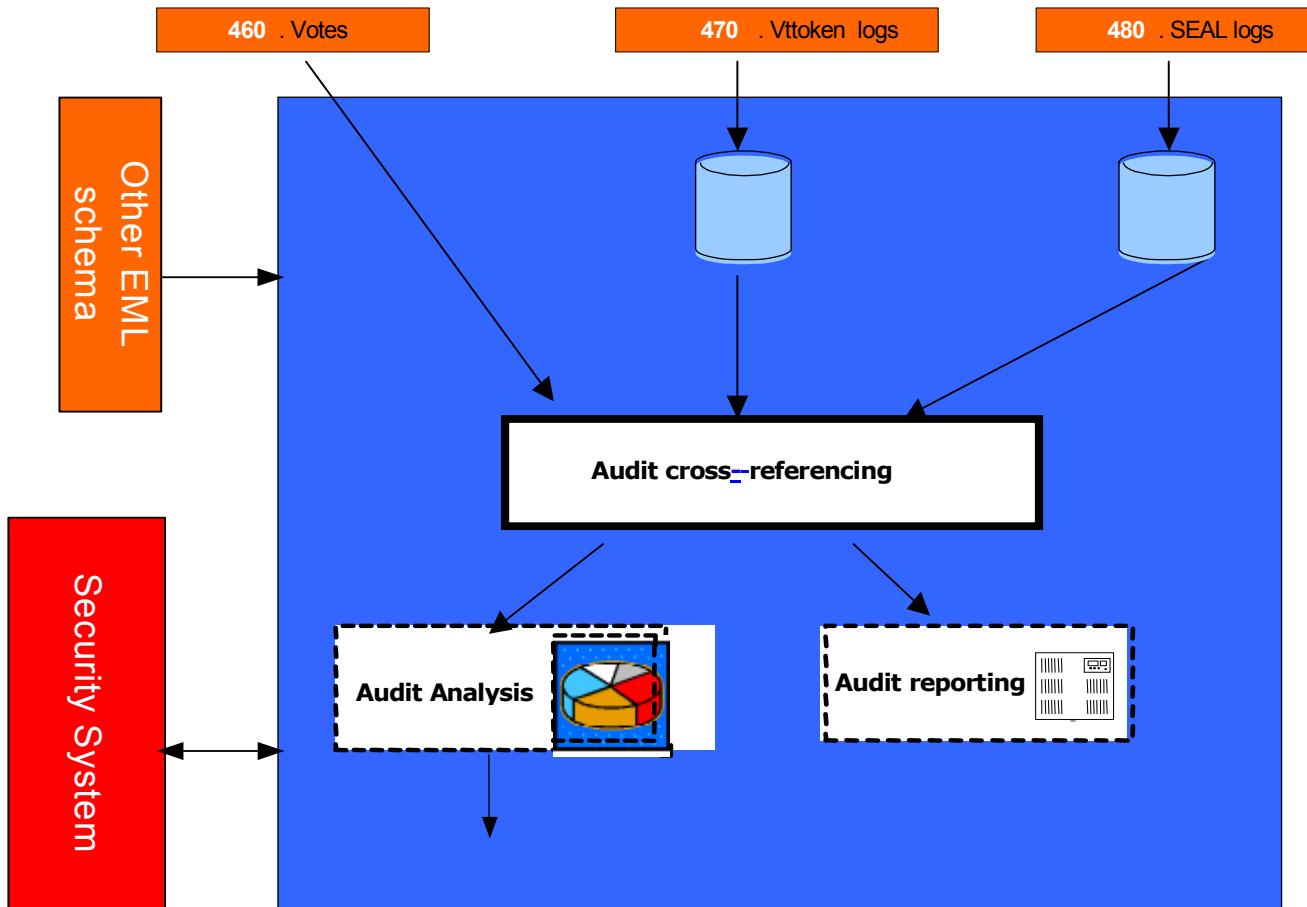
The voting system should communicate a bulk of data representing the votes to the counting system or the analysis system-using schema **460**. The result by itself, which is the compilation of the **460**, is to be communicated by the schema **510**.

Recount can be very simply accommodated by a re-run of the schema **460**, on the same or another counting system.

The votes schema **460** also feeds into an analysis system, which is used to provide for demographic or other types of election reports. The output of the analysis system is outside the scope of this document.

Further schemas may be developed that make use of the Vote and Count schemas. For example, schemas for messages that report election results to the Press.

Figure 2G: Auditing System



Audit is the process by which a legal body consisting of election officers and candidates' representatives can examine the processes used to collect and count the vote, thereby proving the authenticity of the result.

The requirement is for the election officer to be able to account for all the ballots. A count of ballots issued should match the total ballots cast, spoiled and unused.

Schemas **460**, **470**, **480** from the voting process provide input data to the audit process. Depending on the audit requirements additional data from other processes may be required. In particular, the security process may provide

additional data about all the issued V-Tokens and qualified V-Tokens (see Figure 3a: Voting system security).

The security process ensures that the right to cast a vote is dictated by the presence of a V-Token, thus in order to provide accountability for all ballots as per the requirement above, reliable data from the security system is required on the total number of:

- Eligible voters
- Issued V-Tokens or qualified V-Tokens.

The audit process can collate the total number of V-Tokens and qualified V-Tokens provided by the security system with the total number reported by the voting system using schema **460** and **470**.

The security system and sealing mechanism should be implemented so that trust can be placed in the seal and hence the sealed data. This implies that the seal should be performed as close to the user submission of the vote as technically possible. The count of the spoiled and unspoiled votes from **460** can then be cross-checked against the count of the number of trusted seals from **480**. This collation confirms that the total number of votes presented by the output of the e-voting system in **460** is consistent with the total number of submitted votes with seals.

The above collation between trusted data provided by the security process and data provided by the voting process prove that no legitimate votes have been lost by the voting system. It also proves that there is consistency between the number of eligible voters and the spoiled, unspoiled and unused votes as recorded by the e-voting system.

Another requirement is for the election officer to be able to prove that voted ballots received and counted are secure from any alteration. This requirement is met because each vote cast is sealed; the seal can be verified by the audit system and proves no alterations have been made since the vote was sealed.

A further requirement is for the election officer to be provided with a mechanism to allow a recount when result is contested. The number of votes from the voting system using schema **460** can be verified by collating the total votes as calculated by the audit system (using schema **480**), with the totals from the counting system. Then either rerunning the count, or running the count on another implementation can verify an individual result.

There is also the requirement for the election officer to be provided with a mechanism that allows for multiple observers to witness all the voting process, how this is achieved is dependant on the implementation of the system and procedures adopted. However, the seals and channel information using schema **480** provides the ability to observe voting inputs per channel while voting is in

progress without revealing the vote itself or the voter's identity. The final count of the seals can then be used to cross check the totals of the final result as described above.

The above defines some of the election data that can be verified by the audit system. However, ideally everything done by the various components of a election system should be independently verifiable. In the scope of EML this means that the audit system may need to be able to process all the standardized EML schemas. The audit system may in addition support proprietary interfaces of voting systems to enhance visibility and correctness of the election process.

2.5 Data Requirements

The diagrams and pictures above are meant to give a clear visual presentation of the overall process and detail main sections. Where a schema is identified as necessary, a three digit number is shown. This section describes the data content of each schema.

To limit the impact of differences such as those related to cultural divide, language, bylaws and different type of service, the current specification limits itself to identifying a set of data common to most election scenarios. Some data is optional and can be omitted when not required. In other cases, extensibility is provided by allowing unspecified data, indicated here using the keyword “ANY”.

The “mandatory” elements below are the minimum set of common data elements that must be present when the schema is used. All other elements are “optional”, which means the optional elements may, or may not, be present in a message using this schema. Any system that claims to support the schema must always generate mandatory elements and must be able to generate optional elements when required. Any system that claims to support the schema must be able to consume all mandatory and optional elements correctly on reception.

Note that some of the optional data will be considered as required in one system and either optional or even not accepted in others. Data Protection legislation and Privacy regulations will play a major role in defining what is to be included and under which section.

The format used to indicate mandatory and optional data is:

MANDATORY DATA
OPTIONAL DATA

In the absence of any National requirement specifying alternatives, the names and addresses shall conform to the xNAL. An example of a name and address attributes are below:

Name-Structure

Title
First Name
Last Name
Middle Name
Maiden Name
Suffix

Address-Structure

Address Line 1

Address Line 2

Street Name

City Name

Postcode

Country

Contact-Structure

Email

Home Telephone

Work Telephone

Personal Mobile

Business Mobile

Fax

Preferred Method of Contact

110 – Election Event

Contains the data about an election. This is the starting point of the whole process. It is made of one or more contests over a period of time.

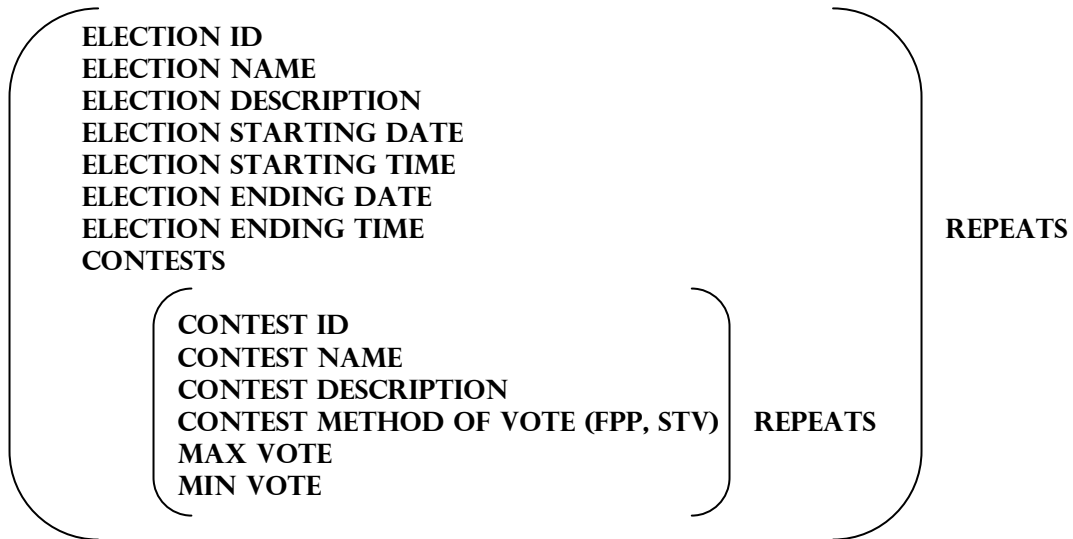
ELECTION EVENT ID

ELECTION EVENT NAME

ELECTION EVENT DESCRIPTION

ALLOWED CHANNELS (POLLING, INTERNET, POSTAL, SMS, TELEPHONE, WAP, KIOSK, DIGITAL TV, OTHERS)

ELECTIONS



SEAL

LANGUAGE ID (ISO STANDARD, MULTIPLE LANGUAGES ALLOWED)

ANY

210 - Candidate Nomination

Describes the data used by a candidate to send in his nomination.

CANDIDATE NAME

NAME-STRUCTURE

CANDIDATE ADDRESS

ADDRESS-STRUCTURE

CANDIDATE CONTACT INFO

CONTACT-STRUCTURE

ELECTION ID

ELECTION NAME

CONTEST ID

CONTEST NAME

PROPOSERS (1 TO N) n=number of maximum of endorsers required.

PROPOSER NAME

NAME-STRUCTURE

CATEGORY (PRIMARY, SECONDARY, OTHER)

PROPOSER ADDRESS

ADDRESS-STRUCTURE

CONTACT INFO

CONTACT-STRUCTURE

JOB STATUS OR TITLE

AFFILIATION

PERSONAL PROFILE OR BIOGRAPHY

SCRUTINY REQUIREMENTS

ELECTION STATEMENT

SEAL

LANGUAGE ID

ANY

220 - Response to Nomination

CANDIDATE NAME

NAME-STRUCTURE

CANDIDATE ADDRESS

ADDRESS-STRUCTURE

CONTACT INFO

CONTACT-STRUCTURE

ELECTION ID

ELECTION NAME

CONTEST ID

CONTEST NAME

NOMINATION ACCEPTED YES/NO

REMARK

AFFILIATION

SEAL

LANGUAGE ID

ANY

230 – Candidate List

ELECTION ID
ELECTION NAME
CONTEST ID
CONTEST NAME
CONTEST DESCRIPTION
CANDIDATES

(
CANDIDATE ID
CANDIDATE NAME
CANDIDATE AFFILIATION
) REPEATS

SEAL
LANGUAGE ID
ANY

310 - Voter Registration

Used for initial registration or changing of any of the voter data. The rules are applied in order to validate that someone has the right to vote.

VOTER ID
NATIONAL/LOCAL ID
(LIKE SOCIAL SECURITY NUMBER, NATIONAL INSURANCE NUMBER,
DRIVER LICENSE NUMBER, ETC...)
NAME
NAME-STRUCTURE
ELECTORAL ADDRESS
ADDRESS-STRUCTURE
ARMED FORCES (Y/N)
PROOF OF ID
MAILING ADDRESS
ADDRESS-STRUCTURE
MAILING CONTACT INFO
CONTACT-STRUCTURE
DATE OF BIRTH
EFFECTIVE DATE ADDED
EFFECTIVE DATE REMOVED
PREFERRED LANGUAGE OF VOTING
AFFILIATION
DATE SUBMITTED
TIME SUBMITTED
PREVIOUS ADDRESS
ADDRESS-STRUCTURE
PLACE OF BIRTH
SEX
ETHNIC GROUP
SPECIAL REQUESTS (VISUALLY IMPAIRED, DISABLED, NEED TRANSLATOR, ETC...)
PREFERRED METHOD OF VOTE (POSTAL, POLLING, ELECTRONIC)

SEAL
LANGUAGE ID
ANY

320 – Inter Db

a) ACTION REQUEST

TRANSACTION ID
SOURCE ID
DESTINATION ID
ACTION
ACTION DATE
ACTION TIME

VOTERS [*310-VOTER REGISTRATION (PER VOTER)*]

SEAL
LANGUAGE ID
ANY

b) REPLY TO ACTION REQUEST

TRANSACTION ID
SOURCE ID
DESTINATION ID
REPLY TO ACTION (Y/N, STRING – “EITHER OR” OR “BOTH”)
ACTION DATE
ACTION TIME

VOTERS [*310-VOTER REGISTRATION (PER VOTER)*]

SEAL
LANGUAGE ID
ANY

330 - Election List

It is a set of voters [310] associated to an election identifier and to a contest ID.

ELECTION EVENT NAME

ELECTION EVENT ID

ELECTIONS

(
 ELECTION NAME
 ELECTION ID
 CONTEST NAME
 CONTEST ID
 ELECTION RULE ID
(
 310-VOTER REGISTRATION (PER VOTER)
)
)

OR

ELECTION RULE ID

(
 310-VOTER REGISTRATION (PER VOTER)
)

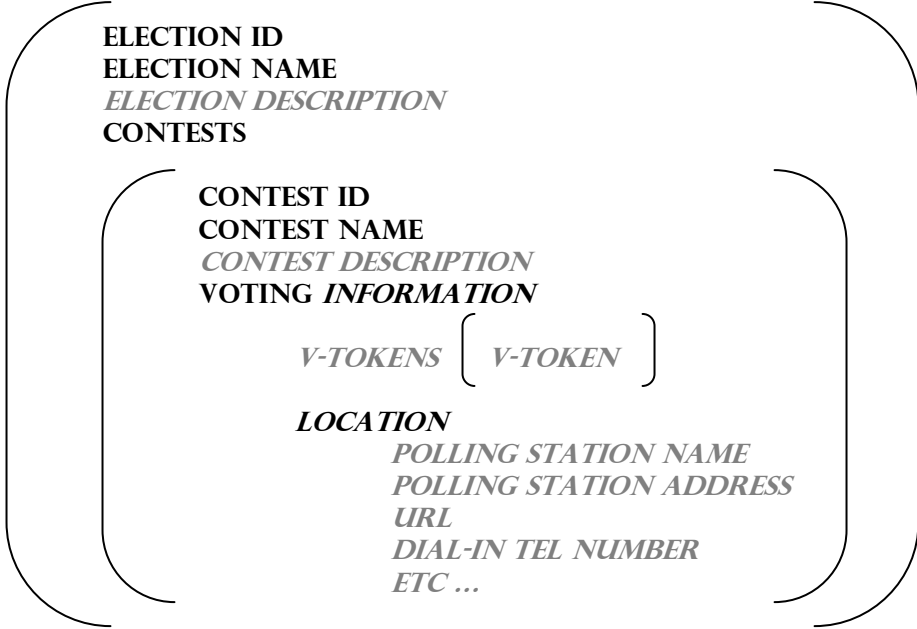
SEAL

LANGUAGE ID

ANY

340 – Polling Information

ELECTION EVENT ID
ELECTION EVENT NAME
ELECTION EVENT DESCRIPTION
VOTE STARTING DATE
VOTE STARTING TIME
VOTE ENDING DATE
VOTE ENDING TIME
VOTER ID
NAME
NAME-STRUCTURE
MAILING ADDRESS
ADDRESS-STRUCTURE
CONTACT INFORMATION
CONTACT-STRUCTURE
ELECTION RULE ID
ELECTIONS



MESSAGE
SEAL
LANGUAGE ID
ANY

NOTE: Outgoing or incoming communications can be in any order.

350 – a) Outgoing - Generic Communications

VOTER ID
TRANSACTION ID
VOTER NAME
NAME-STRUCTURE
MAILING ADDRESS
ADDRESS-STRUCTURE
CONTACT INFO
CONTACT-STRUCTURE
ELECTION EVENT NAME
ELECTION NAME
CONTEST NAME
GENERIC MESSAGE
RETURN ADDRESS
ADDRESS-STRUCTURE
RETURN CONTACT INFO
CONTACT-STRUCTURE
SEAL
LANGUAGE ID
ANY

350 – b) Incoming - Generic Communications

VOTER ID
TRANSACTION ID
VOTER NAME
NAME-STRUCTURE
GENERIC MESSAGE
CONTACT INFO
CONTACT-STRUCTURE
MAILING ADDRESS
ADDRESS-STRUCTURE
ELECTION EVENT NAME
ELECTION NAME
CONTEST NAME
SEAL
LANGUAGE ID
ANY

360 – a) Outgoing – Channel Options

Voters will be notified of an election with related information and are required to select method of vote.

Consists of outgoing generic communications with an additional mandatory element called Allowed channels.

VOTER ID

TRANSACTION ID

VOTER NAME

NAME-STRUCTURE

MAILING ADDRESS

ADDRESS-STRUCTURE

CONTACT INFO

CONTACT-STRUCTURE

ELECTION EVENT NAME

ELECTION NAME

CONTEST NAME

GENERIC MESSAGE

RETURN ADDRESS

ADDRESS-STRUCTURE

RETURN CONTACT INFO

CONTACT-STRUCTURE

SEAL

LANGUAGE ID

ANY

ALLOWED VOTING CHANNELS (ALLOW MULTIPLE SELECTION)

POLLING

INTERNET

POSTAL

SMS

TELEPHONE

WAP

KIOSK

DIGITAL

TV

OTHERS

360 – b) Incoming – Channel Options

Incoming generic communication with an additional mandatory element called preferred method of vote.

Note: (This message may be sent in response to the message 360a. It can also be an unsolicited message from a voter wishing to select a preferred voting channel.)

PREFERRED METHOD OF VOTE

VOTER ID

TRANSACTION ID

VOTER NAME

NAME-STRUCTURE

GENERIC MESSAGE

CONTACT INFO

CONTACT-STRUCTURE

MAILING ADDRESS

ADDRESS-STRUCTURE

ELECTION EVENT NAME

ELECTION NAME

CONTEST NAME

SEAL

LANGUAGE ID

ANY

410 - Ballot

ELECTION EVENT ID
ELECTION EVENT NAME
ELECTION EVENT DESCRIPTION
BALLOT

BALLOT ID
REPORTING UNIT
ELECTIONS

ELECTION ID
ELECTION NAME
ELECTION DESCRIPTION
CONTESTS

CONTEST ID
CONTEST NAME
CONTEST DESCRIPTION
VOTING INFORMATION
ROTATION
MAX VOTES
MIN VOTES
MAXIMUM WRITE-INS
METHOD OF VOTING
MESSAGE
OPTIONS

OPTION ID
OPTION NAME
OPTION AFFILIATION

repeats

WRITE-IN OPTIONS

WI-OPTION ID
WI-OPTION NAME
WI-OPTION AFFILIATION

repeats

MESSAGE
ELECTION RULE ID
OR
VOTERS
VOTER ID
VOTER NAME
V-TOKEN
OR
V-TOKEN-QUALIFIED
REASON
V-TOKEN
TYPE (TENDERED OR SUPPLEMENTARY, ...)
CONTACT DETAILS
CONTACT-STRUCTURE

MESSAGE
SEAL
LANGUAGE ID
ANY

420 – Authentication

The mechanism of ensuring that a voter has the right to cast a vote for a specific ballot. Referring to *Figure 3a* it is assumed a v-token is generated according to mechanism and criteria defined.

TRANSACTION ID
CHANNEL ID
V-TOKEN
OR
V-TOKEN-QUALIFIED
REASON
V-TOKEN
TYPE (TENDERED OR SUPPLEMENTARY, ...)
LOGIN METHOD
LANGUAGE ID
AUDIT INFORMATION
ORIGINATING DEVICE ID
GATEWAY ID (CHANNEL TYPE, ...)
USER INFORMATION
ANY
SEAL
LANGUAGE ID
ANY

430 – Authentication Reply

Respond to authentication request to allow or deny access.

TRANSACTION ID
AUTHENTICATED (Y/N)
REMARK (REASON WHY NOT AUTHENTICATED.)

BALLOT ID
OR
BALLOT SCHEMA (1 BALLOT ONLY)

SEAL
LANGUAGE ID
ANY

440 – Cast Vote

V-TOKEN

OR

V-TOKEN-QUALIFIED

REASON

V-TOKEN

TYPE (TENDERED OR SUPPLEMENTARY, ...)

ELECTION EVENT ID

ELECTION EVENT NAME

ELECTION ID

ELECTION NAME

CONTEST ID

CONTEST NAME

SELECTION

**(OPTION ID/NAME OR WRITE-IN OPTION NAME
OPTION VALUE OR V-TOKEN OR BOTH)**

SEAL

(When the v-token is present, the seal proves that V-token is associated and bound to a certain vote indefinitely.)

V-TOKEN

OR

V-TOKEN-QUALIFIED

REASON

V-TOKEN

TYPE (TENDERED OR SUPPLEMENTARY, ...)

REPORTING UNIT

AUDIT INFORMATION

VOTING CHANNEL

PROCESSING UNIT

ORIGINATING

GATEWAY

OTHER

ANY

SEAL

LANGUAGE ID

ANY

450 – Vote Confirmation

Is meant to be a certain mechanism to respond to voter to confirm his vote was successfully and safely recorded. Whether the confirmation is a thank you message or a confirmation number that allows him to log to a certain page to check the status of his vote as in voted or not with timestamp but not the content of his vote. So again the content of the confirmation is system specific.

ELECTION EVENT ID
ELECTION EVENT NAME
MESSAGE
V-TOKEN
OR
V-TOKEN-QUALIFIER
REASON
V-TOKEN
TYPE (TENDERED OR SUPPLEMENTARY, ...)
CONFIRMATION REFERENCE
SEAL
LANGUAGE ID
ANY

460 – Votes

It is a collection of sealed votes/contest.

(**440 – CAST VOTE**) repeat

AUDIT INFORMATION
PROCESSING UNIT
VOTING SYSTEM
OTHER

SEAL
LANGUAGE ID
ANY

470 – V-Token Log

V-TOKEN
OR
V-TOKEN-QUALIFIER
REASON
V-TOKEN
TYPE (TENDERED OR SUPPLEMENTARY, ...)
STATUS (VOTED OR NOT)

ELECTION EVENT ID
ELECTION EVENT NAME
ELECTION ID
ELECTION NAME
ELECTION RULE ID
CHANNEL
AUDIT INFORMATION
PROCESSING UNIT
VTOKEN LOGGING SYSTEM
OTHER

480 – Seal Log

ELECTION ID
ELECTION NAME
SEAL
ORIGINATING DEVICE ID
GATEWAY ID
CHANNEL TYPE
USER INFORMATION
AUDIT INFORMATION
PROCESSING UNIT
SEAL LOGGING SYSTEM
OTHER

ANY

510 – Count/Result

ELECTION EVENT ID
ELECTION EVENT NAME
ELECTION

ELECTION ID
ELECTION NAME
ELECTION RULE ID
CONTESTS

CONTEST
CONTEST ID
CONTEST NAME
MAX VOTE

REPORTING UNIT

OPTIONS

OPTION ID
OPTION NAME
AFFILIATION
VALID VOTES

REJECTED VOTES (MANDATORY REASONS, OPTIONAL REASONS)
ABSTENTIONS (BLANK)

TOTAL VOTES

OPTIONS

OPTION ID
OPTION NAME
AFFILIATION
VALID VOTES

REJECTED VOTES (MANDATORY REASONS, OPTIONAL REASONS)
ABSTENTIONS (BLANK)

SEAL
LANGUAGE ID
ANY

Note: The message should contain either the results of a single reporting unit or a total result, optionally with a breakdown by reporting unit.

3. SECURITY CONSIDERATIONS

This section presents a general discussion of many of the security considerations commonly found in many election environments. As presented previously, these standards apply at EML interface points and define data security mechanisms at such interface points. This document is not intended to provide a complete description, nor a set of requirements for, secure election systems. In fact, the data security mechanisms described in this document are all optional, enabling compliance with these standards without regard for system security at all.

This discussion is included here simply to show how the information passed through the various interfaces described in these standards could be secured and used to help meet some of the requirements commonly found in some elections scenarios.

3.1 Basic security requirements

The security governing an election starts before the actual vote casting. It is not only a matter of securing the location where the votes are stored. An intensive analysis into security related concerns and possible threats that could in one way or another affect the election event resulted in the following:

Security considerations of e-voting systems include:

Authentication:

This is checking the truth of a claim of identity or right to vote. It aims to answer questions such as “Who are you and do you have the right to vote?”

There are two aspects of authentication in e-voting systems:

- Checking a claim of identity.
- Checking a right to vote.

In some e-voting scenarios the two aspects of authentication, checking a claim of identity and checking a right to vote, may be closely linked. Having checked the identity of the voter, a list of authorized voters may be used to check the right to vote.

In other scenarios the voter’s identity must remain private and must not be revealed by a ballot. In which case some systems may provide a clear separation between checking of the claim of identity, which may be done some time before the ballot takes place, from checking the right to vote at the time of the vote is cast. Alternatively, other mechanism may be used to

ensure the privacy of the voter's identity on cast votes (i.e. by anonymizing the ballot).

In the physical voting world, authentication of identity is made by using verifiable characteristics of the voter like handwritten signatures, address, etc and physical evidence like physical ids, driver's license, employee ID, Passport, etc. all of this can be termed a physical **credential**. This is often done at the time an electoral register is set up, which can be well before the actual ballot takes place.

Checking the authenticity of the right to vote may be performed at various stages in the process. Initial authenticity checks may be done related to the voter's identity during registration.

Where an election scenario demands anonymity of the voter and privacy of the voter's ballot, the identity of the voter and the cast votes must be separated at some time within the voting process. This can be done in several ways by a voting system including, but not restricted to, the following options:

1. Authentication of the right to vote by itself does not reveal a voter's identity, but does verify he has a legitimate right to vote (e.g. the V-token data provides authentication of the right to vote but has anonymous properties as to the identification of the person voting).
2. An voter's identity and the right to vote are both validated (i.e. the v-token data has both "voter identification" and "right to vote" authentication properties) and then the cast votes are clearly separated from the identity of the voter (i.e. the voters identification occurs before the ballot is "anonymized")

In all cases any verification of the authenticity that take place after the voter has indicated his/her choices must preserve the privacy of those choices according to the laws of the jurisdiction and the election rules.

Finally, when counting and auditing votes it is necessary to be able to check that the votes were placed by those whose right to vote has been authenticated.

Public democratic elections in particular will place specific demands on the trust and quality of the authentication data. Because of this and because different implementations will use different mechanisms to provide the voter credential, precise mechanisms are outside the scope of this document.

Privacy/Confidentiality:

This is concerned with ensuring information about voters and how votes are cast is not revealed except as necessary to count and audit the votes. In most cases, it must not be possible to find out how a particular voter voted. Also, before an election is completed, it should not be possible to obtain a count of how votes are being cast.

Where the user is remote from the voting system then there is a danger of voting information being revealed to someone listening in to the communications. This is commonly stopped by encrypting data as it passes over the communications network.

The other major threat to the confidentiality of votes is within the system that is collecting votes. It should not be possible for malicious software that can collect votes, to infiltrate the voting system. Risks of malicious software may be reduced by physical controls, careful audit of the system operation and other means of protecting the voting systems.

Furthermore, the results of voting should not be accessible until the election is complete. Potential approaches to meeting this goal might include access control mechanisms, very careful procedural control over the voting system, and various methods of protecting the election data using encryption techniques.

Integrity:

This is concerned with ensuring that ballot options and votes are correct and unaltered. Having established the choices within a particular ballot and the voter community to which these choices apply, the correct ballot information must be presented to each voter. Also, when a vote is placed it is important that the vote is kept correctly until required for counting and auditing purposes.

Using authentication check codes on information being sent to and from a remote voter's terminal over a communications network generally protects against attacks on the integrity of ballot information and votes. Integrity of the ballot and voting information held within computer systems may be protected to a degree by physical controls and careful audit of the system operation. However, much greater confidence in the integrity of voting information can be achieved by using digital signatures or some similar cryptographic protection to "seal" the data.

The fundamental challenge to be met is one of maintaining voter privacy and maintaining the integrity of the ballot.

Non-repudiation:

Non-repudiation is a derivative of the identification problem. Identification in e-voting requires that the system provide some level of assurance that the persons representing themselves as valid participants (voters, election workers, etc.) are, in fact, who they claim to be. Non-repudiation requires that the system provides some level of assurance that the identified participant is not able to successfully assert that the actions attributed to them via the identification mechanism were, in fact, performed by someone else. The two requirements are related in that a system with a perfect identification mechanism and undisputable proof of all actions would leave no room for successful repudiation claims.

Non-repudiation also requires that the system provide assurance that data or actions properly associated with an identified participant can be shown to have remained unaltered once submitted or performed. For example, approved candidate lists should be verified as having come from an authorized election worker, and voted ballots from a valid voter. In both cases the system should also provide a way to ensure that the data has remained unchanged since the participant prepared it.

Non-repudiation is not only a technical quality of the system. It also requires a certain amount of pure policy, depending on the technology selected. For example, in a digital signature environment, signed data can be very reliably attributed to the holder of the private key(s), and can be shown to be subsequently unmodified. The policy behind the acceptance of these properties, however, must be very clear about the responsibilities of the private key holders and the required procedures for reporting lost or stolen private keys. Further, and especially in “mixed-mode” elections (where voters can choose between multiple methods of voting), it may often be desirable to introduce trusted time stamps into the election data stream, which could be used to help determine acceptance criteria between ballots, or help resolve issues with respect to the relative occurrence of particular events (e.g. ballot cast and lost keys reported). The presence of the time information itself would not necessarily enable automatic resolution of these types of issues, but by providing a clear ordering of events could provide data that can be fed into decisions to be made according to established election policy.

3.2 Terms

The following security terms are used in this document:

- **Identity Authentication:** the means by which a voter registration system checks the validity of the claimed identity.

- **Right to vote authentication:** the means by which the voting system checks the validity of a voter's right to vote.
- **V-token:** the means by which a voter proves to an e-voting system that he/she has the right to vote in a contest.
- **V-token Qualified:** the means by which a V-token can be qualified. The reason for the qualification is always appended to a V-token that is qualified. For example, a qualified V-token may be issued to a challenged voter.
- **Vote sealing:** the means by which the integrity of voting data (ballot choices, vote cast against a given V-token) can be protected (e.g. using a digital signature or other authentication code) so that it can be proved that a voter's authentication and one or more votes are related.

3.3 Specific Security Requirements

Electronic voting systems have some very specific security requirements that include:

1. Only legitimate voters are allowed to vote (i.e. voters must be authenticated as having the right to cast a vote).
2. Only one set of choices is allowed per voter, per contest.
3. The vote cannot be altered from the voter's intention.
4. The vote may not be observed until the proper time.
5. The voting system must be accountable and auditable.
6. Information used to authenticate the voter or his/her right to vote should be protected against misuse (e.g. passwords should be protected from copying).
7. Voter privacy must be maintained according to the laws of the election jurisdiction. (Legal requirements of various countries conflict. Some countries require that the vote cannot be tracked back to the voter's identity, while others mandate that it must be possible to track every vote to a legitimate voter's identity).
8. The casting options available to the voter must be genuine.
9. Proof that all genuine votes have been accurately counted.

There are some specific complications that arise with respect to security and electronic voting that include:

1. Several technologies may be employed in the voting environment.
2. The voting environment may be made up of systems from multiple vendors.

3. A voter may have the option to vote through alternative delivery channels (i.e. physically presenting themselves at a polling station, by post, by electronic means).
4. The voting systems need to be able to meet various national legal requirements and local voting rules for both private and public elections.
5. Need to verify that all votes are recorded properly without having access to the original input.
6. The mechanism used for voter authentication may vary depending on legal requirements of the contest, the voter registration and the e-voting systems for private and public elections.
7. The user may be voting from an insecure environment (e.g. a PC with no anti-virus checking or user access controls).

Objectives of this security architecture include:

1. Be open.
2. Not to restrict the authentication mechanisms provided by e-voting systems.
3. Specify the security characteristic required of an implementation, allowing for freedom in its precise implementation.

3.4 Security Architecture

The architecture proposed here is designed to meet the security requirements and objectives detailed above, allowing for the security complications of e-voting systems listed.

The architecture is illustrated in figure 3a below, and consists of distinct areas:

- Voter identification and registration.
- Right to vote authentication.
- Protecting exchanges with remote voters.
- Validating Right to Vote and contest vote sealing
- Vote confidentiality.
- Candidate list Integrity
- Vote counting accuracy
- Voting system security controls

Voter identification and registration:

The Voter identification and registration is used to identify an entity (e.g. person) for the purpose of registering the person has a right to vote in one or more contests, thus identifying legitimate voters. The security characteristics for voter identification are to be able to authenticate the identity of the legal person

allowed to vote in a contest and to authenticate each person's voting rights. The precise method of voter identification is not defined here, as it will be specific to particular voting environments, and designed to meet specific legal requirements, private or public election and contest rules. The voter registration system may interact with the e-voting system and other systems to define how to authenticate a voter for a particular contest.

Voter identification and registration ensures that only legitimate voters are allowed to register for voting. Successful voter registration will eventually result in legitimate voters being given a means of proving their right to vote to the voting system in a contest. Depending on national requirements or specific voting rules/bylaws the voter may or may not need to be anonymous. If the voter is to be anonymous, then there must not be a way of identifying a person by the means used to authenticate a right to vote to the e-voting system. Right to vote authentication is the means of ensuring a person has the right to cast a vote, but it is not the identification of the person.

Right to vote Authentication:

Proof of the right to vote is done by means of V-token, which is generated for the purpose of authentication that the voter has a legitimate right to vote in a particular contest.

The security characteristic of the V-token and hence its precise contents may vary depend on the precise requirements of a contest, the supplier of the voter registration system, the e-voting system, the voting channel or other parts of the electoral environment. Thus, the content of the V-token will vary to accommodate a range of authentication mechanisms that could be used, including; pin and password, encoded or cryptographic based password, hardware tokens, digital signatures, etc.

The contents of the V-token may also depend on the requirements of a particular contest, which may mandate a particular method be used to identify the person and the voter. For example, if a country has a national identity card system, it could be used for the dual purpose of identifying the person and providing proof that the person is entitled to vote, provided the legal system (or the voting rules of a private election) allow a personal identify to be associated with a vote. However, this would not work for countries or private voting scenarios that require the voter to be anonymous. For such a contest the mechanism used to identify that a person has the right to cast a vote must not reveal the identity of the actual person, thus under such voting rules voter identity authentication and right to vote authentication do not use the same information or semantics.

The security characteristic required of the V-token may also vary depending on legal requirements of a country or electoral rules used in a particular contest. Also, the threats to misuse of v-tokens will depend to a large degree on the

voting channels used (e.g. physical presence at voting station, Internet, mobile phone). Bearing this in mind the XML schema of the V-token components must allow for various data types of authentication information to be contained within it.

It must be possible to prove that a V-token is associated with vote cast and the rules of the contest are followed, such as only one vote being allowed per voter, per contest. Thus providing proof /non-repudiation that all votes were genuine, they were cast in accordance with the rules of the contest, that no vote has been altered in any way and that all the votes counted in a contest were valid when audited to do so.

Depending on the legal requirements of a country or electoral rules a voter may be challenged as to the right to vote, or may be given a temporary right to vote. In such cases the V-token may need to be qualified with a reason. In this document this is called a V-token Qualified. Before a vote is considered legitimate and counted the reason for the qualification must have been suitable scrutinized, which could be done by the voting officials.

Protecting exchanges with remote voters:

The V-token may be generated as part of the registration system, the e-voting system, or as interaction between various components of a voting environment, as illustrate in Figure 3a. The V-token will need to be provided securely to the voter so that this can be used to prove the right to vote.

The exchange of information when casting a vote must be protected by secure channels to ensure the confidentiality, integrity of voting data (V-token(s) and vote(s) cast) and that this is correctly delivered to the authenticated e-voting system. If the channel isn't inherently secure then this will require additional protection using mechanisms. Possible mechanisms might include: a postal system with sealed envelopes, dedicated phone channel, secure e-mail, secure internet link (SSL), peer to peer server/client authentication and a seal.

Wherever technically possible the exchange of information should be secured and integrity guaranteed even if non-secure communications channels are used.

Validating Right to Vote and contest vote sealing:

When a vote is cast, to ensure that it cannot be altered from the voter's intention, all the information used to authenticate the right to vote and define the vote cast must be sealed to ensure the integrity and non-repudiability of the vote. This seal may be implemented using several mechanisms ranging from digital signatures (XML and CMS), cryptographic seals, trusted timestamps and other undefined mechanisms. The seal provides the following security functions:

- The vote cannot be altered from the voter's intention.

- The voting system must be accountable and auditable.

The right to vote may be validated at the time the vote was cast. If votes are not checked for validity before sealing then the right to vote must be validated at the time that votes are subsequently counted. Also, when counting or otherwise checking votes, the validity of the seal must be checked.

If votes are sealed and recorded without being checked for validity at the time they were cast, then the time that the vote was cast must be included in the seal, so that they may be checked for validity before they are counted.

In some election scenarios it is required to audit a vote cast to a particular voter, in this case a record is also needed of the allocation of a V-token to a voter's identity. Such systems also provide non-repudiation of the voter's actions. In such cases a voter cannot claim to have not voted or to have voted a different way, or that his vote was not counted. In many election scenarios where this type of auditing is required, it must not be easy to associate a V-Token to the Voter's identity, therefore this type of records must be under strict control and protected by security mechanism and procedures, such as; encryption, key escrow and security operating procedures.

Vote confidentiality:

All cast votes must not be observed until the proper time, this requires confidentiality of the vote over the voting period, how this is achieved will vary from e-voting system to e-voting system. Mechanism of vote confidentiality, range from trust in the e-voting systems internal security functions (processes and mechanisms) to encryption of the data, with key escrow tools.

Candidate list integrity:

To ensure that the voter is present and that the candidate list is genuine, there must be a secure channel between the voting system and the person voting or the data must be sealed. The approach selected must ensure that there is no man-in-the-middle that can change a vote from what the voter intended. There are various ways this requirement can be met, ranging from the candidate list having unpredictable characteristics with a trusted path to convey that information to the voter, to trust placed in the complete ballot/vote delivery channel.

As an example, there may be a secure path to convey the V-token to the person entitled to vote, a way of ensuring that a voter is always presented with a genuine list of candidates might be to encode the candidate list as part of a sealed V-token.

In summary, there must be a way of ensuring the validity of the ballot options and voter selection.

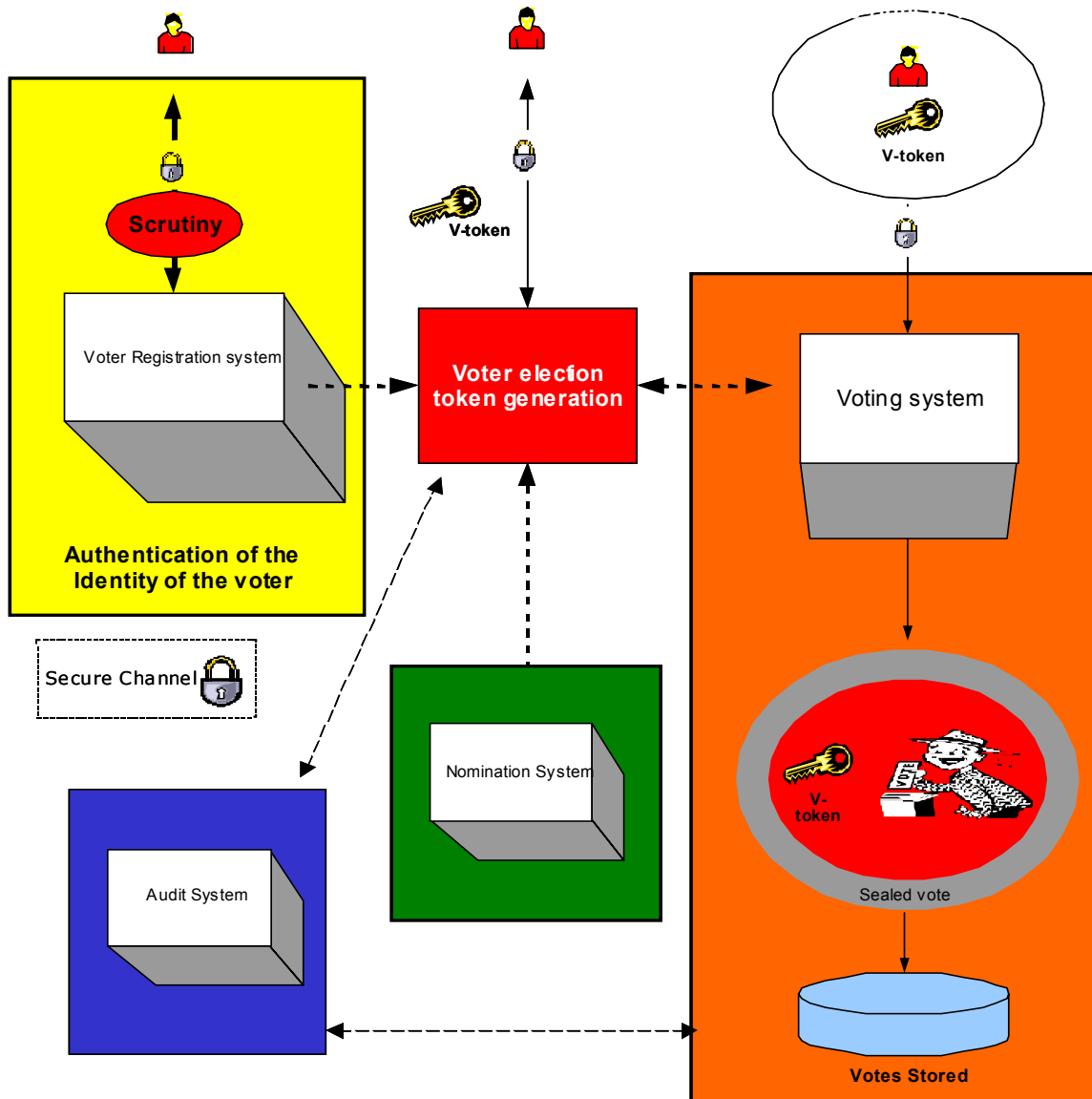
Vote counting accuracy:

Audit of the system must be able to prove that all vote casts were genuine and that all genuine votes were included within the vote count. Voters may need to be able to exercise that proof should they so desire. Thus auditing needs data that has non-repudiation characteristics, such as the V-token/vote sealing, see schema **470** and **480**.

Voting System Security:

The overall operation of the voting systems and its physical environment must be secure. Appropriate procedural, physical and computing system controls must be in place to ensure that risks to the e-voting systems are met. There must be a documented security policy based upon a risk analysis, which identifies the security objectives and necessary security controls.

Figure 3a: Voting system security



3.5 Remote voting security concerns

Many new election systems are currently under evaluation. These systems tend to offer deployment options in which the communication between the voter and the election officials is carried out in an environment that is not completely under the control and monitoring of the election officials and/or election observers (e.g., the Internet, private network, telephones, cable TV networks, etc.). In these “remote” or “unattended” environments, several particular security concerns and questions like:

- How do I know that the candidate information I am being presented with is the correct information?
- How do I know that my vote will be recorded properly?
- How do I know there isn't a man-in-the-middle who is going to alter my ballot when I place it?
- How do I know that it is the genuine e-voting server I'm connected to that will record my vote rather than one impersonating it that's just going to throw my vote away?
- How do I know that some component of the system does not have malicious software which will attempt to alter the ballot choices as represented to the voter or alter the voter's selection?

The type and importance of a particular contest will have an effect on whether the above concerns exist and whether they do, or do not, represent a tangible threat to the voting process and its outcome. The table listed at Appendix B shows the concerns that have been identified as possibilities for one such remote or unattended environment (the Internet) that could be used in public election voting scenarios. The table shows how the concerns can be translated to technical threats and characterizes security services that may be used to counter such threats. Many of the items are not unique to the Internet, and can serve as a useful reference or starting point in developing similar threat analysis for other digital and/or unattended voting environments. How the security services are implemented in any particular environment or deployment is outside the scope of this document allowing freedom to the system providers.

Appendix A: Glossary/Terminology

E-VOTING TERMS

The table below contains a list of voting terms used within this process document. The entries in bold relate to core terms that have been centrally defined by the committee and are essential to understanding the use of terminology within this document.

Additional suggestions from committee members have also been included..

TERM	DEFINTION	ORIGIN
BALLOT	Appropriate to one voter and will contain the set of candidates or options for a particular contest within one or more elections.	E&VSTC
BALLOT FORMAT	A format for rendering a ballot	USA
BALLOT LAYOUT	A template for a physical ballot	USA
BALLOT MESSAGE	Fixed text, image, instructions, etc. that appears on a ballot page	USA
BALLOT STYLE	Unique combination of contest and candidates	USA
CANDIDATE	An individual in standing in a contest or one of a set of proposal on an issue [See option]	E&VSTC
CANDIDATE LIST	A list of candidates or issues involved in a contest.	E&VSTC
CAST VOTE	This is a ballot containing the voters Preferences	E&VSTC
CONSTITUENCY	The whole area to which the elective office relates and may include a number of POLLING DISTRICTS	UK
CONTEST	A competition between a set of candidates for a particular post or on a particular issue	E&VSTC
ELECTION EVENT	An election event is a series of elections that for some reason are grouped together into one event. For example they may be completely different elections but for logistic reason they are all run on the same day.	E&VSTC
ELECTION	An election is used in the traditional sense, such as a country’s government election, local government election, or other local community elections. An election comprises a collection of related contests over a defined period of time. A series of elections may, or may not, be combined into one ballot for a voter within an election	E&VSTC

TERM	DEFINITION	ORIGIN
	event.	
FOOTER	Text, image, or other detail that appears immediately after a contest or candidate listing	USA
HEADER	Text, image, or other detail that appears immediately before a contest or candidate listing	USA
ITEM	The thing voted upon whether it is an office, position-elect or referendum	USA
ITEM_TYPE	Describes the type of ITEM (such as first-past-the-post, plurality, proportional vote, etc	USA
POLL SITE INTERNET VOTING	This refers to the casting of ballots at public sites where election officials control the voting platform	US
REMOTE INTERNET VOTING	This refers to the casting of ballots at private sites, where the voter or a third party controls the voting client.	US
NON-VOTER	Someone either who is on the register but has not voted, or someone who is ineligible to vote on Age or other grounds	UK
OPTION	The options are the choices presented to a voter for a particular contest and can comprise the list of candidates, choices, answers, etc.	E&VSTC
PARTY AFFILIATION	Political party affiliation associated to a CONTEST or CANDIDATE	USA
POLLING DISTRICT	The smallest geographical entity within which the VOTERS are subdivided for registration and voting purposes	UK
POLLING DISTRICT	A specific geo-political area that defines a boundary for a BALLOT CONTEST	USA
POLLING DISTRICTS SPLIT	Unique combination of all DISTRICTS in a specific jurisdiction	USA
REPORTING UNIT	A sub-unit within a CONTEST.	E&VSTC
ROTATION	The concept of presenting candidates (for the same contest) in a different order for different ballots	USA
SELECTION	The CANDIDATE, answer, etc which is the option or choice for ELECTION	USA
SEQUENCE	Order in which a CANDIDATE or CONTEST appears on a BALLOT	USA
UNDERVOTE	Indicates whether it is allowable to VOTE for fewer than the allowable SELECTIONS	USA
VOTE	A positive act, which records the voter's choice of CANDIDATE but in such a way as to ensure the secrecy of the BALLOT	UK

TERM	DEFINITION	ORIGIN
VOTELIMIT	Defines the number of vacancies to be filled in a particular ITEM	USA
VOTER	A voter is someone who is on the election list	E&VSTC
WRITEIN	Describes the number of write in CANDIDATES allowed	USA

E-VOTING PROCESS TERMINOLOGY

PROCESS	DEFINITION	ORIGIN/LINKS
REGISTER VOTER	This involves getting personal data onto the electoral roll	E&VSTC
CANDIDATE NOMINATION	The method of confirming eligibility to be a candidate in a contest and storing the relevant data.	E&VSTC
VOTING PROCESS	This involves the following two activities, the authentication of the voter and the casting of an individual vote.	E&VSTC
COUNTING PROCESS	The process of turning voted ballots into the results of a contest.	E&VSTC
VOTER IDENTIFICATION	The means by which a voter registration system identifies the entity (e.g human) entitled to vote.	E&VSTC
VOTER AUTHENTICATION	The means by which an e-voting system identifies that a voter has the right to cast a vote in a contest.	E&VSTC
VOTE SEALING	The means by which voter authentication and one or more vote can be proved to be related (e.g. possibly the a cryptographic way of sealing together a vote and proof the voter was legitimate).	E&VSTC

Appendix B: Internet Voting Security Concerns

Concerns raised on Internet voting	Resulting Technical Threats	Possible generic security service countermeasure
<p><i>1: Impersonation of the right to vote.</i></p> <p><i>The concern here is that a person attempts to impersonate to be a legitimate voter when he/she is not.</i></p> <p><i>The initial task of verifying that a person has the right to vote must be part of the voter registration process.</i></p> <p><i>A person must not be given the right to vote until after proper due diligence has been undertaken during voter registration that the person has a right to vote in a contest.</i></p>	<p>Inadequate, incorrect or improper identification of person during registration of voters</p> <p>Inadequate privacy of the exchange between the person and the electoral system during voter registration</p>	<p>Trusted voter identification and registration using:</p> <ul style="list-style-type: none"> • Security Procedures. • Best Practices. • Secure communications channels. <p>The voter registration authority must follow standard Security Operating Procedures (SOPs) which ensure due diligence has been done.</p> <p>Channel between voter and registration system must provide:</p> <ul style="list-style-type: none"> • Connection Confidentiality • Connection Integrity
<p><i>2: Voter is not presented with correct ballot information due to incorrect candidate identification.</i></p>	<p>Incorrect identification during candidate registration.</p>	<p>Trusted candidate identification and registration are needed using:</p> <ul style="list-style-type: none"> • Security Procedures. • Best Practices. • Secure communications channels. • Authentication and identification of candidates

Concerns raised on Internet voting	Resulting Technical Threats	Possible generic security service countermeasure
		The candidate registration must follow standard Security Operating Procedures (SOPs) which ensure due diligence has been done.
3: Registration system impersonation	Inadequate authentication of registration system	Channels to and from the registration system must provide point to point authentication.
4: Impersonation of a legitimate registered voter	Incorrect authentication at the time of casting vote.	Trusted voter authentication (i.e. the right to cast a vote in this contest)
	Inadequate privacy of the exchange between the voter and the electoral system when vote is cast.	Channel to provide: <ul style="list-style-type: none"> • Connection Confidentiality • Connection Integrity Between voter and e-voting system
5: Obtaining the right to vote illegally from a legitimate voter. <i>This may be by intimidation, theft or by any other means by which voting right has been obtained illegally.</i> <i>For example, by Stealing a voting card from a legitimate voter.</i>	Stealing the voter's voting card (e.g. the V-token data)	Some secret data only known to the voter's is required to be presented at the time of casting a vote. Before a vote is counted as a valid vote proof must be provided that the voter's secret data was present at the time of casting the vote.
	Any means of getting a legitimate voter to reveal his V-token data.	
6: Voting system impersonation	Inadequate authentication of registration system	Channel to provide: Point to point authentication
	Inadequate authentication of voting casting point (e.g. polling station/ballot box)	Channel to provide: Point to point authentication

Concerns raised on Internet voting	Resulting Technical Threats	Possible generic security service countermeasure
7: Voter is not presented with correct ballot information	Inadequate integrity of the ballot information <ul style="list-style-type: none"> Given to the user Held in the voting system 	Trusted path to voter on ballot options
		Integrity of the ballot information
	The casting options available to the voter are not genuine	Integrity of cast votes
	Trojan horse, man in the middle attack	Trusted path between voter and vote recording
8: How do I know the voting system records votes properly	Integrity of the voting system	Trusted path to voter on ballot options
		Non-repudiation of the vote
		Non-repudiation the vote was cast by a genuine voter
		Audit of voting system
	Insecure channel between the voter and the vote casting point	Connection confidentiality
		Connection Integrity
	Voter's intent is recorded accurately	Connection Confidentially
Trusted path between voter and vote recording		
Proof that a genuine vote has been accurately counted.	Non-repudiation of the vote recorded	
9: How can I be sure the voting system will not disclose whom I have voted for.	Voter's identification is revealed	Audit
		Voter's identification is anonymous
		Vote confidentiality
10: How can it be sure that my vote has been recorded	Loss of vote	Proof of vote submission
11: How can I be sure there is no man-in-the-middle that can alter my ballot	Vulnerable client environment; <ul style="list-style-type: none"> Trojan horses Virus 	Physical security
		Procedural security
	Interception of communication	Unpredictable Coded voting information
		Integrity of communications channel between client and server system

Concerns raised on Internet voting	Resulting Technical Threats	Possible generic security service countermeasure
12: All votes counted must be have been cast by a legitimate voter	Voter impersonation	Voter authentication
	Audit facility fails to provide adequate proof.	Non-repudiation of the vote record
		Non-repudiation that legitimate voters have cast all votes.
Breaking the vote counting mechanisms	Independent audit	
13: Only one vote is allowed per voter, per contest	Voter impersonation at registration	User registration security <ul style="list-style-type: none"> • Procedures • Voter Identification
	Multiple registration applications	
	Multiple allocation of voters credentials	Voter authentication
14: The vote cannot be altered from the voter's intention.	Vulnerable client environment; <ul style="list-style-type: none"> • Trojan horses • Virus 	Trusted path from voter's intent to vote record.
		Vote integrity
		Vote non-repudiation
15: The vote may not be observed until the proper time	Votes may be observed before the end of the contest	Voter confidentiality
16: The voting system must be accountable and auditable		Non-repudiation of vote data.
		Audit tools
17: Identification and authentication information to and from the voter must be privacy protected	Loss of privacy	Channel to provide: <ul style="list-style-type: none"> • Connection Confidentiality
18: The voter's actual identity may need to be anonymous	Voter's identification is revealed	Voter's identification is anonymous

Concerns raised on Internet voting	Resulting Technical Threats	Possible generic security service countermeasure
<i>19: Denied access to electronic voting station</i>	Denial of service attack	This needs to be counted by engineering the system to provide survivability when under denial of service attack.